UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

Polar coding for the wiretap broadcast channel

Jaume del Olmo Alòs

Ph.D Thesis:

Polar Coding for the Wiretap Broadcast Channel

Ph.D Thesis:

Polar Coding for the Wiretap Broadcast Channel

Author:
Jaume del Olmo Alòs
jaume.del.olmo@upc.edu

Advisor:
Javier Rodríguez Fonollosa
javier.fonollosa@upc.edu

UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH

Departament de Teoria del Senyal i Comunicacions (TSC)
Carrer Jordi Girona 1-3, Campus Nord, Edifici D5
08034 Barcelona, Spain

Barcelona, October 2019

Acknowledgments

First of all, I would like to express my deepest gratitude to my supervisor Prof. Javier R. Fonollosa. At a *difficult time*, I was honored to receive his support and confidence, which encouraged me to begin this enjoyable adventure. During all this time he always offered me guidance and advice, and his constructive criticism has been essential to the successful development of this thesis.

Further, I would like to extend my gratitude to Prof. Ignacio Santamaria, Dr. Josep Font-Segura, and Dr. Gonzalo Vázquez-Vilar for agreeing to serve in this thesis' committee. My gratitude also extends to Prof. Deniz Gunduz, together with Dr. Gonzalo Vázquez-Vilar, for reviewing this thesis.

I am also sincerely grateful to Prof. Josep Vidal for giving me the opportunity to participate in the European project TUCAN3G when I was an undergraduate student. I learned a lot from him and his team: Prof. Antonio Pascual, Dr. Adrian Agustín, Prof. Olga Muñoz and Dr. Javier Rubio.

During these years I had been fortunate to interact with a lot of people from UPC and other universities. To avoid the risk of omitting any of them, I would like to thank them all for having shared time with me, which has resulted in interesting conversations of any kind. Nevertheless, I should specially mention my colleagues and friends Pedro and Miquel, with whom I had spent a lot of time talking about everything in the universe, and Sandra, who helped me a lot with whatever I needed.

Voldria donar les gracies també a la meva família, especialment a la meva mare i al meu pare, ja que aquesta tesi no hagués estat possible sense el seu suport incondicional i la seva confiança. Moltes gràcies també als meus amics, per estar sempre al meu costat durant tots aquests anys. Per últim, m'agradaria agrair de manera molt especial el recolçament per part la meva parella. "Marga, gràcies per estar al meu costat sempre, tant en els bons moments com en els dolents. Ets la millor companya de vida."

Summary

In the next era of communications, where heterogeneous, asynchronous and ultra-low latency networks are drawn on the horizon, classical cryptography might be inadequate due to the excessive cost of maintaining a public-key infrastructure and the high computational capacity required in the devices. Moreover, it is becoming increasingly difficult to guarantee that the computational capacity of adversaries would not be able to break the cryptograms. Consequently, information-theoretic security, and particularly its application to keyless secrecy communication, might play an important role in the future development of these systems. The notion of secrecy in this case does not rely on any assumption of the computational power of eavesdroppers, and is based instead on guaranteeing statistical independence between the information message and the observed cryptogram. This is possible by constructing channel codes that exploit the noisy behavior of the channels involved in the communication.

Although there has been very substantial research in the last two decades regarding information-theoretic security, little has gone to study and design practical codes for keyless secret communication. In recent years, polar codes have changed the lay of the land because they are the first constructive and provable channel codes that are able to provide reliability and information-theoretical secrecy simultaneously. Additionally, their explicit construction and the low complexity of the encoding/decoding schemes makes them suitable for the new generation of communication systems, so much so that they have been chosen as part of the channel coding scheme for the 5th generation wireless systems (5G) standardization process.

The main objective of this dissertation is to provide polar coding schemes that achieve the best known inner-bounds on the capacity regions of different multiuser models over the discrete memoryless broadcast channel. These models not only impose a reliability constraint, but also some sort of information-theoretical secrecy condition in the presence of eavesdroppers. In general, we focus on describing the construction and the encoding/decoding schemes of the the proposed polar code for a particular setting. Then, we analyze the reliability and the secrecy performance of schemes in order to prove that they are able to achieve these inner-bounds as the blocklength tends to infinity.

The first part of the thesis drives the attention to two different models over the degraded

broadcast channel that commonly appear in real communication systems. In this models, there are a set of legitimate receivers and a set of eavesdroppers that can be ordered based on the quality of their channels. According to this ordering, different reliability or secrecy constraints apply for each legitimate receiver or eavesdropper respectively. Moreover, we propose practical methods for constructing the polar codes for both models and analyze the performance of the coding schemes by means of simulations. Despite we only evaluate the construction for these two particular settings, the proposed methods are also suitable for any polar coding scheme that must satisfy some reliability and secrecy conditions simultaneously.

In the second part of the dissertation we describe and analyze two different polar coding schemes for the general broadcast channel (where channels are not necessarily degraded) with two legitimate receivers and one eavesdropper. We consider a model where a confidential and a non-confidential message must be reliably decoded by both legitimate receivers in presence of an eavesdropper. Despite it is almost immediate to find an inner-bound on the capacity for this model using random coding arguments, how to secretly convey the same confidential message to both legitimate receivers using polar codes is not straightforward. We also analyze the setting where a transmitter wants to send different confidential and non-confidential messages to the corresponding legitimate receivers. We compare two inner-bounds on the capacity of this model, and we design a polar coding scheme that achieves the inner-bound that surely includes the other.

Resum

La criptografia clàssica o computacional pot suposar certs inconvenients en els sistemes de comunicació de nova generació que es basen en xarxes heterogènies, asíncrones i que requereixen molt baixa latència. Els motius principals són l'alt cost que suposa mantenir una infraestructura de clau pública i l'elevada capacitat computacional que requereix als dispositius electrònics. A més, cada cop és més difícil garantir que aquesta capacitat computacional dels dispositius adversaris no sigui suficient per trencar els criptogrames. Per tant, la seguretat basada en la teoria de la informació, i particularment la seva aplicació en la transmissió d'informació confidencial sense la necessitat d'utilitzar una clau secreta, pot tenir un rol molt important pel futur desenvolupament d'aquests sistemes. La noció de seguretat en aquest cas no es basa en cap suposició sobre la potència computacional dels adversaris, sinó que consisteix en garantir que el missatge que es vol transmetre i el criptograma enviat pel canal siguin independents estadísticament. Això és possible utilitzant una codificació que aprofita el comportament sorollós del canal involucrat en la comunicació.

Malgrat durant les dues darreres dècades la recerca en el camp de la seguretat basada en la teoria de la informació ha estat important, s'han destinat pocs esforços al disseny de codis pràctics per tal de transmetre informació confidencial sense utilitzar claus secretes. Així i tot, en els últims anys, els *codis polars*, un tipus de codis bloc lineals, han demostrat ser molt útils per tal de transmetre informació sense errors i de forma confidencial des d'un punt de vista de la teoria de la informació. A més, gràcies a que la seva construcció és explícita i a la seva baixa complexitat, els codis polars són apropiats per a la nova generació de sistemes de comunicació, tant que han estat escollits com a part de l'esquema de codificació del nou estàndard de 5G per a comunicacions sense fil.

L'objectiu principal d'aquesta tesis és construir esquemes de codificació basats en codis polars que assoleixin la capacitat (o la millor aproximació coneguda) per diferents models sobre el canal de difusió (*broadcast channel*) amb presència d'adversaris. Aquests models no només imposen restriccions sobre la fiabilitat de la transmissió, sinó que també imposen restriccions sobre la confidencialitat des del punt de vista de la teoria de la informació. En general, per a cada model descriurem un esquema de codificació i després analitzarem el

seu rendiment per demostrar que són capaços de transmetre informació de forma fiable i confidencial a la màxima taxa de transmissió possible quan la longitud del codi tendeix a infinit.

La primera part d'aquesta tesis centra l'atenció en dos models de comunicació diferents pel canal degradat de difusió (*degraded broadcast channel*) que representen molts de sistemes de comunicació reals. En aquests models, hi ha un conjunt de receptors legítims i un conjunt d'adversaris, i els canals de tots ells es poden ordenar en base a la seva qualitat. En base a aquest ordre, s'apliquen condicions de fiabilitat i de seguretat diferents per a cada receptor o adversari, respectivament. També, en aquesta part proposem mètodes pràctics de construcció dels codis polars i analitzem el seu rendiment mitjançant simulacions. Malgrat que només avaluem la construcció per aquests dos models particulars, els mètodes proposats es poden generalitzar per qualsevol esquema de codificació polar que hagi de satisfer condicions de fiabilitat i seguretat de forma simultània.

En la segona part de la tesi es descriuen i s'analitzen dos esquemes de codificació basats en codis polars pel canal de difusió general (on els canals individuals no necessàriament són degradats) compost per dos usuaris legítims i un adversari. Primer, considerem un model en el que dos missatges s'han de transmetre de forma fiable als dos receptors de manera que un ha de ser confidencial davant la presència d'un adversari. Encara que trobar una aproximació teòrica de la capacitat de canal en aquest model és pràcticament immediat, com dissenyar un sistema de codificació polar que permeti enviar el mateix missatge confidencial a dos receptors diferents no és un problema directe. En segon lloc, considerem un model on el transmissor vol enviar diferents missatges confidencials i no confidencials als dos receptors. En aquest cas, comparem dues aproximacions a la capacitat d'aquest model i observem que una és almenys igual o millor que l'altra. Finalment, dissenyem un esquema de codificació basat en codis polars que permet transmetre a una taxa igual a aquesta aproximació de la capacitat.

Resumen

La criptografía clásica o computacional puede suponer ciertos inconvenientes en los sistemas de comunicación de nueva generación que se basan en redes heterogéneas, asíncronas y que requieren muy baja latencia. Los motivos principales son el elevado coste que supone mantener una infraestructura de clave pública i la elevada capacidad computacional que requieren los dispositivos electrónicos. Además, cada vez es mas difícil garantizar que esta capacidad computacional de los adversarios no sea suficiente para romper los criptogramas. Por tanto, la seguridad basada en la teoría de la información, y en particular su aplicación en la transmisión de información confidencial sin la necesidad de utilizar una llave secreta, puede tener un rol muy importante para el futuro desarrollo de estos sistemas. La noción de seguridad en esta caso no se basa en ninguna suposición sobre la potencia computacional de los adversarios, sino que consiste en garantizar que el mensaje que se quiere transmitir y el criptograma enviado por el canal sean independientes estadísticamente. Esto es posible utilizando una codificación que aproveche el comportamiento ruidoso del canal involucrado en la comunicación.

A pesar que durante las dos últimas décadas la investigación en el campo de la seguridad basada en la teoría de la información haya sido importante, se han destinado pocos esfuerzos en el diseño de códigos prácticos para transmitir información confidencial sin utilizar claves secretas. Aún así en los últimos años los *códigos polares*, un tipo de códigos bloque lineales, han demostrado ser muy útiles para transmitir información sin errores y de forma confidencial desde un punto de vista de la teoría de la información. Además, gracias a que su construcción es explícita y a su baja complejidad, los códigos polares son apropiados para la nueva generación de sistemas de comunicación, tanto que han sido escogidos como parte del esquema de codificación del nuevo estándar de 5G para las comunicaciones inalámbricas.

El objetivo principal de esta tesis es construir esquemas de codificación basados en códigos polares que alcancen la capacidad (o la mejor aproximación conocida) para diferentes modelos sobre el canal de difusión (*broadcast channel*) con presencia de adversarios. Estos modelos no solo imponen restricciones sobre la fiabilidad de la transmisión, sino que también imponen restricciones sobre la confidencialidad des de un punto de vista de la teoría de

la información. En general, para cada modelo describiremos un esquema de codificación y después analizaremos su rendimiento para demostrar que son capaces de enviar información de forma fiable y confidencial a la máxima tasa de transmisión posible cuando la longitud del código tiende a infinito.

La primera parte de esta tesis centra la atención en dos modelos de comunicación diferentes para el canal degradado de difusión (*degraded broadcast channel*) que representan muchos sistemas de comunicación reales. En estos modelos, hay un conjunto de receptores legítimos y un conjunto de adversarios, y los canales de todos ellos se pueden ordenar dependiendo de su calidad. En función de este orden se aplican condiciones de fiabilidad y de seguridad diferentes para cada receptor o adversario, respectivamente. También, en esta parte proponemos métodos prácticos de construcción de los códigos polares y analizamos su rendimiento mediante simulaciones. A pesar de que solo evaluamos la construcción para estos dos modelos particulares, los métodos que se proponen se pueden generalizar para cualquier esquema de codificación polar que tenga que satisfacer condiciones de fiabilidad y seguridad de forma simultánea.

En la segunda parte de la tesis se describen y analizan dos esquemas de codificación basados en códigos polares para el canal de difusión general (donde los canales individuales no necesariamente son degradados) compuestos por dos receptores legítimos y un adversario. Primero, consideramos un modelo en el que los dos mensajes se tienen que transmitir de forma fiable a los dos receptores y uno de forma confidencial delante de la presencia del adversario. Aunque encontrar una aproximación teórica de la capacidad de este modelo es prácticamente inmediato, como diseñar un sistema de codificación polar que permita enviar el mismo mensaje confidencial a dos receptores diferentes no es un problema directo. En segundo lugar, consideramos un modelo donde el transmisor quiere enviar diferentes mensajes confidenciales y no confidenciales a los dos receptores. En este caso, comparamos dos aproximaciones a la capacidad de este modelo y encontramos que una es mejor o igual que la otra. Después diseñamos un esquema de codificación basado en códigos polares que permite transmitir a una tasa igual a esta aproximación de la capacidad.

Contents

Notation

Mathematical notation

$\mathbb{Z}$	set of integers
$\mathbb{Z}_+$	set of strictly positive integers
$\mathbb{R}$	set of reals
$\mathbb{R}_+$	set of strictly positive reals
$\mathbb{R}^m$	set of real vectors of dimension m
$\mathbb{R}_+^m$	set of strictly positive real vectors of dimension m
$[a, b]$	set of positive integers between a and b, where $a, b \in \mathbb{Z}_+$ and $a \leq b$
ln	natural logarithm
log	logarithm base 2
$\mathcal{U}$	generic alphabet or set ($\mathcal{E}$ is reserved)
$\lvert\mathcal{U}\rvert$	cardinality of $\mathcal{U}$
$\mathcal{U}^{\mathrm{C}}$	set complement in $[1, n]$, where $n \in \mathbb{Z}_+$, that is, $\mathcal{S}^{\mathrm{C}} = [1, n] \setminus \mathcal{S}$
U	random variable
u	realization of random variable
U^n	row vector $(U(1), \ldots, U(n))$ of length $n \in \mathbb{Z}_+$
$U^{1:j}$	shorthand for subvector $(U(1), \ldots, U(j))$, where $j \in [1, n]$
$U[\mathcal{S}]$	elements $\{U(j)\}_{j \in \mathcal{S}}$, where $\mathcal{S} \subseteq [1, n]$
$U_{a:b}^n$	ordered set of vectors $\{U_a^n, \ldots, U_b^n\}$, where $a, b \in \mathbb{Z}^+$ and and $a \leq b$
$\mathcal{E}$	generic event
$\mathcal{E}^{\mathrm{C}}$	complement of event $\mathcal{E}$

$\mathbb{P}[\mathcal{E}]$	probability of event $\mathcal{E}$
$\mathbb{E}_X$	expectation over random variable X
$H(X)$	Shannon entropy of X
$H(X\|Y)$	Shannon conditional entropy of X given Y
$I(X;Y)$	mutual information between X and Y
$\mathbb{D}(\cdot\|\cdot)$	Kullback-Leibler divergence between two distributions
$\mathbb{V}(\cdot,\cdot)$	total variation between two distributions
$h_2(\cdot)$	binary entropy function, i.e., $h_2(p) = -p\log p - (1-p)\log(1-p)$
$\{x\}^+$	positive part of x, that is, $\max\{0, x\}$
$\lceil\cdot\rceil$	ceiling function
$f(n) = O(g(n))$	$\lim_{n\to\infty} \lvert f(n)/g(n)\rvert \leq \infty$, where g is non-zero
$f(n) = o(g(n))$	$\lim_{n\to\infty} f(n)/g(n) = 0$, where g is non-zero

Acronyms and Abbreviations

BCC	Broadcast channel with Confidential Messages.
BE-BC	Binary Erasure Broadcast Channel.
BEC	Binary Erasure Channel.
BS-BC	Binary Symmetric Broadcast Channel.
BSC	Binary Symmetric Channel.
CI-WTBC	Common Information over the Wiretap Broadcast Channel.
DBC	Degraded Broadcast Channel.
DBC-LD-NLS	DBC with Layered Decoding and Non-Layered Secrecy.
DBC-NLD-LS	DBC with Non-Layered Decoding and Layered Secrecy.
DMC	Discrete Memoryless Channel.
DMS	Discrete Memoryless Source.
DWTC	Degraded Wiretap Channel.
MI-WTBC	Multiple Information over the Wiretap Broadcast Channel.
PCS	Polar Coding Scheme.
SC	Successive Cancellation.
WTBC	Wiretap Broadcast Channel.
WTC	Wiretap Channel.

1

Introduction

One of the most important problems in communications is how to securely transmit messages between legitimate receivers over an insecure communication channel without eavesdroppers being able to leak any information about them. Up to know, *computational security* has provided a wide variety of tools (cyphers) for solving this problem, which rely mainly on the assumption of limited computational power at eavesdroppers. These cyphers are broadly used in practice and they assume that eavesdroppers have full knowledge of the cryptogram sent through the channel. Nevertheless, the assumption of limited computational power at eavesdroppers ensure that they cannot break the cryptogram due to the "unproven" difficulty of recovering the message without the knowledge of some key that is shared between legitimate receivers.

Otherwise, *information-theoretic security* is defined based on a condition on some information theoretic measure that is fully quantifiable and does not make any assumption regarding the computational power of eavesdroppers. This notion of security was introduced first by Shannon in his seminal paper [Wyn75], who proved that one transmitter can send a message to a receiver with *prefect secrecy* through an insecure error-free communication channel. Here, perfect secrecy refers to statistical independence between the message and the transmitted cryptogram that is observed directly by an eavesdropper. To do so, transmitter and legitimate receiver must share a uniformly distributed random secret-key of the same size as the message and this key can be used only once.

Based on Shannon's result, it might seem that information-theoretic security is unpractical. Nevertheless, real communications usually take place in physical environments that are not

error-free but noisy, and the perfect secrecy condition can be replaced by a less stringent one. In this sense, Wyner [Wyn75] and later Csiszár and Körner [CK78] proposed a new model, called the *wiretap channel*. In this setting, secure transmission between two legitimate receivers is possible without using any pre-shared secret key by designing a particular encoder (*stochastic encoder*) that takes advantage of the statistical knowledge of the channel noise.

Despite upper layers of communication protocols already have cryptographic primitives for secret transmission (also for authentication or privacy), information-theoretic security over noisy channels aims to provide secrecy at the physical layer[1], on which all other upper layers rely. Therefore, computational and information-theoretic security should not be seen as mutually exclusive, but as supplementing and supporting each other.

In the last two decades, information-theoretic security has been extended to a large variety of contexts (keyless secret communication, secret key generation over noisy channels, authentication, etc.) and models (single-user communications, multi-user communications, MIMO channels, etc.). However, most of the work done until know has been focused on characterizing communication limits by using random coding schemes that are nonconstructive in practice. Otherwise, little progress has been made toward the design of constructive coding schemes that will allow physical-layer security to become a practical solution for the emerging communication technologies.

In recent years, polar codes have changed the lay of the land because they are the first constructive and provable channel codes that are able to provide reliability and information-theoretical secrecy simultaneously. These codes are a class of linear block codes originally proposed by Arikan in [Ari09] for reliable transmission over the binary-input symmetric point-to-point channel, and rapidly attracted the attention of the academia and industry due to their provably capacity-achieving property, their explicit construction and the low complexity of the encoding/decoding schemes.

This dissertation focuses on providing polar coding schemes that achieve the best-known inner-bounds on the secrecy-capacity region of different models for the wiretap broadcast channel. In this channel there is an arbitrary set of legitimate receivers and an arbitrary set of eavesdroppers. Then, each model imposes different reliability conditions for the former, while different secrecy constraints are established for the later.

1.1 Information-theoretic security

In information-theoretic security, one of the most commonly used measures of secrecy is the *information leakage*. This information-theoretic measure is defined as the mutual information

[1] Information-theoretic security is referred also as *physical-layer security*.

$I(W;Z^n)$ between some transmitted random message W and the eavesdropper's channel observations Z^n. Based on the information leakage, different secrecy conditions can be imposed to the coding schemes. As mentioned previously, one of this measures is the perfect secrecy, which requires $I(W;Z^n)=0$, where W is distributed according to some arbitrary distribution p_W. Usually, the random message is considered to be distributed uniformly and two less stringent secrecy conditions are broadly used under this assumption: *weak secrecy* and *strong secrecy*. The weak secrecy condition requires the rate of information leakage to vanish for the blocklength n, that is, $\lim_{n\to\infty}\frac{1}{n}I(W;Z^n)=0$. On the other hand, the strong secrecy condition requires the information leakage to vanish, i.e., $\lim_{n\to\infty}I(W;Z^n)=0$.

In the following, the Wyner's wiretap channel [Wyn75], also referred as Degraded Wiretap Channel (DWTC), is analyzed formally in order to introduce some of the important definitions related to information-theoretic security for keyless secure communication. In this model, one transmitter wishes to reliably send one uniformly distributed random message W to the legitimate receiver that observes the channel $(\mathcal{X},p_{Y|X},\mathcal{Y})$, while keeping it secret from an eavesdropper that observes the channel $(\mathcal{X},p_{Z|X},\mathcal{Z})$ such that is (stochastically or physically) degraded with respect to that of the legitimate receiver.

Definition 1.1 (Physically degraded channel). *A point-to-point channel $(\mathcal{X},p_{Z|X},\mathcal{Z})$ is physically degraded with respect to other channel $(\mathcal{X},p_{Y|X},\mathcal{Y})$ if $X-Y-Z$ forms a Markov chain, that is, $p_{YZ|X}(y,z|x)=p_{Y|X}(y|x)p_{Z|Y}(z|y)$*

Definition 1.2 (Stochastically degraded channel). *A channel $(\mathcal{X},p_{Z|X},\mathcal{Z})$ is stochastically degraded with respect to channel $(\mathcal{X},p_{Y|X},\mathcal{Y})$ if there exists some distribution $p'_{Z|Y}$ such that $p_{Z|X}(z|x)=\sum_y p_{Y|X}(y|x)p'_{Z|Y}(z|y)$. This property is denoted as $p_{Y|X}\succeq p_{Z|X}$.*

A $(2^{nR},n)$ code C_n for the DWTC consists of a message set $\mathcal{W}=[1,\lceil 2^{nR}\rceil]$, an *stochastic encoding* $f:\mathcal{W}\to\mathcal{X}^n$ that maps a message $w\in\mathcal{W}$ to a codeword $x^n\in\mathcal{X}^n$ according to a transition probability function $p_{X^n|W}$ (the encoding process is not deterministic), and a decoding function $g:\mathcal{Y}^n\to\mathcal{W}$ that maps the channel observations of the legitimate receiver y^n to a message $\hat{w}\in\mathcal{W}$. The reliability performance of this code is measured in terms of the average probability of error, $\mathbb{P}[\hat{W}\neq W]$, and the secrecy performance is measured in terms of the information leakage $I(W;Z^n)$.

Definition 1.3 (Achievable rate). *A rate R is full-secrecy achievable for the DWTC if there exists a sequence of $(2^{nR},n)$ codes $\{\mathrm{C}_n\}_{n\geq 1}$ such that*

$$\lim_{n\to\infty}\mathbb{P}[\hat{W}\neq W]=0 \qquad \textit{(reliability condition)},$$

$$\lim_{n\to\infty}I(W;Z^n)=0 \qquad \textit{(strong secrecy condition)}.$$

Definition 1.4 (Achievable region). *The full-secrecy achievable region $\mathfrak{R}$ is defined as the closure of all full-secrecy achievable rates, that is, $\mathfrak{R} \triangleq \mathrm{cl}\{R : R \text{ is full-secrecy achievable}\}$.*

Definition 1.5 (Secrecy-capacity). *The secrecy-capacity C is defined as the supremum of the full-secrecy achievable region $\mathfrak{R}$, that is, $C \triangleq \sup_R \{R : R \in \mathfrak{R}\}$.*

Remark 1.1. *Originally, [Wyn75] considers the weak secrecy condition for the previous definitions. Nevertheless, [MW00] proved that both secrecy conditions result in the same achievable region. Despite this surprisingly result, the weak secrecy requirement in practical applications can result in important system vulnerabilities [BB11](Section 3.3).*

Remark 1.2. *The term full-secrecy in the previous definitions means that the entire message W is hidden from the eavesdropper, i.e., $\lim_{n\to\infty} I(W;Z^n) = 0$ and has nothing to do with perfect secrecy. Indeed, [Wyn75] defines an achievable region where $\lim_{n\to\infty} I(W;Z^n)$ is not necessarily zero, but some arbitrary level of secrecy that is referred as equivocation rate.*

Therefore, notice that the secrecy-capacity is defined as the maximum information bits that the transmitter can send satisfying both the reliability and secrecy conditions.

Proposition 1.1 ([Wyn75]). *Let $(\mathcal{X}, p_{YZ|X}, \mathcal{Y}\times\mathcal{Z})$ be an arbitrary DWTC where $p_{YZ|X}$ is such that $p_{Y|X} \succeq p_{Z|X}$ or $X - Y - Z$. The secrecy-capacity of this model is*

$$C^{\mathrm{DWTC}} = \max_{p_X} \left(I(X;Y) - I(X;Z)\right).$$

The key point of the achievability proof is the use of the stochastic encoder, which takes advantage of the statistical knowledge of the channel noise in order to confuse the eavesdropper about the message transmitted over the DWTC. Since the eavesdropper's channel is degraded with respect to that of the legitimate receiver, notice that $C^{\mathrm{DWTC}} \geq 0$ with equality only if $I(X;Y) = I(X;Z)$, that is, both channels have the same *quality*.

The major drawback of the previous model is the assumption of the legitimate receiver having significant advantage over the eavesdropper due to the degradedness condition imposed to the channels. In this sense, Csiszár and Körner in [CK78] generalized Wyner's results to the Wiretap Channel (WTC), in which eavesdropper's channel is not necessarily degraded[2].

Proposition 1.2 ([CK78]). *Let $(\mathcal{X}, p_{YZ|X}, \mathcal{Y}\times\mathcal{Z})$ be an arbitrary WTC. The secrecy-capacity of this model is*

$$C^{\mathrm{WTC}} = \max_{p_{VX}} (I(V;Y) - I(V;Z)).$$

[2]Indeed, [CK78] introduces a more general model, called the Broadcast channel with Confidential Messages (BCC), where besides the confidential message to be transmitted secretly to the legitimate receiver, both the legitimate receiver and the eavesdropper must be able to reliably decode a common message.

where p_{VXYZ} is such that $V - X - YZ$ forms a Markov chain.

In this setting, the coding scheme that achieves the secrecy-capacity uses channel prefixing $p_{X|V}$ to introduce additional randomness at the encoding, which is necessary because the eavesdropper's channel is not degraded with respect to the legitimate receiver one.

Certainly, the most important limitation of information-theoretic security is the transmitter having to know the statistics of eavesdropper's channel in order to construct a *good* wiretap code. Nevertheless, as pointed out in [BB11] (Proposition 3.3), one can design a *good* code ensuring the strong secrecy condition for some arbitrary eavesdropper's channel $(\mathcal{X}, p_{Z_{(\mathrm{a})}|X}, \mathcal{Z}_{(\mathrm{a})})$ and, by the date processing inequality [CT12], this code will also ensure the strong secrecy condition for any other eavesdropper's channel $(\mathcal{X}, p_{Z_{(\mathrm{b})}|X}, \mathcal{Z}_{(\mathrm{b})})$ such that is degraded with respect to the previous one because, in this case, $I(X; Z_{(\mathrm{b})}) \leq I(X; Z_{(\mathrm{a})})$.

1.2 Outline of the dissertation and related publications

Chapter 2

In this chapter we revisit the fundamental theorems of polar codes and their application for different channel coding problems. Generally, channel coding for different scenarios by using polar codes has been addressed from two viewpoints: source polarization or channel polarization. For a better understanding, we review the polar coding schemes for different models –those on which our work rely– by means of source polarization.

Furthermore, in Section 2.5 we present a generic polar-based encoder for multi-user settings that uses an asymptotically negligible amount of randomness, and induces a distribution that is statistically close to the one that attains the capacity of the model. This result is stated in Lemma 2.3, which generalizes the results in [CB15] (for single-user scenarios). This statement will be crucial for the construction and the performance analysis of the polar coding schemes that we propose in the following chapters.

Chapter 3

In this chapter we describe two different polar coding schemes for two different models over the degraded wiretap broadcast channel. One model assumes a layered decoding structure that requires receivers with better channel quality to reliably decode more messages, while the other imposes a layered secrecy structure that requires eavesdroppers with worse channel quality to be kept ignorant of more messages. We show that the proposed polar codes are secrecy-capacity achieving in Theorem 3.1 and Theorem 3.2.

Moreover, in Section 3.4 we propose practical methods for constructing polar codes that must satisfy reliability and secrecy constraints simultaneously, and we analyze their performance for a finite blocklength by means of simulations. It is important to mention that, despite we propose a construction for two particular models, our method can be extended to any model with information-theoretic secrecy constraints.

Publications:

J. del Olmo and J. R. Fonollosa, "Strong Secrecy on a Class of Degraded Broadcast Channels Using Polar Codes," in *2016 IEEE Conference on Communications and Network Security (CNS)*, pp. 601-605, 2016.

J. del Olmo and J. R Fonollosa, "Strong Secrecy on a Class of Degraded Broadcast Channels Using Polar Codes," *Entropy*, vol. 20, no. 6, 467, June 2018.

Chapter 4

This chapter focuses on a model for the wiretap broadcast channel where the transmitter wishes to send common public and confidential information to two different receivers with the presence of one eavesdropper. We describe a polar coding scheme that achieves the best-known inner-bound on the secrecy-capacity region of this setting (Theorem 4.1).

The main novelty in this chapter is the introduction of a new chaining structure that allows the polar coding scheme to convey common confidential information to different receivers. This chaining construction induces bidirectional dependencies between adjacent encoding blocks that need to be analyzed carefully in the secrecy analysis of the polar code.

Publications:

J. del Olmo and J. R. Fonollosa, "Polar Coding for Common Message Only Wiretap Broadcast Channel", in *International Symposium on Information Theory (ISIT)*, pages 1762-1766, July 2019.

J. del Olmo and J.R. Fonollosa, "Polar Coding for Common Message Only Wiretap Broadcast Channel," *arXiv preprint arXiv:1901.07649*, 2019.

Chapter 5

This chapter focuses on a model for the wiretap broadcast channel where the transmitter wishes to send different public and confidential information to two different legitimate receivers with the presence of one eavesdropper. There exists two different inner-bounds on the secrecy-capacity of this model in the literature, one being strictly larger for a particular input

distribution (consequently, it includes the other). The stronger inner-bound is obtained by considering joint decoding, whereas the second is derived by considering successive decoding.

We describe a polar coding scheme that achieves the stronger inner-bound on the secrecy-capacity region of this model (Theorem 5.1) and we show that, for a particular input distribution, polar-based joint decoding is crucial. Indeed, the achievability of this inner-bound by means of polar codes requires a chaining construction that induces not only bidirectional dependencies between adjacent encoding blocks, but also these dependencies can occur between different encoding layers.

Publications:

J. del Olmo Alos and J.R. Fonollosa, "Polar Coding for the Wiretap Broadcast Channel with Multiple Messages," *arXiv preprint arXiv:1909.04898*, 2019.

2

Polar coding

In his seminal paper [Ari09], Arikan proved that polar codes achieve the capacity of binary-input, symmetric, point-to-point channels under Successive Cancellation (SC) decoding. Moreover, they are low-complexity codes and, consequently, practical: the proposed encoding/decoding algorithms in [Ari09] have complexity $O(n \log n)$, n being the blocklength. Later, Arikan showed in [Ari10] that the same principle underlying polar codes for channel coding, that is *polarization*, can be applied for optimal lossless source coding. Afterward, Korada and Urbanke in [KU10] proved that polar coding is also optimal for lossy source coding. Indeed, as pointed out in [Ari10], *source polarization* (or *channel polarization*) can be applied to channel coding (source coding) due to the duality between the two problems.

In this chapter, the fundamental theorems of polar codes and their application for different channel coding problems are revisited from a source polarization viewpoint. In Section 2.1, we introduce the source polarization theorem and prove that polar codes are optimal for lossless source coding. Then, Section 2.2 describes the Polar Coding Scheme (PCS) proposed in [Ari10] for symmetric channel coding. In Section 2.3, we outline the PCSs for the DWTC introduced in [MV11] and [SV13], which are secrecy-capacity achieving under the weak and the strong secrecy condition, respectively. These coding schemes were based originally on channel polarization, but we revisit them by using source polarization. In Section 2.4, the PCS for the WTC introduced in [CB16] is summarized. Finally, Section 2.5 generalizes the results in [CB15] by introducing a generic encoding that uses the minimum amount of randomness for multi-user settings and causes a distortion (regarding the distribution that attains the capacity of the model) that is asymptotically negligible.

2.1 Source polarization

Let $(\mathcal{X} \times \mathcal{Y}, p_{XY})$ be a Discrete Memoryless Source (DMS), where[1] $X \in \{0,1\}$ and $Y \in \mathcal{Y}$. The polar transform over the n-sequence X^n, n being any power of 2, is defined as

$$U^n \triangleq X^n G_n, \tag{2.1}$$

where $G_n \triangleq \left[\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right]^{\otimes n}$ is the source polarization matrix [Ari10]. Since $G_n = G_n^{-1}$, then we have $X^n = U^n G_n$ and $p_{U^n}(u^n) = p_{X^n}(u^n G_n)$. Also, for polar coding purposes, we write

$$p_{U^n}(u^n) = \prod_{j=1}^{n} p_{U(j)|U^{1:j-1}}(u(j)|u^{1:j-1}). \tag{2.2}$$

Associated to this polar transform, define the following set of indices:

$$\mathcal{H}_{X|Y}^{(n)} \triangleq \left\{ j \in [1,n] : H\left(U(j) \middle| U^{1:j-1} Y^n\right) \geq 1 - \delta_n \right\}, \tag{2.3}$$

$$\mathcal{L}_{X|Y}^{(n)} \triangleq \left\{ j \in [1,n] : H\left(U(j) \middle| U^{1:j-1} Y^n\right) \leq \delta_n \right\}. \tag{2.4}$$

where $\delta_n \triangleq 2^{-n^\beta}$, and $\beta \in \left(0, \frac{1}{2}\right)$.

Theorem 2.1 (Source polarization, adapted from [Ari10]). *Consider the sets $\mathcal{H}_{X|Y}^{(n)}$ and $\mathcal{L}_{X|Y}^{(n)}$ defined as in (2.3) and (2.4) respectively. It holds that*

$$\lim_{n\to\infty} \frac{1}{n} \left|\mathcal{H}_{X|Y}^{(n)}\right| = H(X|Y) \quad \text{and} \quad \lim_{n\to\infty} \frac{1}{n} \left|\mathcal{L}_{X|Y}^{(n)}\right| = 1 - H(X|Y).$$

Notice that the source polarization theorem states that the polar transform extracts the randomness of X^n in the sense that, as $n \to \infty$, the set of indices $j \in [1,n]$ can be divided practically into two disjoint sets, namely $\mathcal{H}_{X|Y}^{(n)}$ and $\mathcal{L}_{X|Y}^{(n)}$, such that $U(j)$ for $j \in \mathcal{H}_{X|Y}^{(n)}$ is practically independent of $(U^{1:j-1}, Y^n)$ and uniformly distributed, that is, $H(U(j)|U^{1:j-1}Y^n) \to 1$, and $U(j)$ for $j \in \mathcal{L}_{X|Y}^{(n)}$ is almost determined by $(U^{1:j-1}, Y^n)$, which means that $H(U(j)|U^{1:j-1}Y^n) \to 0$. Consequently, the number of elements $U(j)$ that *have not polarized* is asymptotically negligible in terms of rate, i.e., $\lim_{n\to\infty} \frac{1}{n} \left| \left(\mathcal{H}_{X|Y}^{(n)}\right)^{\mathrm{C}} \setminus \mathcal{L}_{X|Y}^{(n)} \right| = 0$.

Definition 2.1. *Generally, the set $\mathcal{H}_{X|Y}^{(n)}$ is referred as the "high entropy set" of X^n given the observations Y^n. On the other hand, $\mathcal{L}_{X|Y}^{(n)}$ is referred as the "low entropy set".*

It is worth mentioning that the entropy terms required to define the sets $\mathcal{H}_{X|Y}^{(n)}$ and $\mathcal{L}_{X|Y}^{(n)}$ can be obtained deterministically from the distribution p_{XY} and the algebraic properties

[1] Throughout this dissertation, we assume binary polarization. Nevertheless, an extension to q-ary alphabets is possible [KT10, ŞTA09].

of the matrix G_n [Ari09, TV13, VVH15, HY13]. Furthermore, consider that the previous sets are defined from the Bhattacharyya parameters instead of the entropy terms, where the Bhattacharyya parameter associated to the element $U(j)$ for any $j \in [1, n]$ is defined as

$$\begin{aligned} &Z(U(j)|U^{1:j-1}Y^n) \\ &\quad \triangleq 2\sum_{y\in\mathcal{Y}} p_{Y^n}(y^n)\sqrt{p_{U(j)|U^{1:j-1}Y^n}(0|u^{1:j-1}y^n)p_{U(j)|U^{1:j-1}Y^n}(1|u^{1:j-1}y^n)}. \end{aligned} \tag{2.5}$$

The following lemma shows that $\{H(U(j)|U^{1:j-1}Y^n)\}_{j=1}^n$ and $\{Z(U(j)|U^{1:j-1}Y^n)\}_{j=1}^n$ polarize simultaneously and, consequently, Theorem 2.1 holds in both cases.

Lemma 2.1 (Adapted from [Ari10]). *Consider the entropy terms and the Bhattacharyya parameters associated to the polar transform $U^n = X^nG_n$. It holds*

$$\begin{aligned} Z(U(j)|U^{1:j-1}Y^n)^2 &\leq H(U(j)|U^{1:j-1}Y^n), \\ H(U(j)|U^{1:j-1}Y^n) &\leq \log(1 + Z(U(j)|U^{1:j-1}Y^n)), \end{aligned}$$

where either both inequalities are strict or both hold with equality; and for equality to hold, it is necessary and sufficient that $U(j)$ is either deterministic or uniformly distributed.

As an example, Figure 2.1 shows the polarization effect when $n = 1024$ for a DMS $(\mathcal{X} \times \mathcal{Y}, p_{XY})$ such that $\mathcal{X} = \{0, 1\}$, $\mathcal{Y} = \{0, 1, E\}$, $p_X(x) = 0.5$ for all $x \in \mathcal{X}$, and $p_{Y|X}(y|x)$ is modeled as a Binary Erasure Channel (BEC) with erasure probability $\epsilon = 0.4$. Notice that most of the entropy terms tend to be near zero and near to one. Indeed, by Theorem 2.1, the number of terms that tend to one will approach $nH(X|Y) = n\epsilon$. However, an asymptotically negligible (in terms of rate) range of entropy terms shows an *erratic* behavior.

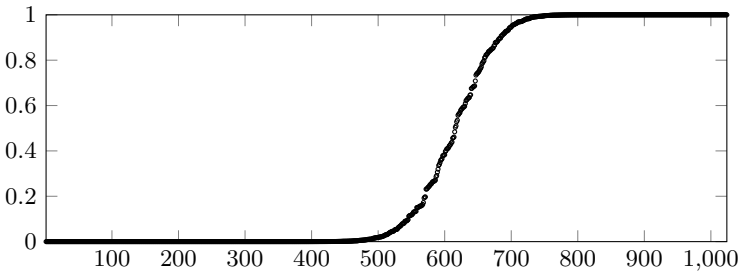

Figure 2.1: Entropy terms $\{H(U(j)|U^{1:j-1}Y^n)\}_{j=1}^n$ (ordered) when $n = 1024$ for a DMS $(\mathcal{X} \times \mathcal{Y}, p_{XY})$ such that $\mathcal{X} = \{0, 1\}$, $\mathcal{Y} = \{0, 1, E\}$, $p_X(x) = 0.5\,\forall x \in \mathcal{X}$, and $p_{Y|X}(y|x)$ is modeled as a BEC ($\epsilon = 0.4$).

Consider a SC decoder that, from $U\left[\left(\mathcal{L}_{X|Y}^{(n)}\right)^{\mathrm{C}}\right]$ and the observations Y^n, constructs an

estimate $\hat{U}^n$ of the entire sequence U^n as follows. For all $j \in [1,n]$, it obtains

$$\hat{U}(j) = \begin{cases} U(j) & \text{if } j \in \big(\mathcal{L}_{X|Y}^{(n)}\big)^{\mathrm{C}}, \\ \arg\max_{u\in\{0,1\}} p_{U(j)|U^{1:j-1}Y^n}\big(u\big|\hat{U}^{1:j-1}Y^n\big) & \text{if } j \in \mathcal{L}_{X|Y}^{(n)}. \end{cases} \tag{2.6}$$

The following theorem proves that SC decoding is able to reconstruct U^n entirely from $U\big[\big(\mathcal{L}_{X|Y}^{(n)}\big)^{\mathrm{C}}\big]$ and Y^n with error probability in $O\big(2^{-n^\beta}\big)$.

Theorem 2.2 (Adapted from [Ari10]). *Let $\delta_n \triangleq 2^{-n^\beta}$, where $\beta \in \big(0, \frac{1}{2}\big)$. Given $U\big[\big(\mathcal{L}_{X|Y}^{(n)}\big)^{\mathrm{C}}\big]$ and Y^n, the SC decoder in (2.6) constructs an estimate $\hat{U}^n$ of U^n with*

$$\mathbb{P}\big[\hat{U}^n \neq U^n\big] \leq \big|\mathcal{L}_{X|Y}^{(n)}\big|\delta_n.$$

Therefore, Theorem 2.2, along with Theorem 2.1, shows that polar codes are optimal for lossless source coding with side information.

2.2 Source polarization for symmetric channel coding

A binary Discrete Memoryless Channel (DMC) $(\mathcal{X}, p_{Y|X}, \mathcal{Y})$ with some arbitrary p_X can be seen as a DMS $(\mathcal{X}\times\mathcal{Y}, p_X p_{Y|X})$. For symmetric channel coding, recall that the capacity achieving input distribution p_X is uniform, that is, $p_X(x) = \frac{1}{2}$ for all $x \in \{0,1\}$.

Let W and F be uniformly distributed vectors of length $\big|\mathcal{L}_{X|Y}^{(n)}\big|$ and $\big|\big(\mathcal{L}_{X|Y}^{(n)}\big)^{\mathrm{C}}\big|$, respectively, where W represents the information message to be sent over the DMC, and F is a source of common randomness that is available to both the transmitter and the receiver.

Consider the following PCS. First, from p_{XY} and the algebraic properties of G_n, define the sets of indices $\mathcal{H}_{X|Y}^{(n)}$ and $\mathcal{L}_{X|Y}^{(n)}$ as in (2.3) and (2.4) respectively (*polar code construction*). Second, consider a polar-based encoder that construct $\tilde{U}^n$ as follows. It stores the information message W into $\tilde{U}\big[\mathcal{L}_{X|Y}^{(n)}\big]$ and the random sequence F into $\tilde{U}\big[\big(\mathcal{L}_{X|Y}^{(n)}\big)^{\mathrm{C}}\big]$. Thus, we have

$$\tilde{U}\big[\mathcal{L}_{X|Y}^{(n)}\big] = W \quad \text{and} \quad \tilde{U}\big[\big(\mathcal{L}_{X|Y}^{(n)}\big)^{\mathrm{C}}\big] = F.$$

Then, the encoder computes the polar transform $\tilde{X}^n = \tilde{U}^n G_n$ and, afterwards, the transmitter sends $\tilde{X}^n$ over the channel, which induces $\tilde{Y}^n$. Finally, the receiver, by using the SC decoder described in (2.6), constructs an estimate $\hat{U}^n$ of the sequence $\tilde{U}^n$ from $\tilde{U}\big[\big(\mathcal{L}_{X|Y}^{(n)}\big)^{\mathrm{C}}\big]$, which is known because F is available to all parties, and the channel output observations $\tilde{Y}^n$.

Remark 2.1. *Since the polar-based encoder will construct random variables that must approach the target distribution of the DMS, throughout this dissertation we use tilde above the random variables to emphasize this purpose.*

The previous PCS approaches the capacity of the binary symmetric DMC because, by applying Theorem 2.1, the information rate is

$$\lim_{n\to\infty}\frac{1}{n}\left|\mathcal{L}_{X|Y}^{(n)}\right| = 1 - H(X|Y),$$

and $I(X;Y) = 1 - H(X|Y)$ when X is binary and uniformly distributed.

It remains to show whether the PCS is capacity-achieving by analyzing the average block error probability. First, since the input distribution of the original DMS is the uniform, that is $p_x(x) = \frac{1}{2}\ \forall x \in \{0,1\}$, and the elements of X^n are i.i.d. then $p_{U^n}(u^n) = p_{X^n}(u^n G_n) = 2^{-n}$. Therefore, since W and F are uniformly distributed, the input distribution induced by the previous encoding, namely $\tilde{q}_{U^n}$, and the distribution p_{U^n} are statistically indistinguishable, that is, $\mathbb{V}(\tilde{q}_{U^n}, p_{U^n}) = 0$. Indeed, since $\tilde{Y}^n$ depends on the channel transition distribution $p_{Y|X}$ and due to the invertibility of G_n, the joint distribution $\tilde{q}_{X^nY^n}$ induced by the encoding and $p_{X^nY^n}$ of the original DMS satisfy that $\mathbb{V}(\tilde{q}_{X^nY^n}, p_{X^nY^n}) = 0$. Consequently, we obtain

$$\mathbb{P}\left[\hat{U}^n \neq \tilde{U}^n\right] = \left[\hat{U}^n \neq U^n\right] \leq n\delta_n,$$

where we have used Theorem 2.2 because $\tilde{U}\left[\left(\mathcal{L}_{X|Y}^{(n)}\right)^{\mathrm{C}}\right] = F$ is available to the receiver. Hence, the previous PCS is capacity-achieving for the binary symmetric channel.

2.3 Polar codes for the symmetric DWTC

Polar coding relying on channel polarization for the binary symmetric DWTC were introduced in [MV11] and [SV13], which provide secrecy-capacity achieving polar codes under the weak and the strong secrecy condition, respectively. This section summarize the relevant techniques of the PCSs proposed by [MV11] and [SV13] from a source-polarization point of view.

Consider a DMS $(\mathcal{X}\times\mathcal{Y}\times\mathcal{Z}, p_X p_{YZ|X})$ that represents the input and output random variables involved in the achievable region of the DWTC defined in Proposition 1.1, where $\mathcal{X} = \{0,1\}$, $p_X(x) = \frac{1}{2}$ for all $x \in \{0,1\}$, and $p_{Y|X} \succeq p_{Z|X}$ (stochastically degraded channels) or $X - Y - Z$ forms a Markov chain (physically degraded channels). Let (X^n, Y^n, Z^n) denote an i.i.d. sequence of this source and define the polar transform $U^n \triangleq X^n G_n$. Associated to this polar transform, define the sets $\mathcal{H}_{X|Y}^{(n)}$ and $\mathcal{L}_{X|Y}^{(n)}$ as in Equations (2.3) and (2.4) respectively. Moreover, for this model define

$$\mathcal{H}_{X|Z}^{(n)} \triangleq \left\{j \in [1,n] : H\left(U(j)\left|U^{1:j-1}Z^n\right.\right) \geq 1-\delta_n\right\}, \tag{2.7}$$

$$\mathcal{L}_{X|Z}^{(n)} \triangleq \left\{j \in [1,n] : H\left(U(j)\left|U^{1:j-1}Z^n\right.\right) \leq \delta_n\right\}, \tag{2.8}$$

where recall that $\delta_n \triangleq 2^{-n^\beta}$ and $\beta \in \left(0, \frac{1}{2}\right)$. Notice that these sets represent the high entropy set and the low entropy set of X^n given the eavesdropper's observations Z^n.

Lemma 2.2 (Subset property of polar codes, adapted from [MV11, GAG15]). *Consider a DMS* $(\mathcal{X} \times \mathcal{Y} \times \mathcal{Z}, p_X p_{YZ|X})$ *such that* $p_{Y|X} \succeq p_{Z|X}$ *(stochastically degradation) or* $X - Y - Z$ *forms a Markov chain (physically degradation). Thus, we have*

$$\mathcal{H}_{X|Y}^{(n)} \subseteq \mathcal{H}_{X|Z}^{(n)}, \quad \text{and} \quad \mathcal{L}_{X|Y}^{(n)} \supseteq \mathcal{L}_{X|Z}^{(n)}.$$

Based on the definition of the previous sets and Lemma 2.2, reference [MV11] proposes the following partition of the set of indices $[1, n]$:

$$\mathcal{I}^{(n)} \triangleq \left(\mathcal{L}_{X|Z}^{(n)}\right)^{\mathrm{C}} \cap \mathcal{L}_{X|Y}^{(n)}, \quad \mathcal{C}^{(n)} \triangleq \mathcal{L}_{X|Z}^{(n)}, \quad \mathcal{F}^{(n)} \triangleq \left(\mathcal{L}_{X|Y}^{(n)}\right)^{\mathrm{C}}, \tag{2.9}$$

which is graphically represented in Figure 2.2.

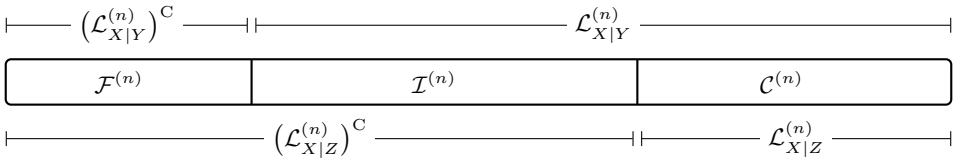

Figure 2.2: Polar code construction for the symmetric DWTC: partition of the set of indices $[1, n]$.

Roughly speaking, according to Theorem 2.1 and Theorem 2.2, the set $\mathcal{I}^{(n)}$ contains those indices that are *good* for the legitimate receiver and *bad* for the eavesdropper, where *good* means that the elements of $U\left[\mathcal{I}^{(n)}\right]$ can be reliably inferred by the receiver, and *bad* means that they can be information-theoretic secured from the eavesdropper. Furthermore, $\mathcal{C}^{(n)}$ contains those indices that are *good* for both the legitimate receiver and the eavesdropper because, by Lemma 2.2, $\mathcal{L}_{X|Y}^{(n)} \subseteq \mathcal{L}_{X|Z}^{(n)}$; and $\mathcal{F}^{(n)}$ contain those indices that are *bad* for both.

Let S and F be uniformly distributed vectors of length $\left|\mathcal{I}^{(n)}\right|$ and $\left|\mathcal{F}^{(n)}\right|$, respectively, where S represents the confidential message and F is a source of common randomness that is available to both the transmitter and the receiver. Moreover, let C be a uniformly distributed random sequence of length $\left|\mathcal{C}^{(n)}\right|$. Consider a PCS for the DWTC that is described as follows:

- *Polar code construction:* from p_{XYZ} and the algebraic properties of G_n, define the sets of indices $\mathcal{H}_{X|Y}^{(n)}$, $\mathcal{L}_{X|Y}^{(n)}$, $\mathcal{H}_{X|Z}^{(n)}$ and $\mathcal{L}_{X|Z}^{(n)}$.
- *Polar-based encoding:* the encoder constructs $\tilde{U}^n$ as follows. It stores the confidential message S into $\tilde{U}\left[\mathcal{I}^{(n)}\right]$, and the random sequences F and C into $\tilde{U}\left[\mathcal{F}^{(n)}\right]$ and $\tilde{U}\left[\mathcal{C}^{(n)}\right]$ respectively. Thus, $\tilde{U}\left[\mathcal{I}^{(n)}\right] = S$, $\tilde{U}\left[\mathcal{F}\right] = F$ and $\tilde{U}\left[\mathcal{C}^{(n)}\right] = C$. Then, the encoder

computes the polar transform $\tilde{X}^n = \tilde{U}^n G_n$. Afterwards, the transmitter sends $\tilde{X}^n$ over the channel inducing the output observations $\tilde{Y}^n$ and $\tilde{Z}^n$.

- *Polar-based decoding:* The receiver uses SC decoding described in (2.6) to form an estimate $\hat{U}^n$ of the sequence $\tilde{U}^n$ from $\tilde{U}\big[\mathcal{F}^{(n)}\big]$, which is known because F is available to all parties, and the observations $\tilde{Y}^n$. Then, it obtains the estimate $\hat{S} = \hat{U}\big[\mathcal{I}^{(n)}\big]$.

Definition 2.2. *Typically, sequence C is referred as* local randomness *and is required to "confuse" the eavesdropper about the confidential message S.*

The previous PCS approaches the capacity of the symmetric DWTC because, by applying standard operations and Lemma 2.2, the confidential message rate is

$$\begin{aligned}\lim_{n\to\infty}\frac{1}{n}\big|\mathcal{I}^{(n)}\big| &= \lim_{n\to\infty}\big|\big(\mathcal{L}^{(n)}_{X|Z}\big)^{\mathrm{C}}\cap\mathcal{L}^{(n)}_{X|Y}\big| \\ &= \lim_{n\to\infty}\big|\big(\mathcal{L}^{(n)}_{X|Z}\big)^{\mathrm{C}}\big| - \lim_{n\to\infty}\big|\big(\mathcal{L}^{(n)}_{X|Y}\big)^{\mathrm{C}}\big| \\ &= H(X|Z) - H(X|Y), \end{aligned} \tag{2.10}$$

where the last step holds by Theorem 2.1 because $\big|\big(\mathcal{L}^{(n)}_{X|Z}\big)^{\mathrm{C}}\big| = \big|\mathcal{H}^{(n)}_{X|Z}\big| + \big|\big(\mathcal{L}^{(n)}_{X|Y}\big)^{\mathrm{C}}\setminus\mathcal{H}^{(n)}_{X|Y}\big|$.

Let $\tilde{q}_{X^nY^nZ^n}$ denote the distribution induced by the previous encoding. Since S, F and C are uniformly distributed, it is clear that $\mathbb{V}(\tilde{q}_{U^n}, p_{U^n}) = 0$. Moreover, due to the invertibility of G_n and because, given $\tilde{X}^n$, $(\tilde{Y}^n, \tilde{Z}^n)$ only depends on the channel transition distribution $p_{Y^nZ^n|X^n}$, we have $\mathbb{V}(\tilde{q}_{X^nY^nZ^n}, p_{X^nY^nZ^n}) = 0$. Therefore, by Theorem 2.2, the reliability performance of the PCS is $\mathbb{P}\big[\hat{U}^n \neq \tilde{U}^n\big] \leq n\delta_n$.

Regarding the information-theoretical security, [MV11] showed that the previous PCS is secrecy-capacity achieving only under the weak secrecy condition. Since F is available to all parties, the information leakage is given by $I(S;\tilde{Z}^nF)$ and, effectively, it holds

$$\begin{aligned} I(S;\tilde{Z}^nF) &\overset{(a)}{\leq} I\big(\tilde{U}\big[\mathcal{I}^{(n)}\cup\mathcal{F}^{(n)}\big];\tilde{Z}^n\big) \\ &\overset{(b)}{=} I\big(U\big[\mathcal{I}^{(n)}\cup\mathcal{F}^{(n)}\big];Z^n\big) \\ &\overset{(c)}{=} \big|\mathcal{H}^{(n)}_{X|Z}\big| - H\big(U\big[\mathcal{H}^{(n)}_{X|Z}\big]\big|Z^n\big) \\ &\quad + \big|\big(\mathcal{L}^{(n)}_{X|Z}\big)^{\mathrm{C}}\setminus\mathcal{H}^{(n)}_{X|Z}\big| - H\big(U\big[\big(\mathcal{L}^{(n)}_{X|Z}\big)^{\mathrm{C}}\setminus\mathcal{H}^{(n)}_{X|Z}\big]\big|U\big[\mathcal{H}^{(n)}_{X|Z}\big]Z^n\big) \\ &\overset{(d)}{\leq} \big|\mathcal{H}^{(n)}_{X|Z}\big|\delta_n + \big|\big(\mathcal{L}^{(n)}_{X|Z}\big)^{\mathrm{C}}\setminus\mathcal{H}^{(n)}_{X|Z}\big| - H\big(U\big[\big(\mathcal{L}^{(n)}_{X|Z}\big)^{\mathrm{C}}\setminus\mathcal{H}^{(n)}_{X|Z}\big]\big|U\big[\mathcal{H}^{(n)}_{X|Z}\big]Z^n\big) \\ &\overset{(e)}{\leq} n\delta_n + o(n), \end{aligned}$$

where (a) holds because $I(S;\tilde{Z}^nF) = I(S;F) + I(S;\tilde{Z}^n|F) = I(S;\tilde{Z}^n|F) \leq I(SF;\tilde{Z}^n)$, and $\tilde{U}\big[\mathcal{I}^{(n)}\big] = S$ and $\tilde{U}\big[\mathcal{F}\big] = F$; (b) holds because $\mathbb{V}(\tilde{q}_{X^nY^nZ^n}, p_{X^nY^nZ^n}) = 0$; (c) holds

because, according to (2.9), we have $\mathcal{I}^{(n)} \cup \mathcal{F}^{(n)} = \big(\mathcal{L}_{X|Z}^{(n)}\big)^{\mathrm{C}}$, the uniformity of $\tilde{U}\big[\mathcal{I}^{(n)} \cup \mathcal{F}^{(n)}\big]$ (confidential message and source of common randomness), and from applying the chain rule of entropy; (d) holds because

$$H\big(U\big[\mathcal{H}_{X|Z}^{(n)}\big]\big|Z^n\big) \geq \sum_{j \in \mathcal{H}_{X|Z}^{(n)}} H\big(U(j)\big|U^{1:j-1}Z^n\big)$$

and $H\big(U(j)\big|U^{1:j-1}Z^n\big) \geq 1-\delta_n$ for any $j \in \mathcal{H}_{X|Z}^{(n)}$; and (e) holds because the set of indices corresponding to those elements that have not polarized is asymptotically negligible only in terms of rate and $\delta_n \leq H\big(U(j)\big|U^{1:j-1}Z^n\big) \leq 1-\delta_n$ for any $j \in \big(\mathcal{L}_{X|Z}^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{H}_{X|Z}^{(n)}$. Thus, the previous PCS fails to provide strong secrecy because

$$I(S;\tilde{Z}^nF) \leq n\delta_n + o(n) \xrightarrow{n\to\infty} o(n).$$

Nevertheless, it is clear that this PCS is secrecy-capacity achieving under the weak secrecy condition because it holds that

$$\frac{1}{n} I(S;\tilde{Z}^nF) \leq \delta_n + \frac{o(n)}{n} \xrightarrow{n\to\infty} 0.$$

Remark 2.2. *References [Ari10] and [MV11] show that the source of common randomness is not necessary for symmetric channels, but F can be deterministic (frozen bits).*

Notice that the previous polar code fails to provide strong secrecy because the indices considered as *bad* for the eavesdropper are not bad enough. In this sense, [SV13] proposes a new partition of the set of indices $[1,n]$:

$$\begin{aligned}
\mathcal{I}^{(n)} &\triangleq \mathcal{H}_{X|Z}^{(n)} \cap \mathcal{L}_{X|Y}^{(n)},\\
\mathcal{F}^{(n)} &\triangleq \mathcal{H}_{X|Z}^{(n)} \cap \big(\mathcal{L}_{X|Y}^{(n)}\big)^{\mathrm{C}},\\
\mathcal{C}^{(n)} &\triangleq \big(\mathcal{H}_{X|Z}^{(n)}\big)^{\mathrm{C}} \cap \mathcal{L}_{X|Y}^{(n)},\\
\mathcal{D}^{(n)} &\triangleq \big(\mathcal{H}_{X|Z}^{(n)}\big)^{\mathrm{C}} \cap \big(\mathcal{L}_{X|Y}^{(n)}\big)^{\mathrm{C}}.
\end{aligned}$$

Now, notice that the *message* set $\mathcal{I}^{(n)}$ does not contain those indices belonging to $\mathcal{L}_{X|Y}^{(n)} \cap \big(\big(\mathcal{L}_{X|Z}^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{H}_{X|Z}^{(n)}\big)$ that were problematic in the previous scheme, but they are included in the set $\mathcal{C}^{(n)}$. Moreover, now the set $\mathcal{F}^{(n)}$ does not contain those indices that belong to $\big(\mathcal{H}_{X|Z}^{(n)}\big)^{\mathrm{C}} \cap \big(\mathcal{L}_{X|Y}^{(n)}\big)^{\mathrm{C}}$, but they are included in the new set $\mathcal{D}^{(n)}$.

The construction of $\tilde{U}\big[\mathcal{D}^{(n)}\big]$ is problematic: the legitimate receiver needs to known these elements to reliably decode the entire sequence $\tilde{U}^n$ because $\mathcal{D}^{(n)} \subseteq \big(\mathcal{L}_{X|Y}^{(n)}\big)^{\mathrm{C}}$ but they cannot store common randomness because $\mathcal{D}^{(n)} \subseteq \big(\mathcal{H}_{X|Z}^{(n)}\big)^{\mathrm{C}}$ and the secrecy will be compromised.

Hence, [SV13] proposes a PCS where transmission takes place over L blocks of size n, and uses a *chaining construction* to convey the problematic elements to the legitimate receiver while keeping masked from the eavesdropper.

Let $\mathcal{R}^{(n)}$ be any subset of $\mathcal{I}^{(n)}$ with size $\big|\mathcal{D}^{(n)}\big|$. For any block $i \in [1, L]$, let S_i and C_i be the random sequences representing the confidential message and the local randomness with size $\big|\mathcal{I}^{(n)}\big| - \big|\mathcal{R}^{(n)}\big|$ and $\big|\mathcal{C}^{(n)}\big|$, respectively. Let F be $\big|\mathcal{F}^{(n)}\big|$-sequence representing the source of common randomness available to all parties (this sequence will be reused at each block). Moreover, for $i \in [0, L]$, let D_i be a uniformly distributed $\big|\mathcal{D}^{(n)}\big|$-sequence that is considered part of the local randomness. At block $i \in [1, L]$, the encoder forms $\tilde{U}_i^n$ as follows:

$$\tilde{U}_i\big[\mathcal{I}^{(n)} \setminus \mathcal{R}^{(n)}\big] = S_i,\ \ \tilde{U}_i\big[\mathcal{F}^{(n)}\big] = F,\ \ \tilde{U}_i\big[\mathcal{C}^{(n)}\big] = C_i,\ \ \tilde{U}_i\big[\mathcal{D}^{(n)}\big] = D_{i-1},\ \ \tilde{U}_i\big[\mathcal{R}^{(n)}\big] = D_i.$$

Thus, notice that the encoder dedicates some of the reliable and *secure* elements of block i, that is $\tilde{U}_i\big[\mathcal{R}^{(n)}\big]$, to send *unsecure* and *unreliable* elements of block $i+1$, that is $\tilde{U}_{i+1}\big[\mathcal{D}^{(n)}\big]$. Then, it computes $\tilde{X}_i^n = \tilde{U}_i^n G_n$, which is transmitted over the DWTC inducing $(\tilde{Y}_i^n, \tilde{Z}_i^n)$.

Additionally, in order to initialize the decoding procedure, before transmitting $\tilde{X}_1^n$ the encoder needs to make available D_0 to the legitimate receiver keeping it masked from the eavesdropper. To do so, one can use a separate channel code to reliably send $D_0 \oplus \kappa$, where κ is a uniformly distributed secret-key shared between transmitter and legitimate receiver. This secret-key is asymptotically negligible in terms of rate because

$$\big|\mathcal{D}^{(n)}\big| = \big|\big(\mathcal{H}_{X|Z}^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{L}_{X|Y}^{(n)}\big| \leq \big|\big(\mathcal{H}_{X|Z}^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{L}_{X|Z}^{(n)}\big| = o(n),$$

where we have used the fact that $\mathcal{L}_{X|Y}^{(n)} \subseteq \mathcal{L}_{X|Z}^{(n)}$. Indeed, since the transmission will take place over L blocks of size n, the rate of this required additional transmission is $\frac{1}{nL}\big|\mathcal{D}^{(n)}\big| = \frac{o(n)}{nL}$.

Consider that D_0 has reliably been estimated by the legitimate receiver. Then, the decoder successively forms an estimate of $\tilde{U}_{1:L}^n$, from $\hat{U}_1^n$ to $\hat{U}_L$, as follows. For $i \in [1, L]$, given $\hat{D}_{i-1}$ from block $i-1$ and F_i, the receiver knows $\hat{U}_i\big[\mathcal{D}^{(n)} \cup \mathcal{F}^{(n)}\big] = \hat{U}_i\big[\big(\mathcal{L}_{X|Y}^{(n)}\big)^{\mathrm{C}}\big]$. Thus, it uses the SC decoder in (2.6) to reliably estimate $\hat{U}_i^n$. Finally, it obtains $\hat{U}_i\big[\mathcal{R}^{(n)}\big] = \hat{D}_i$, which will be used at the next block $i+1$ to reliably estimate $\tilde{U}_{i+1}^n$.

Since the size of $\mathcal{D}^{(n)}$ is $o(n)$, the rate cost of conveying the problematic elements by means of the chaining construction is asymptotically negligible. Formally, we have

$$\lim_{n\to\infty} \frac{L\big(\big|\mathcal{I}^{(n)}\big| - \big|\mathcal{R}^{(n)}\big|\big)}{n(L+1)} = \lim_{n\to\infty} \frac{L\big|\mathcal{H}_{X|Z}^{(n)} \cap \mathcal{L}_{X|Y}^{(n)}\big| - L\big|\mathcal{R}^{(n)}\big|}{n(L+1)} = \frac{L}{L+1}(H(X|Z) - H(X|Y)),$$

where we have used Theorem 2.1 and similar reasoning as in (2.10). Thus, the PCS can operate as close to the secrecy-capacity as desired by choosing a sufficiently large L.

Let $\tilde{q}_{X_i^n Y_i^n Z_i^n}$ denote the distribution induced by the previous encoding at block $i \in [1, L]$. Due to the uniformity of the random sequences involved in the encoding, it is clear that $\mathbb{V}(\tilde{q}_{X_i^n Y_i^n Z_i^n}, p_{X^n Y^n Z^n}) = 0$. For $i \in [1, L]$, define the error event $\mathcal{E}_{D_i} \triangleq \mathbb{P}\big[\hat{D}_i \neq D_i\big]$. The average average block error probability, for any block $i \in [1, L]$, is given by

$$\begin{aligned}
\mathbb{P}\big[\hat{U}_i^n \neq \tilde{U}_i^n\big] &= \mathbb{P}\big[\hat{U}_i^n \neq \tilde{U}_i^n \big| \mathcal{E}_{D_{i-1}}^{\mathrm{C}}\big]\mathbb{P}\big[\mathcal{E}_{D_{i-1}}^{\mathrm{C}}\big] + \mathbb{P}\big[\hat{U}_i^n \neq \tilde{U}_i^n \big| \mathcal{E}_{D_{i-1}}\big]\mathbb{P}\big[\mathcal{E}_{D_{i-1}}\big] \\
&\leq \mathbb{P}\big[\hat{U}_i^n \neq \tilde{U}_i^n \big| \mathcal{E}_{D_{i-1}}^{\mathrm{C}}\big] + \mathbb{P}\big[\mathcal{E}_{D_{i-1}}\big] \\
&\overset{(a)}{\leq} n\delta_n + \mathbb{P}\big[\mathcal{E}_{D_{i-1}}\big] \\
&\overset{(b)}{\leq} n\delta_n + \mathbb{P}\big[\hat{U}_{i-1}^n \neq \tilde{U}_{i-1}^n\big] \\
&\overset{(c)}{\leq} in\delta_n
\end{aligned} \tag{2.11}$$

where (a) holds because $\mathbb{V}(\tilde{q}_{X_i^n Y_i^n Z_i^n}, p_{X^n Y^n Z^n}) = 0$ and, therefore, by Theorem 2.2—recall that $(D_{i-1}, F_i) = \tilde{U}_i\big[\big(\mathcal{L}_{X|Y}\big)^{\mathrm{C}}\big]$; (b) holds because $D_{i-1} = \tilde{U}_{i-1}\big[\mathcal{R}^{(n)}\big]$; and (c) holds by induction. Consequently, the average probability of incorrectly decoding $\tilde{U}_{1:L}^n$ is

$$\mathbb{P}\big[\hat{U}_{1:L}^n \neq \tilde{U}_{1:L}^n\big] \leq \sum_{i=1}^{L} \mathbb{P}\big[\hat{U}_i^n \neq \tilde{U}_i^n\big] = \frac{L(L+1)}{2} n\delta_n,$$

where we have used the union bound and (2.11).

Finally, this PCS is secrecy-capacity achieving under the strong secrecy condition. Now, notice that the information leakage is given by $I(S_{1:L}; \tilde{Z}_{1:L}^n F)$ and, therefore, to evaluate this measure one must consider the dependencies between the random variables of different blocks. These dependencies are graphically represented in Figure 2.3.

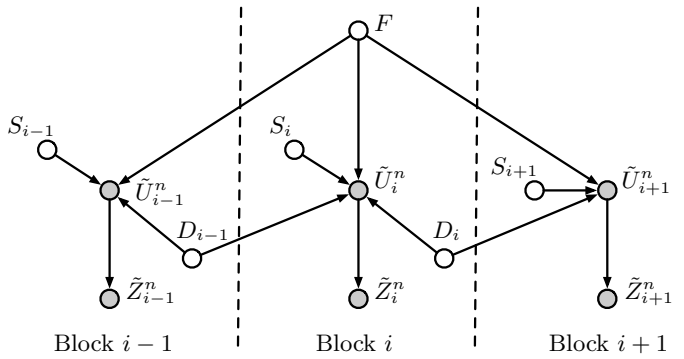

Figure 2.3: Bayesian graph plotting the dependencies between the random variables of different blocks that are involved in the secrecy analysis when we consider a transmission over several blocks of size n.

Thus, by applying the chain rule of mutual information, we have

$$I(S_{1:L};\tilde{Z}_{1:L}^n F)=\sum_{i=1}^{L} I(S_{1:L};\tilde{Z}_i^n|F\tilde{Z}_{1:i-1}^n)\leq Ln\delta_n, \tag{2.12}$$

where the last inequality holds because

$$\begin{aligned}
I(S_{1:L};\tilde{Z}_i^n|F\tilde{Z}_{1:i-1}^n) &= I(S_{1:i};\tilde{Z}_i^n|F\tilde{Z}_{1:i-1}^n)+I(S_{i+1:L};\tilde{Z}_i^n|FS_{1:i}\tilde{Z}_{1:i-1}^n)\\
&\leq I(S_{1:i}\tilde{Z}_{1:i-1}^n;\tilde{Z}_i^n|F)+I(S_{i+1:L};\tilde{Z}_{1:i}^n FS_{1:i})\\
&\overset{(a)}{=} I(S_{1:i}\tilde{Z}_{1:i-1}^n;\tilde{Z}_i^n|F)\\
&\leq I(S_{1:i}\tilde{Z}_{1:i-1}^n D_i;\tilde{Z}_i^n|F)\\
&\leq I(S_iD_i;\tilde{Z}_i^n|F)+I(S_{1:i-1}\tilde{Z}_{1:i-1}^n;\tilde{Z}_i^n|FS_iD_i)\\
&\overset{(b)}{=} I(S_iD_i;\tilde{Z}_i^n|F)\\
&\leq I(S_iD_iF;\tilde{Z}_i^n)\\
&\overset{(c)}{\leq} I\big(\tilde{U}_i\big[\mathcal{H}_{X|Z}^{(n)}\big];\tilde{Z}_i^n\big)\\
&\overset{(d)}{\leq} n\delta_n.
\end{aligned}$$

where (a) follows from applying *d-separation* [Pea09] over graph in Figure 2.3 to prove that $S_{i+1:L}$ are independent of F and all random variables of previous blocks $[1,i]$; (b) also follows from applying *d-separation* because $S_{1:i-1}\tilde{Z}_{1:i-1}^n - FS_iD_i - \tilde{Z}_i^n$ forms a Markov chain; (c) holds because, by definition, $(S_i,D_i,F)=\tilde{U}_i\big[\mathcal{H}_{X|Z}^{(n)}\big]$; and (d) holds because $\mathbb{V}(\tilde{q}_{X_i^nY_i^nZ_i^n},p_{X^nY^nZ^n})=0$ and, by definition, $H(U(j)|U^{1:j-1}Z^n)\geq 1-\delta_n$ for any $j\in\mathcal{H}_{X|Z}^{(n)}$.

2.4 Polar codes for the general WTC

Polar coding has been extended to the general WTC in [RRS13, WU16, GB17, CB16]. Indeed, [GB17, CB16] generalize their results providing PCSs for the BCC, and [WU16] also proposes polar coding strategies to achieve the best-known inner bounds on the secrecy-capacity region of different multi-user settings. A good overview of the similarities and differences between the polar codes proposed in [RRS13, WU16, GB17, CB16] for the general wiretap channel can be found in [CB16] (Figure 1).

This section overviews polar coding for the WTC based mainly on the techniques introduced in [CB16] due to the following reasons: to guarantee strong secrecy and to provide polar coding schemes that are implementable in practice. In [WU16], the proposed PCSs are secrecy-capacity achieving only under the weak secrecy condition. Moreover, the coding

scheme presented in [RRS13] relies on a construction for which no efficient code is presently known, and the PCS in [GB17] only relies on the existence (through averaging) of certain deterministic mappings for the encoding/decoding process.

Consider a DMS $(\mathcal{V} \times \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}, p_{VXYZ})$ that represents the input and output random variables involved in the achievable region of the WTC defined in Proposition 1.2, where $\mathcal{V} = \mathcal{X} = \{0, 1\}$, and p_{VXYZ} such that $V - X - YZ$ forms a Markov chain.

In this model it is clear that the optimal input distribution is not necessarily uniformly distributed. Consequently, the previous PCS described for the DWTC will fail to provide reliability and strong secrecy because the encoder could induce a distribution that is not sufficiently close to $p_{V^n X^n Y^n Z^n}$. In this sense, the PCS uses a similar construction of that for asymmetric settings introduced in [HY13, MUH14].

Furthermore, in this setting the subset property of polar codes, that is Lemma 2.2, does not hold because the eavesdropper channel is not degraded with respect to the legitimate receiver one. Thus, $\mathcal{H}_{X|Y}^{(n)} \not\subseteq \mathcal{H}_{X|Z}^{(n)}$ and, consequently, $\mathcal{D}^{(n)}$ is not asymptotically negligible in general. This means that the previous chaining construction does not allow to convey the problematic elements at negligible rate penalty, and the PCS uses a new chaining construction based on that given in [HU14]. Also, in the previous PCS all the elements of $\tilde{U}_i\big[\mathcal{H}_{X|Y}^{(n)}\big]$, for any $i \in [1, L]$, were known by the receiver because they contained common randomness. The use of this source was possible because $\mathcal{H}_{X|Y}^{(n)} \subseteq \mathcal{H}_{X|Z}^{(n)}$ and, hence, the secrecy was not compromised. Now, since $\mathcal{H}_{X|Y}^{(n)} \not\subseteq \mathcal{H}_{X|Z}^{(n)}$ in general, these elements required by the receiver must be secretly conveyed also by means of the chaining construction.

Let (V^n, X^n, Y^n, Z^n) denote an i.i.d. sequence of the DMS $(\mathcal{V} \times \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}, p_{VXYZ})$, and define the polar transforms $U^n \triangleq V^n G_n$ and $T^n \triangleq X^n G_n$. Now, associated to U^n, define

$$\begin{aligned}
\mathcal{H}_{V}^{(n)} &\triangleq \left\{j \in [1,n] : H\left(U(j) \middle| U^{1:j-1}\right) \geq 1 - \delta_n\right\}, \\
\mathcal{L}_{V}^{(n)} &\triangleq \left\{j \in [1,n] : H\left(U(j) \middle| U^{1:j-1}\right) \leq \delta_n\right\}, \\
\mathcal{H}_{V|Z}^{(n)} &\triangleq \left\{j \in [1,n] : H\left(U(j) \middle| U^{1:j-1} Z^n\right) \geq 1 - \delta_n\right\}, \\
\mathcal{L}_{V|Y}^{(n)} &\triangleq \left\{j \in [1,n] : H\left(U(j) \middle| U^{1:j-1} Y^n\right) \leq \delta_n\right\};
\end{aligned}$$

and associated to the transform T^n, define

$$\begin{aligned}
\mathcal{H}_{X|V}^{(n)} &\triangleq \left\{j \in [1,n] : H\left(T(j) \middle| T^{1:j-1} V^n\right) \geq 1 - \delta_n\right\}, \\
\mathcal{L}_{X|V}^{(n)} &\triangleq \left\{j \in [1,n] : H\left(T(j) \middle| T^{1:j-1} V^n\right) \leq \delta_n\right\}, \\
\mathcal{H}_{X|VZ}^{(n)} &\triangleq \left\{j \in [1,n] : H\left(T(j) \middle| T^{1:j-1} V^n Z^n\right) \geq 1 - \delta_n\right\}.
\end{aligned}$$

The sets $\mathcal{H}_V^{(n)}$ and $\mathcal{L}_V^{(n)}$, and $\mathcal{H}_{X|V}^{(n)}$ and $\mathcal{L}_{X|V}^{(n)}$, correspond to the input random variables V^n and X^n, respectively, when considering that channel observations are absent. Since conditioning does not increase entropy, then $\mathcal{H}_V^{(n)} \supseteq \mathcal{H}_{V|Z}^{(n)}$, $\mathcal{L}_V^{(n)} \subseteq \mathcal{L}_{V|Z}^{(n)}$ and $\mathcal{H}_{X|V}^{(n)} \supseteq \mathcal{H}_{X|VZ}^{(n)}$.

2.4.1 Encoding

Consider that the transmission takes place over L blocks of size n. The encoder forms $\tilde{U}_{1:L}^n$ sequentially from $\tilde{U}_1^n$ to $\tilde{U}_L^n$. At block i, the encoder will construct $\tilde{U}_i^n$, which will carry the confidential message. Then, given $\tilde{V}_i^n = \tilde{U}_i^n G_n$, the encoder will perform the polar-based channel prefixing to construct $\tilde{T}_i^n$. Finally, it will obtain $\tilde{X}_i^n = \tilde{T}_i^n G_n$, which will be transmitted over the WTC inducing the channel outputs $(\tilde{Y}_i^n, \tilde{Z}_i^n)$.

Confidential message encoding

Besides the previous sets of indices associated to the polar transform U^n, define

$$\mathcal{R}^{(n)} \triangleq \text{any subset of } \mathcal{H}_{X|Z}^{(n)} \text{ with size } \mathcal{H}_V^{(n)} \setminus \mathcal{L}_{V|Y}^{(n)}.$$

For any block $i \in [1, L]$, let the uniformly distributed random sequence C_i representing the local randomness has size $\left|\mathcal{H}_V^{(n)} \setminus \mathcal{H}_{V|Z}^{(n)}\right|$. Also, let random message S_1 has size $\left|\mathcal{H}_{V|Z}^{(n)}\right|$ and, for $i \in [2, L]$, let S_i has size $\left|\mathcal{H}_{V|Z}^{(n)} \setminus \mathcal{R}^{(n)}\right|$.

At block 1, the encoder constructs $\tilde{U}_1\big[\mathcal{H}_{V|Z}^{(n)}\big] = S_1$ and $\tilde{U}_1\big[\mathcal{H}_V^{(n)} \setminus \mathcal{H}_{V|Z}^{(n)}\big] = C_1$. Then, it successively and randomly draws the remaining entries of $\tilde{U}_1^n$, that is $\tilde{U}_1\big[\big(\mathcal{H}_V^{(n)}\big)^{\mathrm{C}}\big]$, from the distribution $p_{U(j)|U^{1:j-1}}(\tilde{U}_1|\tilde{U}_1^{1:j-1})$. Also, from $\tilde{U}_1^n$, the encoder obtains

$$\Psi_i^{(V)} = \tilde{U}_i\big[\mathcal{H}_X^{(n)} \setminus \mathcal{L}_{V|Y}^{(n)}\big], \tag{2.13}$$

$$\Phi_i^{(V)} = \tilde{U}_i\big[\big(\mathcal{H}_X^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{L}_{V|Y}^{(n)}\big], \tag{2.14}$$

where $i = 1$. Notice that $\big(\Psi_1^{(V)}, \Phi_1^{(V)}\big) = \tilde{U}_1\big[\big(\mathcal{L}_{V|Y}^{(n)}\big)^{\mathrm{C}}\big]$, which is required by the legitimate receiver to reliably reconstruct $\tilde{U}_1^n$ by performing SC decoding.

At block $i \in [2, L]$, the encoder constructs $\tilde{U}_i\big[\mathcal{H}_{V|Z}^{(n)} \setminus \mathcal{R}^{(n)}\big] = S_i$ and $\tilde{U}_i\big[\mathcal{H}_V^{(n)} \setminus \mathcal{H}_{V|Z}^{(n)}\big] = C_i$. Also, it forms $\tilde{U}_i\big[\mathcal{R}^{(n)}\big] = \Psi_{i-1}^{(V)}$. Then, the encoder uses random SC encoding to construct $\tilde{U}_i\big[\big(\mathcal{H}_V^{(n)}\big)^{\mathrm{C}}\big]$ from the distribution $p_{U(j)|U^{1:j-1}}(\tilde{U}_i|\tilde{U}_i^{1:j-1})$. Also, from $\tilde{U}_i^n$, the encoder obtains $\Psi_i^{(V)}$ and $\Phi_i^{(V)}$ as in (2.13) and (2.14), respectively.

Notice that only $\Psi_i^{(V)}$, for $i \in [1, L-1]$, is reused in the next block. However, $\Psi_L^{(V)}$ is required to initialize the decoding process and $\Phi_{1:L}^{(V)}$, which is not uniformly distributed, is also necessary to reliably reconstruct the sequence $\tilde{U}_i^n$. In this sense, the PCS separately and secretly sends $\big(\Psi_L^{(V)}, \Phi_{1:L}^{(V)}\big)$ to the receiver by using a uniformly distributed random key

that is privately shared between receiver and transmitter. This secret-key is asymptotically negligible in terms of rate because, since $\mathcal{L}_V^{(n)} \supseteq \mathcal{L}_{V|Y}^{(n)}$ and by Theorem 2.1, we have

$$\frac{\left|\mathcal{H}_V^{(n)} \setminus \mathcal{L}_{V|Y}^{(n)}\right|}{nL} + \frac{L\left|\left(\mathcal{H}_V^{(n)}\right)^{\mathrm{C}} \setminus \mathcal{L}_{V|Y}^{(n)}\right|}{nL} \leq \frac{\left|\left(\mathcal{L}_{V|Y}^{(n)}\right)^{\mathrm{C}}\right|}{nL} + \frac{L\left|\left(\mathcal{H}_V^{(n)}\right)^{\mathrm{C}} \setminus \mathcal{L}_V^{(n)}\right|}{nL} \xrightarrow{n\to\infty} \frac{H(V|Y)}{L}.$$

Therefore, one can incur an arbitrary rate penalty by choosing a sufficiently large L.

Finally, for any $i \in [1, L]$, the encoder computes $\tilde{V}_i^n = \tilde{U}_i^n G_n$, which is used for the polar-based channel prefixing.

Channel prefixing

For $i \in [1, L]$, let R_i be a uniformly distributed random sequence with size $\left|\mathcal{H}_{X|V}^{(n)} \setminus \mathcal{H}_{X|VZ}^{(n)}\right|$ that represents the additional randomness introduced by the encoding. Moreover, let F be a uniformly distributed random sequence with size $\left|\mathcal{H}_{X|VZ}^{(n)}\right|$.

For any block $i \in [1, L]$, the encoder forms $\tilde{T}_i^n$ as follows. It forms $\tilde{T}_i\left[\mathcal{H}_{X|V}^{(n)} \setminus \mathcal{H}_{X|VZ}^{(n)}\right] = R_i$ and $\tilde{T}_i\left[\mathcal{H}_{X|VZ}^{(n)}\right] = F$. Then, the encoder uses random SC encoding to construct $\tilde{T}_i\left[\left(\mathcal{H}_{X|V}^{(n)}\right)^{\mathrm{C}}\right]$ from the distribution $p_{T(j)|T^{1:j-1}V^n}(\tilde{T}_i|T_i^{1:j-1}\tilde{V}_i^n)$. Finally, it computes $\tilde{X}^n = \tilde{T}^n G_n$ and transmits it over the WTC, which induces $(\tilde{Y}_i^n, \tilde{Z}_i^n)$.

Notice that the legitimate receiver does not have to estimate $\tilde{X}_{1:L}^n$ because it does not carry information, but only contains additional randomness.

2.4.2 Decoding

Consider that $\Psi_L^{(V)}$ and $\Phi_{1:L}^{(V)}$ have reliably been estimated by the legitimate receiver. Then, the decoder successively forms an estimate of $\tilde{U}_{1:L}^n$ by going backward, that is, from $\hat{U}_L^n$ to $\hat{U}_1$, as follows. For $i \in [1, L]$, given $\Psi_i^{(V)}$ and $\Phi_i^{(V)}$, the receiver knows $\hat{U}_i\left[\left(\mathcal{L}_{V|Y}^{(n)}\right)^{\mathrm{C}}\right]$. Thus, it uses the SC decoder in (2.6) to reliably construct $\hat{U}_i^n$ from observations $\tilde{Y}_i^n$. Then, it obtains $\hat{\Psi}_{i-1}^{(V)} = \hat{U}_i\left[\mathcal{R}^{(n)}\right]$, which will be used at block $i-1$ to reliably estimate $\tilde{U}_{i-1}^n$.

2.4.3 Performance of the polar coding scheme

First, the rate of the confidential message is given by

$$\frac{\left|\mathcal{H}_{V|Z}^{(n)}\right| + (L-1)\left|\mathcal{H}_{V|Z}^{(n)} \setminus \mathcal{R}^{(n)}\right|}{nL} = \frac{\left|\mathcal{H}_{V|Z}^{(n)}\right|}{nL} + (L-1)\frac{\left|\mathcal{H}_{V|Z}^{(n)}\right| - \left|\mathcal{H}_V^{(n)} \setminus \mathcal{L}_{V|Y}^{(n)}\right|}{nL} \xrightarrow{n\to\infty} \frac{H(V|Z)}{L} + (L-1)\frac{H(V|Z) - H(V|Y)}{L}.$$

Thus, the PCS can operate as close to the secrecy-capacity (see Proposition 1.2) as desired by choosing a sufficiently large L.

Let $\tilde{q}_{V_i^n X_i^n Y_i^n Z_i^n}$ denote the joint distribution of $(\tilde{V}_i^n, \tilde{X}_i^n, \tilde{Y}_i^n, \tilde{Z}_i^n)$ at block $i \in [1, L]$. Now, the encoder introduces some distortion that causes $\mathbb{V}(\tilde{q}_{V_i^n X_i^n Y_i^n Z_i^n}, p_{V^n X^n Y^n Z^n}) \neq 0$. Nevertheless, [CB16] proves that distributions $\tilde{q}_{V_i^n X_i^n Y_i^n Z_i^n}$ and $p_{V^n X^n Y^n Z^n}$ are statistically close for sufficiently large n. This happens because the encoder introduces uniformly distributed random bits into $\tilde{U}_i\big[\mathcal{H}_V^{(n)}\big]$ and $\tilde{U}_i\big[\mathcal{H}_{X|V}^{(n)}\big]$, and recall that $U(j)$ for $j \in \mathcal{H}_V^{(n)}$ and $T(j)$ for $j \in \mathcal{H}_{X|V}^{(n)}$ are defined to be asymptotically independent from $U^{1:j-1}$ and $(T^{1:j-1}, V^n)$, respectively, and uniformly distributed; and, moreover, because the entries $\tilde{U}_i\big[\big(\mathcal{H}_V^{(n)}\big)^{\mathrm{C}}\big]$ and $\tilde{U}_i\big[\big(\mathcal{H}_{X|V}^{(n)}\big)^{\mathrm{C}}\big]$ are randomly drawn from the marginal distributions $p_{U(j)|U^{1:j-1}}$ and $p_{T(j)|T^{1:j-1}V^n}$, respectively, of the original DMS.

Having to randomly construct part of $\tilde{U}_i^n$ and $\tilde{T}_i^n$ is an important drawback for practical implementation of polar codes. In this sense, [CB15] proposed a modification of the previous encoder, where only $\tilde{U}_i\big[\big(\mathcal{H}_V^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{L}_V^{(n)}\big]$ and $\tilde{T}_i\big[\big(\mathcal{H}_{X|V}^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{L}_{X|V}^{(n)}\big]$ are randomly sampled from $p_{U(j)|U^{1:j-1}}$ and $p_{T(j)|T^{1:j-1}V^n}$, respectively. Hence, the randomness required for SC encoding is, by applying Theorem 2.1, negligible in terms of rate. By contrast, the elements $\tilde{U}_i(j)$ such that $j \in \mathcal{L}_V^{(n)}$ are constructed by performing deterministic SC encoding, that is,

$$U(j) = \underset{u \in \{0,1\}}{\arg\max}\, p_{U(j)|U^{1:j-1}}(u|U^{1:j-1}),$$

and, similarly, the elements $\tilde{T}_i(j)$ such that $j \in \mathcal{L}_{X|V}^{(n)}$ are deterministically sampled as

$$T(j) = \underset{t \in \{0,1\}}{\arg\max}\, p_{T(j)|T^{1:j-1}V^n}(t|T^{1:j-1}V^n).$$

For the general DMC, [CB15] showed that part of the random decisions can be exchanged by the previous deterministic functions and yet $\mathbb{V}(\tilde{q}_{V_i^n X_i^n Y_i^n Z_i^n}, p_{V^n X^n Y^n Z^n})$ vanishes for n large enough. In Section 2.5 we generalize this result for any multi-user channel with arbitrary number of input random variables for the encoding.

Given $\mathbb{V}(\tilde{q}_{V_i^n X_i^n Y_i^n Z_i^n}, p_{V^n X^n Y^n Z^n}) = \epsilon_n$, where $\epsilon_n \xrightarrow{n\to\infty} 0$ for any $i \in [1, L]$, the reliability performance can be analyzed by using similar techniques as those in [KU10]. Consider an optimal coupling [LPW09] (Proposition 4.7) between marginals $\tilde{q}_{U_i^n Y_i^n}$ and $p_{U^n Y^n}$ such that

$$\mathbb{P}\big[\mathcal{E}_{U_i^n Y_i^n}\big] = \mathbb{V}(\tilde{q}_{U_i^n Y_i^n}, p_{U^n Y^n}),$$

where $\mathcal{E}_{U_i^n Y_i^n} \triangleq \mathbb{P}\big[\big(\tilde{U}_i^n, \tilde{Y}_i^n\big) \neq \big(U^n, Y^n\big)\big]$. According to [LPW09], this optimal coupling always exists. Moreover, for $i \in [1, L]$, define the error event $\mathcal{E}_{\Psi_i} \triangleq \mathbb{P}\big[\hat{\Psi}_i^{(V)} \neq \Psi_i^{(V)}\big]$. The

average average block error probability, for any block $i \in [1, L]$, is given by

$$\begin{aligned}\mathbb{P}\big[\hat{U}_i^n \neq \tilde{U}_i^n\big] &= \mathbb{P}\big[\hat{U}_i^n \neq \tilde{U}_i^n \big| \mathcal{E}_{\Psi_i}^{\mathrm{C}} \cap \mathcal{E}_{U^nY^n}^{\mathrm{C}}\big]\mathbb{P}\big[\mathcal{E}_{\Psi_i}^{\mathrm{C}} \cap \mathcal{E}_{U^nY^n}^{\mathrm{C}}\big] \\ &\quad + \mathbb{P}\big[\hat{U}_i^n \neq \tilde{U}_i^n \big| \mathcal{E}_{\Psi_i} \cup \mathcal{E}_{U^nY^n}\big]\mathbb{P}\big[\mathcal{E}_{\Psi_i} \cup \mathcal{E}_{U^nY^n}\big] \\ &\leq \mathbb{P}\big[\hat{U}_i^n \neq \tilde{U}_i^n \big| \mathcal{E}_{\Psi_i}^{\mathrm{C}} \cap \mathcal{E}_{U^nY^n}^{\mathrm{C}}\big] + \mathbb{P}\big[\mathcal{E}_{U^nY^n}\big] + \mathbb{P}\big[\mathcal{E}_{\Psi_i}\big] \\ &\leq i(n\delta_n + \epsilon_n),\end{aligned}$$

where we have used that $\mathbb{P}\big[\mathcal{E}_{U^nY^n}\big] = \mathbb{V}(\tilde{q}_{V_i^nY_i^n}, p_{V^nY^n}) \leq \mathbb{V}(\tilde{q}_{V_i^nX_i^nY_i^nZ_i^n}, p_{V^nX^nY^nZ^n}) = \epsilon_n$, and similar reasoning as in (2.11).

Regarding the secrecy performance, now the information leakage is given by $I(S_{1:L}; \tilde{Z}_{1:L}^n)$. Due to the chaining construction, the dependencies between random variables of different blocks must be considered. Indeed, the Bayesian graph representing these dependencies is similar to the one in Figure 2.3, where now we have $(\tilde{U}_{1:L}^n, \tilde{T}_{1:L}^n)$ instead of only $\tilde{U}_{1:L}^n$ in intermediate nodes, $\Psi_i^{(V)}$ from Block i is repeated in *secure* positions of Block $i+1$, and F does not represent common randomness available to all receivers but is a random sequence that is sampled by the encoding and is replicated in all blocks for channel prefixing. Thus, dependencies between blocks can be broken in a similar way as in Equation (2.12) and

$$I(S_{1:L}; \tilde{Z}_{1:L}^n) = \sum_{i=1}^{L} I(S_{1:L}; \tilde{Z}_i^n | \tilde{Z}_{1:i-1}^n) \leq LI\big(\tilde{U}_i\big[\mathcal{H}_{X|Z}^{(n)}\big]; \tilde{Z}_i^n\big), \tag{2.15}$$

Finally, given $\mathbb{V}(\tilde{q}_{V_i^nZ_i^n}, p_{V^nZ^n}) \leq \mathbb{V}(\tilde{q}_{V_i^nX_i^nY_i^nZ_i^n}, p_{V^nX^nY^nZ^n}) = \epsilon_n$ and by applying [CK11] (Lemma 2.7), it is easy to prove that

$$H\big(\tilde{U}_i\big[\mathcal{H}_{X|Z}^{(n)}\big] \big| \tilde{Z}_i^n\big) \leq H\big(U_i\big[\mathcal{H}_{X|Z}^{(n)}\big] \big| Z_i^n\big) + \gamma_{\epsilon_n},$$

where $\gamma_{\epsilon_n} \xrightarrow{n\to\infty} 0$ if $\epsilon_n \xrightarrow{n\to\infty} 0$. Thus, by the uniformity of $\tilde{U}_i\big[\mathcal{H}_{X|Z}^{(n)}\big]$ and the definition of $\mathcal{H}_{X|Z}^{(n)}$, we obtain $I\big(\tilde{U}_i\big[\mathcal{H}_{X|Z}^{(n)}\big]; \tilde{Z}_i^n\big) \xrightarrow{n\to\infty} 0$ and the strong secrecy condition is fulfilled.

Regarding the complexity of the previous PCS, notice that the encoding/decoding process requires a high memory capacity to either the encoding or the decoding. The encoder constructs $\tilde{U}_{1:L}^n$ forward, that is, from $\tilde{U}_1^n$ to $\tilde{U}_L^n$, and the receiver must wait until $\tilde{Y}_L^n$ is available in order to perform SC decoding. This implies the receiver having to keep all the observations $\tilde{Y}_{1:L}^n$ before starting to reconstruct $\tilde{U}_{1:L}^n$ backward.

Remark 2.3. *Notice that the PCSs for the DWTC and WTC require the legitimate receiver to reliably decode the local randomness. Then, these coding schemes can achieve the capacity region of the model described in [XC08], which introduces a new message with no secrecy constraints, by simply exchanging the local randomness for this uniformly distributed message.*

2.5 SC encoding with negligible amount of randomness

In this section, we generalize the results in [CB15] for any multi-user model. Specifically, we present a generic encoder for multi-user settings that uses a negligible amount of randomness (in terms of rate) for SC encoding. Also, the distribution induced by this encoding is statistically close to the one that attains the capacity and is used for the code construction.

Consider a DMS representing the random variables involved in the capacity region of an arbitrary setting with T_{V} input (encoding) layers and T_{O} receivers, that is,

$$(\mathcal{V}_1 \times \cdots \times \mathcal{V}_{T_{\mathrm{V}}} \times \mathcal{O}_1 \times \cdots \times \mathcal{O}_{T_{\mathrm{O}}}, p_{V_{1:T_{\mathrm{V}}} O_{1:T_{\mathrm{O}}}}),$$

where $V_\ell \in \mathcal{V}_\ell = \{0,1\}$ (binary polarization) denotes the random variable associated to encoding layer $\ell \in [1, T_{\mathrm{V}}]$, the random variable $O_k \in \mathcal{O}_k$ denotes the channel output associated to Receiver $k \in [1, T_{\mathrm{O}}]$, and $p_{V_{1:T_{\mathrm{V}}} O_{1:T_{\mathrm{O}}}}$ is any arbitrary distribution.

Let $(V_{1:T_{\mathrm{V}}}^n, O_{1:T_{\mathrm{O}}}^n)$ denote an i.i.d. n-sequence of this DMS, n being any power of two. For any input random variable V_ℓ, $\ell \in [1, T_{\mathrm{V}}]$, define the polar transform $U_\ell^n \triangleq V_\ell^n G_n$. Associated to each polar transform, define the following set of indices:

$$\begin{aligned}
\mathcal{H}_{V_\ell|V_{1:\ell-1}}^{(n)} &\triangleq \big\{j \in [1,n] : H\big(U_\ell(j)\big|U_\ell^{1:j-1} V_{1:\ell-1}^n\big) \geq 1 - \delta_n\big\},\\
\mathcal{L}_{V_\ell|V_{1:\ell-1}}^{(n)} &\triangleq \big\{j \in [1,n] : H\big(U_\ell(j)\big|U_\ell^{1:j-1} V_{1:\ell-1}^n\big) \leq \delta_n\big\},
\end{aligned}$$

where $\delta_n = 2^{-n^\beta}$ for some $\beta \in \big(0, \frac{1}{2}\big)$, and $V_0^n \triangleq \varnothing$. These sets represent the high and the low entropy sets, respectively, of V_ℓ^n given the input random sequences $V_{1:\ell-1}^n$.

Consider an encoder that successively forms $\tilde{U}_{1:T_{\mathrm{V}}}^n$ from $\tilde{U}_1^n$ to $\tilde{U}_{T_{\mathrm{V}}}^n$ as follows. For any $\ell \in [1, T_{\mathrm{V}}]$, given $\tilde{V}_{1:\ell-1}^n$, where recall that $\tilde{V}_{\ell'}^n = \tilde{U}_{\ell'}^n G_n$ ($\ell' \in [1, \ell-1]$), $\tilde{U}_\ell^n$ is drawn from

$$\tilde{q}_{U_\ell^n|V_{1:\ell-1}^n}\big(\tilde{U}_\ell^n\big|\tilde{V}_{1:\ell-1}^n\big) \triangleq \prod_{j=1}^n \tilde{q}_{U_\ell(j)|U_\ell^{1:j-1} V_{1:\ell-1}^n}\big(\tilde{U}_\ell(j)\big|\tilde{U}_\ell^{1:j-1}\tilde{V}_{1:\ell-1}^n\big), \tag{2.16}$$

where

$$\begin{aligned}
&\tilde{q}_{U_\ell(j)|U_\ell^{1:j-1} V_{1:\ell-1}^n}\big(\tilde{U}_\ell(j)\big|\tilde{U}_\ell^{1:j-1}\tilde{V}_{1:\ell-1}^n\big)\\
&= \begin{cases}
\frac{1}{2} & \text{if } j \in \mathcal{H}_{V_\ell|V_{1:\ell-1}}^{(n)},\\
\mathbb{1}\big\{\tilde{U}_\ell(j) = \arg\max_{u\in\{0,1\}} p_{U(j)|U_\ell^{1:j-1} V_{1:\ell-1}^n}\big(u\big|\tilde{U}_\ell^{1:j-1}\tilde{V}_{1:\ell-1}^n\big)\big\} & \text{if } j \in \mathcal{L}_{V_\ell|V_{1:\ell-1}}^{(n)},\\
p_{U_\ell(j)|U_\ell^{1:j-1} V_{1:\ell-1}^n}\big(\tilde{U}_\ell(j)\big|\tilde{U}_\ell^{1:j-1}\tilde{V}_{1:\ell-1}^n\big) & \text{otherwise.}
\end{cases}
\end{aligned}$$

Hence, for any $\ell \in [1, T_{\mathrm{V}}]$, this encoder stores uniformly distributed random sequences into $\tilde{U}_\ell\big[\mathcal{H}_{V_\ell|V_{1:\ell-1}}^{(n)}\big]$ (for instance: information messages, local randomness, repeated sequences

due to a chaining construction, etc.). Then, it constructs the remaining entries by using deterministic and random SC encoding. Indeed, if $T_{\mathrm{V}} \ll n$, by Theorem 2.1 the amount of randomness that is required for SC encoding is asymptotically negligible in terms of rate.

The following lemma proves that, for sufficiently large n, the joint distribution $\tilde{q}_{U_{1:T_{\mathrm{V}}}^n}$ of $\tilde{U}_{1:T_{\mathrm{V}}}^n$ induced by the encoding process given in (2.16) is statistically close to the marginal distribution $p_{U_{1:T_{\mathrm{V}}}^n}$ of the original DMS.

Lemma 2.3. *The joint distributions $\tilde{q}_{U_{1:T_{\mathrm{V}}}^n}$ and $p_{U_{1:T_{\mathrm{V}}}^n}$ satisfy*

$$\mathbb{V}(\tilde{q}_{U_{1:T_{\mathrm{V}}}^n}, p_{U_{1:T_{\mathrm{V}}}^n}) \leq n \sum_{\ell=1}^{T_V} \sqrt{2\sqrt{\ell n \delta_n 2 \ln 2}\big(\ell n - \log \sqrt{\ell n \delta_n 2 \ln 2}\big) + \delta_n} + \sqrt{T_V}\sqrt{n\delta_n 2 \ln 2}.$$

Proof. See Appendix 2.A □

Corollary 2.1. *If $p_{U_{1:T_{\mathrm{V}}}^n}$ and $\tilde{q}_{U_{1:T_{\mathrm{V}}}^n}$ are such that $U_1^n - U_2^n - \cdots - U_{T_V}^n$ and $\tilde{U}_1^n - \tilde{U}_2^n - \cdots - \tilde{U}_{T_V}^n$ form a Markov chain, then it holds that*

$$\mathbb{V}(\tilde{q}_{U_{1:T_{\mathrm{V}}}^n}, p_{U_{1:T_{\mathrm{V}}}^n}) \leq n T_V \sqrt{2\sqrt{4n\delta_n \ln 2}\big(\ell n - \log \sqrt{n\delta_n 4 \ln 2}\big) + \delta_n} + \sqrt{n\delta_n 4 \ln 2}.$$

Proof. The proof follows the same steps of the one for Lemma 2.3 but, in this case, we have that $\tilde{q}_{U_\ell|U_{1:\ell-1}}$ is equivalent to $\tilde{q}_{U_\ell|U_{\ell-1}}$ and $p_{U_\ell|U_{1:\ell-1}}$ to $p_{U_\ell|U_{\ell-1}}$. □

Corollary 2.2. *If $\tilde{q}_{U_{1:T_{\mathrm{V}}}^n O_{1:T_{\mathrm{O}}}^n} = \tilde{q}_{U_{1:T_{\mathrm{V}}}^n} p_{O_{1:T_{\mathrm{O}}}^n|U_{1:T_{\mathrm{V}}}^n}$ and $p_{U_{1:T_{\mathrm{V}}}^n O_{1:T_{\mathrm{O}}}^n} = p_{U_{1:T_{\mathrm{V}}}^n} p_{O_{1:T_{\mathrm{O}}}^n|U_{1:T_{\mathrm{V}}}^n}$, then*

$$\mathbb{V}(\tilde{q}_{U_{1:T_{\mathrm{V}}}^n O_{1:T_{\mathrm{O}}}^n}, p_{U_{1:T_{\mathrm{V}}}^n O_{1:T_{\mathrm{O}}}^n}) = \mathbb{V}(\tilde{q}_{U_{1:T_{\mathrm{V}}}^n}, p_{U_{1:T_{\mathrm{V}}}^n}).$$

Thus, according to Lemma 2.3, if $T_{\mathrm{V}} \ll n$ then $\mathbb{V}(\tilde{q}_{U_{1:T_V}^n}, \check{q}_{U_{1:T_V}^n}) = O\big(n^{\frac{7}{4}} 2^{-n^\beta}\big) \xrightarrow{n\to\infty} 0$. Moreover, Corollary 2.2 proves that if an encoding of the PCS satisfies Lemma 2.3, then $\tilde{q}_{U_{1:T_V}^n O_{1:T_O}^n}$ and $p_{U_{1:T_V}^n O_{1:T_O}^n}$ are also statistically indistinguishable for n sufficiently large. Finally, the following lemma relates total variation distance with entropies.

Lemma 2.4. *Define $\mathcal{J}_\ell$ as any subset of $[1, n]$, where $\ell \in [1, T_{\mathrm{V}}]$. Consider the sequence $\big(\tilde{U}_{1:T_{\mathrm{V}}}^n, \tilde{O}_{1:T_{\mathrm{O}}}^n\big)$ with distribution $\tilde{q}_{U_{1:T_{\mathrm{V}}}^n O_{1:T_{\mathrm{O}}}^n}$, and $\big(U_{1:T_{\mathrm{V}}}^n O_{1:T_{\mathrm{O}}}^n\big)$ with distribution $p_{U_{1:T_{\mathrm{V}}}^n O_{1:T_{\mathrm{O}}}^n}$. Let $\mathbb{V}(\tilde{q}_{U_{1:T_{\mathrm{V}}}^n O_{1:T_{\mathrm{O}}}^n}, p_{U_{1:T_{\mathrm{V}}}^n O_{1:T_{\mathrm{O}}}^n}) \leq \epsilon$, where $\epsilon \xrightarrow{n\to\infty} 0$. Then, for sufficiently large n,*

$$\big|H\big(\tilde{U}_1[\mathcal{J}_1] \ldots \tilde{U}_{T_{\mathrm{V}}}[\mathcal{J}_{T_{\mathrm{V}}}]\big|\tilde{O}_{1:T_{\mathrm{O}}}^n\big) - H\big(U_1[\mathcal{J}_1] \ldots U_{T_{\mathrm{V}}}[\mathcal{J}_{T_{\mathrm{V}}}]\big|O_{1:T_{\mathrm{O}}}^n\big)\big| \leq (T_{\mathrm{V}} + 2T_{\mathrm{O}}) n\epsilon - 2\epsilon \log \epsilon.$$

Proof. See Appendix 2.B □

The results provided in this section are crucial for the analysis of the reliability and the secrecy performance of the PCSs that will be introduced in the following chapters.

Appendix

2.A Proof of Lemma 2.3

Consider another encoder that omits the use of the deterministic arg max function in SC encoding but, for any $\ell \in [1, T_{\mathrm{V}}]$, it randomly draws those elements whose indices belong to $\big(\mathcal{H}^{(n)}_{V_\ell|V_{1:\ell-1}}\big)^{\mathrm{C}}$. Let $\check{U}^n_{1:T_{\mathrm{V}}} \sim \check{q}_{U^n_\ell|V^n_{1:\ell-1}}$ denote the sequences formed by this encoder. Then,

$$\check{q}_{U^n_\ell|V^n_{1:\ell-1}}\big(\check{U}^n_\ell\big|\check{V}^n_{1:\ell-1}\big) \triangleq \prod_{j=1}^{n} \check{q}_{U_\ell(j)|U^{1:j-1}_\ell V^n_{1:\ell-1}}\big(\check{U}_\ell(j)\big|\check{U}^{1:j-1}_\ell \check{V}^n_{1:\ell-1}\big), \tag{2.17}$$

where

$$\begin{aligned}
&\check{q}_{U_\ell(j)|U^{1:j-1}_\ell V^n_{1:\ell-1}}\big(\check{U}_\ell(j)\big|\check{U}^{1:j-1}_\ell \check{V}^n_{1:\ell-1}\big) \\
&= \begin{cases} \frac{1}{2} & \text{if } j \in \mathcal{H}^{(n)}_{V_\ell|V_{1:\ell-1}}, \\ p_{U_\ell(j)|U^{1:j-1}_\ell V^n_{1:\ell-1}}\big(\check{U}_\ell(j)\big|\check{U}^{1:j-1}_\ell \check{V}^n_{1:\ell-1}\big) & \text{otherwise.} \end{cases}
\end{aligned}$$

The following lemma shows that the joint distributions $\check{q}_{U^n_{1:T_{\mathrm{V}}}}$ and $p_{U^n_{1:T_{\mathrm{V}}}}$ of the original DMS are nearly statistically indistinguishable for sufficiently large n.

Lemma 2.5. *For any $\ell' \in [1, T_V]$, we have $\mathbb{V}(\check{q}_{U^n_{1:\ell'}}, p_{U^n_{1:\ell'}}) \le \sqrt{\ell'}\sqrt{2n\delta_n \ln 2}$.*

Proof. The Kullback-Leibler distance between the distributions $p_{U^n_{1:M}}$ and $\check{q}_{U^n_{1:M}}$ is

$$\begin{aligned}
\mathbb{D}\big(p_{U^n_{1:\ell'}}\big\|\check{q}_{U^n_{1:\ell'}}\big) &\overset{(a)}{=} \sum_{i=1}^{\ell'} \mathbb{E}_{V^n_{1:i-1}}\Big[\mathbb{D}\big(p_{U^n_i|V^n_{1:i-1}}\big\|\check{q}_{U^n_i|V^n_{1:i-1}}\big)\Big] \\
&= \sum_{i=1}^{\ell'}\sum_{j=1}^{n} \mathbb{E}_{U^{1:j-1}_i V^n_{1:i-1}}\Big[\mathbb{D}\big(p_{U_i(j)|U^{1:j-1}_i V^n_{1:i-1}}\big\|\check{q}_{U_i(j)|U^{1:j-1}_i V^n_{1:i-1}}\big)\Big],
\end{aligned}$$

where (a) holds by the chain rule and the invertibility of G_n. Thus, we obtain

$$\mathbb{D}\big(p_{U^n_{1:\ell'}}\big\|\check{q}_{U^n_{1:\ell'}}\big) \overset{(a)}{=} \sum_{i=1}^{\ell'} \sum_{j\in\mathcal{H}^{(n)}_{V_i|V_{1:i-1}}} \big(1 - H\big(U_i(j)\big|U_i^{1:j-1}, V^n_{1:i-1}\big)\big)$$
$$\overset{(b)}{\leq} \ell'\delta_n\big|\mathcal{H}^{(n)}_{V_i|V_{1:i-1}}\big|, \tag{2.18}$$

where (a) holds by (2.17) and [GAG15] (Lemma 10), i.e., $\mathbb{D}(p_1\|p_2) = 1 - H(p_1)$ if p_2 denotes the uniform distribution; and (b) holds by the definition of $\mathcal{H}^{(n)}_{V_i|V_{1:i-1}}$. Finally, we obtain $\mathbb{V}(\check{q}_{U^n_{1:\ell'}}, p_{U^n_{1:\ell'}}) \leq \sqrt{2\ln 2}\sqrt{\ell' n\delta_n}$ by Pinsker's inequality and because $\big|\mathcal{H}^{(n)}_{V_i|V_{1:i-1}}\big| \leq n$. □

Now, the following lemma proves that the joint distribution $\tilde{q}_{U^n_{1:T_\mathrm{V}}}$ corresponding to the encoder in (2.16) that uses deterministic SC encoding is asymptotically close to the distribution $\check{q}_{U^n_{1:T_\mathrm{V}}}$ in terms of total variation distance.

Lemma 2.6. *The joint distributions $\tilde{q}_{U^n_{1:T_\mathrm{V}}}$ and $\check{q}_{U^n_{1:T_\mathrm{V}}}$ satisfy*

$$\mathbb{V}(\tilde{q}_{U^n_{1:T_\mathrm{V}}}, \check{q}_{U^n_{1:T_\mathrm{V}}}) \leq n\sum_{\ell=1}^{T_V} \sqrt{2\sqrt{\ell n\delta_n 2\ln 2}\big(\ell n - \log\sqrt{\ell n\delta_n 2\ln 2}\big) + \delta_n}.$$

Proof. Define a coupling [LPW09] for $\check{U}^n_{1:T_\mathrm{V}}$ and $\tilde{U}^n_{1:T_\mathrm{V}}$ such that, for any $\ell \in [1, M]$, $\check{U}_\ell\big[\big(\mathcal{L}^{(n)}_{V_\ell|V_{1:\ell-1}}\big)^\mathrm{C}\big] = \tilde{U}_\ell\big[\big(\mathcal{L}^{(n)}_{V_\ell|V_{1:\ell-1}}\big)^\mathrm{C}\big]$. Thus, we have

$$\begin{aligned}
\mathbb{V}(\tilde{q}_{U^n_{1:T_\mathrm{V}}}, \check{q}_{U^n_{1:T_\mathrm{V}}}) &\overset{(a)}{\leq} \mathbb{P}\big[\tilde{U}^n_{1:T_\mathrm{V}} \neq \check{U}^n_{1:T_\mathrm{V}}\big] \\
&\overset{(b)}{\leq} \sum_{\ell=1}^{T_\mathrm{V}} \mathbb{P}\big[\tilde{U}^n_\ell \neq \check{U}^n_\ell\big|\tilde{V}^n_{1:\ell-1} = \check{V}^n_{1:\ell-1}\big] \\
&\overset{(c)}{\leq} \sum_{\ell=1}^{T_\mathrm{V}}\sum_{j=1}^{n} \mathbb{P}\Big[\tilde{U}_\ell(j) \neq \check{U}_\ell(j)\Big|\big(\check{U}_\ell^{1:j-1}, \check{V}^n_{1:\ell-1}\big) = \big(\tilde{U}_\ell^{1:j-1}, \tilde{V}^n_{1:\ell-1}\big)\Big] \\
&\overset{(d)}{=} \sum_{\ell=1}^{T_\mathrm{V}} \sum_{j\in\mathcal{L}^{(n)}_{V_\ell|V_{1:\ell-1}}} \mathbb{E}_{\check{U}_\ell^{1:j-1}\check{V}^n_{1:\ell-1}}\Big[1 - p_{U_\ell(j)|U_\ell^{1:j-1}V^n_{1:\ell-1}}\big(u^*_\ell(j)|\check{U}_\ell^{1:j-1}, \check{V}^n_{1:\ell-1}\big)\Big],
\end{aligned} \tag{2.19}$$

where (a) holds by the coupling lemma [LPW09] (Proposition 4.7); (b) holds by the union bound and the invertibility of G_n; (c) also holds by the union bound; and (d) follows from (2.16) and (2.17) given that $\check{U}_\ell[(\mathcal{L}^{(n)}_{V_\ell|V_{1:\ell-1}})^\mathrm{C}] = \tilde{U}_\ell[(\mathcal{L}^{(n)}_{V_\ell|V_{1:\ell-1}})^\mathrm{C}]$ and from defining

$$u^*_\ell(j) \triangleq \arg\max_{u\in\{0,1\}} p_{U_\ell(j)|U_\ell^{1:j-1}V^n_{1:\ell-1}}(u\big|\check{U}_\ell^{1:j-1}, \check{V}^n_{1:\ell-1}).$$

Next, for any $j \in [n]$ and sufficiently large n, we have

$$\begin{aligned}
&\big|H\big(U_\ell(j)\big|U_\ell^{1:j-1}, V_{1:\ell-1}^n\big) - H\big(U_\ell(j)\big|\check{U}_\ell^{1:j-1}, \check{V}_{1:\ell-1}^n\big)\big| \\
&\overset{(a)}{\leq} \Big|H\big(U_\ell^{1:j-1}, V_{1:\ell-1}^n\big) - H\big(\check{U}_\ell^{1:j-1}, \check{V}_{1:\ell-1}^n\big)\Big| + \Big|H\big(U_\ell^{1:j}, V_{1:\ell-1}^n\big) - H\big(U_\ell(j), \check{U}_\ell^{1:j-1}, \check{V}_{1:\ell-1}^n\big)\Big| \\
&\overset{(b)}{\leq} 2\mathbb{V}\big(\check{q}_{U_\ell^{1:j-1}U_{1:\ell-1}^n}, p_{U_\ell^{1:j-1}U_{1:\ell-1}^n}\big) \log \frac{2^{(\ell-1)n+j-1}}{\mathbb{V}\big(\check{q}_{U_\ell^{1:j-1}U_{1:\ell-1}^n}, p_{U_\ell^{1:j-1}U_{1:\ell-1}^n}\big)} \\
&\overset{(c)}{\leq} 2\sqrt{\ell n \delta_n 2\ln 2}\big(\ell n - \log\sqrt{\ell n\delta_n 2\ln 2}\big),
\end{aligned} \tag{2.20}$$

where (a) holds by the chain rule of entropy and the triangle inequality; (b) holds by [CK11] (Lemma 2.7), the invertibility of G_n, and because

$$\mathbb{V}(p_{U_\ell(j)|U_\ell^{1:j-1}U_{1:\ell-1}^n}\check{q}_{U_\ell^{1:j-1}U_{1:\ell-1}^n}, p_{U_\ell^{1:j}U_{1:\ell-1}^n}) = \mathbb{V}(\check{q}_{U_\ell^{1:j-1}U_{1:\ell-1}^n}, p_{U_\ell^{1:j-1}U_{1:\ell-1}^n});$$

and (c) holds by Lemma 2.5 (taking $\ell' = \ell$) because

$$\mathbb{V}(\check{q}_{U_\ell^{1:j-1}U_{1:\ell-1}^n}, p_{U_\ell^{1:j-1}U_{1:\ell-1}^n}) \leq \mathbb{V}(\check{q}_{U_{1:\ell}^n}, p_{U_{1:\ell}^n}),$$

$x \mapsto x\log x$ is decreasing for $x > 0$ small enough, and $j - 1 \leq n$. Thus, for any $\ell \in [1, T_{\mathrm{V}}]$ and $j \in \mathcal{L}_{V_\ell|V_{1:\ell-1}}^{(n)}$, we have

$$\begin{aligned}
&2\sqrt{\ell n\delta_n 2\ln 2}\big(\ell n - \log\sqrt{\ell n\delta_n 2\ln 2}\big) + \delta_n \\
&\overset{(a)}{\geq} 2\sqrt{\ell n\delta_n 2\ln 2}\big(\ell n - \log\sqrt{\ell n\delta_n 2\ln 2}\big) + H\big(U_\ell(j)|U_\ell^{1:j-1}, V_{1:\ell-1}^n\big) \\
&\overset{(b)}{\geq} H\big(U_\ell(j)|U_\ell^{1:j-1}, V_{1:\ell-1}^n\big) \\
&= \mathbb{E}_{\check{U}_\ell^{1:j-1}\check{U}_{1:\ell-1}^n}\Big[h_2\Big(p_{U_\ell(j)|U_\ell^{1:j-1}V_{1:\ell-1}^n}\big(u_\ell^\star(j)\big|\check{U}_\ell^{1:j-1}, \check{V}_{1:\ell-1}^n\big)\Big)\Big] \\
&\geq \mathbb{E}_{\check{U}_\ell^{1:j-1}\check{U}_{1:\ell-1}^n}\Big[-\Big(1 - p_{U_\ell(j)|U_\ell^{1:j-1}V_{1:\ell-1}^n}\big(u_\ell^\star(j)\big|\check{U}_\ell^{1:j-1}, \check{V}_{1:\ell-1}^n\big)\Big) \\
&\quad \times \log\Big(1 - p_{U_\ell(j)|U_\ell^{1:j-1}V_{1:\ell-1}^n}\big(u_\ell^\star(j)\big|\check{U}_\ell^{1:j-1}, \check{V}_{1:\ell-1}^n\big)\Big)\Big] \\
&\overset{(c)}{\geq} \mathbb{E}_{\check{U}_\ell^{1:j-1}\check{U}_{1:\ell-1}^n}\Big[\Big(1 - p_{U_\ell(j)|U_\ell^{1:j-1}V_{1:\ell-1}^n}\big(u_\ell^\star(j)\big|\check{U}_\ell^{1:j-1}, \check{V}_{1:\ell-1}^n\big)\Big)^2\Big] \\
&\overset{(d)}{\geq} \mathbb{E}^2_{\check{U}_\ell^{1:j-1}\check{U}_{1:\ell-1}^n}\Big[\Big(1 - p_{U_\ell(j)|U_\ell^{1:j-1}V_{1:\ell-1}^n}\big(u_\ell^\star(j)\big|\check{U}_\ell^{1:j-1}, \check{V}_{1:\ell-1}^n\big)\Big)\Big]
\end{aligned} \tag{2.21}$$

where (a) holds by the definition of $\mathcal{L}_{V_\ell|V_{1:\ell-1}}^{(n)}$; (b) holds by (2.20); (c) holds because $p_{U_\ell(j)|U_\ell^{1:j-1}V_{1:\ell-1}^n}(u_\ell^\star(j)|\check{U}_\ell^{1:j-1}, \check{V}_{1:\ell-1}^n) \geq 1/2$ and $\log(x) < -x$ if $x \in [0, 1/2)$; and (d) follows from applying Jensen's inequality.

Lastly, by combining Equations (2.19) and (2.21), and because $|\mathcal{L}^{(n)}_{V_\ell|V_{\ell-1}}| \leq n$, we have

$$\begin{aligned}\mathbb{V}(\tilde{q}_{U^n_{1:T_\mathrm{V}}}, \check{q}_{U^n_{1:T_\mathrm{V}}}) &\leq \sum_{\ell=1}^{T_\mathrm{V}} \sum_{j\in\mathcal{L}^{(n)}_{V_\ell|V_{1:\ell-1}}} \mathbb{E}_{\check{U}_\ell^{1:j-1}\check{V}^n_{1:\ell-1}}\Big[1 - p_{U_\ell(j)|U_\ell^{1:j-1}V^n_{1:\ell-1}}\big(u^*_\ell(j)|\check{U}_\ell^{1:j-1}, \check{V}^n_{1:\ell-1}\big)\Big] \\ &\leq n\sum_{\ell=1}^{T_\mathrm{V}} \sqrt{2\sqrt{\ell n\delta_n 2\ln 2}\big(\ell n - \log\sqrt{\ell n\delta_n 2\ln 2}\big) + \delta_n},\end{aligned}$$

□

Finally, by Lemma 2.5, Lemma 2.6 and by applying the triangle inequality, we obtain

$$\begin{aligned}\mathbb{V}(\tilde{q}_{U^n_{1:T_\mathrm{V}}}, p_{U^n_{1:T_\mathrm{V}}}) &\leq \mathbb{V}(\tilde{q}_{U^n_{1:T_\mathrm{V}}}, \check{q}_{U^n_{1:T_\mathrm{V}}}) + \mathbb{V}(\check{q}_{U^n_{1:T_\mathrm{V}}}, p_{U^n_{1:T_\mathrm{V}}}) \\ &\leq n\sum_{\ell=1}^{T_\mathrm{V}} \sqrt{2\sqrt{\ell n\delta_n 2\ln 2}\big(\ell n - \log\sqrt{\ell n\delta_n 2\ln 2}\big) + \delta_n} + \sqrt{n\delta_n T_\mathrm{V} 2\ln 2},\end{aligned}$$

and the proof is complete.

2.B Proof of Lemma 2.4

From applying [CK11, Lemma 2.7], for n large enough we have

$$\begin{aligned}&\big|H\big(\tilde{U}_1[\mathcal{J}_1]\dots\tilde{U}_{T_\mathrm{V}}[\mathcal{J}_{T_\mathrm{V}}]\big|\tilde{O}^n_{1:T_\mathrm{O}}\big) - H\big(U_1[\mathcal{J}_1]\dots U_{T_\mathrm{V}}[\mathcal{J}_{T_\mathrm{V}}]\big|O^n_{1:T_\mathrm{O}}\big)\big| \\ &\overset{(a)}{=} \big|H\big(\tilde{O}^n_{1:T_\mathrm{O}}\big) - H\big(O^n_{1:T_\mathrm{O}}\big)\big| \\ &\quad + \big|H\big(\tilde{U}_1[\mathcal{J}_1]\dots\tilde{U}_{T_\mathrm{V}}[\mathcal{J}_{T_\mathrm{V}}]\tilde{O}^n_{1:T_\mathrm{O}}\big) - H\big(U_1[\mathcal{J}_1]\dots U_{T_\mathrm{V}}[\mathcal{J}_{T_\mathrm{V}}]O^n_{1:T_\mathrm{O}}\big)\big| \\ &\overset{(b)}{\leq} \mathbb{V}\big(\tilde{q}_{O^n_{1:T_\mathrm{O}}}, p_{O^n_{1:T_\mathrm{O}}}\big)\log\frac{2^{nT_\mathrm{O}}}{\mathbb{V}\big(\tilde{q}_{O^n_{1:T_\mathrm{O}}}, p_{O^n_{1:T_\mathrm{O}}}\big)} \\ &\quad + \mathbb{V}\big(\tilde{q}_{U_1[\mathcal{J}_1]\dots U_{T_\mathrm{V}}[\mathcal{J}_{T_\mathrm{V}}]O^n_{1:T_\mathrm{O}}}, p_{U_1[\mathcal{J}_1]\dots U_{T_\mathrm{V}}[\mathcal{J}_{T_\mathrm{V}}]O^n_{1:T_\mathrm{O}}}\big) \\ &\qquad \times\log\frac{2^{nT_\mathrm{O}+\sum_{\ell=1}^{T_\mathrm{V}}|\mathcal{J}_\ell|}}{\mathbb{V}\big(\tilde{q}_{U_1[\mathcal{J}_1]\dots U_{T_\mathrm{V}}[\mathcal{J}_{T_\mathrm{V}}]O^n_{1:T_\mathrm{O}}}, p_{U_1[\mathcal{J}_1]\dots U_{T_\mathrm{V}}[\mathcal{J}_{T_\mathrm{V}}]O^n_{1:T_\mathrm{O}}}\big)} \\ &\overset{(c)}{\leq} n(T_\mathrm{V}+2T_\mathrm{O})\epsilon - 2\epsilon\log\epsilon\end{aligned}$$

where (a) holds by the chain rule of entropy and the triangle inequality; (b) follows from applying [CK11] (Lemma 2.7); and (c) holds by Corollary 2.2, by assumption and because the function $x \mapsto x\log x$ is decreasing for $x > 0$ small enough.

3

Polar coding for the degraded wiretap broadcast channel

This section focuses on two different models for the discrete memoryless Degraded Broadcast Channel (DBC) surveyed in [ZLL+15]: (a) DBC with Non-Layered Decoding and Layered Secrecy (DBC-NLD-LS) and (b) DBC with Layered Decoding and Non-Layered Secrecy (DBC-LD-NLS). In these models, the transmitter wishes to send a set of messages through the DBC, and each message must be reliably decoded by a particular set of receivers and kept masked from a particular set of eavesdroppers. The degradedness condition of the channel implies that individual channels can be ordered based on the quality of their received signals. The layered decoding structure requires receivers with better channel quality to reliably decode more messages, while the layered secrecy requires eavesdroppers with worse channel quality to be kept ignorant of more messages.

The secrecy-capacity region of these models was first characterized in [ZLL+15, LLPS14, EU09]. However, the achievable schemes used by these works rely on random coding arguments that are nonconstructive in practice. In this sense, this chapter provides two secrecy-capacity achieving PCSs for each model. As mentioned in [ZLL+15], these settings capture practical scenarios in wireless systems, in which channels can be ordered based on the quality of the received signals (for example, Gaussian channels are degraded). Hence, the ultimate goal of this chapter is not only to prove the existence of two asymptotic secrecy-capacity achieving PCSs for these models under the strong secrecy condition, but also to discuss their practical construction and evaluate their performance for a finite blocklength by means of simulations.

The degradedness condition of the channel and the strong secrecy requirement on one side and the non-necessarily symmetry of individual channels on the other mean that the proposed

PCSs combine techniques from the coding schemes described in Section 2.3 and Section 2.4 for the symmetric DWTC and the general WTC, respectively. Although Section 2.3 proposes a chaining construction to convey the problematic elements to the legitimate receivers, we omit its use for practical reasons: in order to evaluate their performance for a finite blocklength, it is desirable that the transmitter could send secret information in just one block of size n. Since the problematic elements are negligible in terms of rate, the rate cost of additionally make them accessible to the receiver is also negligible. The omission of the chaining construction is only possible if a source of common randomness is accessible to all parties and, moreover, transmitter and legitimate receivers must share a secret-key with size in $o(n)$.

The remainder of this paper is organized as follows. In Section 3.1, the channel models DBC-NLD-LS and DBC-LD-NLS are introduced formally, and their secrecy-capacity regions are characterized. In Section 3.2 and Section 3.3, two PCSs are proposed for the DBC-NLD-LS and DBC-LD-NLS, respectively, and we prove that both are asymptotic secrecy-capacity achieving. In Section 3.4, practical polar code constructions are discussed for both models, and the performances of the polar codes are evaluated by means of simulations. Finally, the concluding remarks are presented in Section 3.5.

3.1 System model and secrecy-capacity region

Formally, a DBC $(\mathcal{X}, p_{Y_K \dots Y_1 Z_M \dots Z_1|X}, \mathcal{Y}_K \times \cdots \times \mathcal{Y}_1 \times \mathcal{Z}_M \times \cdots \times \mathcal{Z}_1)$ with K legitimate receivers and M eavesdroppers is characterized by the probability transition function $p_{Y_K \dots Y_1 Z_M \dots Z_1|X}$, where $X \in \mathcal{X}$ denotes the channel input, $Y_k \in \mathcal{Y}_k$ denotes the output corresponding to Receiver $k \in [1, K]$ and $Z_m \in \mathcal{Z}_m$ denotes the channel output corresponding to Eavesdropper $m \in [1, M]$. The broadcast channel is assumed to gradually degrade in such a way that each legitimate receiver has a better channel than any eavesdropper, that is,

$$X - Y_K - \cdots - Y_1 - Z_M - \cdots - Z_1 \tag{3.1}$$

forms a Markov chain. Although we consider physically degradation, the polar coding schemes proposed in this paper are also suitable for stochastically degraded channels (see Remark 3.1).

3.1.1 DBC with non-layered decoding and layered secrecy

In this model (see Figure 3.1), the transmitter wishes to send M messages $\{W_m\}_{m=1}^{M}$ to the K legitimate receivers. The non-layered decoding structure requires legitimate Receiver $k \in [1, K]$ to reliably decode all M messages, and the layered secrecy structure requires Eavesdropper $m \in [1, M]$ to be kept ignorant about messages $\{W_i\}_{i=m}^{M}$. Consider a

$(\lceil 2^{nR_1} \rceil, \ldots, \lceil 2^{nR_M} \rceil, n)$ code for the DBC-NLD-LS, where $W_m \in [\lceil 2^{nR_m} \rceil]$ for any $m \in [1, M]$. The reliability condition to be satisfied by this code is measured in terms of the average block error probability and is given, for any Receiver $k \in [1, K]$, by

$$\lim_{n\to\infty} \mathbb{P}\left[(\hat{W}_1, \ldots, \hat{W}_M) \neq (W_1, \ldots, W_M)\right] = 0. \tag{3.2}$$

On the other hand, the strong secrecy condition to be satisfied by the code is measured in terms of the information leakage and is given, for Eavesdropper $m \in [1, M]$, by

$$\lim_{n\to\infty} I(W_m, W_{m+1}, \ldots, W_M; Z_m^n) = 0. \tag{3.3}$$

A tuple of rates $(R_1, \ldots, R_M) \in \mathbb{R}_+^M$ is achievable for the DBC-NLD-LS if there exists a sequence of $(\lceil 2^{nR_1} \rceil, \ldots, \lceil 2^{nR_M} \rceil, n)$ codes satisfying Equations (3.2) and (3.3).

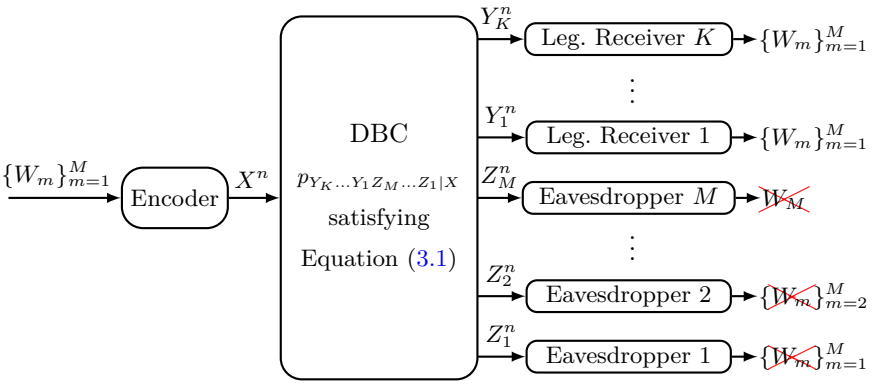

Figure 3.1: Channel model DBC-NLD-LS.

Proposition 3.1 (Adapted from [ZLL+15, LLPS14]). *The achievable region of the DBC-NLD-LS is the union of all M-tuples of rates $(R_1, \ldots, R_M) \in \mathbb{R}_+^M$ satisfying*

$$\sum_{i=m}^{M} R_i \leq I(X; Y_1) - I(X; Z_m), \qquad m = 1, \ldots, M,$$

where the union is taken over all distributions p_X.

The proof for the case of only one legitimate receiver in the context of the fading wiretap channel is provided in [LLPS14]. Due to the degradedness condition of Equation (3.1), by applying the data processing inequality and Fano's inequality, an achievable scheme ensuring the reliability condition in Equation (3.2) for legitimate Receiver 1 will satisfy it for any legitimate Receiver $k \in [2, K]$.

Corollary 3.1. *The achievable subregion of the DBC-NLD-LS without considering rate sharing is a K-orthotope defined by the closure of all K-tuples of rates $(R_1, \ldots, R_M) \in \mathbb{R}_+^M$ satisfying*

$$\begin{aligned} R_m &\leq I(X; Z_{m+1}) - I(X; Z_m), \qquad m = 1, \ldots, M-1, \\ R_M &\leq I(X; Y_1) - I(X; Z_M). \end{aligned}$$

3.1.2 DBC with layered decoding and non-layered secrecy

In this model (see Figure 3.2), the transmitter wishes to send K messages $\{W_\ell\}_{\ell=1}^K$ to the K legitimate receivers. The layered decoding structure requires Receiver $k \in [1, K]$ to reliably decode the messages $\{W_\ell\}_{\ell=1}^k$, and the non-layered secrecy structure requires Eavesdropper $m \in [1, M]$ to be kept ignorant of all K messages. Consider a $(\lceil 2^{nR_1} \rceil, \ldots, \lceil 2^{nR_K} \rceil, n)$ code for the DBC-LD-NLS, where $W_\ell \in [\lceil 2^{nR_\ell} \rceil]$ for any $\ell \in [1, K]$. For Receiver $k \in [1, K]$, the reliability condition to be satisfied by this code is given by

$$\lim_{n \to \infty} \mathbb{P}\left[(\hat{W}_1, \ldots, \hat{W}_{k-1}, \hat{W}_k) \neq (W_1, \ldots, W_{k-1}, W_k) \right] = 0. \tag{3.4}$$

On the other hand, for any Eavesdropper $m \in [1, M]$, the strong secrecy condition to be satisfied by the code is given by

$$\lim_{n \to \infty} I(W_1, \ldots, W_K; Z_m^n) = 0. \tag{3.5}$$

A tuple of rates $(R_1, \ldots, R_K) \in \mathbb{R}_+^K$ is achievable for the DBC-LD-NLS if there exists a sequence of $(\lceil 2^{nR_1} \rceil, \ldots, \lceil 2^{nR_K} \rceil, n)$ codes such that they satisfy Equations (3.4) and (3.5).

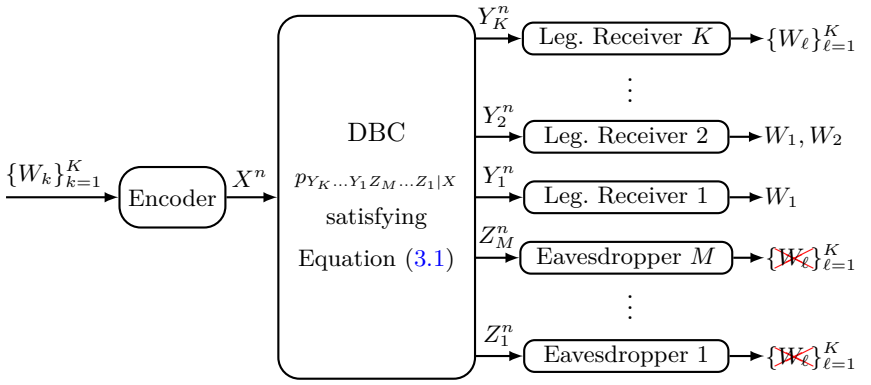

Figure 3.2: Channel model DBC-LD-NLS.

Proposition 3.2 (Adapted from [ZLL+15, EU09]). *The achievable region of the DBC-LD-NLS is the union of all K-tuples of rates $(R_1, \ldots, R_K) \in \mathbb{R}_+^K$ satisfying the following inequalities:*

$$\sum_{\ell=1}^{k} R_\ell \leq \sum_{\ell=1}^{k} I(V_\ell; Y_\ell | V_{\ell-1}) - I(V_k, Z_M), \qquad k = 1, \ldots, K,$$

where $V_0 \triangleq \varnothing$ and $V_K \triangleq X$, and the union is taken over all distributions $p_{V_1 \ldots V_K}$ such that $V_1 - V_2 - \cdots - V_K$ forms a Markov chain.

The proof for the case of only one eavesdropper is provided in [EU09]. Due to the degradedness condition of Equation (3.1), note that any achievable scheme ensuring the strong secrecy condition in Equation (3.5) for the Eavesdropper M will also satisfy it for any Eavesdropper $m \in [1, M-1]$.

Corollary 3.2. *The achievable subregion of the DBC-LD-NLS without considering rate sharing is a K-orthotope defined by the closure of all K-tuples of rates $(R_1, \ldots, R_K) \in \mathbb{R}_+^K$ satisfying*

$$R_\ell \leq I(V_\ell; Y_\ell | V_{\ell-1}) - I(V_\ell; Z_M | V_{\ell-1}), \qquad \ell = 1, \ldots, K.$$

3.2 Polar coding scheme for the DBC-NLD-LS

The PCS provided in this section is designed to achieve the supremum of the achievable rates given in Corollary 3.1. Thus, consider the DMS

$$\left(\mathcal{X} \times \mathcal{Y}_K \times \cdots \times \mathcal{Y}_1 \times \mathcal{Z}_M \times \cdots \times \mathcal{Z}_1, p_{X Y_K \ldots Y_1 Z_M \ldots Z_1}\right)$$

that represents the input and output random variables involved in the achievable region of Corollary 3.1, where $\mathcal{X} = \{0, 1\}$. Let $(X^n, Y_K^n, \ldots, Y_1^n, Z_M^n, \ldots, Z_1^n)$ be an i.i.d. n-sequence of this source. Define the polar transform $U^n \triangleq X^n G_n$ with distribution $p_{U^n}(u^n) = p_{X^n}(u^n G_n)$ due to the invertibility of matrix G_n. Moreover, for polar coding purposes, we write

$$p_{U^n}(u^n) \triangleq \prod_{j=1}^{n} p_{U(j)|U^{1:j-1}}\left(u(j) \middle| u^{1:j-1}\right). \tag{3.6}$$

3.2.1 Polar code construction

Let $\delta_n \triangleq 2^{-n^\beta}$, where $\beta \in (0, \frac{1}{2})$. Based on $p_{X Y_K \ldots Y_1 Z_M \ldots Z_1}$, we define the sets of indices

$$\mathcal{H}_X^{(n)} \triangleq \left\{j \in [n] : H\left(U(j) \middle| U^{1:j-1}\right) \geq 1 - \delta_n\right\}, \tag{3.7}$$

$$\mathcal{L}_X^{(n)} \triangleq \left\{j \in [n] : H\left(U(j) \middle| U^{1:j-1}\right) \leq \delta_n\right\}; \tag{3.8}$$

and, for any $k \in [1, L]$ and $m \in [1, M]$, we also define

$$\mathcal{L}_{X|Y_k}^{(n)} \triangleq \big\{j \in [n] : H\big(U(j)\big|U^{1:j-1}, Y_k^n\big) \leq \delta_n\big\}, \tag{3.9}$$

$$\mathcal{H}_{X|Y_k}^{(n)} \triangleq \big\{j \in [n] : H\big(U(j)\big|U^{1:j-1}, Y_k^n\big) \geq 1 - \delta_n\big\}; \tag{3.10}$$

$$\mathcal{H}_{X|Z_m}^{(n)} \triangleq \big\{j \in [n] : H\big(U(j)\big|U^{1:j-1}, Z_m^n\big) \geq 1 - \delta_n\big\}. \tag{3.11}$$

The following proposition particularizes the subset lemma of polar codes (Lemma 2.2) to the particular sets defined in (3.7)–(3.11).

Proposition 3.3. *Consider the sets of indices defined in* (3.7)–(3.11)*. Due to degradedness condition of the channel in* (3.1)*, it holds that*

$$\mathcal{L}_X^{(n)} \subseteq \mathcal{L}_{X|Z_1}^{(n)} \subseteq \cdots \subseteq \mathcal{L}_{X|Z_M}^{(n)} \subseteq \mathcal{L}_{X|Y_1}^{(n)} \subseteq \cdots \subseteq \mathcal{L}_{X|Y_K}^{(n)},$$
$$\mathcal{H}_X^{(n)} \supseteq \mathcal{H}_{X|Z_1}^{(n)} \supseteq \cdots \supseteq \mathcal{H}_{X|Z_M}^{(n)} \supseteq \mathcal{H}_{X|Y_1}^{(n)} \supseteq \cdots \supseteq \mathcal{H}_{X|Y_K}^{(n)}.$$

Remark 3.1. *According to Lemma 2.2, the subset property also holds if the channels are stochastically degraded. Therefore, since the construction of the polar codes proposed in the following sections is based basically on Proposition 3.3, the PCSs are suitable for physically and stochastically degraded channels.*

Based on the sets (3.7)–(3.11) and Proposition 3.3, we define the following partition of the set of indices $[1, n]$:

$$\mathcal{I}_M^{(n)} \triangleq \mathcal{H}_{X|Z_M}^{(n)} \setminus \mathcal{H}_{X|Y_1}^{(n)}, \tag{3.12}$$

$$\mathcal{I}_m^{(n)} \triangleq \mathcal{H}_{X|Z_m}^{(n)} \setminus \mathcal{H}_{X|Z_{m+1}}^{(n)}, \quad m = 1, \ldots, M-1, \tag{3.13}$$

$$\mathcal{F}^{(n)} \triangleq \mathcal{H}_{X|Y_1}^{(n)}, \tag{3.14}$$

$$\mathcal{C}^{(n)} \triangleq \mathcal{H}_X^{(n)} \setminus \mathcal{H}_{X|Z_1}^{(n)}, \tag{3.15}$$

$$\mathcal{T}^{(n)} \triangleq \big(\mathcal{H}_X^{(n)}\big)^{\mathrm{C}}. \tag{3.16}$$

This partition is graphically represented in Figure 3.3. The distribution of $\tilde{U}^n$ after the encoding must be close in terms of statistical distance to the one given in (3.6) corresponding to the original DMS. Thus, the elements $U(j)$ such that $j \in \mathcal{H}_X^{(n)}$, that is, $U\big[[1, n] \setminus \mathcal{T}^{(n)}\big]$, will be suitable for storing uniformly-distributed random sequences, and $U[\mathcal{T}^{(n)}]$ will not.

For any $m \in [1, M]$, the set $\mathcal{I}_m^{(n)}$ belongs to $\mathcal{H}_{X|Z_m}^{(n)}$ and, by Proposition 3.3, we have $\mathcal{H}_{X|Z_m}^{(n)} \subseteq \mathcal{H}_{X|Z_{m'}}^{(n)}$ for any $m' < m$. Hence, $U[\mathcal{I}_m^{(n)}]$ will be suitable for storing information to be secured from Eavesdroppers 1–m. Otherwise, $\mathcal{C}^{(n)} \subseteq \big(\mathcal{H}_{X|Z_1}^{(n)}\big)^{\mathrm{C}}$ and, by Proposition 3.3, we have $\big(\mathcal{H}_{X|Z_1}^{(n)}\big)^{\mathrm{C}} \subseteq \big(\mathcal{H}_{X|Z_m}^{(n)}\big)^{\mathrm{C}}$ for any $m \in [1, M]$. Thus, $U\big[\mathcal{C}^{(n)}\big]$ cannot contain information

to be secured from any eavesdropper, and it will be used to store the local randomness required to confuse the eavesdroppers.

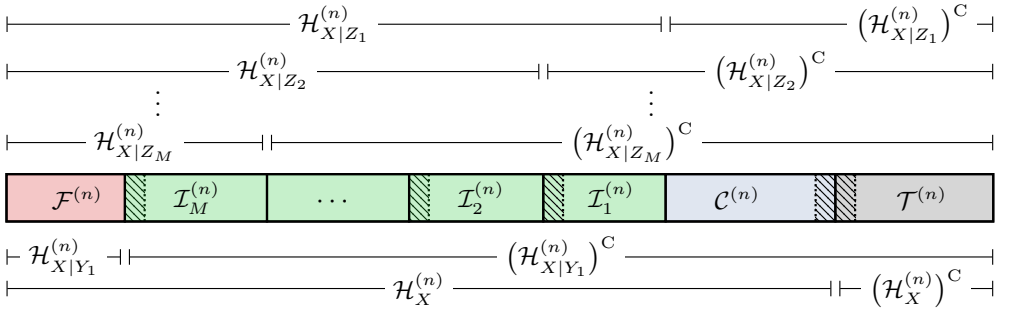

Figure 3.3: Polar code construction for the DBC-NLD-LS. The hatched area represents those indices $j \in (\mathcal{H}^{(n)}_{X|Y_1})^{\mathrm{C}} \setminus \mathcal{L}^{(n)}_{X|Y_1}$, which can belong to $\mathcal{I}^{(n)}_m$ ($m \in [1, M]$), $\mathcal{C}^{(n)}$, $\mathcal{F}^{(n)}$ or $\mathcal{T}^{(n)}$.

According to Theorem 2.2, legitimate Receiver 1 will be able to reliably infer $U[\mathcal{L}^{(n)}_{X|Y_1}]$ given Y_1^n and $U[(\mathcal{L}^{(n)}_{X|Y_1})^{\mathrm{C}}]$. Hence, if the polar coding scheme somehow make the entries $U(j)$ such that j belongs to $\mathcal{F}^{(n)} = \mathcal{H}^{(n)}_{X|Y_1}$ and $\left(\mathcal{H}^{(n)}_{X|Y_1}\right)^{\mathrm{C}} \setminus \mathcal{L}^{(n)}_{X|Y_1}$ (hatched areas in Figure 3.3) available to the legitimate Receiver 1, this receiver will be able to reliably infer the entire sequence U^n. In this sense, $U[\mathcal{F}^{(n)}]$ will be used to store the uniformly-distributed random sequence provided by a source of common randomness that will be available to all parties. Since, by Proposition 3.3, $\mathcal{F}^{(n)} \subseteq \mathcal{H}^{(n)}_{X|Z_m}$ for any $m \in [1, M]$, the knowledge of $U[\mathcal{F}^{(n)}]$ from the eavesdroppers will not compromise the strong secrecy condition. On the other hand, $U\big[(\mathcal{H}^{(n)}_{X|Y_1})^{\mathrm{C}} \setminus \mathcal{L}^{(n)}_{X|Y_1}\big]$ will contain secret information or elements that cannot be known directly by all the eavesdroppers without compromising the secrecy. Therefore, the transmitter somehow will additionally and secretly send it to the legitimate receivers. Nevertheless, as will be seen later, this additional transmission will incur an asymptotically negligible rate penalty. Finally, by Proposition 3.3, we have $(\mathcal{L}^{(n)}_{X|Y_1})^{\mathrm{C}} \supseteq (\mathcal{L}^{(n)}_{X|Y_k})^{\mathrm{C}}$ for any $k > 1$. Hence, given $U[(\mathcal{L}^{(n)}_{X|Y_1})^{\mathrm{C}}]$, all the legitimate receivers will be able to reliably infer the entire sequence U^n from their own channel observations.

The goal of the polar code construction is to obtain, with as low complexity as possible, the entropy terms $\{H(U(j)\big|U^{1:j-1})\}_{j=1}^n$, $\{H(U(j)\big|U^{1:j-1}, Y_1^n)\}_{j=1}^n$ and $\{H(U(j)\big|U^{1:j-1}, Z_m^n)\}_{j=1}^n$ for all $m \in [1, M]$ required to define the sets (3.7)–(3.11) and, consequently, to obtain the partition of $[1, n]$ defined in (3.12)–(3.16). Although construction of polar codes is covered in a large number of references (for instance, see [TV13, VVH15, HY13]), they only focus on constructions under reliability constraints. In Section 3.4 we discuss further how to construct polar codes under both reliability and secrecy constraints.

3.2.2 Polar encoding

The polarization-based encoder aims to construct the sequence $\tilde{U}^n$ and is summarized in Algorithm 3.1. Let W_m for all $m \in [1, M]$ and C be uniformly-distributed random vectors of size $|\mathcal{I}_m^{(n)}|$ and $|\mathcal{C}^{(n)}|$, respectively, where C represents the local randomness and recall that W_m represents the message m that is intended for all legitimate receivers. Let F be a given uniformly-distributed random $|\mathcal{F}^{(n)}|$-sequence, which represents the source of common randomness that is available to all parties. First, notice in Algorithm 3.1 that the encoder constructs $\tilde{U}\big[\mathcal{H}_X^{(n)}\big] = \tilde{U}\big[\big(\cup_{m=1}^{M} \mathcal{I}_m^{(n)}\big) \cup \mathcal{C}^{(n)} \cup \mathcal{F}^{(n)}\big]$ from $\{W_m\}_{m=1}^{M}$, C and F.

Algorithm 3.1 Polar encoding for the DBC-NLD-LS

Require: Messages $\{W_m\}_{m=1}^{M}$; common randomness F; local randomness C; and key κ_Φ privately shared between transmitter and all legitimate receivers

for $m = 1$ to M **do**
  $\tilde{U}\big[\mathcal{I}_m^{(n)}\big] \leftarrow W_m$
end for
$\tilde{U}\big[\mathcal{C}^{(n)}\big] \leftarrow C$
$\tilde{U}\big[\mathcal{F}^{(n)}\big] \leftarrow F$
for $j \in \mathcal{T}^{(n)}$ **do**
  if $j \in \big(\mathcal{H}_X^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{L}_X^{(n)}$ **then**
    $\tilde{U}(j) \leftarrow p_{U(j)|U^{1:j-1}}\big(\tilde{U}^{1:j-1}\big)$
  else if $j \in \mathcal{L}_X^{(n)}$ **then** ▷ Deterministic SC encoding
    $\tilde{U}(j) \leftarrow \arg\max_{u\in\{0,1\}} p_{U(j)|U^{1:j-1}}\big(u|\tilde{U}^{1:j-1}\big)$
  end if
end for
$\tilde{X}^n = \tilde{U}^n G_n$
$\Phi \leftarrow \tilde{U}\big[\big(\mathcal{H}_{X|Y_1}^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{L}_{X|Y_1}^{(n)}\big]$
Send $\Phi \oplus \kappa_\Phi$ to legitimate Receivers 1–K
return $\tilde{X}^n$

Given $\tilde{U}\big[\mathcal{H}_X^{(n)}\big]$, the encoder forms the remaining entries of $\tilde{U}^n$, that is, $\tilde{U}\big[\mathcal{T}^{(n)}\big]$ as follows. If $j \in \mathcal{L}_X^{(n)}$, it constructs $\tilde{U}(j)$ deterministically by using SC encoding. Otherwise, if $j \in \big(\mathcal{H}_X^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{L}_X^{(n)}$ then $\tilde{U}(j)$ is constructed randomly from the distribution $p_{U(j)|U^{1:j-1}}$.

Then, the encoder computes $\tilde{X}^n = \tilde{U}^n G_n$ and transmits it over the DBC inducing $(\tilde{Y}_K, \ldots, \tilde{Y}_1, \tilde{Z}_M, \ldots, \tilde{Z}_1)$. Finally, besides the sequence $\tilde{X}^n$, the encoder obtains

$$\Phi \triangleq \tilde{U}\big[\big(\mathcal{H}_{X|Y_1}^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{L}_{X|Y_1}^{(n)}\big]. \tag{3.17}$$

This sequence Φ must be additionally transmitted to all legitimate receivers keeping it masked from eavesdroppers. To do so, the transmitter can perform a modulo-two addition between

Φ and a uniformly distributed secret key κ_Φ that is privately shared with the legitimate receivers and somehow additionally send it to them. Nevertheless, by Theorem 2.1, this additional transmission is asymptotically negligible in terms of rate.

Remark 3.2. *The sequence Φ can be divided into two parts: one that is uniformly distributed, $\tilde{U}\big[\mathcal{H}_X^{(n)} \cap (\mathcal{H}_{X|Y_1}^{(n)})^{\mathrm{C}} \setminus \mathcal{L}_{X|Y_1}^{(n)}\big]$, and the remaining part that is not. The transmitter could make this uniformly distributed part available to legitimate receivers by using a chaining structure as the one in Section 2.3 for the DWTC. However, such a scheme will require the transmission to take place over several blocks of size n. Indeed, since Φ is made available confidentially to the legitimate receivers, the PCS can include part of the indices belonging to the set $\big(\mathcal{H}_{X|Y_1}^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{L}_{X|Y_1}^{(n)}$ into the set $\cup_{m=1}^{M} \mathcal{I}_m^{(n)}$. Thus, according to the previous encoding, part of the messages $W_{1:M}$ have been sent by means of this additional transmission.*

3.2.3 Polar decoding

Consider that the realization of the source of common randomness F is available to all parties and the sequence Φ has been successfully received by all legitimate receivers. The decoding process at Receiver $k \in [1, K]$ is summarized in Algorithm 3.2. Given F and Φ, notice that it knows $\tilde{U}\big[\big(\mathcal{L}_{X|Y_1}^{(n)}\big)^{\mathrm{C}}\big]$. Since by Proposition 3.3 we have $\big(\mathcal{L}_{X|Y_1}^{(n)}\big)^{\mathrm{C}} \supseteq \big(\mathcal{L}_{X|Y_k}^{(n)}\big)^{\mathrm{C}}$ for any $k > 1$, Receiver k performs SC decoding to construct the estimate $\hat{U}^n$ of $\tilde{U}^n$ from $\tilde{U}\big[\big(\mathcal{L}_{X|Y_1}^{(n)}\big)^{\mathrm{C}}\big]$ and its channel output observations $\tilde{Y}_k^n$. In Section 3.2.4, we show formally that the reliability condition in Equation (3.2) is satisfied at each legitimate receiver $k \in [1, K]$.

Algorithm 3.2 Decoding at Receiver $k \in [1, K]$ for the DBC-NLD-LS

Require: Common randomness F; additional sequence Φ

1: $\hat{U}[(\mathcal{L}_{X|Y_1}^{(n)})^{\mathrm{C}}] \leftarrow (F, \Phi)$
2: **for** $j \in \mathcal{L}_{X|Y_1}^{(n)}$ **do** ▷ SC decoding
3: $\quad \hat{U}(j) \leftarrow \arg\max_{u \in \{0,1\}} p_{U(j)|U^{1:j-1}Y_k^n}\big(u|\hat{U}^{1:j-1}, \tilde{Y}_k^n\big)$
4: **end for**
5: **return** $\{\hat{W}_m\}_{m=1}^{M} \leftarrow \hat{U}^n\big[\cup_{m=1}^{M} \mathcal{I}_m^{(n)}\big]$

3.2.4 Performance of the polar coding scheme

The analysis of the polar coding scheme described previously leads to the following theorem.

Theorem 3.1. *Let $\big(\mathcal{X}, p_{Y_K \dots Y_1 Z_M \dots Z_1|X}, \mathcal{Y}_K \times \cdots \times \mathcal{Y}_1 \times \mathcal{Z}_M \times \cdots \times \mathcal{Z}_1\big)$ be an arbitrary DBC such that $\mathcal{X} \in \{0, 1\}$ and the distribution $p_{Y_K \dots Y_1 Z_M \dots Z_1|X}$ satisfies the Markov chain condition*

$X - Y_K - \cdots - Y_1 - Z_M - \cdots - Z_1$. The polar coding scheme described in Sections 3.2.1–3.2.3 achieves any rate tuple of the region defined in Corollary 3.1.

Corollary 3.3. *Since $\tilde{U}[\mathcal{I}_m^{(n)}]$ for some $m \in [1, M]$ can contain information to be secured from Eavesdroppers 1–m, the polar coding scheme described in Sections 3.2.1–3.2.3 can achieve the entire region considering rate sharing of Proposition 3.1 by storing part of any message $W_{m'}$ such that $m' < m$ into $\tilde{U}[\mathcal{I}_m^{(n)}]$ instead of part of W_m.*

The proof of Theorem 3.1 follows in four steps, and is provided hereafter. First, we prove that the PCS approaches the corner point of the region defined in Corollary 3.1. Second, we show that the joint distribution $\tilde{q}_{X^n Y_K^n \ldots Y_1^n Z_M^n \ldots Z_1^n}$ of $\left(\tilde{X}^n, \tilde{Y}_K^n, \ldots, \tilde{Y}_1^n, \tilde{Z}_M^n, \ldots, \tilde{Z}_1^n\right)$ induced by the encoder described in Section 3.2.2 is statistically close to the distribution $p_{X^n Y_K^n \ldots Y_1^n Z_M^n \ldots Z_1^n}$ of the original DMS from which the polarization sets were defined. In steps three and four, we prove that the corresponding average error probability at Receiver $k \in [1, K]$ and the information leakage for Eavesdropper $m \in [1, M]$ vanishes for sufficiently large n and, consequently, the PCS satisfy the reliability and the strong secrecy conditions given in (3.2) and (3.3). On the other hand, the proof of Corollary 3.3 is immediate.

Transmission Rates

For any $m \in [1, M-1]$, the rate R_m corresponding to the message W_m satisfies

$$\begin{aligned}\lim_{n\to\infty} R_m = \lim_{n\to\infty} \frac{1}{n}\left|\mathcal{I}_m^{(n)}\right| &\overset{(a)}{=} \lim_{n\to\infty} \frac{1}{n}\left|\mathcal{H}_{X|Z_m}^{(n)} \setminus \mathcal{H}_{X|Z_{m+1}}^{(n)}\right| \\ &\overset{(b)}{=} \lim_{n\to\infty} \frac{1}{n}\left|\mathcal{H}_{X|Z_m}^{(n)}\right| - \lim_{n\to\infty} \frac{1}{n}\left|\mathcal{H}_{X|Z_{m+1}}^{(n)}\right| \\ &\overset{(c)}{=} H(X|Z_{m+1}) - H(X|Z_m),\end{aligned}$$

where (a) follows from the definition of the set $\mathcal{I}_m^{(n)}$ in Equation (3.13); (b) holds because, by Proposition 3.3, $\mathcal{H}_{X|Z_m}^{(n)} \supseteq \mathcal{H}_{X|Z_{m+1}}^{(n)}$; and (c) follows from Theorem 2.1. Similarly, according to Equation (3.12), the rate of message W_M satisfies

$$\lim_{n\to\infty} R_M = \lim_{n\to\infty} \frac{1}{n}\left|\mathcal{I}_M^{(n)}\right| = \lim_{n\to\infty} \frac{1}{n}\left|\mathcal{H}_{X|Z_M}^{(n)} \setminus \mathcal{H}_{X|Y_1}^{(n)}\right| = I(X;Y_1) - I(X;Z_M).$$

Distribution of the DMS after the Polar Encoding

Let $\tilde{q}_{U^n}$ be the distribution of $\tilde{U}^n$ after the encoding in Section 3.2.2. The following lemma shows that $\tilde{q}_{U^n}$ and the distribution p_{U^n} in Equation (3.6) of the original DMS are nearly statistically indistinguishable for sufficiently large n and, consequently, so are the overall distributions $\tilde{q}_{X^n Y_K^n \ldots Y_1^n Z_M^n \ldots Z_1^n}$ and $p_{X^n Y_K^n \ldots Y_1^n Z_M^n \ldots Z_1^n}$.

Lemma 3.1. *Let $\delta_n = 2^{-n^\beta}$ for some $\beta \in \left(0, \frac{1}{2}\right)$. Then,*

$$\mathbb{V}(\tilde{q}_{U^n}, p_{U^n}) \leq \delta_{\text{nld-ls}}^{(n)},$$
$$\mathbb{V}(\tilde{q}_{X^n Y_K^n \ldots Y_1^n Z_M^n \ldots Z_1^n}, p_{X^n Y_K^n \ldots Y_1^n Z_M^n \ldots Z_1^n}) = \mathbb{V}(\tilde{q}_{U^n}, p_{U^n}) \leq \delta_{\text{nld-ls}}^{(n)},$$

where $\delta_{\text{nld-ls}}^{(n)} \triangleq n\sqrt{2\sqrt{n\delta_n 2\ln 2}\left(n - \log\sqrt{n\delta_n 2\ln 2}\right) + \delta_n} + \sqrt{n\delta_n 2\ln 2}$.

Proof. For the first claim, see Lemma 2.3 taking $T_{\text{V}} \triangleq 1$. The second claim holds by Corollary 2.2 due to the invertibility of G_n and $\tilde{q}_{X^n Y_K^n \ldots Y_1^n Z_M^n \ldots Z_1^n} \equiv \tilde{q}_X p_{Y_K^n \ldots Y_1^n Z_M^n \ldots Z_1^n | X^n}$. □

Remark 3.3. *The first term of $\delta_{\text{nld-ls}}^{(n)}$ bounds the impact on the total variation distance of using deterministic SC encoding for the entries $\tilde{U}\left[\mathcal{L}_X^{(n)}\right]$, while the second term bounds the impact of storing uniformly-distributed random sequences (messages, local randomness and common randomness) into the entries $\tilde{U}\left[\mathcal{H}_X^{(n)}\right]$.*

As will be seen in the following subsections, an encoding process satisfying Lemma 3.1 is crucial for the reliability and the secrecy performance of the polar code.

Reliability Performance

Consider the probability of incorrectly decoding all messages $\{W_m\}_{m=1}^M$ at legitimate Receiver $k \in [1, K]$. Let $\tilde{q}_{X^n Y_k^n}$ and $p_{X^n Y_k^n}$ be the marginal distributions of $\tilde{q}_{X^n Y_K^n \ldots Y_1^n Z_M^n \ldots Z_1^n}$ and $p_{X^n Y_K^n \ldots Y_1^n Z_M^n \ldots Z_1^n}$, respectively. Consider an optimal coupling [LPW09] (Proposition 4.7) between $\tilde{q}_{X^n Y_k^n}$ and $p_{X^n Y_k^n}$ such that

$$\mathbb{P}\left[\mathcal{E}_{X^n Y_k^n}\right] = \mathbb{V}(\tilde{q}_{X^n Y_k^n}, p_{X^n Y_k^n}),$$

where $\mathcal{E}_{X^n Y_k^n} \triangleq \{(\tilde{X}^n, \tilde{Y}_k^n) \neq (X^n, Y_k^n)\}$ or, equivalently, $\mathcal{E}_{X^n Y_k^n} \triangleq \{(\tilde{U}^n, \tilde{Y}_k^n) \neq (U^n, Y_k^n)\}$ because of the invertibility of G_n. Thus, for the legitimate Receiver $k \in [1, K]$, we obtain

$$\begin{aligned}
&\mathbb{P}\left[(\hat{W}_1, \ldots \hat{W}_M) \neq (W_1, \ldots, W_M)\right] \\
&\quad \leq \mathbb{P}\left[\hat{U}^n \neq \tilde{U}^n\right] \\
&\quad = \mathbb{P}\left[\hat{U}^n \neq \tilde{U}^n \middle| \mathcal{E}_{X^n Y_k^n}^{\text{C}}\right]\mathbb{P}\left[\mathcal{E}_{X^n Y_k^n}^{\text{C}}\right] + \mathbb{P}\left[\hat{U}^n \neq \tilde{U}^n \middle| \mathcal{E}_{X^n Y_k^n}\right]\mathbb{P}\left[\mathcal{E}_{X^n Y_k^n}\right] \\
&\quad \leq \mathbb{P}\left[\hat{U}^n \neq \tilde{U}^n \middle| \mathcal{E}_{X^n Y_k^n}^{\text{C}}\right] + \mathbb{P}\left[\mathcal{E}_{X^n Y_k^n}\right] \\
&\quad \overset{(a)}{\leq} n\delta_n + \mathbb{P}\left[\mathcal{E}_{X^n Y_k^n}\right] \\
&\quad \overset{(b)}{\leq} n\delta_n + \delta_{\text{nld-ls}}^{(n)},
\end{aligned} \tag{3.18}$$

where (a) holds by Theorem 2.2 because recall that $(F,\Phi)=\tilde{U}\big[\big(\mathcal{L}_{X|Y_1}^{(n)}\big)^{\mathrm{C}}\big]$ is available to all legitimate receivers and, by Proposition 3.4, we have $\big(\mathcal{L}_{X|Y_1}^{(n)}\big)^{\mathrm{C}}\supseteq\big(\mathcal{L}_{X|Y_k}^{(n)}\big)^{\mathrm{C}}$ for any $k\in[1,K]$; and (b) holds by the optimal coupling and Lemma 3.1. Therefore, the probability of incorrectly decoding $\{W_m\}_{m=1}^M$ at legitimate Receiver $k\in[1,K]$ is in $O\big(n^{\frac{7}{4}}2^{-n^\beta}\big)\xrightarrow{n\to\infty}0$ and the PCS satisfies the reliability condition given in Equation (3.2).

Secrecy performance

Recall that the secrecy condition in (3.3) requires Eavesdropper $m\in[1,M]$ to be kept ignorant about messages $(W_m,W_{m+1},\ldots,W_M)$. Due to the existence of the source of common randomness, the information leakage at Eavesdropper $m\in[1,M]$ is given by $I(W_mW_{m+1}\ldots W_M;\tilde{Z}^nF)$. Hence, for n large enough we have

$$\begin{aligned}
&I(W_mW_{m+1}\ldots W_M;F\tilde{Z}_m^n)\\
&\overset{(a)}{\leq} I\big(\tilde{U}\big[\cup_{i=m}^M\mathcal{I}_i^{(n)}\big]\tilde{U}\big[\mathcal{F}^{(n)}\big];\tilde{Z}_m^n\big)\\
&\overset{(b)}{=}\sum_{i=m}^M\big|\mathcal{I}_i^{(n)}\big|+\big|\mathcal{F}^{(n)}\big|-H\big(\tilde{U}\big[\cup_{i=m}^M\mathcal{I}_i^{(n)}\big]\tilde{U}\big[\mathcal{F}^{(n)}\big]\big|\tilde{Z}_m^n\big)\\
&\overset{(c)}{\leq}\sum_{i=m}^M\big|\mathcal{I}_i^{(n)}\big|+\big|\mathcal{F}^{(n)}\big|-H\big(U\big[\cup_{i=m}^M\mathcal{I}_i^{(n)}\big]U\big[\mathcal{F}^{(n)}\big]\big|Z_m^n\big)+3n\delta_{\text{nld-ls}}^{(n)}-2\delta_{\text{nld-ls}}^{(n)}\log\delta_{\text{nld-ls}}^{(n)}\\
&\overset{(d)}{\leq} n\delta_n+3n\delta_{\text{nld-ls}}^{(n)}-2\delta_{\text{nld-ls}}^{(n)}\log\delta_{\text{nld-ls}}^{(n)},
\end{aligned}\tag{3.19}$$

where (a) follows from independence between $\{W_i\}_{i=m}^M$ and F, and from the encoding in Algorithm 3.1; (b) holds by the uniformity of $\{W_i\}_{i=m}^M$ and F; (c) follows from applying Lemma 2.4 (taking $T_{\mathrm{V}}=T_{\mathrm{O}}=1$) and Lemma 3.1; and (d) holds because by definition we have $\mathcal{F}^{(n)},\mathcal{I}_{m'}^{(n)}\subseteq\mathcal{H}_{V|Z_m}^{(n)}$ for $m\in[1,M]$ and $m'\in[m,M]$. Thus, the corresponding information leakage is in $O\big(n^{\frac{11}{4}}2^{-n^\beta}\big)\xrightarrow{n\to\infty}0$ for Eavesdropper $m\in[1,M]$, and the PCS satisfies the strong secrecy condition in (3.3) and the proof of Theorem 3.1 is concluded.

3.3 Polar coding scheme for the DBC-LD-NLS

The PCS provided in this section is designed to achieve the supremum of the achievable rates given in Corollary 3.2 (secrecy-capacity without rate sharing). In this model, there are K input random variables $\{V_\ell\}_{\ell=1}^K$, where $V_K\triangleq X$, each one corresponding to a different superposition encoding layer. Consider the DMS

$$\big(\mathcal{V}_1\times\cdots\times\mathcal{V}_K\times\mathcal{Y}_K\times\cdots\times\mathcal{Y}_1\times\mathcal{Z}_M\times\cdots\times\mathcal{Z}_1,p_{V_1\ldots V_KY_K\ldots Y_1Z_M\ldots Z_1}\big)$$

that represents the random variables involved in the achievable region, where $\mathcal{V}_\ell \triangleq \{0,1\}$ for $\ell \in [1,K]$. Let $(V_1^n,\dots,V_K^n,Y_K^n,\dots,Y_1^n,Z_M^n,\dots,Z_1^n)$ be an i.i.d. n-sequence of this source. Define K polar transforms $U_\ell^n \triangleq V_\ell^n G_n$, $\ell \in [1,K]$. Since $V_1 - V_2 - \cdots - V_K$ and, consequently, $U_1 - U_2 - \cdots - U_K$ (by the invertibility of G_n) form a Markov chain, we have

$$p_{U_1^n \dots U_K^n}(u_1^n,\dots,u_K^n) \triangleq \prod_{\ell=1}^{K}\prod_{j=1}^{n} p_{U_\ell(j)|U_\ell^{1:j-1}V_{\ell-1}^n}\big(u_\ell(j)\big|u_\ell^{1:j-1},u_{\ell-1}^n G_n\big). \tag{3.20}$$

3.3.1 Polar code construction

Based on $p_{V_1\dots V_K Y_K \dots Y_1 Z_M \dots Z_1}$, the construction is carried out similarly at each superposition layer. Consider the polar construction at layer $\ell \in [1,K]$. Let $\delta_n \triangleq 2^{-n^\beta}$, where $\beta \in \big(0,\frac{1}{2}\big)$. For the polar transform $U_\ell^n = V_\ell^n G_n$ associated with the ℓ-th layer, we define the sets

$$\mathcal{H}_{V_\ell|V_{\ell-1}}^{(n)} \triangleq \big\{j \in [n] : H\big(U_\ell(j)\big|U_\ell^{1:j-1},V_{\ell-1}^n\big) \geq 1-\delta_n\big\}, \tag{3.21}$$

$$\mathcal{L}_{V_\ell|V_{\ell-1}}^{(n)} \triangleq \big\{j \in [n] : H\big(U_\ell(j)\big|U_\ell^{1:j-1},V_{\ell-1}^n\big) \leq \delta_n\big\}, \tag{3.22}$$

$$\mathcal{L}_{V_\ell|V_{\ell-1}Y_k}^{(n)} \triangleq \big\{j \in [n] : H\big(U_\ell(j)\big|U_\ell^{1:j-1},V_{\ell-1}^n,Y_k^n\big) \leq \delta_n\big\}, \qquad k=\ell,\dots,K, \tag{3.23}$$

$$\mathcal{H}_{V_\ell|V_{\ell-1}Y_k}^{(n)} \triangleq \big\{j \in [n] : H\big(U_\ell(j)\big|U_\ell^{1:j-1},V_{\ell-1}^n,Y_k^n\big) \geq 1-\delta_n\big\}, \qquad k=\ell,\dots,K, \tag{3.24}$$

$$\mathcal{H}_{V_\ell|V_{\ell-1}Z_m}^{(n)} \triangleq \big\{j \in [n] : H\big(U_\ell(j)\big|U_\ell^{1:j-1},V_{\ell-1}^n,Z_m^n\big) \geq 1-\delta_n\big\}, \qquad m=1,\dots,M, \tag{3.25}$$

where recall that $V_0 = \varnothing$ when $\ell = 1$ and $V_K \triangleq X$ when $\ell = K$.

Proposition 3.4. *Consider the sets of indices defined in (3.21)–(3.25). For any $\ell \in [1,K]$, due to degradedness condition of the channel in (3.1), it holds that*

$$\mathcal{L}_{V_\ell|V_{\ell-1}}^{(n)} \subseteq \mathcal{L}_{V_\ell|V_{\ell-1}Z_1}^{(n)} \subseteq \cdots \subseteq \mathcal{L}_{V_\ell|V_{\ell-1}Z_M}^{(n)} \subseteq \mathcal{L}_{V_\ell|V_{\ell-1}Y_1}^{(n)} \subseteq \cdots \subseteq \mathcal{L}_{V_\ell|V_{\ell-1}Y_K}^{(n)},$$
$$\mathcal{H}_{V_\ell|V_{\ell-1}}^{(n)} \supseteq \mathcal{H}_{V_\ell|V_{\ell-1}Z_1}^{(n)} \supseteq \cdots \supseteq \mathcal{H}_{V_\ell|V_{\ell-1}Z_M}^{(n)} \supseteq \mathcal{H}_{V_\ell|V_{\ell-1}Y_1}^{(n)} \supseteq \cdots \supseteq \mathcal{H}_{V_\ell|V_{\ell-1}Y_K}^{(n)}.$$

At each layer $\ell \in [1,K]$, based on these previous sets, we define the following partition of the set of indices $[1,n]$:

$$\mathcal{I}_\ell^{(n)} \triangleq \mathcal{H}_{V_\ell|V_{\ell-1}Z_M}^{(n)} \setminus \mathcal{H}_{V_\ell|V_{\ell-1}Y_\ell}^{(n)}, \tag{3.26}$$

$$\mathcal{F}_\ell^{(n)} \triangleq \mathcal{H}_{V_\ell|V_{\ell-1}Y_\ell}^{(n)}, \tag{3.27}$$

$$\mathcal{C}_\ell^{(n)} \triangleq \mathcal{H}_{V_\ell|V_{\ell-1}}^{(n)} \setminus \mathcal{H}_{V_\ell|V_{\ell-1}Z_M}^{(n)}, \tag{3.28}$$

$$\mathcal{T}_\ell^{(n)} \triangleq \big(\mathcal{H}_{V_\ell|V_{\ell-1}}^{(n)}\big)^{\mathrm{C}}, \tag{3.29}$$

which is graphically represented in Figure 3.4. The way we define this partition at the ℓ-th

layer follows similar reasoning as the one to define the partition in Section 3.2.1 for the DBC-NLD-LS. In this sense, $U_\ell\big[\mathcal{H}^{(n)}_{V_\ell|V_{\ell-1}}\big]$ will be suitable for storing uniformly-distributed random sequences and $U_\ell\big[\mathcal{T}^{(n)}_\ell\big]$ will not. Since, by Proposition 3.4, $\mathcal{I}^{(n)}_\ell \subseteq \mathcal{H}^{(n)}_{V_\ell|V_{\ell-1}Z_M} \subseteq \mathcal{H}^{(n)}_{V_\ell|V_{\ell-1}Z_m}$ for any $m \in [1, M-1]$, then $U_\ell\big[\mathcal{I}^{(n)}_\ell\big]$ will be suitable for storing information to be secured from all eavesdroppers. Otherwise, we have $\mathcal{C}^{(n)}_\ell \subseteq \big(\mathcal{H}^{(n)}_{V_\ell|V_{\ell-1}Z_M}\big)^{\mathrm{C}}$. Therefore, $U_\ell\big[\mathcal{C}^{(n)}_\ell\big]$ cannot contain information to be secured from all eavesdroppers, but it will be used to store the local randomness required to confuse them about all confidential messages.

According to Theorem 2.2, legitimate Receiver $k \in [1, K]$ will be able to reliably infer $U_\ell\big[\mathcal{L}^{(n)}_{V_\ell|V_{\ell-1}Y_k}\big]$ given Y^n_k and $U_\ell\big[\big(\mathcal{L}^{(n)}_{V_\ell|V_{\ell-1}Y_k}\big)^{\mathrm{C}}\big]$. Moreover, by Proposition 3.4, we have $\big(\mathcal{L}^{(n)}_{V_\ell|V_{\ell-1}Y_\ell}\big)^{\mathrm{C}} \supseteq \big(\mathcal{L}^{(n)}_{V_\ell|V_{\ell-1}Y_k}\big)^{\mathrm{C}}$ for any $\ell < k$. Consequently, given $U_\ell\big[\big(\mathcal{L}^{(n)}_{V_\ell|V_{\ell-1}Y_\ell}\big)^{\mathrm{C}}\big]$, legitimate Receivers ℓ–K will be able to reliably reconstruct U^n_ℓ from its own channel observations. Therefore, the PCS must make the entries $U_\ell(j)$ such that j belongs to $\mathcal{F}^{(n)}_\ell = \mathcal{H}^{(n)}_{V_\ell|V_{\ell-1}Y_\ell}$ and $\big(\mathcal{H}^{(n)}_{V_\ell|V_{\ell-1}Y_\ell}\big)^{\mathrm{C}} \setminus \mathcal{L}^{(n)}_{V_\ell|V_{\ell-1}Y_\ell}$ (hatched areas in Figure 3.3) available to Receivers ℓ–K. In this sense, the random sequence provided by a source of common randomness that is available to all parties will be stored into $U_\ell\big[\mathcal{F}^{(n)}_\ell\big]$. Since, by Proposition 3.4, $\mathcal{F}^{(n)}_\ell \subseteq \mathcal{H}^{(n)}_{V_\ell|V_{\ell-1}Z_m}$ for any $m \in [1, M]$, the use of this source will not compromise the secrecy condition. Otherwise, $U_\ell\big[\big(\mathcal{H}^{(n)}_{V_\ell|V_{\ell-1}Y_\ell}\big)^{\mathrm{C}} \setminus \mathcal{L}^{(n)}_{V_\ell|V_{\ell-1}Y_\ell}\big]$ will contain secret information or elements that cannot be known directly by eavesdroppers without compromising the secrecy. Hence, the transmitter somehow will additionally and secretly send it to the corresponding legitimate receivers.

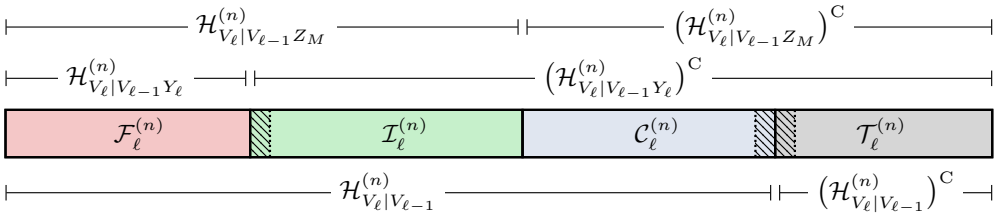

Figure 3.4: Polar code construction for the DBC-LD-NLS at the ℓ-th layer. The hatched area represents those indices $j \in \big(\mathcal{H}^{(n)}_{V_\ell|V_{\ell-1}Y_\ell}\big)^{\mathrm{C}} \setminus \mathcal{L}^{(n)}_{V_\ell|V_{\ell-1}Y_\ell}$, which can belong to the sets $\mathcal{I}^{(n)}_\ell$, $\mathcal{C}^{(n)}_\ell$ or $\mathcal{T}^{(n)}_\ell$.

As mentioned in Section 3.2.1, the goal of the polar construction is to obtain, with as low complexity as possible, the entropy terms associated with the sets in Equations (3.21)–(3.25) and then define the partition of $[1, n]$ given in Equations (3.26)–(3.29).

3.3.2 Polar encoding

The polarization-based encoder consists of K encoding blocks operating sequentially at each superposition layer, the block at layer $\ell \in [1, K]$ being responsible for the construction of $\tilde{U}^n_\ell$.

In order to construct $\tilde{U}_\ell^n$ for some $\ell \in [2, K]$, the encoder block needs $\tilde{V}_{\ell-1}^n = \tilde{U}_{\ell-1}^n G_n$, which has been constructed previously by the encoding block operating at the $(\ell-1)$-th layer.

Consider the encoding procedure at layer $\ell \in [1, K]$, which is summarized in Algorithm 3.3. Let W_ℓ and C_ℓ be uniformly-distributed random vectors of size $\left|\mathcal{I}_\ell^{(n)}\right|$ and $\left|\mathcal{C}_\ell^{(n)}\right|$, respectively, where W_ℓ represents the message intended for Receivers ℓ–K, and C_ℓ the local randomness required at the ℓ-th layer to confuse all eavesdroppers about this message. Moreover, let F_ℓ be a uniformly-distributed random $\left|\mathcal{F}_\ell^{(n)}\right|$-sequence, which represents the source of common randomness that is available to all parties. At each layer, notice in Algorithm 3.1 that the encoder constructs $\tilde{U}_\ell\big[\mathcal{H}_{V_\ell|V_{\ell-1}}^{(n)}\big] = \tilde{U}_\ell\big[\mathcal{I}_\ell^{(n)} \cup \mathcal{C}_\ell^{(n)} \cup \mathcal{F}_\ell^{(n)}\big]$ from W_ℓ, C_ℓ and F_ℓ.

Algorithm 3.3 Polar encoding for the DBC-LD-NLS

Require: Messages $\{W_\ell\}_{\ell=1}^K$; common randomness $\{F_\ell\}_{\ell=1}^K$; local randomness $\{C_\ell\}_{\ell=1}^K$; and secret keys $\{\kappa_{\Phi_\ell}\}_{\ell=1}^K$.

$\tilde{V}_0^n \leftarrow \varnothing$
for $\ell = 1$ to K **do** ▷ Encoding block for the ℓ-th layer
  $\tilde{U}_\ell\big[\mathcal{I}_\ell^{(n)}\big] \leftarrow W_\ell$
  $\tilde{U}_\ell\big[\mathcal{C}_\ell^{(n)}\big] \leftarrow C_\ell$
  $\tilde{U}_\ell\big[\mathcal{F}_\ell^{(n)}\big] \leftarrow F_\ell$
  for $j \in \mathcal{T}_\ell^{(n)}$ **do**
    if $j \in \big(\mathcal{H}_{V_\ell|V_{\ell-1}}^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{L}_{V_\ell|V_{\ell-1}}^{(n)}$ **then**
      $\tilde{U}_\ell(j) \leftarrow p_{U_\ell(j)|U_\ell^{1:j-1}V_{\ell-1}^n}\big(\tilde{U}_\ell^{1:j-1}, \tilde{V}_{\ell-1}^n\big)$
    else if $j \in \mathcal{L}_{V_\ell|V_{\ell-1}}^{(n)}$ **then**
      $\tilde{U}_\ell(j) \leftarrow \arg\max_{u\in\mathcal{V}_\ell} p_{U_\ell(j)|U_\ell^{1:j-1}V_{\ell-1}^n}\big(u\big|\tilde{U}_\ell^{1:j-1}, \tilde{V}_{\ell-1}^n\big)$
    end if
  end for
  $\tilde{V}_\ell^n = \tilde{U}_\ell^n G_n$
  $\Phi_\ell \leftarrow \tilde{U}_\ell\big[\big(\mathcal{H}_{V_\ell|V_{\ell-1}Y_\ell}^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{L}_{V_\ell|V_{\ell-1}Y_\ell}^{(n)}\big]$
  Send $\Phi_\ell \oplus \kappa_{\Phi_\ell}$ to legitimate Receivers ℓ–K.
end for
return $\tilde{V}_\ell^n$

Given $\tilde{U}_\ell\big[\mathcal{H}_{V_\ell|V_{\ell-1}}^{(n)}\big]$, the encoding forms $\tilde{U}_\ell\big[\mathcal{T}_\ell^{(n)}\big]$ as follows. If $j \in \mathcal{L}_{V_\ell|V_{\ell-1}}^{(n)}$, it constructs $\tilde{U}_\ell(j)$ deterministically by using SC encoding. Otherwise, if $j \in \big(\mathcal{H}_{V_\ell|V_{\ell-1}}^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{L}_{V_\ell|V_{\ell-1}}^{(n)}$ then $\tilde{U}_\ell(j)$ is constructed randomly from the distribution $p_{U_\ell(j)|U_\ell^{1:j-1}V_{\ell-1}^n}$. After constructing $\tilde{U}_\ell^n$, the ℓ-th encoding block computes the sequence $\tilde{V}_\ell^n = \tilde{U}_\ell^n G_n$ and delivers it to the next encoding block. If $\ell = K$, then $\tilde{V}_K^n \triangleq \tilde{X}^n$, and the encoder transmits it over the DBC, which induces the channel output observations $(\tilde{Y}_K^n, \ldots, \tilde{Y}_1^n, \tilde{Z}_M^n, \ldots, \tilde{Z}_1^n)$.

Besides the sequence $\tilde{V}_\ell^n$, the encoding block for the ℓ-th superposition layer obtains

$$\Phi_\ell \triangleq \tilde{U}_\ell\big[\big(\mathcal{H}^{(n)}_{V_\ell|V_{\ell-1}Y_\ell}\big)^{\mathrm{C}} \setminus \mathcal{L}^{(n)}_{V_\ell|V_{\ell-1}Y_\ell}\big], \tag{3.30}$$

which must be additionally transmitted to legitimate Receivers ℓ–K keeping it masked from all eavesdroppers. To do so, the transmitter performs a modulo-two addition between Φ_ℓ and a uniformly distributed secret key κ_{Φ_ℓ} that is privately shared with the legitimate Receivers ℓ–K and somehow additionally send it to them. If $K \ll n$, by Theorem 2.1, we know that the cost of the overall transmission is asymptotically negligible in terms of rate.

As for the previous model (see Remark 3.2), the uniformly-distributed part of any Φ_ℓ could be made available to the corresponding legitimate receivers by using a chaining structure as in [SV13]. In this model, notice that the encoding block operating at superposition layer $\ell \in [1, K]$ would be responsible for the chaining construction that conveys Φ_ℓ.

3.3.3 Polar decoding

Suppose that $\{F_\ell\}_{\ell=1}^K$ are available to all parties and the sequences $\{\Phi_\ell\}_{\ell=1}^K$ have been successfully received by the corresponding legitimate receivers. The decoding process at legitimate Receiver $k \in [1, K]$ constructs the estimates $\{\hat{U}_k^n\}_{k=1}^K$ of $\{\tilde{U}_k^n\}_{k=1}^K$ in a sequential manner, from $\hat{U}_1^n$ to $\hat{U}_k^n$, and is summarized in Algorithm 3.4.

Consider the construction of $\hat{U}_\ell^n$ for any $\ell \in [1, k]$. Given F_ℓ and Φ_ℓ, notice that Receiver k knows $\tilde{U}_\ell\big[\big(\mathcal{L}^{(n)}_{V_\ell|V_{\ell-1}Y_\ell}\big)^{\mathrm{C}}\big]$. Since, by Proposition 3.4, $\big(\mathcal{L}^{(n)}_{V_\ell|V_{\ell-1}Y_\ell}\big)^{\mathrm{C}} \supseteq \big(\mathcal{L}^{(n)}_{V_\ell|V_{\ell-1}Y_k}\big)^{\mathrm{C}}$ for any $\ell \in [1, k]$, Receiver k performs SC decoding to construct $\hat{U}_\ell^n$ from $\tilde{U}_\ell\big[\big(\mathcal{L}^{(n)}_{V_\ell|V_{\ell-1}Y_\ell}\big)^{\mathrm{C}}\big]$ and its channel output observations $\tilde{Y}_k^n$. In Section 3.3.4, we show formally that the reliability condition in Equation (3.4) is satisfied for all legitimate receivers.

Algorithm 3.4 Decoding at Receiver $k \in [1, K]$ for the DBC-LD-NLS

Require: Common randomness $\{F_\ell\}_{\ell=1}^k$; additional sequences $\{\Phi_\ell\}_{\ell=1}^k$

$\hat{V}_0 \leftarrow \varnothing$
for $\ell = 1$ to k **do**
  $\hat{U}_\ell\big[\big(\mathcal{L}^{(n)}_{V_\ell|V_{\ell-1}Y_\ell}\big)^{\mathrm{C}}\big] \leftarrow (F_\ell, \Phi_\ell)$
  for $j \in \mathcal{L}^{(n)}_{V_\ell|V_{\ell-1}Y_\ell}$ **do** ▷ SC decoding
    $\hat{U}_\ell(j) \leftarrow \arg\max_{u \in \mathcal{V}_\ell} p_{U_\ell(j)|U_\ell^{1:j-1}V_{\ell-1}^n Y_k^n}\big(u|\hat{U}_\ell^{1:j-1}\hat{V}_{\ell-1}^n\tilde{Y}_k^n\big)$
  end for
  $\hat{W}_\ell^{(n)} \leftarrow \hat{U}_\ell\big[\mathcal{I}_\ell^{(n)}\big]$
  $\hat{V}_\ell^n \leftarrow \hat{U}_\ell^n G_n$
end for
return $\{\hat{W}_\ell\}_{\ell=1}^k$

3.3.4 Performance of the polar coding scheme

The analysis of the previous polar coding scheme leads to the following theorem.

Theorem 3.2. *Let* $\left(\mathcal{X}, p_{Y_K \dots Y_1 Z_M \dots Z_1|X}, \mathcal{Y}_K \times \cdots \times \mathcal{Y}_1 \times \mathcal{Z}_M \times \cdots \times \mathcal{Z}_1\right)$ *be an arbitrary DBC such that* $\mathcal{X} \in \{0,1\}$ *and the distribution* $p_{Y_K \dots Y_1 Z_M \dots Z_1|X}$ *satisfies the Markov chain condition* $X - Y_K - \cdots - Y_1 - Z_M - \cdots - Z_1$. *The polar coding scheme described in Sections 3.3.1–3.3.3 achieves any rate tuple of the achievable region defined in Corollary 3.2.*

Corollary 3.4. *Since* $\tilde{U}_\ell[\mathcal{I}_\ell^{(n)}]$ *for some* $\ell \in [1, K]$ *can contain any information to be reliably decoded by the legitimate receivers* ℓ*–*K*, the coding scheme in Sections 3.3.1–3.3.3 can achieve the entire region considering rate sharing of Proposition 3.2 by storing part of any message* $W_{\ell'}$ *such that* $\ell' > \ell$ *into* $\tilde{U}_\ell[\mathcal{I}_\ell^{(n)}]$ *instead of part of* W_ℓ.

First, we prove that the PCS approaches the corner point of the region defined in Corollary 3.2. Second, we show that the joint distribution $\tilde{q}_{V_1^n \dots V_K^n Y_K^n \dots Y_1^n Z_M^n \dots Z_1^n}$ of $\left(\tilde{V}_1^n, \dots, \tilde{V}_K^n, \tilde{Y}_K^n, \dots, \tilde{Y}_1^n, \tilde{Z}_M^n, \dots, \tilde{Z}_1^n\right)$ induced by the encoder described in Section 3.3.2 is statistically close to the distribution $p_{V_1^n \dots V_K^n Y_K^n \dots Y_1^n Z_M^n \dots Z_1^n}$ of the original DMS from which the polarization sets were defined. Finally, in steps three and four, we prove that the PCS satisfy the reliability and the strong secrecy conditions given in Equation (3.4) and Equation (3.5), respectively. On the other hand, the proof of Corollary 3.4 is immediate.

Transmission Rates

For any $\ell \in [1, K]$, the transmission rate R_ℓ corresponding to the message W_ℓ satisfies

$$\begin{aligned}
\lim_{n\to\infty} R_\ell &= \lim_{n\to\infty} \frac{1}{n}\left|\mathcal{I}_\ell^{(n)}\right| \overset{(a)}{=} \lim_{n\to\infty} \frac{1}{n}\left|\mathcal{H}^{(n)}_{V_\ell|V_{\ell-1}Z_M} \setminus \mathcal{H}^{(n)}_{V_\ell|V_{\ell-1}Y_\ell}\right| \\
&\overset{(b)}{=} \lim_{n\to\infty} \frac{1}{n}\left|\mathcal{H}^{(n)}_{V_\ell|V_{\ell-1}Z_M}\right| - \lim_{n\to\infty} \frac{1}{n}\left|\mathcal{H}^{(n)}_{V_\ell|V_{\ell-1}Y_\ell}\right| \\
&\overset{(c)}{=} I(V_\ell; Y_\ell|V_{\ell-1}) - I(V_\ell; Z_M|V_{\ell-1}),
\end{aligned}$$

where (a) follows from the definition of the set $\mathcal{I}_\ell^{(n)}$ in Equation (3.26), (b) holds because, by Proposition 3.4, $\mathcal{H}^{(n)}_{V_\ell|V_{\ell-1}Z_M} \supseteq \mathcal{H}^{(n)}_{V_\ell|V_{\ell-1}Y_\ell}$ for any $\ell \in [1, K]$, and (c) holds by Theorem 2.1.

Distribution of the DMS after the polar encoding

Let $\tilde{q}_{U_1^n \dots U_K^n}$ be the distribution of $(\tilde{U}_1^n, \dots, \tilde{U}_K^n)$ after the encoding in Section 3.3.2. The following lemma shows that $\tilde{q}_{U_1^n \dots U_K^n}$ and $p_{U_1^n \dots U_K^n}$ of the original DMS given in Equation (3.20) are nearly statistically indistinguishable for sufficiently large n and, consequently, so are the overall distributions $\tilde{q}_{V_1^n \dots V_K^n Y_K^n \dots Y_1^n Z_M^n \dots Z_1^n}$ and $p_{V_1^n \dots V_K^n Y_K^n \dots Y_1^n Z_M^n \dots Z_1^n}$.

Lemma 3.2. *Let $\delta_n = 2^{-n^\beta}$ for some $\beta \in \left(0, \frac{1}{2}\right)$. Then,*

$$\begin{aligned}\mathbb{V}(\tilde{q}_{U_1^n \ldots U_K^n}, p_{U_1^n \ldots U_K^n}) &\leq \delta_{\text{ld-nls}}^{(n)},\\ \mathbb{V}(\tilde{q}_{V_1^n \ldots V_K^n Y_K^n \ldots Y_1^n Z_M^n \ldots Z_1^n}, p_{V_1^n \ldots V_K^n Y_K^n \ldots Y_1^n Z_M^n \ldots Z_1^n}) &= \mathbb{V}(\tilde{q}_{U_1^n \ldots U_K^n}, p_{U_1^n \ldots U_K^n}) \leq \delta_{\text{ld-nls}}^{(n)},\end{aligned}$$

where $\delta_{\text{ld-nls}}^{(n)} \triangleq nK\sqrt{2\sqrt{4n\delta_n \ln 2}\big(\ell n - \log\sqrt{n\delta_n 4\ln 2}\big) + \delta_n} + \sqrt{n\delta_n 4\ln 2}$.

Proof. For the first claim, see Lemma 2.3 and Corollary 2.1 taking $T_{\mathrm{V}} \triangleq K$. The second claim holds by Corollary 2.2 because $\tilde{q}_{V_1^n \ldots V_K^n Y_K^n \ldots Y_1^n Z_M^n \ldots Z_1^n} \equiv \tilde{q}_{V_1^n \ldots V_K^n} p_{Y_K^n \ldots Y_1^n Z_M^n \ldots Z_1^n | X^n}$. □

Remark 3.4. *The first term of $\delta_{\text{ld-nls}}^{(n)}$ models the impact on the total variation distance of using deterministic SC encoding for $\tilde{U}_\ell\big[\mathcal{L}_{V_\ell|V_{\ell-1}}^{(n)}\big]$. The second term bounds the impact of storing uniformly-distributed random sequences that are independent of $\tilde{V}_{\ell-1}^n$ into $\tilde{U}_\ell\big[\mathcal{H}_{V_\ell|V_{\ell-1}}^{(n)}\big]$.*

Reliability Performance

Consider the probability of incorrectly decoding $\{W_\ell\}_{\ell=1}^k$ at legitimate Receiver $k \in [1, K]$. Let $\tilde{q}_{V_\ell^n Y_k^n}$ and $p_{V_\ell^n Y_k^n}$ be marginals of $\tilde{q}_{V_1^n \ldots V_K^n Y_K^n \ldots Y_1^n Z_M^n \ldots Z_1^n}$ and $p_{V_1^n \ldots V_K^n Y_K^n \ldots Y_1^n Z_M^n \ldots Z_1^n}$, respectively, where $\ell \in [1, k]$. Consider an optimal coupling [LPW09] (Proposition 4.7) between $\tilde{q}_{V_\ell^n Y_k^n}$ and $p_{V_\ell^n Y_k^n}$ such that

$$\mathbb{P}\big[\mathcal{E}_{V_\ell^n Y_k^n}\big] = \mathbb{V}(\tilde{q}_{V_\ell^n Y_k^n}, p_{V_\ell^n Y_k^n}),$$

where $\mathcal{E}_{V_\ell^n Y_k^n} \triangleq \{(\tilde{V}_\ell^n, \tilde{Y}_k^n) \neq (V_\ell^n, Y_k^n)\}$ or, equivalently, $\mathcal{E}_{V_\ell^n Y_k^n} \triangleq \{(\tilde{U}_\ell^n, \tilde{Y}_k^n) \neq (U_\ell^n, Y_k^n)\}$ due to the invertibility of G_n. Furthermore, for all $\ell \in [1, k]$, we define the error event $\mathcal{E}_{\hat{V}_\ell^n} \triangleq \{\hat{V}_\ell^n \neq \tilde{V}_\ell^n\}$, and $\mathcal{E}_{\hat{V}_0^n} \triangleq \emptyset$. Hence, for any $\ell \in [1, k]$, the average probability of incorrectly decoding the message W_ℓ at the k-th receiver can be upper-bounded as

$$\begin{aligned}\mathbb{P}[\hat{W}_\ell \neq W_\ell] &\leq \mathbb{P}\big[\hat{U}_\ell^n \neq \tilde{U}_\ell^n \big| \mathcal{E}^{\mathrm{C}}_{V_\ell^n Y_k^n} \cap \mathcal{E}^{\mathrm{C}}_{\hat{V}_{\ell-1}^n}\big]\mathbb{P}\big[\mathcal{E}^{\mathrm{C}}_{V_\ell^n Y_k^n} \cap \mathcal{E}^{\mathrm{C}}_{\hat{V}_{\ell-1}^n}\big]\\ &\quad + \mathbb{P}\big[\hat{U}_\ell^n \neq \tilde{U}_\ell^n \big| \mathcal{E}_{V_\ell^n Y_k^n} \cup \mathcal{E}_{\hat{V}_{\ell-1}^n}\big]\mathbb{P}\big[\mathcal{E}_{V_\ell^n Y_k^n} \cup \mathcal{E}_{\hat{V}_{\ell-1}^n}\big]\\ &\leq \mathbb{P}\big[\hat{U}_\ell^n \neq \tilde{U}_\ell^n \big| \mathcal{E}^{\mathrm{C}}_{V_\ell^n Y_k^n} \cap \mathcal{E}^{\mathrm{C}}_{\hat{V}_{\ell-1}^n}\big] + \mathbb{P}\big[\mathcal{E}_{V_\ell^n Y_k^n} \cup \mathcal{E}_{\hat{V}_{\ell-1}^n}\big]\\ &\overset{(a)}{\leq} \mathbb{P}\big[\hat{U}_\ell^n \neq \tilde{U}_\ell^n \big| \mathcal{E}^{\mathrm{C}}_{V_\ell^n Y_k^n} \cap \mathcal{E}^{\mathrm{C}}_{\hat{V}_{\ell-1}^n}\big] + \mathbb{P}\big[\mathcal{E}_{V_\ell^n Y_k^n}\big] + \mathbb{P}\big[\mathcal{E}_{\hat{V}_{\ell-1}^n}\big]\\ &\overset{(b)}{\leq} n\delta_n + \mathbb{P}\big[\mathcal{E}_{V_\ell^n Y_k^n}\big] + \mathbb{P}\big[\mathcal{E}_{\hat{V}_{\ell-1}^n}\big]\\ &\overset{(c)}{\leq} n\delta_n + \delta_{\text{ld-nls}}^{(n)} + \mathbb{P}\big[\mathcal{E}_{\hat{V}_{\ell-1}^n}\big]\\ &\overset{(d)}{\leq} i\big(n\delta_n + \delta_{\text{ld-nls}}^{(n)}\big),\end{aligned} \tag{3.31}$$

where (a) holds by the union bound; (b) holds by Theorem 2.2 because for $\ell \in [1,k]$ recall that $\tilde{U}_\ell\big[\big(\mathcal{L}^{(n)}_{V_\ell|V_{\ell-1}Y_\ell}\big)^{\mathrm{C}}\big]$ is available to legitimate Receiver k and $\big(\mathcal{L}^{(n)}_{V_\ell|V_{\ell-1}Y_\ell}\big)^{\mathrm{C}} \supseteq \big(\mathcal{L}^{(n)}_{V_\ell|V_{\ell-1}Y_k}\big)^{\mathrm{C}}$, and we have assumed $\hat{V}^n_{\ell-1} = \tilde{V}^n_{\ell-1}$; (c) holds by the optimal coupling and by Lemma 3.2; and (d) holds by induction. Thus, by the union bound, we obtain

$$\mathbb{P}\big[(\hat{W}_1,\dots\hat{W}_k) \neq (W_1,\dots,W_k)\big] \leq \sum_{\ell=1}^{k} \mathbb{P}\big[\hat{U}_\ell \neq \tilde{U}_\ell\big] \leq \frac{k(k+1)}{2}\big(n\delta_n + \delta^{(n)}_{\text{ld-nls}}\big). \tag{3.32}$$

Consequently, if $K \ll n$, the PCS satisfies the reliability condition in (3.4) because the probability of incorrectly decoding $\{W_\ell\}_{\ell=1}^k$ at Receiver $k \in [1,K]$ is in $O\big(n^{\frac{7}{4}}2^{-n^\beta}\big) \xrightarrow{n\to\infty} 0$.

Secrecy Performance

The secrecy condition in Equation 3.5 requires Eavesdropper $m \in [1,M]$ to be kept ignorant about all messages $\{W_m\}_{m=1}^M$. Due to the existence of the source of common randomness for each encoding layer, the information leakage at Eavesdropper $m \in [1,M]$ is given by $I\big(W_1\dots W_K; \tilde{Z}^n_m F_1 \dots F_K\big)$. Hence, for sufficiently large n we have

$$\begin{aligned}
&I\big(W_1\dots W_K; \tilde{Z}^n_m F_1\dots F_K\big)\\
&\overset{(a)}{\leq} I\big(W_1\dots W_K F_1\dots F_K; \tilde{Z}^n_m\big)\\
&\overset{(b)}{\leq} I\big(\tilde{U}_1\big[\mathcal{I}^{(n)}_1 \cup \mathcal{F}^{(n)}_1\big]\dots\tilde{U}_K\big[\mathcal{I}^{(n)}_K \cup \mathcal{F}^{(n)}_K\big]; \tilde{Z}^n_m\big)\\
&\overset{(c)}{=} \sum_{\ell=1}^{K}\big|\mathcal{I}^{(n)}_\ell \cup \mathcal{F}^{(n)}_\ell\big| - H\big(\tilde{U}_1\big[\mathcal{I}^{(n)}_1 \cup \mathcal{F}^{(n)}_1\big]\dots\tilde{U}_K\big[\mathcal{I}^{(n)}_K \cup \mathcal{F}^{(n)}_K\big]\big|\tilde{Z}^n_m\big)\\
&\overset{(d)}{\leq} \sum_{\ell=1}^{K}\big|\mathcal{I}^{(n)}_\ell \cup \mathcal{F}^{(n)}_\ell\big| - H\big(U_1\big[\mathcal{I}^{(n)}_1 \cup \mathcal{F}^{(n)}_1\big]\dots U_K\big[\mathcal{I}^{(n)}_K \cup \mathcal{F}^{(n)}_K\big]\big|Z^n_m\big)\\
&\quad + (K+2)n\delta^{(n)}_{\text{ld-nls}} - 2\delta^{(n)}_{\text{ld-nls}}\log\delta^{(n)}_{\text{ld-nls}}\\
&\overset{(e)}{\leq} Kn\delta_n + (K+2)n\delta^{(n)}_{\text{ld-nls}} - 2\delta^{(n)}_{\text{ld-nls}}\log\delta^{(n)}_{\text{ld-nls}}
\end{aligned} \tag{3.33}$$

where (a) holds by independence between $\{W_k\}_{k=1}^K$ and $\{F_k\}_{k=1}^K$; (b) follows from the encoding in Algorithm 3.3; (c) holds by the uniformity of $\{W_k\}_{k=1}^K$ and $\{F_k\}_{k=1}^K$; (d) follows from applying Lemma 2.4 (taking $T_{\mathrm{V}} \triangleq K$ and $T_{\mathrm{O}} \triangleq 1$) and by Lemma 3.2; and (e) holds because, since conditioning does not increase entropy, we have

$$H\big(U_1\big[\mathcal{I}^{(n)}_1 \cup \mathcal{F}^{(n)}_1\big]\dots U_K\big[\mathcal{I}^{(n)}_K \cup \mathcal{F}^{(n)}_K\big]\big|Z^n_m\big) \geq \sum_{\ell=1}^{K}\sum_{j\in\mathcal{I}^{(n)}_\ell\cup\mathcal{F}^{(n)}_\ell} H\big(U_\ell(j)\big|U^{1:j-1}_\ell V^n_{\ell-1}Z^n_m\big),$$

and then by the definition of $\mathcal{I}_\ell^{(n)}$ and $\mathcal{F}_\ell^{(n)}$, which according to Proposition 3.4 are subsets of $\mathcal{H}_{V_\ell|V_{\ell-1}Z_m}$ for any $\ell \in [1,K]$ and $m \in [1,M]$.

Therefore, the corresponding information leakage is in $O\big(n^{\frac{11}{4}}2^{-n^\beta}\big) \xrightarrow{n\to\infty} 0$ for Eavesdropper $m \in [1,M]$. Consequently, the PCS satisfies the strong secrecy condition given in Equation (3.5), and the proof of Theorem 3.2 is concluded.

3.4 Polar construction and performance evaluation

In this section, we discuss further how to construct the polar codes for the DBC-NLD-LS and DBC-LD-NLS proposed in Sections 3.2 and 3.3, respectively. Moreover, we evaluate the reliability and the secrecy performance of both PCSs according to different parameters involved in the polar code construction. As mentioned previously, although the construction of polar codes has been covered in a large number of references (for instance, see [TV13, VVH15, HY13]), they only focus on polar codes under reliability constraints.

For the DBC-NLD-LS, we consider the Binary Erasure Broadcast Channel (BE-BC), where each individual channel is a BEC. On the other hand, for the DBC-LD-NLS, we consider the Binary Symmetric Broadcast Channel (BS-BC), where each individual channel is a Binary Symmetric Channel (BSC). Throughout this section, as in [Ari09], we say that a channel or a distribution $p_{Y|X}(y|x)$ with $x \in \mathcal{X} \triangleq \{0,1\}$ and $y \in \mathcal{Y} \triangleq \{0,\dots,|\mathcal{Y}|-1\}$ is symmetric if the columns of the probability transition matrix $\mathbf{P}_{Y|X} \triangleq \begin{bmatrix} p_{Y|X}(0|0) & \cdots & p_{Y|X}(|\mathcal{Y}|-1|0) \\ p_{Y|X}(0|1) & \cdots & p_{Y|X}(|\mathcal{Y}|-1|1) \end{bmatrix}$ can be grouped into sub-matrices such that for each sub-matrix, each row is a permutation of each other row and each column is a permutation of each other column. Consequently, notice that the individual channels of both the BE-BC and the BS-BC are symmetric.

Due to the symmetry of BE-BC, we will see that the distribution induced by the encoding described in Section 3.2.2 for the DBC-NLD-LS will approach exactly the optimum distribution of the original DMS used in the polar code construction. Consequently, the performance of the polar code will depend only on the parameters involved in this construction. On the other hand, despite the symmetry of the BS-BC, due to the superposition-based structure, the encoding described in Section 3.3.2 for the DBC-LD-NLS only approaches the target distribution asymptotically. Hence, this encoding will impact the reliability and secrecy performance of the polar code when we consider a finite blocklength.

3.4.1 DBC-NLD-LS

For this model, we consider BE-BC with two legitimate receivers ($K = 2$) and two eavesdroppers ($M = 2$). Therefore, each individual channel is a BEC with $\mathcal{X} \triangleq \{0,1\}$ and

$\mathcal{Y}_k = \mathcal{Z}_m \triangleq \{0, 1, E\}$, E being the erasure symbol and $k, m \in \{1, 2\}$. The individual channels are defined simply by their erasure probability, which is denoted by ϵ_{Y_k} for the corresponding legitimate Receiver k ($\mathbb{P}[Y_k = E] = \epsilon_{Y_k}$) and ϵ_{Z_m} for the Eavesdropper m ($\mathbb{P}[Z_m = E] = \epsilon_{Z_m}$). Due to the degradedness condition of the broadcast channel given in Equation (3.1), we have $\epsilon_{Y_2} < \epsilon_{Y_1} < \epsilon_{Z_2} < \epsilon_{Z_1}$. By properly applying [BB11] (Proposition 3.2), it is easy to shown that the secrecy-capacity achieving distribution $p^\star_X$ for this model is the uniform, i.e., $p^\star_X(x) = \frac{1}{2}\ \forall x \in \{0, 1\}$. For the simulations, we consider a BE-BC such that $\epsilon_{Y_2} = 0.01$, $\epsilon_{Y_1} = 0.04$, $\epsilon_{Z_2} = 0.2$ and $\epsilon_{Z_1} = 0.35$. For this setting, the corner point $(R^\star_1, R^\star_2)$ of the secrecy-capacity region of Corollary 3.1 is such that $R^\star_1 = 0.15$ and $R^\star_2 = 0.16$.

Practical polar code construction

According to [Ari09] (Proposition 5) the Bhattacharyya parameters associated with the sets in Equations (3.7)–(3.11) can be computed exactly because each individual channel is a BEC. Moreover, by Lemma 2.1, this Bhattacharyya parameters match exactly with the entropy terms due to the symmetry of the BEC.

Given the blocklength n and the distribution $p^\star_{XY_2Y_1Z_2Z_1}$, the goal of the polar code construction is to obtain the partition of the universal set $[1, n]$ defined in (3.12)–(3.16) and graphically represented in Figure 3.3. Hence, we need to define first the required sets of indices defined in Equations (3.7)–(3.11), which means having to compute the entropy terms $\{H(U(j)|U^{1:j-1})\}_{j=1}^n$, $\{H(U(j)|U^{1:j-1}Y_1^n)\}_{j=1}^n$ and $\{H(U(j)|U^{1:j-1}Z_m^n)\}_{j=1}^n$ for all $m \in \{1, 2\}$ associated with the polar transform $U^n = X^n G_n$. Since each individual channel is a symmetric BEC, we can compute exactly the previous terms with very low complexity. To do so, we use the recursive algorithm [VVH15] (PCC-0) adapted to the BEC, which, for instance, will obtain $\{H(U(j)|U^{1:j-1}Y_1^n)\}_{j=1}^n$ from the initial value $H(X|Y_1) = \epsilon_{Y_1}$. Regarding $\{H(U(j)|U^{1:j-1})\}_{j=1}^n$, since $p^\star_X$ is uniform, it is clear that $H(U(j)|U^{1:j-1}) = 1$ for all $j \in [1, n]$, which means $\mathcal{H}_X^{(n)} = [1, n]$. Consequently, the set $\mathcal{T}^{(n)}$ of the partition in (3.12)–(3.16) is empty ($\mathcal{T}^{(n)} = \emptyset$) and, hence, according to Algorithm 3.1 neither random nor deterministic SC encoding will be needed.

In order to compare the performance of the PCS according to different parameters and provide flexibility in the design, instead of using only δ_n to define the sets in (3.7)–(3.11), we introduce the pair $\left(\delta_n^{(\mathrm{r})}, \delta_n^{(\mathrm{s})}\right)$, where $\delta_n^{(\mathrm{r})} \triangleq 2^{-n^{\beta^{(\mathrm{r})}}}$ and $\delta_n^{(\mathrm{s})} \triangleq 2^{-n^{\beta^{(\mathrm{s})}}}$ for $\beta^{(\mathrm{r})}, \beta^{(\mathrm{s})} \in \left(0, \frac{1}{2}\right)$. Let (R'_1, R'_2) such that $R'_1 \leq R^\star_1$ and $R'_2 \leq R^\star_2$ denote the target rates that the PCS must approach. Since the PCS must operate at particular rates (R'_1, R'_2), and not necessarily at secrecy-capacity, we obtain the partition in (3.12)–(3.16) as follows. First, we define $\left(\mathcal{H}_{X|Y_1}^{(n)}\right)^{\mathrm{C}} \triangleq \left\{j \in [1, n] : H\left(U(j)\left|U^{1:j-1}Y_1^n\right.\right) \leq 1 - \delta_n^{(\mathrm{s})}\right\}$, where one can notice that we have

used $\delta_n^{(\mathrm{s})}$. Then, we form $\mathcal{I}_2^{(n)}$ by taking the $\lceil nR_2' \rceil$ indices $j \in \big(\mathcal{H}_{X|Y_1}^{(n)}\big)^{\mathrm{C}}$ that correspond to the highest entropy terms $\{H(U(j)|U^{1:j-1}Z_2^n)\}_{j=1}^n$ associated to Eavesdropper 2. Second, we form $\mathcal{I}_1^{(n)}$ by taking the $\lceil nR_1' \rceil$ indices $j \in \big(\mathcal{H}_{X|Y_1}^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{I}_2^{(n)}$ that correspond to the highest entropy terms $\{H(U(j)|U^{1:j-1}, Z_1^n)\}_{j=1}^n$ for Eavesdropper 1. Finally, we obtain $\mathcal{C}^{(n)} = \big(\mathcal{H}_{X|Y_1}^{(n)}\big)^{\mathrm{C}} \setminus \big(\mathcal{I}_1^{(n)} \cup \mathcal{I}_2^{(n)}\big)$ and $\mathcal{F}^{(n)} = \mathcal{H}_{X|Y_1}^{(n)}$. Furthermore, in order to evaluate the reliability performance, we define $\mathcal{L}_{X|Y_1}^{(n)} \triangleq \big\{j \in [1,n] : H\big(U(j)\big|U^{1:j-1}Y_1^n\big) \leq \delta_n^{(\mathrm{r})}\big\}$, where one can notice that we have used $\delta_n^{(\mathrm{r})}$. Since the additional secret sequence Φ corresponds to those entries whose indices belong to $\big(\mathcal{H}_{X|Y_1}^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{L}_{X|Y_1}^{(n)}$, its length will depend on $\big(\delta_n^{(\mathrm{r})}, \delta_n^{(\mathrm{s})}\big)$. According to the polar code construction proposed in this section, notice that $\delta_n^{(\mathrm{s})}$ must be small enough to guarantee that $\frac{1}{n}\big|\big(\mathcal{H}_{X|Y_1}^{(n)}\big)^{\mathrm{C}}\big| \geq R_1' + R_2'$.

Performance evaluation

The encoding of Algorithm 3.1 induces a distribution $\tilde{q}_{X^nY_2^nY_1^nZ_2^nZ_1^n} \equiv p^{\star}_{X^nY_2^nY_1^nZ_2^nZ_1^n}$ because $\mathcal{T}^{(n)} = \emptyset$ (we do not use SC encoding) and the encoder will store uniformly-distributed sequences into entries $U(j)$ that satisfy $H(U(j)|U^{1:j-1}) = 1$ for all $j \in \mathcal{H}_X^{(n)} = [1,n]$. Therefore, we have $V_{\tilde{q}p^{\star}} \triangleq \mathbb{V}(\tilde{q}_{X^nY_2^nY_1^nZ_2^nZ_1^n}, p^{\star}_{X^nY_2^nY_1^nZ_2^nZ_1^n}) = 0$, and the performance only depends on the code construction.

To evaluate the reliability performance, we obtain an upper-bound $P_{\mathrm{b}}^{\mathrm{ub}(1)}$ on the average bit error probability at legitimate Receiver 1. Since $V_{\tilde{q}p^{\star}} = 0$, from Equation (3.18) we obtain

$$P_{\mathrm{b}}^{\mathrm{ub}(1)} \triangleq \frac{1}{\big|\mathcal{L}_{X|Y_1}^{(n)}\big|}\mathbb{P}\big[\hat{U}^n \neq U^n\big] = \frac{1}{\big|\mathcal{L}_{X|Y_1}^{(n)}\big|}\sum_{j\in\mathcal{L}_{X|Y_1}^{(n)}} H\big(U(j)\big|U^{1:j-1}Y_1^n\big), \tag{3.34}$$

where we have used the fact that $U\big[\big(\mathcal{L}_{X|Y_1}^{(n)}\big)^{\mathrm{C}}\big]$ is available to legitimate Receiver 1, [Ari10] (Theorem 2) to tight the bound in (3.18), and Lemma 2.1. Because of the degradedness condition of the BE-BC and, consequently, by Proposition 3.3, the average bit error probability at legitimate Receiver 2 will be always less than the one at legitimate Receiver 1. Since SC decoding requires both legitimate receivers to estimate all the entries belonging to $\mathcal{L}_{X|Y_1}^{(n)}$ regardless of $\big(\mathcal{H}_{X|Y_1}^{(n)}\big)^{\mathrm{C}}$ and the target rates (R_1', R_2'), the reliability performance for the proposed code construction only depends on the pair $(n, \delta_n^{(\mathrm{r})})$.

In order to evaluate the secrecy performance, from Equation (3.19), we compute an upper-bound $I^{\mathrm{ub}}(W_1W_2; \tilde{Z}_1^nF)$ on the information leakage corresponding to Eavesdropper 1:

$$I^{\mathrm{ub}}(W_1W_2; \tilde{Z}_1^nF) \triangleq \sum_{i=1}^{2}\big|\mathcal{I}_i^{(n)}\big| + \big|\mathcal{F}^{(n)}\big| - \sum_{j\in\mathcal{I}_1^{(n)}\cup\mathcal{I}_2^{(n)}\cup\mathcal{F}^{(n)}} H\big(U(j)\big|U^{1:j-1}Z_1^n\big), \tag{3.35}$$

where we have applied the chain rule and the fact that conditioning does not increase the entropy to tight the bound in Equation (3.19). Similarly, we compute an upper-bound $I^{\mathrm{ub}}(W_2; \tilde{Z}_2^n F)$ on the information leakage corresponding to Eavesdropper 2:

$$I^{\mathrm{ub}}(W_2; \tilde{Z}_2^n F) \triangleq \left|\mathcal{I}_2^{(n)}\right| + \left|\mathcal{F}^{(n)}\right| - \sum_{j \in \mathcal{I}_2^{(n)} \cup \mathcal{F}^{(n)}} H\big(U(j)\big|U^{1:j-1} Z_2^n\big), \tag{3.36}$$

According to the proposed polar code construction, the secrecy performance will depend on $(n, \delta_n^{(\mathrm{s})})$ and the rates (R_1', R_2'), but not on $\delta_n^{(\mathrm{r})}$.

Additionally, we evaluate the rate of the additional sequence Φ simply by computing:

$$\frac{1}{n}|\Phi| = \frac{1}{n}\Big|\big(\mathcal{H}_{X|Y_1}^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{L}_{X|Y_1}^{(n)}\Big|, \tag{3.37}$$

which will depend on the triple $(n, \delta_n^{(\mathrm{r})}, \delta_n^{(\mathrm{s})})$, but not on (R_1', R_2').

Let ρ_{R} be the normalized target rate in which the polar coding scheme operates, that is $\rho_{\mathrm{R}} \triangleq \frac{R_1'}{R_1^*} = \frac{R_2'}{R_2^*}$. In Figure 3.5A,B, we evaluate the upper-bounds on the information leakage defined in Equations (3.35) and (3.36), respectively, as a function of the blocklength n for different values of ρ_{R}. To do so, we set $\beta^{(\mathrm{r})} = 0.16$ and $\beta^{(\mathrm{s})} = 0.30$, which defines a particular pair $(\delta_n^{(\mathrm{r})}, \delta_n^{(\mathrm{s})})$ for each value of n (recall that $\delta_n^{(\mathrm{r})}$ does not impact on the secrecy performance of the polar code). As we proved in Section 3.2.4, for large enough n, the secrecy performance improves as n increases.

Moreover, to achieve a particular secrecy performance level, notice that the polar code will require a larger blocklength n as the rates approach the capacity. This happens because, given $(n, \delta_n^{(\mathrm{s})})$ and, consequently, $\big(\mathcal{H}_{X|Y_1}^{(n)}\big)^{\mathrm{C}}$, the parameter ρ_{R} only determines the amount of indices that will belong to $\mathcal{I}_1^{(n)} \cup \mathcal{I}_2^{(n)} \subseteq \big(\mathcal{H}_{X|Y_1}^{(n)}\big)^{\mathrm{C}}$. Since, by construction, we take those indices corresponding to the highest entropy terms associated with the eavesdroppers, taking more elements always increases the corresponding leakage.

For rates approaching the capacity and small values of n, notice that we obtain a secrecy performance that is getting worse as n increases (for instance, for $\rho_{\mathrm{R}} = 0.94$, we obtain that the information leakage is increasing from $n = 2^9$ to $n = 2^{12}$). This behavior is mainly explained because the elements of U^n have not polarized enough for small values of n. Consequently, for a given value of $\beta^{(\mathrm{s})}$, not all the entropy terms associated with the eavesdroppers corresponding to the sets $\mathcal{I}_1^{(n)}$ and $\mathcal{I}_2^{(n)}$ are sufficiently close to one. Since, for a given ρ_{R}, the cardinality of $\mathcal{I}_1^{(n)}$ and $\mathcal{I}_2^{(n)}$ increases with n, then the information leakage can increase with n when it is not large enough. Moreover, since operating at lower rates means taking a fewer number of indices in $\mathcal{I}_1^{(n)}$ and $\mathcal{I}_2^{(n)}$, but taking those that are closest to one, this behavior appears only for large values of ρ_{R}.

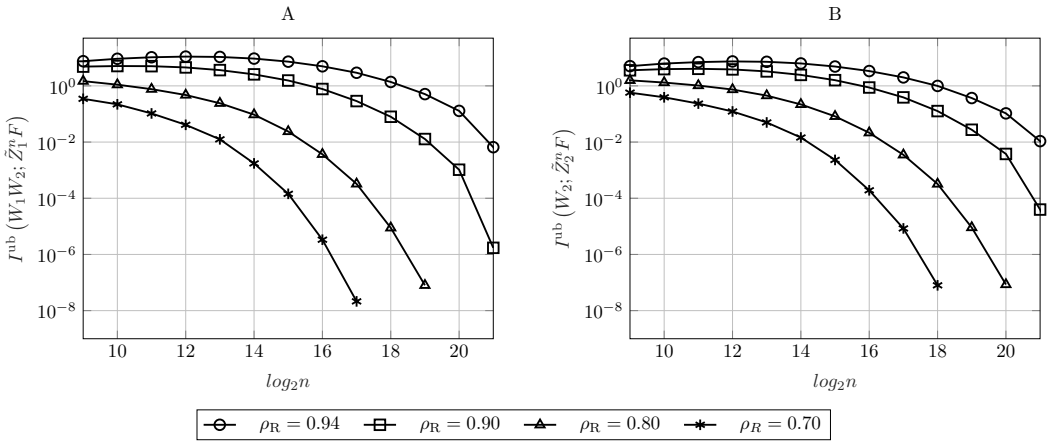

Figure 3.5: Secrecy performance of the polar coding scheme for the DBC-NLD-LS over the BE-BC as a function of the blocklength n and the normalized target rate ρ_{R} when we set $\beta^{(\text{r})} = 0.16$ and $\beta^{(\text{s})} = 0.30$. (**A**) Upper-bound on the information about (W_1, W_2) leaked to Eavesdropper 1 defined as in Equation (3.35). (**B**) Upper-bound on the information about W_2 leaked to Eavesdropper 2 defined as in Equation (3.36).

The impact of $\delta_n^{(\text{s})}$ on the secrecy performance is graphically represented in Figure 3.6A,B, where the former plots the upper-bound defined in Equation (3.35) and the latter the bound in Equation (3.36) as a function of the blocklength n for different values of $\beta^{(\text{s})}$. Now, for the simulations we set the parameters $\beta^{(\text{r})} = 0.16$ and $\rho_{\text{R}} = 0.90$.

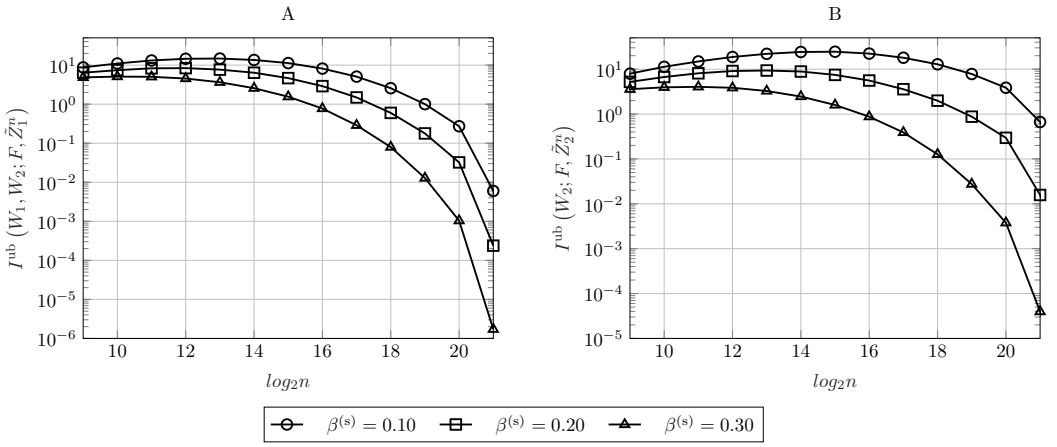

Figure 3.6: Secrecy performance of the polar coding scheme for the DBC-NLD-LS over the BE-BC as a function of the blocklength n and $\beta^{(\text{s})}$, which defines $\delta_n^{(\text{s})}$ for each n, when we set $\beta^{(\text{r})} = 0.16$ and $\rho_{\text{R}} = 0.90$. (**A**) Upper-bound on the information about (W_1, W_2) leaked to Eavesdropper 1 defined as in Equation (3.35). (**B**) Upper-bound on the information about W_2 leaked to Eavesdropper 2 defined as in Equation (3.36).

As can be seen in Figure 3.6, the secrecy performance improves as the value of $\beta^{(\text{s})}$

increases (or equivalently, as $\delta_n^{(\mathrm{s})}$ decreases). This behavior is as expected because notice that $\delta_n^{(\mathrm{s})}$ defines the value of the highest term $H\big(U(j)\big|U^{1:j-1}Y_1^n\big)$ that will belong to $\big(\mathcal{H}_{X|Y_1}^{(n)}\big)^{\mathrm{C}}$, that is the set containing the possible candidates for $\mathcal{I}_1^{(n)} \cup \mathcal{I}_2^{(n)}$. Since the polar construction chooses the indices that will belong to $\mathcal{I}_1^{(n)}$ and $\mathcal{I}_2^{(n)}$ by taking the ones corresponding to the highest entropy terms associated with the eavesdroppers and since, by Proposition 3.3, $H\big(U(j)\big|U^{1:j-1}Z_1^n\big) \geq H\big(U(j)\big|U^{1:j-1}Z_2^n\big) \geq H\big(U(j)\big|U^{1:j-1}Y_1^n\big)$ for any $j \in [1,n]$, the sums in Equations (3.35) and (3.36) over the indices $j \in \mathcal{I}_1^{(n)} \cup \mathcal{I}_2^{(n)}$ will be larger as $\beta^{(\mathrm{s})}$ increases (as $\delta_n^{(\mathrm{s})}$ decreases), while their cardinality remains the same for a given ρ_{R}. Furthermore, note that $\delta_n^{(\mathrm{s})}$ also defines $\mathcal{F}^{(n)} = \mathcal{H}_{X|Y_1}^{(n)} = \{j \in [1,n] : H\big(U(j)\big|U^{1:j-1}Y_1^n\big) > 1 - \delta_n^{(\mathrm{s})}\}$. Thus, the larger is the value of $\beta^{(\mathrm{s})}$ (the lower is $\delta_n^{(\mathrm{s})}$), the smaller is the cardinality of $\mathcal{F}^{(n)}$ and the higher are the entropy terms associated with the eavesdroppers that will belong to this set.

Figure 3.7 plots the upper-bound on the average bit error probability at the legitimate Receiver 1 defined in Equation (3.34) as a function of the blocklength n for different values of $\beta^{(\mathrm{r})}$ (which defines a particular $\delta_n^{(\mathrm{r})}$ for each n). For this figure, we set $\beta^{(\mathrm{s})} = 0.30$ and $\rho_{\mathrm{R}} = 0.90$. As can be seen in Figure 3.7, the higher is the value of $\beta^{(\mathrm{r})}$ (the smaller is the value of $\delta_n^{(\mathrm{r})}$), the better is the reliability performance of the polar code. This is because $\delta_n^{(\mathrm{r})}$ defines the higher entropy term associated with the legitimate Receiver 1 whose corresponding index will belong to the set $\mathcal{L}_{X|Y_1}^{(n)}$ (recall that this set contains the indices of those entries that the legitimate receivers have to estimate by using SC encoding). Hence, it is clear that the upper-bound in Equation (3.34) is decreasing as $\delta_n^{(\mathrm{r})}$ decreases (as $\beta^{(\mathrm{r})}$ increases). Moreover, as we have proven in Section 3.2.4, we can see that the reliability performance is always improving as the blocklength n increases.

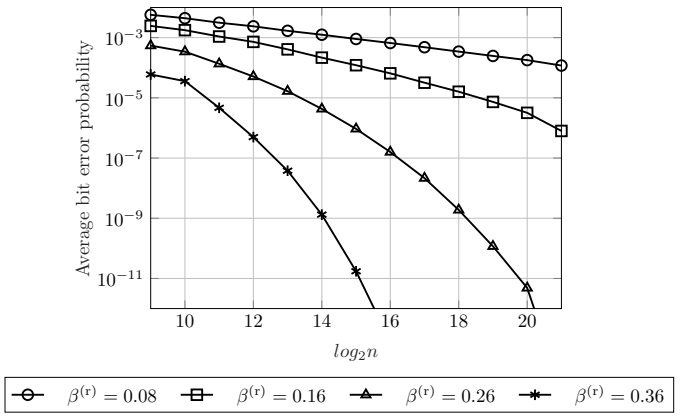

Figure 3.7: Reliability performance of the polar coding scheme for the DBC-NLD-LS over the BE-BC as a function of the blocklength n and $\beta^{(\mathrm{r})}$, which defines $\delta_n^{(\mathrm{r})}$ for each n, when we set $\beta^{(\mathrm{s})} = 0.30$ and $\rho_{\mathrm{R}} = 0.90$. That is, the bound $P_{\mathrm{b}}^{\mathrm{ub}(1)}$ on the average bit error probability at the legitimate Receiver 1 in Equation (3.34).

Finally, how the values of the pair $(\beta^{(\mathrm{r})}, \beta^{(\mathrm{s})})$, or equivalently, the values of $(\delta_n^{(\mathrm{r})}, \delta_n^{(\mathrm{s})})$, impact on the rate of the additional secret sequence Φ given in Equation (3.37) is represented graphically in Figure 3.8. In Figure 3.8A, we set $\rho_{\mathrm{R}} = 0.90$ and $\beta^{(\mathrm{r})} = 0.16$, and we represent the rate of Φ as a function of the blocklength n for different values of $\beta^{(\mathrm{s})}$. Otherwise, in Figure 3.8B, we evaluate the rate of Φ as a function of n for different values of $\beta^{(\mathrm{r})}$ when $\rho_{\mathrm{R}} = 0.90$ and $\beta^{(\mathrm{s})} = 0.30$. Recall that, by Theorem 2.1, this rate tends to be negligible for sufficiently large n. Moreover, according to the polar code construction proposed previously, for a fixed n, the cardinality of the set $\left(\mathcal{H}_{X|Y_1}^{(n)}\right)^{\mathrm{C}} \setminus \mathcal{L}_{X|Y_1}^{(n)}$ will be higher for larger values of $(\beta^{(\mathrm{r})}, \beta^{(\mathrm{s})})$—or smaller values of $(\delta_n^{(\mathrm{r})}, \delta_n^{(\mathrm{s})})$. Clearly, this behavior can be seen in Figure 3.8.

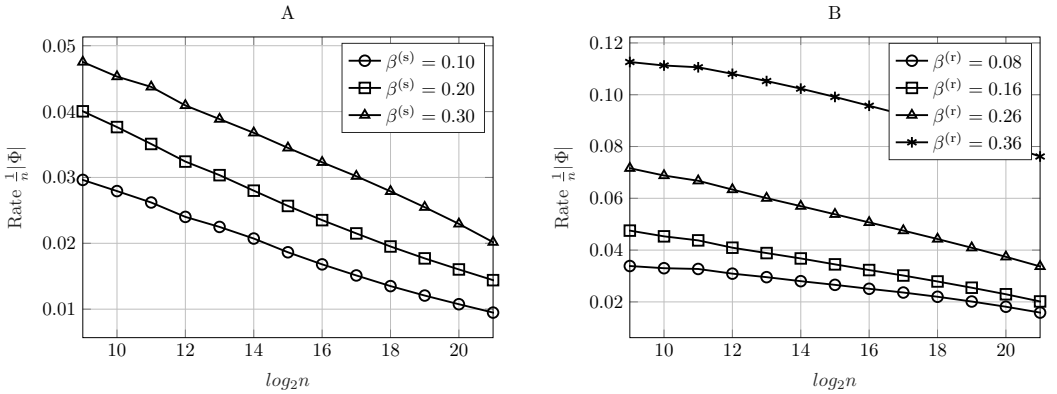

Figure 3.8: Rate of the additional secret sequence Φ computed as in Equation (3.37) for the DBC-NLD-LS over the BE-BC as a function of the blocklength n for different values of $(\beta^{(\mathrm{r})}, \beta^{(\mathrm{s})})$, which defines $(\delta_n^{(\mathrm{r})}, \delta_n^{(\mathrm{s})})$ for each n. (**A**) Rate of Φ for different values of $\beta^{(\mathrm{s})}$ when $\beta^{(\mathrm{r})} = 0.16$ and $\rho_{\mathrm{R}} = 0.90$. (**B**) Rate of Φ for different values of $\beta^{(\mathrm{r})}$ when $\beta^{(\mathrm{s})} = 0.30$ and $\rho_{\mathrm{R}} = 0.90$.

In conclusion, Figures 3.5–3.8 show that, for a particular value of the blocklength n, there is a trade-off between the reliability or the secrecy performance of the polar code and the length of the additional secret sequence Φ, which can be controlled by the value of $\beta^{(\mathrm{r})}$ or $\beta^{(\mathrm{s})}$, respectively, in the polar code construction. Moreover, for sufficiently large n, the performance of the polar coding scheme always is improving as n increases. Indeed, these figures show that one can transmit at rates very close to the capacity providing good reliability and secrecy performance levels.

3.4.2 DBC-LD-NLS

For this model, we consider a BS-BC with two legitimate receivers ($K = 2$) and two eavesdroppers ($M = 2$). Thus, each individual channel is a BSC where $\mathcal{X} = \mathcal{Y}_k = \mathcal{Z}_m = \{0, 1\}$, and $k, m \in \{1, 2\}$. The individual channels are defined by their crossover probability, which

is denoted by α_{Y_k} for the corresponding legitimate Receiver k, that is

$$\alpha_{Y_k} \triangleq \mathbb{P}[Y_k = 0|X = 1] = \mathbb{P}[Y_k = 1|X = 0],$$

and α_{Z_m} for the corresponding Eavesdropper m, that is

$$\alpha_{Z_m} \triangleq \mathbb{P}[Z_m = 0|X = 1] = \mathbb{P}[Z_m = 0|X = 1].$$

Due to the degradedness condition of the broadcast channel given in Equation (3.1), we have $\alpha_{Y_2} < \alpha_{Y_1} < \alpha_{Z_2} < \alpha_{Z_1}$. Due to the symmetry of the channel, it is easy to prove by using similar reasoning as in [CT12] (Example 15.6.5) and by properly applying [BB11] (Proposition 3.2) that the secrecy-capacity achieving distribution $p^\star_{VX}$ satisfies $p^\star_V(v) = p^\star_X(x) = \frac{1}{2}$ for all $v, x \in \{0, 1\}$, and consequently, $p^\star_{X|V}$ is symmetric. Thus, the input distribution $p^\star_{X|V}$ can be characterized simply by the crossover probability $\alpha_{X|V} \triangleq p^\star_{X|V}(0|1) = p^\star_{X|V}(1|0)$, where $0 \leq \alpha_{X|V} \leq \frac{1}{2}$. Indeed, the overall rate in Proposition 3.2, that is, $R_1 + R_2$, is maximized when $\alpha_{X|V} = \frac{1}{2}$, which implies that $R_1 = 0$. Then, by taking $\alpha_{X|V} < \frac{1}{2}$, we can transfer part of the rate associated with the message W_2 to the rate R_1, where $R_2 = 0$ and R_1 is maximum if $\alpha_{X|V} = 0$. For the simulations, we consider a BS-BC with $\alpha_{Y_2} = 0.01$, $\alpha_{Y_1} = 0.04$, $\alpha_{Z_2} = 0.2$ and $\alpha_{Z_1} = 0.35$. We set $\alpha_{X|V} = 0.1084$, which corresponds to the distribution that maximizes $\ln(R_1) + \ln(R_2)$ for this particular channel (proportional fair allocation). Thus, according to Corollary 3.2, the maximum achievable rates are $R^\star_1 = 0.2507$ and $R^\star_2 = 0.3254$.

From [Ari09] (Proposition 5), we know that the previous method used for the DBC-NLD-LS to compute the exact values of the entropy terms for a BEC provides an upper-bound on the entropy terms of the BSC. Although this method can be useful to construct polar codes under reliability constraints [TV13, VVH15, HY13], it fails when the code must guarantee some secrecy condition based on the information leakage. Indeed, in order to upper-bound the information leakage in Equation (3.33), notice that we need a lower-bound on the entropy terms. Hence, for this model, we focus more on proposing a new polar code construction.

Practical polar code construction

Given the blocklength n and the distribution $p^\star_{VXY_2Y_1Z_2Z_1}$, the goal of the polar code construction is to obtain the partition of the universal set $[1, n]$ defined in Equations (3.26)–(3.29) and graphically represented in Figure 3.4. Hence, we need to define first the sets in Equations (3.21)–(3.25), which means having to compute the entropy terms $\{H(U_1(j)|U_1^{1:j-1})\}_{j=1}^n$, $\{H(U_1(j)|U_1^{1:j-1}Y_1^n)\}_{j=1}^n$ and $\{H(U_1(j)|U_1^{1:j-1}Z_2^n)\}_{j=1}^n$ associated with the polar transform $U_1^n = V^nG_n$ for the first superposition encoding layer, and $\{H(U_2(j)|U_2^{1:j-1}V^n)\}_{j=1}^n$,

$\{H(U_2(j)|U_2^{1:j-1}V^nY_2^n)\}_{j=1}^n$ and $\{H(U_2(j)|U_2^{1:j-1}V^nZ_2^n)\}_{j=1}^n$ associated with the polar transform $U_2^n = X^nG_n$ for the second layer. In the following, we propose an adaptation of the Monte Carlo method [VVH15] (PCC-1), which is based on the butterfly algorithm described in [Ari09] for SC decoding, to directly estimate these entropy terms.

Monte-Carlo method to estimate the entropy terms. First, consider the entropy terms associated to the first layer. As for the previous model, since $p_V^\star(v) = \frac{1}{2}$ for all $v \in \{0,1\}$, then $H(U_1(j)|U_1^{1:j-1}) = 1$ for all $j \in [1,n]$. In order to compute $\{H(U_1(j)|U_1^{1:j-1}Y_k^n)\}_{j=1}^n$ and $\{H(U_1(j)|U_1^{1:j-1}Z_m^n)\}_{j=1}^n$ for some $k,m \in \{1,2\}$, we run the Monte Carlo simulation as follows. First, due to the symmetry of the channel and the symmetry of $p_{X|V}^\star$, as in [VVH15] (PCC-1), we can set $v^n = u_1^n = 0^n$ at each iteration. For the realization $\tau \in [1, N_\tau]$, N_τ being the number of realizations, we randomly generate $y_k^{n(\tau)}$ and $z_m^{n(\tau)}$ from $p_{Y_k^n|V^n}^\star$ and $p_{Z_m^n|V^n}^\star$, respectively (by abuse of notation, we use (τ) in any sequence $a^{n(\tau)}$ to emphasize that it is generated at iteration $\tau \in [1, N_\tau]$). Next, we obtain the log-likelihood ratios $\{L_{Y_k|V}^{(\tau)}(j)\}_{j=1}^n$ and $\{L_{Z_m|V}^{(\tau)}(j)\}_{j=1}^n$ by using the algorithm [VVH15] (PCC-1). For instance, consider $\{L_{Y_k|V}^{(\tau)}(j)\}_{j=1}^n$. From the initial values $\{p_{Y_k|V}^\star(y_k^{(\tau)}(j)|0)/p_{Y_k|V}^\star(y_k^{(\tau)}(j)|1)\}_{j=1}^n$, the algorithm recursively computes:

$$L_{Y_k|V}^{(\tau)}(j) \triangleq \ln \frac{p^\star_{Y_k^nU_1^{1:j-1}|U_1(j)}(y_k^{n(\tau)}0^{j-1}|0)}{p^\star_{Y_k^nU_1^{1:j-1}|U_1(j)}(y_k^{n(\tau)}0^{j-1}|1)} \overset{(a)}{=} \frac{p^\star_{U_1(j)|U_1^{1:j-1}Y_k^n}(0|0^{j-1}y_k^{n(\tau)})}{1 - p^\star_{U_1(j)|U_1^{1:j-1}Y_k^n}(0|0^{j-1}y_k^{n(\tau)})} \quad \forall j \in [1,n],$$

where (a) follows from the fact that $p^\star_{U_1(j)}(u) = \frac{1}{2}$ for $u \in \{0,1\}$ because $H(U_1(j)|U_1^{1:j-1}) = 1$. Hence, we can obtain $p^\star_{U_1(j)|U_1^{1:j-1}Y_k^n}(0|0^{j-1}y_k^{n(\tau)})$ from $L_{Y_k|V}^{(\tau)}(j)$, and since

$$H(U_1(j)|U_1^{1:j-1}, Y_k^n) = \mathbb{E}_{U_1^{1:j-1}Y_k^n}\left[h_2\left(p^\star_{U_1(j)|U_1^{1:j-1}Y_k^n}(0|u_1^{1:j-1}, y_k^n)\right)\right],$$

then, after N_τ realizations, we can estimate $H(U_1(j)|U_1^{1:j-1}, Y_k^n)$ by computing the empirical mean, that is,

$$H(U_1(j)|U_1^{1:j-1}Y_k^n) \approx \frac{1}{N_\mathrm{r}} \sum_{\tau=1}^{N_\tau} h_2\left(p^\star_{U_1(j)|U_1^{1:j-1}Y_k^n}(0|0^{j-1}y_k^{n(\tau)})\right).$$

Now, consider the Monte Carlo method to estimate $\{H(U_2(j)|U_2^{1:j-1}V^n)\}_{j=1}^n$, $\{H(U_2(j)|U_2^{1:j-1}V^nY_k^n)\}_{j=1}^n$ and $\{H(U_2(j)|U_2^{1:j-1}V^nZ_m^n)\}_{j=1}^n$ for any $k,m \in \{1,2\}$ associated with the second layer. To obtain $\{H(U_2(j)|U_2^{1:j-1}V^n)\}_{j=1}^n$, we can see X and V as the input and output random variables respectively of a symmetric channel with distribution $p_{V|X}^\star$. Now, although $p_X^\star$ is uniform and, consequently, $H(U_2(j)|U_2^{1:j-1}) = 1$ for all $j \in [1,n]$, notice

that $\mathcal{H}_{X|V}^{(n)} \neq [1,n]$ and $\mathcal{T}_2^{(n)} \neq \emptyset$ because $\mathcal{H}_{X|V}^{(n)}$ and its complementary set depend on $p_{X|V}^{\star}$. On the other hand, to obtain $\{H(U_2(j)|U_2^{1:j-1}V^nY_k^n)\}_{j=1}^n$ or $\{H(U_2(j)|U_2^{1:j-1}V^nZ_m^n)\}_{j=1}^n$, we can see (V,Y_k) or (V,Z_m) as the output of a symmetric channel with distribution $p_{VY_k|X}^{\star}$ or $p_{VZ_m|X}^{\star}$, respectively, where notice that $p_{VY_k|X}^{\star} \equiv p_{V|X}^{\star}p_{Y_k|X}^{\star}$ and $p_{VZ_m|X}^{\star} \equiv p_{V|X}^{\star}p_{Z_m|X}^{\star}$ because $V - X - Y_k - Z_m$ forms a Markov chain. Hence, due to the symmetry of the previous distributions, we can set $x^n = u_2^n = 0^n$ at each iteration. Then, for the realization $\tau \in [1, N_\tau]$, we draw $v^{n(\tau)}$, $y_k^{n(\tau)}$ and $z_m^{n(\tau)}$ from the distributions $p_{V^n|X^n}^{\star}$, $p_{Y_k^n|X^n}$ and $p_{Z_m^n|X^n}$, respectively. Next, we obtain the log-likelihood ratios $\{L_{V|X}^{(\tau)}(j)\}_{j=1}^n$, $\{L_{VY_k|X}^{(\tau)}(j)\}_{j=1}^n$ and $\{L_{VZ_m|X}^{(\tau)}(j)\}_{j=1}^n$ by using [VVH15] (PCC-1). Similarly to the previous encoding layer, since $p_X^{\star}$ is uniform, we can obtain

$$
\begin{aligned}
&p_{U_2(j)|U_2^{1:j-1}V^n}^{\star}(0|0^{j-1}v^{n(\tau)}),\\
&p_{U_2(j)|U_2^{1:j-1}V^nY_k^n}^{\star}(0|0^{j-1}v^{n(\tau)}y_k^{n(\tau)}),\\
&p_{U_2(j)|U_2^{1:j-1}V^nZ_m^n}^{\star}(0|0^{j-1}v^{n(\tau)}z_m^{n(\tau)},
\end{aligned}
$$

from the corresponding log-likelihood ratios. Finally, after N_τ realizations, we can estimate the corresponding entropy terms by computing the empirical mean of the binary entropy function associated with each of the above probabilities.

Partition of the universal set. In order to provide more flexibility on the design, now we introduce $(\delta_n^{(1,\mathrm{r})}, \delta_n^{(1,\mathrm{s})})$ for the first layer, where $\delta_n^{(1,\mathrm{r})} \triangleq 2^{-n^{\beta^{(1,\mathrm{r})}}}$ and $\delta_n^{(1,\mathrm{s})} \triangleq 2^{-n^{\beta^{(1,\mathrm{s})}}}$ for some $\beta^{(1,\mathrm{r})}, \beta^{(1,\mathrm{s})} \in (0, \frac{1}{2})$. For the second layer, we introduce $(\delta_n^{(2,\mathrm{r})}, \delta_n^{(2,\mathrm{s})})$ and $(\delta_n^{(2,\mathrm{L})}, \delta_n^{(2,\mathrm{H})})$, where $\delta_n^{(2,\mathrm{r})} \triangleq 2^{-n^{\beta^{(2,\mathrm{r})}}}$, $\delta_n^{(2,\mathrm{s})} \triangleq 2^{-n^{\beta^{(2,\mathrm{s})}}}$, $\delta_n^{(2,\mathrm{L})} \triangleq 2^{-n^{\beta^{(2,\mathrm{L})}}}$ and $\delta_n^{(2,\mathrm{H})} \triangleq 2^{-n^{\beta^{(2,\mathrm{H})}}}$ for some $\beta^{(2,\mathrm{r})}, \beta^{(2,\mathrm{s})}, \beta^{(2,\mathrm{L})}, \beta^{(2,\mathrm{H})} \in (0, \frac{1}{2})$.

Consider the partition of $[1,n]$ for the first layer ($\ell = 1$ in Equations (3.26)–(3.29)). As mentioned before, since $p_V^{\star}(v) = \frac{1}{2}$, we have $\mathcal{H}_V^{(n)} = [1,n]$ and $\mathcal{T}_1^{(n)} = \emptyset$. Let $R_1' \leq R_1^{\star}$ denotes the target rate of message W_1 that the PCS must approach. Since this PCS does not necessarily operate at the secrecy-capacity, we obtain the partition in (3.26)–(3.29) as follows. First, we define $(\mathcal{H}_{V|Y_1}^{(n)})^{\mathrm{C}} \triangleq \{j \in [1,n] : H(U_1(j)|U_1^{1:j-1}Y_1^n) \leq 1 - \delta_n^{(1,\mathrm{s})}\}$. Then, we choose $\mathcal{I}_1^{(n)}$ by taking the $\lceil nR_1' \rceil$ indices $j \in (\mathcal{H}_{V|Y_1}^{(n)})^{\mathrm{C}}$ that correspond to the highest entropy terms $\{H(U_1(j)|U_1^{1:j-1}, Z_2^n)\}_{j=1}^n$ associated with Eavesdropper 2. Note that $\delta_n^{(1,\mathrm{s})}$ must guarantee $\frac{1}{n}|(\mathcal{H}_{V|Y_1}^{(n)})^{\mathrm{C}}| \leq R_1'$. Finally, we obtain $\mathcal{C}_1^{(n)} \triangleq (\mathcal{H}_{V|Y_1}^{(n)})^{\mathrm{C}} \setminus \mathcal{I}_1^{(n)}$ and $\mathcal{F}_1^{(n)} \triangleq \mathcal{H}_{V|Y_1}^{(n)}$. To evaluate the reliability performance, we define $\mathcal{L}_{V|Y_1}^{(n)} \triangleq \{j \in [1,n] : H(U_1(j)|U_1^{1:j-1}Y_1^n) \leq \delta_n^{(1,\mathrm{r})}\}$.

Consider the partition of $[1,n]$ for the second layer ($\ell = 2$ in Equations (3.26)–(3.29)). Since $\mathcal{H}_{X|V}^{(n)} \neq [1,n]$ and $\mathcal{T}_2^{(n)} \neq \emptyset$, let $\mathcal{H}_{X|V}^{(n)} \triangleq \{j \in [1,n] : H(U_2(j)|U_2^{1:j-1}V^n) \geq 1 - \delta_n^{(2,\mathrm{H})}\}$ and $\mathcal{L}_{X|V}^{(n)} \triangleq \{j \in [1,n] : H(U_2(j)|U_2^{1:j-1}V^n) \leq \delta_n^{(2,\mathrm{L})}\}$, where we have used $\delta_n^{(2,\mathrm{H})}$ and

$\delta_n^{(2,\mathrm{L})}$, respectively. Let $R_2' \leq R_2^\star$ denote the target rate corresponding to W_2. We define $(\mathcal{H}_{X|VY_2}^{(n)})^{\mathrm{C}} \triangleq \{j \in \mathcal{H}_{X|V}^{(n)} : H(U_2(j)|U_2^{1:j-1}, V^n, Y_2^n) \leq 1 - \delta_n^{(2,\mathrm{s})}\}$. Then, we choose $\mathcal{I}_2^{(n)}$ by taking the $\lceil nR_2' \rceil$ indices $j \in \mathcal{H}_{X|V}^{(n)} \cap \big(\mathcal{H}_{X|VY_2}^{(n)}\big)^{\mathrm{C}}$ that correspond to the highest entropy terms $\{H(U_2(j)|U_2^{1:j-1}V^nZ_2^n)\}_{j=1}^n$ associated with Eavesdropper 2. Thus, notice that $\delta_n^{(2,\mathrm{H})}$ and $\delta_n^{(2,\mathrm{s})}$ must guarantee $|\mathcal{H}_{X|V}^{(n)}| \geq |(\mathcal{H}_{X|VY_2}^{(n)})^{\mathrm{C}}| \geq nR_2'$. Then, we obtain $\mathcal{C}_2^{(n)} \triangleq (\mathcal{H}_{X|VY_2}^{(n)})^{\mathrm{C}} \backslash \mathcal{I}_2^{(n)}$ and $\mathcal{F}_2^{(n)} \triangleq \mathcal{H}_{X|VY_2}^{(n)}$. Finally, in order to evaluate the reliability performance, we define $\mathcal{L}_{X|VY_2}^{(n)} \triangleq \{j \in [n] : H(U_2(j)|U_2^{1:j-1}V^nY_2^n) \leq \delta_n^{(2,\mathrm{r})}\}$.

Performance evaluation

The encoding at the first layer will induce a distribution $\tilde{q}_{V^n} \equiv p_{V^n}$. For the second layer, the entries $U_2[\mathcal{H}_{X|V}^{(n)}]$ of the original DMS only are almost independent of V^n because $H(U_2(j)|U_2^{1:j-1}V^n) \leq 1 - \delta_n^{(2,\mathrm{H})}$ for $j \in \mathcal{H}_{X|V}^{(n)}$. Nevertheless, the encoder will construct $\tilde{U}_2[\mathcal{H}_{X|V}^{(n)}]$ by storing uniformly-distributed sequences that are totally independent of V^n. On the other hand, since $\mathcal{L}_{X|V}^{(n)} \subseteq \mathcal{T}_2^{(n)} \neq \emptyset$, the encoder will use deterministic SC encoding to construct $\tilde{U}_2[\mathcal{L}_{X|V}^{(n)}]$. Therefore, according to Lemma 3.2 and Remark 3.4, we will have $V_{\tilde{q}p^\star} \triangleq \mathbb{V}(\tilde{q}_{V^nX^nY_2^nY_1^nZ_2^nZ_1^n}, p^\star_{V^nX^nY_2^nY_1^nZ_2^nZ_1^n}) \neq 0$ for a finite n. As seen in Section 3.3.4, this total variation distance impacts on the performance. Hence, we define the following upper-bound $d_{\mathrm{TV}}^{\mathrm{ub}}$ on the total variation distance $V_{\tilde{q}p^\star}$:

$$d_{\mathrm{TV}}^{\mathrm{ub}} \triangleq d_{\mathrm{TV}}^{\mathrm{ub(L)}} + d_{\mathrm{TV}}^{\mathrm{ub(H)}},$$

where $d_{\mathrm{TV}}^{\mathrm{ub(L)}}$ will measure the impact of using deterministic SC encoding for $\tilde{U}_2\big[\mathcal{L}_{X|V}^{(n)}\big]$, and $d_{\mathrm{TV}}^{\mathrm{ub(H)}}$ will measure the impact of storing uniform sequences into $\tilde{U}_2\big[\mathcal{H}_{X|V}^{(n)}\big]$.

Consider $d_{\mathrm{TV}}^{\mathrm{ub(L)}}$, which corresponds to the analytic bound found in Lemma 2.6. For the simulations, we can use the Monte Carlo method and compute the empirical mean to obtain an upper-bound of Equation (2.19):

$$d_{\mathrm{TV}}^{\mathrm{ub(L)}} \triangleq \frac{1}{N_{\tau'}} \sum_{\tau'=1}^{N_{\tau'}} \sum_{j \in \mathcal{L}_{X|V}^{(n)}} \Big(1 - p^\star_{U_2(j)|U_2^{1:j-1}V^n}\big(u_2^*(j)\big|\check{u}_2^{1:j-1(\tau')}\check{v}^{n(\tau')}\big)\Big), \tag{3.38}$$

where $(\check{v}^{n(\tau')}, \check{u}_2^{n(\tau')})$ must be drawn at each iteration $\tau' \in [1, N_{\tau'}]$ according to (2.17), the set $\mathcal{L}_{X|V}^{(n)}$ has been obtained previously in the polar code construction and, according to Equation (2.19), $u_2^*(j) \triangleq \arg\max_{u \in \{0,1\}} p^\star_{U_2(j)|U_2^{1:j-1}V^n}(u|\check{u}_2^{1:j-1(\tau')}, \check{v}^{n(\tau')})$. Due to the symmetry of $p^\star_{V|X}$, the probabilities $p^\star_{U_2(j)|U_2^{1:j-1}V^n}$ can be obtained with low complexity by means of the butterfly algorithm described in [Ari09].

Consider now $d_{\mathrm{TV}}^{\mathrm{ub(H)}}$, which corresponds to the analytic bound found in Lemma 2.5. We

can compute exactly the Kullback-Leibler divergence as in (2.18) from the corresponding entropy terms. Then, by using Pinsker's inequality, we define

$$d_{\mathrm{TV}}^{\mathrm{ub(H)}} \triangleq \left(2\ln 2 \sum_{j\in\mathcal{H}_{X|V}^{(n)}} \left(1 - H\left(U_2(j)\middle|U_2^{1:j-1}V^n\right)\right)\right)^{1/2}. \tag{3.39}$$

According to the polar code construction, $\left|\mathcal{L}_{X|V}^{(n)}\right|$ and $\left|\mathcal{H}_{X|V}^{(n)}\right|$ will depend only on the values of $\delta_n^{(2,\mathrm{L})}$ and $\delta_n^{(2,\mathrm{H})}$, respectively, for a particular n. Hence, the value of $d_{\mathrm{TV}}^{\mathrm{ub}}$ can be controlled by adjusting $\left(\beta^{(2,\mathrm{L})}, \beta^{(2,\mathrm{H})}\right)$. It is clear that higher values of $\left(\beta^{(2,\mathrm{L})}, \beta^{(2,\mathrm{H})}\right)$ or, equivalently, lower values of $\left(\delta_n^{(2,\mathrm{L})}, \delta_n^{(2,\mathrm{H})}\right)$, mean lower cardinalities of the sets $\mathcal{L}_{X|V}^{(n)}$ and $\mathcal{H}_{X|V}^{(n)}$ and, consequently, lower $d_{\mathrm{TV}}^{\mathrm{ub}}$. However, $\left|\left(\mathcal{H}_{X|V}^{(n)}\right)^{\mathrm{C}} \setminus \mathcal{L}_{X|V}^{(n)}\right|$ increases with $\left(\beta^{(2,\mathrm{L})}, \beta^{(2,\mathrm{H})}\right)$, and the encoder described in Algorithm (3.3) will require more randomness to form $\tilde{U}_2\left[\left(\mathcal{H}_{X|V}^{(n)}\right)^{\mathrm{C}} \setminus \mathcal{L}_{X|V}^{(n)}\right]$.

To evaluate the reliability performance, from Equation (3.31) we obtain the following upper-bound $P_{\mathrm{b}}^{\mathrm{ub}(1)}$ on the average bit error probability for Receiver 1:

$$P_{\mathrm{b}}^{\mathrm{ub}(1)} \triangleq d_{\mathrm{TV}}^{\mathrm{ub}} + \frac{1}{\left|\mathcal{L}_{V|Y_1}^{(n)}\right|} \sum_{j\in\mathcal{L}_{V|Y_1}^{(n)}} H\left(U_1(j)\middle|U_1^{1:j-1}Y_1^n\right). \tag{3.40}$$

Similarly, for Receiver 2, we obtain the following upper-bound on the average error probability:

$$P_{\mathrm{b}}^{\mathrm{ub}(2)} \triangleq 3d_{\mathrm{TV}}^{\mathrm{ub}} + \sum_{j\in\mathcal{L}_{V|Y_1}^{(n)}} \frac{H\left(U_1(j)\middle|U_1^{1:j-1}Y_2^n\right)}{\left|\mathcal{L}_{V|Y_1}^{(n)}\right|} + \sum_{j\in\mathcal{L}_{X|VY_2}^{(n)}} \frac{H\left(U_2(j)\middle|U_2^{1:j-1}V^nY_2^n\right)}{\left|\mathcal{L}_{X|VY_2}^{(n)}\right|}. \tag{3.41}$$

To evaluate the secrecy performance, from Equation (3.33) we compute a tight upper-bound $I^{\mathrm{ub}}(W_1W_2; \tilde{Z}_2^nF_1F_2)$ on the information leakage for Eavesdropper 2:

$$\begin{aligned} I^{\mathrm{ub}}(W_1W_2; \tilde{Z}_2^nF_1F_2) \triangleq\ & 4nd_{\mathrm{TV}}^{\mathrm{ub}} - 2d_{\mathrm{TV}}^{\mathrm{ub}}\log d_{\mathrm{TV}}^{\mathrm{ub}} \\ & + \sum_{\ell=1}^{2}\left(\left|\mathcal{I}_\ell^{(n)} \cup \mathcal{F}_\ell^{(n)}\right| - \sum_{j\in\mathcal{I}_\ell^{(n)}\cup\mathcal{F}_\ell^{(n)}} H\left(U_\ell(j)\middle|U_\ell^{1:j-1}V_\ell^nZ_\ell^n\right)\right), \end{aligned} \tag{3.42}$$

Due to the degradedness condition of the BS-BC, the information leakage corresponding to Eavesdropper 1 will be always less than the one of Eavesdropper 2.

Finally, we evaluate the overall rate of the additional sequences $\{\Phi_1, \Phi_2\}$ by computing:

$$\frac{1}{n}\left(|\Phi_1| + |\Phi_2|\right) = \frac{1}{n}\left|\left(\mathcal{H}_{V|Y_1}^{(n)}\right)^{\mathrm{C}} \setminus \mathcal{L}_{V|Y_1}^{(n)}\right| + \frac{1}{n}\left|\left(\mathcal{H}_{X|VY_2}^{(n)}\right)^{\mathrm{C}} \setminus \mathcal{L}_{X|VY_2}^{(n)}\right|). \tag{3.43}$$

The performance of the polar coding scheme is graphically shown in Figure 3.9. As for the previous model, let ρ_{R} be the normalized target rate in which the PCS operates, that is

$\rho_{\mathrm{R}} \triangleq \frac{R_1'}{R_1^\star} = \frac{R_2'}{R_2^\star}$. In Figure 3.9A, we evaluate the upper-bound on the information leakage defined in Equation (3.42) when we consider $d_{\mathrm{TV}}^{\mathrm{ub}} = 0$, as a function of the blocklength n for different values of ρ_{R}. For this plot, we set $\beta^{(1,\mathrm{s})} = 0.30$ and $\beta^{(2,\mathrm{s})} = 0.36$. Notice that $(\beta^{(1,\mathrm{r})}, \beta^{(2,\mathrm{r})})$, and $(\beta^{(2,\mathrm{L})}, \beta^{(2,\mathrm{H})})$ if we consider $d_{\mathrm{TV}}^{\mathrm{ub}} = 0$, will not impact on the information leakage. As we have showed in Section 3.3.4, the secrecy performance is improving as n increases. Moreover, to satisfy a particular secrecy performance level, the polar code will need higher values of n as the target rates approach the capacity.

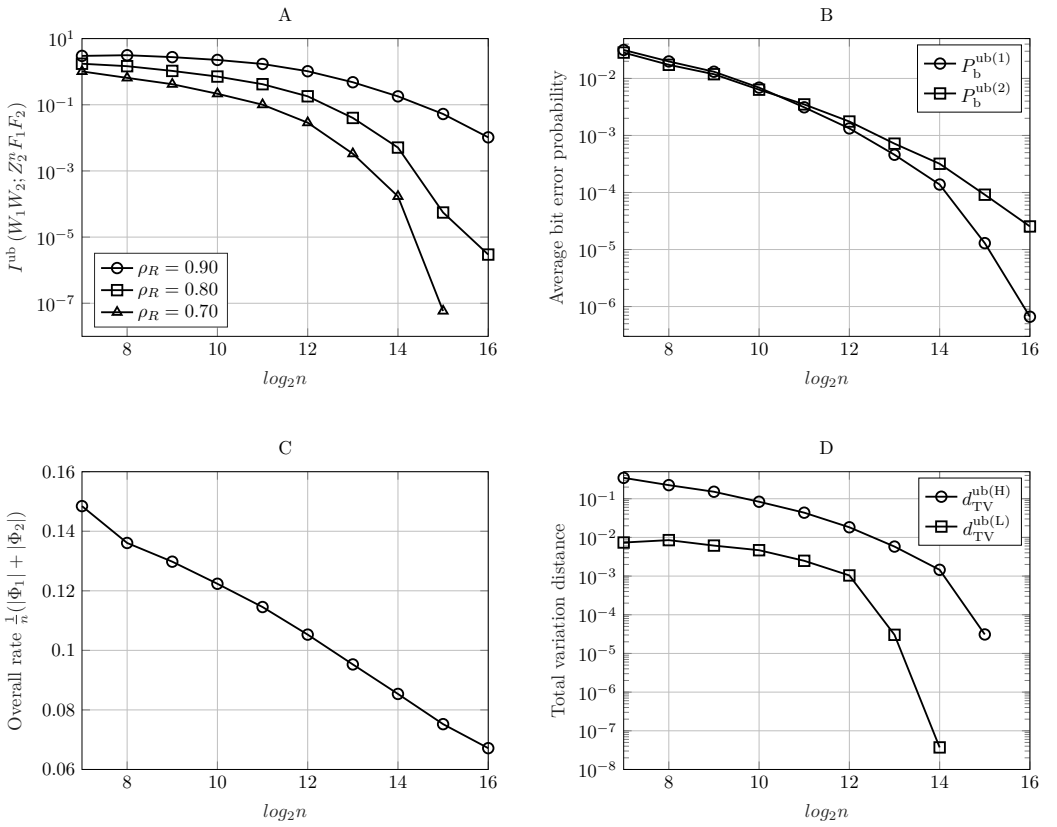

Figure 3.9: Performance of the PCS for the DBC-LD-NLS over the BS-BC as a function of the blocklength n when $\beta^{(1,\mathrm{r})} = \beta^{(2,\mathrm{r})} = 0.24$, $\beta^{(1,\mathrm{s})} = 0.30$, $\beta^{(2,\mathrm{s})} = 0.36$ and $\beta^{(2,\mathrm{L})} = \beta^{(2,\mathrm{H})} = 0.36$. (**A**) Upper-bound on the information about (W_1, W_2) leaked to Eavesdropper 2 defined as in Equation (3.42) for different normalized target rates ρ_{R} when we set $d_{\mathrm{TV}}^{\mathrm{ub}} = 0$. (**B**) Upper-bounds on the average error probability at legitimate Receivers 1 and 2 defined as in Equations (3.40) and (3.41), respectively, when $d_{\mathrm{TV}}^{\mathrm{ub}} = 0$. (**C**) Overall rate of $\{\Phi_1, \Phi_2\}$ computed as in Equation (3.43). (**D**) Terms $d_{\mathrm{TV}}^{\mathrm{ub}(\mathrm{H})}$ and $d_{\mathrm{TV}}^{\mathrm{ub}(\mathrm{L})}$ that contribute to the bound on the total variation distance $d_{\mathrm{TV}}^{\mathrm{ub}}$ defined as in Equations (3.38) and (3.39), respectively.

In Figure 3.9B, we evaluate the upper-bounds $P_{\mathrm{b}}^{\mathrm{ub}(1)}$ and $P_{\mathrm{b}}^{\mathrm{ub}(2)}$, which correspond

to the bounds on the average bit error probability for the legitimate Receivers 1 and 2, respectively, when we set $d_{\mathrm{TV}}^{\mathrm{ub}} = 0$, as a function of the blocklength n. For this plot, we set $\beta^{(1,\mathrm{r})} = \beta^{(2,\mathrm{r})} = 0.24$ and, according to the polar code construction, recall that the reliability performance will not depend on the values of $(\beta^{(1,\mathrm{s})}, \beta^{(2,\mathrm{s})})$ and ρ_{R}. If we set $d_{\mathrm{TV}}^{\mathrm{ub}} = 0$, then it is clear that it will not depend on $(\beta^{(2,\mathrm{L})}, \beta^{(2,\mathrm{H})})$ either. As shown theoretically in Section 3.3.4, the error probability becomes lower as the blocklength n increases.

Figure 3.9C plots the overall rate of the additional secret sequences computed as in Equation (3.43) when we set $\beta^{(1,\mathrm{r})} = \beta^{(2,\mathrm{r})} = 0.24$, $\beta^{(1,\mathrm{s})} = 0.30$ and $\beta^{(2,\mathrm{s})} = 0.36$. We can see that this rate tends to be negligible for n sufficiently large.

Finally, Figure 3.9D plots the upper-bounds $d_{\mathrm{TV}}^{\mathrm{ub(L)}}$ and $d_{\mathrm{TV}}^{\mathrm{ub(H)}}$ defined in Equations (3.38) and (3.39), respectively, when we set $\beta^{(2,\mathrm{L})} = \beta^{(2,\mathrm{H})} = 0.36$. As we have proven theoretically in Lemma 3.2, notice that the total variation distance will decay with the blocklength n. Precisely, notice that $d_{\mathrm{TV}}^{\mathrm{ub(L)}}$ is lower than $d_{\mathrm{TV}}^{\mathrm{ub(H)}}$ and, indeed, the bound on the total variation distance is practically governed by $d_{\mathrm{TV}}^{\mathrm{ub(H)}}$ ($d_{\mathrm{TV}}^{\mathrm{ub}} \approx d_{\mathrm{TV}}^{\mathrm{ub(H)}}$). This happens because although we can compute exactly the Kullback-Leibler divergence as in Equation (2.18) from the entropy terms estimated in the polar code construction, Pinsker's inequality to obtain $d_{\mathrm{TV}}^{\mathrm{ub(H)}}$ as in Equation (3.39) can be too loose for n not large enough. Consider the impact of $d_{\mathrm{TV}}^{\mathrm{ub}}$ on the reliability performance of the code. The average error probability bounds in Equations (3.40) and (3.41) are modeled as the sum of two terms, one depending directly on $d_{\mathrm{TV}}^{\mathrm{ub}}$ and the other depending on the polar construction (which has been plotted in Figure 3.9B). Since $d_{\mathrm{TV}}^{\mathrm{ub}(H)}$ is too loose, we obtain that the reliability performance of the code will be governed practically by the bound $d_{\mathrm{TV}}^{\mathrm{ub}}$ for small values of the blocklength n. Now, consider the impact of $d_{\mathrm{TV}}^{\mathrm{ub}}$ on the secrecy performance of the code. The bound on the information leakage in Equation (3.42) is modeled as the sum of two terms, one also depending only on the polar code construction (which has been plotted in Figure 3.9A) and the other depending on $d_{\mathrm{TV}}^{\mathrm{ub}}$. However, in this situation, $d_{\mathrm{TV}}^{\mathrm{ub}}$ impacts the information leakage approximately as $nd_{\mathrm{TV}}^{\mathrm{ub}}$, which means that this term will totally govern the secrecy performance. Recall that this term follows from Lemma 2.4, which bounds the impact of the encoding described in Algorithm 3.3 on the information leakage as a function of the total variation distance.

3.5 Concluding remarks

In this chapter, we have described two polar coding schemes for two different models over the degraded broadcast channel: DBC-NLD-LS and DBC-LD-NLS. For both models, we have proven that the proposed PCSs are asymptotically secrecy-capacity achieving, providing

reliability and strong secrecy. Then, we have discussed how to construct these polar codes in practice, and we have evaluated their performance for finite blocklength by means of simulations. Although several polar code constructions methods have been proposed in the literature, as far as we know it is the the first attempt to discuss practical constructions for polar codes that must satisfy both reliability and secrecy constraints. In addition, we have evaluated the secrecy performance of the polar code by evaluating the strong secrecy condition, which has been possible by obtaining an upper-bound on the corresponding information leakage at the eavesdroppers. Indeed, we have shown that the proposed PCSs can perform well in practice for a finite blocklength.

For convenience, we have described a PCS that provides reliability and strong secrecy in one block of size n, which is only possible if the system model provides a source of common randomness and an additional medium for which transmitter can secretly convey a problematic sequence of the encoding to legitimate receivers. Fortunately, we have showed that this additionally transmission incurs a negligible rate penalty. It may be worth mentioning that if one consider a system where transmission takes places over several blocks of size n then the source of common randomness could be reused at each block without worsening the performance, and the rate of the previous additional transmission could be reduced by using a chaining construction in a similar manner as in Section 2.3 for the symmetric DWTC. As mentioned in Remark 3.2, recall that only the part of the problematic sequence that is uniformly distributed could be repeated by means of the chaining construction. Moreover, notice in both models that the legitimate receivers have to reliably decode the local randomness; therefore, we can substitute this randomness by a uniformly distributed common message without any secrecy requirement.

The PCSs described for both models aim to minimize the amount of random decisions for SC encoding. The use of common randomness may seem contradictory with the previous objective, but notice that these two types of randomness have different implications on the practical design: while the common randomness is uniformly distributed and can be provided by the communication system, the randomness for SC encoding is not and must be drawn by the encoder, which implies a significant increase of the encoding complexity.

Despite the good performance of the PCSs showed in Section 3.4, some issues still persist. How to avoid sending the additional secret sequences is a problem that remains open. Despite this transmission is negligible in terms of rate, it can be problematic in practical scenarios. Furthermore, despite the rate of the amount of randomness required for SC encoding is negligible, how to replace the random decisions entirely by deterministic ones is a problem that still remains unsolved. Lastly, in order to design polar codes based on the proposed performance evaluation of Section 3.4, it might seem necessary to find tighter upper-bounds

on the total variation distance between the distribution induced by the encoder and the original distribution used in the code construction. Also, for the secrecy performance analysis, it would be interesting to find a tighter upper-bound to measure the impact of the distortion introduced by the encoding on the information leakage.

Finally, as pointed out in Section 1.1, one of the main drawbacks of information-theoretic security is the requirement of transmitter having to know the statistics of eavesdropper channels. Nevertheless, for the polar code construction, one can consider virtual eavesdroppers with some target channel qualities. For DBC-LD-NLS, one can design a polar code according to the statistics of a virtual eavesdropper, and due to the degradedness condition of the channel, this code will perform well if the real eavesdroppers have worse channel quality (worst-case design). On the other hand, for the DBC-NLD-LS, one can simply consider different levels of secrecy depending on different target channel qualities. Depending on the channel quality of the real eavesdropper with respect to the virtual ones considered for the design, the polar coding scheme will provide a particular secrecy performance level.

4

Polar coding for common message only wiretap broadcast channel

This chapter provides a polar coding scheme that allows to transmit *strongly* confidential common information to two legitimate receivers over the Wiretap Broadcast Channel (WTBC). The PCS is based mainly on the one introduced in [CB16] for the BCC and described in Section 2.4 for the general WTC. Since no degradedness condition is assumed for the channel model, the transmission will take place over several blocks and the use of a chaining construction is required to convey non-negligible problematic elements to the legitimate receivers. Also, the PCS aims to use the optimal amount of randomness in the encoding and, consequently, it uses deterministic SC encoding. In order to construct an explicit PCS that provides strong secrecy, the distribution induced by the encoder must be close in terms of statistical distance to the original one considered for the code construction.

The particularization of the PCS described in [CB16] is not straightforward for the model proposed in this chapter. Specifically, we propose a new chaining construction that is crucial to secretly transmit common information to different legitimate receivers when the channel of one of them is not degraded with respect to the other. This construction introduces new bidirectional dependencies between encoding random variables of adjacent blocks that must be considered carefully in the secrecy analysis. Indeed, we need to make use of an additional secret key of negligible size in terms of rate that is privately shared between transmitter and legitimate receivers, which will be used to prove that dependencies between blocks can be broken and, therefore, the strong secrecy condition will be satisfied.

The remaining of this chapter is organized as follows. Section 4.1 introduces the channel model formally. Section 4.2 describes the proposed PCS, and Section 4.3 proves that this

PCS achieves the best known inner-bound on the secrecy-capacity of this model. Finally, the concluding remarks are presented in Section 4.4.

4.1 Channel model and achievable region

Formally, a WTBC $(\mathcal{X}, p_{Y_{(1)}Y_{(2)}Z|X}, \mathcal{Y}_{(1)} \times \mathcal{Y}_{(2)} \times \mathcal{Z})$ with 2 legitimate receivers and an external eavesdropper is characterized by the probability transition function $p_{Y_{(1)}Y_{(2)}Z|X}$, where $X \in \mathcal{X}$ denotes the channel input, $Y_{(k)} \in \mathcal{Y}_{(k)}$ denotes the channel output corresponding to the legitimate Receiver $k \in [1,2]$, and $Z \in \mathcal{Z}$ denotes the channel output corresponding to the eavesdropper. We consider a model, namely Common Information over the Wiretap Broadcast Channel (CI-WTBC), in which the transmitter wishes to send a private message W and a confidential message S to both legitimate receivers. A code $\left(\lceil 2^{nR_W} \rceil, \lceil 2^{nR_S} \rceil, \lceil 2^{nR_R} \rceil, n\right)$ for the CI-WTBC consists of a private message set $\mathcal{W} \triangleq \left[1, \lceil 2^{nR_W} \rceil\right]$, a confidential message set $\mathcal{S} \triangleq \left[1, \lceil 2^{nR_S} \rceil\right]$, a randomization sequence set $\mathcal{R} \triangleq \left[1, \lceil 2^{nR_R} \rceil\right]$ (needed to confuse the eavesdropper about the confidential message S), an encoding function $f : \mathcal{W} \times \mathcal{S} \times \mathcal{R} \to \mathcal{X}^n$ that maps (w, s, r) to a codeword x^n, and two decoding functions $g_{(1)}$ and $g_{(2)}$ such that $g_{(k)} : \mathcal{Y}_{(k)}^n \to \mathcal{W} \times \mathcal{S}$ $(k \in [1,2])$ maps the k-th legitimate receiver observations $y_{(k)}^n$ to the estimates $(\hat{w}^{(k)}, \hat{s}^{(k)})$. The reliability condition to be satisfied by this code is measured in terms of the average probability of error and is given by

$$\lim_{n\to\infty} \mathbb{P}\left[(W,S) \neq (\hat{W}^{(k)}, \hat{S}^{(k)})\right] = 0, \quad k \in [1,2]. \tag{4.1}$$

The *strong* secrecy condition is measured in terms of the information leakage and is given by

$$\lim_{n\to\infty} I\left(S; Z^n\right) = 0. \tag{4.2}$$

This model is graphically illustrated in Figure 4.1. A triple of rates $(R_W, R_S, R_R) \in \mathbb{R}_+^3$ will be achievable for the CI-WTBC if there exists a sequence of $(\lceil 2^{nR_W} \rceil, \lceil 2^{nR_S} \rceil, \lceil 2^{nR_R} \rceil, n)$ codes such that satisfy the reliability and secrecy conditions (4.1) and (4.2) respectively.

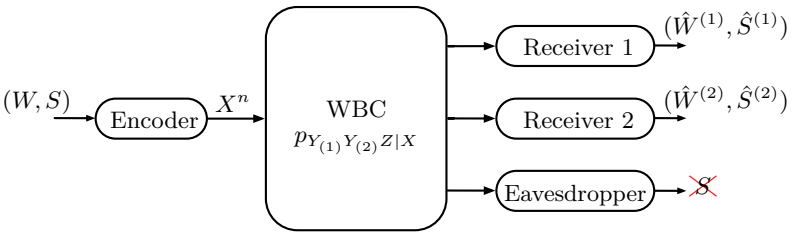

Figure 4.1: Channel model: CI-WTBC.

The achievable rate region is defined as the closure of the set of all achievable rate triples (R_W, R_S, R_R). The following proposition defines an inner-bound on this region.

Proposition 4.1 (Adapted from [CEG12, WO15]). *The region $\mathfrak{R}_{\text{CI-WTBC}}$ defined by the union over the triples of rates $(R_W, R_S, R_R) \in \mathbb{R}_+^3$ satisfying*

$$\begin{aligned} R_W + R_S &\leq \min\left\{I(V;Y_{(1)}), I(V;Y_{(2)})\right\}, \\ R_S &\leq \min\left\{I(V;Y_{(1)}), I(V;Y_{(2)})\right\} - I(V;Z), \\ R_W + R_R &\geq I(X;Z), \\ R_R &\geq I(X;Z|V), \end{aligned}$$

where the union is taken over all distributions p_{VX} such that $V - X - (Y_{(1)}, Y_{(2)}, Z)$ forms a Markov chain, defines an inner-bound on the achievable region of the CI-WTBC.

In this model, the private message W introduces part of the randomness required to confuse the eavesdropper about the confidential message S, and the randomization sequence R denotes the additional randomness that is required for channel prefixing.

4.2 Polar coding scheme

Let $(\mathcal{V} \times \mathcal{X} \times \mathcal{Y}_{(1)} \times \mathcal{Y}_{(2)} \times \mathcal{Z}, p_{VXY_{(1)}Y_{(2)}Z})$ denote the DMS that represents the input (V, X) and output $(Y_{(1)}, Y_{(2)}, Z)$ random variables of the CI-WTBC, where $|\mathcal{V}| = |\mathcal{X}| \triangleq 2$. Without loss of generality, and to avoid the trivial case $R_S = 0$ in Proposition 4.1, we assume that

$$H(V|Z) > H(V|Y_{(1)}) \geq H(V|Y_{(2)}). \tag{4.3}$$

If $H(V|Y_{(1)}) < H(V|Y_{(2)})$, one can simply exchange the role of $Y_{(1)}$ and $Y_{(2)}$ in the PCS described in Section 4.2. We propose a PCS that achieves the following rate triple,

$$(R_W, R_S, R_R) = (I(V;Z), I(V;Y_{(1)}) - I(V;Z), I(X;Z|V)), \tag{4.4}$$

which corresponds to the one of the region in Proposition 4.1 such that the private and the confidential message rate are maximum and the amount of randomness is minimum.

For the input random variable V, we define the polar transform $A^n \triangleq V^n G_n$ and the sets

$$\mathcal{H}_V^{(n)} \triangleq \left\{j \in [1,n] : H\left(A(j)\middle|A^{1:j-1}\right) \geq 1 - \delta_n\right\}, \tag{4.5}$$

$$\mathcal{H}_{V|Z}^{(n)} \triangleq \left\{j \in [1,n] : H\left(A(j)\middle|A^{1:j-1}Z^n\right) \geq 1 - \delta_n\right\}, \tag{4.6}$$

$$\mathcal{L}_{V|Y_{(k)}}^{(n)} \triangleq \left\{j \in [1,n] : H\left(A(j)\middle|A^{1:j-1}Y_{(k)}^n\right) \leq \delta_n\right\}, \quad k = 1,2. \tag{4.7}$$

For the input random variable X, we define $T^n \triangleq X^n G_n$ and the associated sets

$$\mathcal{H}_{X|V}^{(n)} \triangleq \big\{j \in [1,n] : H\big(T(j)\big|T^{1:j-1}V^n\big) \geq 1-\delta_n\big\}. \tag{4.8}$$
$$\mathcal{H}_{X|VZ}^{(n)} \triangleq \big\{j \in [1,n] : H\big(T(j)\big|T^{1:j-1}V^nZ^n\big) \geq 1-\delta_n\big\}. \tag{4.9}$$

We have $p_{A^nT^n}(a^n,t^n) = p_{V^nX^n}(a^nG_n, t^nG_n)$ due to the invertibility of G_n and we write

$$p_{A^nT^n}(a^n,t^n) = \left(\prod_{j=1}^{n} p_{A(j)|A^{1:j-1}}(a(j)|a^{1:j-1})\right)\left(\prod_{j=1}^{n} p_{T(j)|T^{1:j-1}V^n}(t(j)|t^{1:j-1},a^nG_n)\right).$$

Consider that the encoding takes place over L blocks indexed by $i \in [1,L]$. At the i-th block, the encoder will construct $\tilde{A}_i^n$, which will carry the private and the confidential messages intended for both legitimate receivers. Additionally, the encoder will store into $\tilde{A}_i^n$ some elements from $\tilde{A}_{i-1}^n$ (if $i \in [2,L]$) and $\tilde{A}_{i+1}^n$ (if $i \in [1,L-1]$) so that both legitimate receivers are able to reliably reconstruct $\tilde{A}_{1:L}^n$. Then, given $\tilde{V}_i^n = \tilde{A}_i^n G_n$, the encoder will perform the polar-based channel prefixing to construct $\tilde{T}_i^n$. Finally, it will obtain $\tilde{X}_i^n = \tilde{T}_i^n G_n$, which will be transmitted over the WTBC inducing the channel output observations $(\tilde{Y}_{(1),i}^n, \tilde{Y}_{(2),i}^n, \tilde{Z}_i^n)$.

Consider the construction of $\tilde{A}_{1:L}^n$. Besides sets in (4.5)–(4.7), define the partition of $\mathcal{H}_V^{(n)}$:

$$\mathcal{G}^{(n)} \triangleq \mathcal{H}_{V|Z}^{(n)}, \tag{4.10}$$
$$\mathcal{C}^{(n)} \triangleq \mathcal{H}_V^{(n)} \cap \big(\mathcal{H}_{V|Z}^{(n)}\big)^{\mathrm{C}}. \tag{4.11}$$

Moreover, we also define the following partition of the set $\mathcal{G}^{(n)}$:

$$\mathcal{G}_0^{(n)} \triangleq \mathcal{G}^{(n)} \cap \mathcal{L}_{V|Y_{(1)}}^{(n)} \cap \mathcal{L}_{V|Y_{(2)}}^{(n)}, \tag{4.12}$$
$$\mathcal{G}_1^{(n)} \triangleq \mathcal{G}^{(n)} \cap \big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}} \cap \mathcal{L}_{V|Y_{(2)}}^{(n)}, \tag{4.13}$$
$$\mathcal{G}_2^{(n)} \triangleq \mathcal{G}^{(n)} \cap \mathcal{L}_{V|Y_{(1)}}^{(n)} \cap \big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}}, \tag{4.14}$$
$$\mathcal{G}_{1,2}^{(n)} \triangleq \mathcal{G}^{(n)} \cap \big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}} \cap \big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}}, \tag{4.15}$$

and the following partition of the set $\mathcal{C}^{(n)}$:

$$\mathcal{C}_0^{(n)} \triangleq \mathcal{C}^{(n)} \cap \mathcal{L}_{V|Y_{(1)}}^{(n)} \cap \mathcal{L}_{V|Y_{(2)}}^{(n)}, \tag{4.16}$$
$$\mathcal{C}_1^{(n)} \triangleq \mathcal{C}^{(n)} \cap \big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}} \cap \mathcal{L}_{V|Y_{(2)}}^{(n)}, \tag{4.17}$$
$$\mathcal{C}_2^{(n)} \triangleq \mathcal{C}^{(n)} \cap \mathcal{L}_{V|Y_{(1)}}^{(n)} \cap \big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}}, \tag{4.18}$$
$$\mathcal{C}_{1,2}^{(n)} \triangleq \mathcal{C}^{(n)} \cap \big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}} \cap \big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}}; \tag{4.19}$$

These sets are graphically represented in Figure 4.2. Roughly speaking, $A[\mathcal{H}_V^{(n)}]$ is the *nearly*

uniformly distributed part of A^n. Thus, $\tilde{A}_i[\mathcal{H}_V^{(n)}]$, $i \in [1, L]$, is suitable for storing uniformly distributed random sequences. The sequence $A[\mathcal{H}_{V|Z}^{(n)}]$ is *almost* independent of Z^n and, hence, $\tilde{A}_i[\mathcal{G}^{(n)}]$ is suitable for storing information to be secured from the eavesdropper, whereas $\tilde{A}_i[\mathcal{C}^{(n)}]$ is not. Sets in (4.12)–(4.19) with subscript 1 (sets inside the red curve in Figure 4.2) form $\mathcal{H}_V^{(n)} \cap \big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}}$, while those with subscript 2 (sets inside the blue curve) form $\mathcal{H}_V^{(n)} \cap \big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}}$. From Theorem 2.2, recall that $\tilde{A}_i\big[\mathcal{H}_V^{(n)} \cap (\mathcal{L}_{V|Y_{(k)}}^{(n)})^{\mathrm{C}}\big]$ is the nearly uniformly distributed part of the sequence $\tilde{A}_i^n$ required by legitimate Receiver k to reliably reconstruct the entire sequence by performing SC decoding.

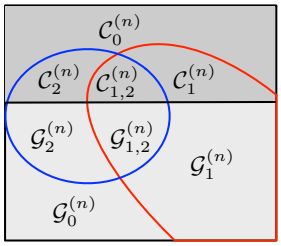

Figure 4.2: Graphical representation of the sets in (4.10)–(4.19). The indices inside the soft and dark gray area form $\mathcal{G}^{(n)}$ and $\mathcal{C}^{(n)}$ respectively. The indices that form $\mathcal{H}_V^{(n)} \cap (\mathcal{L}_{V|Y_{(1)}}^{(n)})^{\mathrm{C}}$ are those inside the red curve, while those inside the blue curve form $\mathcal{H}_V^{(n)} \cap (\mathcal{L}_{V|Y_{(2)}}^{(n)})^{\mathrm{C}}$.

For sufficiently large n, assumption (4.3) imposes the following restriction on the size of the previous sets:

$$\big|\mathcal{G}_1^{(n)}\big| - \big|\mathcal{C}_2^{(n)}\big| \geq \big|\mathcal{G}_2^{(n)}\big| - \big|\mathcal{C}_1^{(n)}\big| > \big|\mathcal{C}_{1,2}^{(n)}\big| - \big|\mathcal{G}_0^{(n)}\big|. \tag{4.20}$$

The left-hand inequality in (4.20) holds from the fact that

$$\begin{aligned}
&\big|\mathcal{C}_1^{(n)} \cup \mathcal{G}_1^{(n)}\big| - \big|\mathcal{C}_2^{(n)} \cup \mathcal{G}_2^{(n)}\big| \\
&\quad = \Big|\mathcal{H}_V^{(n)} \cap \big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{H}_V^{(n)} \cap \big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}}\Big| - \Big|\mathcal{H}_V^{(n)} \cap \big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{H}_V^{(n)} \cap \big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}}\Big| \\
&\quad = \Big|\mathcal{H}_V^{(n)} \cap \big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}}\Big| - \Big|\mathcal{H}_V^{(n)} \cap \big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}}\Big| \geq 0,
\end{aligned}$$

where the positivity holds by Theorem 2.1 because, for any $k \in [1, 2]$, we have

$$\frac{1}{n}\Big|\mathcal{H}_V^{(n)} \cap \big(\mathcal{L}_{V|Y_{(k)}}^{(n)}\big)^{\mathrm{C}}\Big| = \frac{1}{n}\big|\mathcal{H}_{V|Y_{(k)}}^{(n)}\big| + \frac{1}{n}\Big|\mathcal{H}_V^{(n)} \cap \big(\mathcal{L}_{V|Y_{(k)}}^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{H}_{V|Y_{(k)}}^{(n)}\Big| \xrightarrow{n\to\infty} H(V|Y_{(k)})$$

Similarly, the right-hand inequality in (4.20) holds by Theorem 2.1 and the fact that

$$\begin{aligned}
\big|\mathcal{G}_0^{(n)} \cup \mathcal{G}_2^{(n)}\big| - \big|\mathcal{C}_1^{(n)} \cup \mathcal{C}_{1,2}^{(n)}\big| &= \Big|\mathcal{H}_{V|Z}^{(n)} \setminus \mathcal{H}_V^{(n)} \cap \big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}}\Big| - \Big|\mathcal{H}_V^{(n)} \cap \big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{H}_{V|Z}^{(n)}\Big| \\
&= \big|\mathcal{H}_{V|Z}^{(n)}\big| - \Big|\mathcal{H}_V^{(n)} \cap \big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}}\Big|.
\end{aligned}$$

Thus, according to (4.20), we must consider four cases:

A. $|\mathcal{G}_1^{(n)}| > |\mathcal{C}_2^{(n)}|$, $|\mathcal{G}_2^{(n)}| > |\mathcal{C}_1^{(n)}|$ and $|\mathcal{G}_0^{(n)}| \geq |\mathcal{C}_{1,2}^{(n)}|$;

B. $|\mathcal{G}_1^{(n)}| > |\mathcal{C}_2^{(n)}|$, $|\mathcal{G}_2^{(n)}| > |\mathcal{C}_1^{(n)}|$ and $|\mathcal{G}_0^{(n)}| < |\mathcal{C}_{1,2}^{(n)}|$;

C. $|\mathcal{G}_1^{(n)}| \geq |\mathcal{C}_2^{(n)}|$, $|\mathcal{G}_2^{(n)}| \leq |\mathcal{C}_1^{(n)}|$ and $|\mathcal{G}_0^{(n)}| > |\mathcal{C}_{1,2}^{(n)}|$;

D. $|\mathcal{G}_1^{(n)}| < |\mathcal{C}_2^{(n)}|$, $|\mathcal{G}_2^{(n)}| < |\mathcal{C}_1^{(n)}|$ and $|\mathcal{G}_0^{(n)}| > |\mathcal{C}_{1,2}^{(n)}|$.

4.2.1 General polar-based encoding

The generic encoding process for all cases is summarized in Algorithm 4.1. For $i \in [1, L]$, let W_i be a uniformly distributed vector of length $|\mathcal{C}^{(n)}|$ that represents the private message. The encoder forms $\tilde{A}_i[\mathcal{C}^{(n)}]$ by simply storing W_i. Indeed, if $i \in [1, L-1]$, notice that the encoder forms $\tilde{A}_{i+1}[\mathcal{C}^{(n)}]$ before constructing $\tilde{A}_i^n$ entirely. From $\tilde{A}_i[\mathcal{C}^{(n)}]$, $i \in [1, L]$, we define

$$\Psi_i^{(V)} \triangleq \tilde{A}_i[\mathcal{C}_2^{(n)}], \tag{4.21}$$

$$\Gamma_i^{(V)} \triangleq \tilde{A}_i[\mathcal{C}_{1,2}^{(n)}], \tag{4.22}$$

$$\Theta_i^{(V)} \triangleq \tilde{A}_i[\mathcal{C}_1^{(n)}]. \tag{4.23}$$

Notice that $[\Psi_i^{(V)}, \Gamma_i^{(V)}] = \tilde{A}_i[\mathcal{C}_2^{(n)} \cup \mathcal{C}_{1,2}^{(n)}]$ is required by legitimate Receiver 2 to reliably estimate $\tilde{A}_i^n$ and, thus, the encoder will repeat $[\Psi_i^{(V)}, \Gamma_i^{(V)}]$, if $i \in [1, L-1]$, conveniently in $\tilde{A}_{i+1}[\mathcal{G}^{(n)}]$ (the function `form_A_G` is responsible of the chaining construction and is described later). On the other hand, $[\Theta_i^{(V)}, \Gamma_i^{(V)}] = \tilde{A}_i[\mathcal{C}_1^{(n)} \cup \mathcal{C}_{1,2}^{(n)}]$ is required by legitimate Receiver 1. Nevertheless, in order to satisfy the strong secrecy condition in (4.2), $[\Theta_i^{(V)}, \Gamma_i^{(V)}]$, $i \in [2, L]$, is not repeated directly into $\tilde{A}_{i-1}[\mathcal{G}^{(n)}]$, but the encoder copies instead $\bar{\Theta}_i^{(V)}$ and $\bar{\Gamma}_i^{(V)}$ obtained as follows. Let $\kappa_\Theta^{(V)}$ and $\kappa_\Gamma^{(V)}$ be uniformly distributed keys with length $|\mathcal{C}_1^{(n)}|$ and $|\mathcal{C}_{1,2}^{(n)}|$ respectively that are privately shared between transmitter and both legitimate receivers. For any $i \in [2, L]$, we define the sequences

$$\bar{\Theta}_i^{(V)} \triangleq \tilde{A}_i[\mathcal{C}_1^{(n)}] \oplus \kappa_\Theta^{(V)}, \tag{4.24}$$

$$\bar{\Gamma}_i^{(V)} \triangleq \tilde{A}_i[\mathcal{C}_{1,2}^{(n)}] \oplus \kappa_\Gamma^{(V)}. \tag{4.25}$$

Since these secret keys are reused in all blocks, their size becomes negligible in terms of rate for L large enough.

The function `form_A_G` in Algorithm 4.1 constructs sequences $\tilde{A}_{1:L}[\mathcal{G}^{(n)}]$ differently depending on which case, among cases A, B, C or D described before, characterizes the given CI-WTBC. This part of the encoding is described in detail in Section 4.2.2 and Algorithm 4.2.

Algorithm 4.1 Generic encoding scheme

Require: Private and confidential messages $W_{1:L}$ and $S_{1:L}$; randomization sequences $R_{1:L}$; random sequence $\Lambda_0^{(X)}$; and secret keys $\kappa_\Theta^{(V)}$, $\kappa_\Gamma^{(V)}$, $\kappa_{\Upsilon\Phi_{(1)}}^{(V)}$ and $\kappa_{\Upsilon\Phi_{(2)}}^{(V)}$.

$\Psi_0^{(V)}, \Gamma_0^{(V)}, \Pi_0^{(V)}, \Lambda_0^{(V)}, \bar{\Theta}_{L+1}^{(V)}, \bar{\Gamma}_{L+1}^{(V)} \leftarrow \varnothing$
$\tilde{A}_1[\mathcal{C}^{(n)}] \leftarrow W_1$
$\Psi_1^{(V)}, \Gamma_1^{(V)} \leftarrow \tilde{A}_1[\mathcal{C}^{(n)}]$
for $i = 1$ to L **do**
  if $i \neq L$ **then**
    $\tilde{A}_{i+1}[\mathcal{C}^{(n)}] \leftarrow W_{i+1}$
    $\Psi_{i+1}^{(V)}, \Gamma_{i+1}^{(V)}, \bar{\Theta}_{i+1}^{(V)}, \bar{\Gamma}_{i+1}^{(V)} \leftarrow \big(\tilde{A}_{i+1}[\mathcal{C}^{(n)}], \kappa_\Theta^{(V)}, \kappa_\Gamma^{(V)}\big)$
  end if
  $\tilde{A}_i\big[\mathcal{G}^{(n)}\big], \Pi_i^{(V)}, \Lambda_i^{(V)} \leftarrow \texttt{form\_A}_\texttt{G}\big(i, S_i, \bar{\Theta}_{i+1}^{(V)}, \bar{\Gamma}_{i+1}^{(V)}, \Psi_{i-1}^{(V)}, \Gamma_{i-1}^{(V)}, \Pi_{i-1}^{(V)}, \Lambda_{i-1}^{(V)}\big)$
  if $i = 1$ **then** $\Upsilon_{(1)}^{(V)} \leftarrow \tilde{A}_1\big[\mathcal{H}_V^{(n)} \cap \big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}}\big]$
  if $i = L$ **then** $\Upsilon_{(2)}^{(V)} \leftarrow \tilde{A}_L\big[\mathcal{H}_V^{(n)} \cap \big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}}\big]$
  for $j \in \big(\mathcal{H}_V^{(n)}\big)^{\mathrm{C}}$ **do**
    if $j \in \big(\mathcal{H}_V^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{L}_V^{(n)}$ **then**
      $\tilde{A}_i(j) \leftarrow p_{A(j)|A^{1:j-1}}\big(\tilde{A}_i(j)\big|\tilde{A}_i^{1:j-1}\big)$
    else if $j \in \mathcal{L}_V^{(n)}$ **then**
      $\tilde{A}_i(j) \leftarrow \arg\max_{a\in\mathcal{V}} p_{A(j)|A^{1:j-1}}\big(\tilde{a}_i(j)\big|\tilde{A}_i^{1:j-1}\big)$
    end if
  end for
  $\Phi_{(1),i}^{(V)} \leftarrow \tilde{A}_i\big[\big(\mathcal{H}_V^{(n)}\big)^{\mathrm{C}} \cap \big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}}\big]$
  $\Phi_{(2),i}^{(V)} \leftarrow \tilde{A}_i\big[\big(\mathcal{H}_V^{(n)}\big)^{\mathrm{C}} \cap \big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}}\big]$
  $\tilde{X}_i^n, \Lambda_i^{(X)} \leftarrow \texttt{pb\_ch\_pref}\big(\tilde{A}_i^n G_n, R_i, \Lambda_{i-1}^{(X)}\big)$
end for
Send $\big(\Phi_{(k),i}^{(V)}, \Upsilon_{(k)}^{(V)}\big) \oplus \kappa_{\Upsilon\Phi_{(k)}}^{(V)}$ to Receiver $k \in [1,2]$
return $\tilde{X}_{1:L}^n$

Then, given $\tilde{A}_i[\mathcal{C}^{(n)} \cup \mathcal{G}^{(n)}]$, the encoder forms the remaining entries of $\tilde{A}_i^n$, i.e., $\tilde{A}_i[(\mathcal{H}_V^{(n)})^{\mathrm{C}}]$, as follows. If $j \in \mathcal{L}_V^{(n)}$, where $\mathcal{L}_V^{(n)} \triangleq \big\{j \in [1,n] : H\big(A(j)\big|A^{1:j-1}\big) \leq \delta_n\big\}$, it constructs $\tilde{A}_i(j)$ deterministically by using SC encoding, and only the part $\tilde{A}_i[(\mathcal{H}_V^{(n)})^{\mathrm{C}} \setminus \mathcal{L}_V^{(n)}]$ of $\tilde{A}_i^n$ is constructed randomly.

Finally, given $\tilde{V}_i^n = \tilde{A}_i^n G_n$, a randomization sequence R_i and a uniformly distributed random sequence $\Lambda_0^{(V)}$, the encoder performs the polar-based channel prefixing (function `pb_ch_pref` in Algorithm 4.1) to obtain $\tilde{X}_i^n$, which is transmitted over the WTBC inducing $\big(\tilde{Y}_{(1),i}^n, \tilde{Y}_{(2),i}^n, \tilde{Z}_i^n\big)$. This part of the encoding is described in detail in Section 4.2.3.

Furthermore, the encoder obtains the sequence

$$\Phi_{(k),i}^{(V)} \triangleq \tilde{A}_i\big[\big(\mathcal{H}_V^{(n)}\big)^{\mathrm{C}} \cap \big(\mathcal{L}_{V|Y_{(k)}}^{(n)}\big)^{\mathrm{C}}\big] \tag{4.26}$$

for any $k \in [1,2]$ and $i \in [1,L]$, which is required by legitimate Receiver k to reliably estimate $\tilde{A}_i^n$ entirely. Since $\Phi_{(k),i}^{(V)}$ is not *nearly uniform*, the encoder cannot make it available to the legitimate Receiver k by means of the chaining structure. Also, the encoder obtains

$$\Upsilon_{(1)}^{(V)} \triangleq \tilde{A}_1\big[\mathcal{H}_V^{(n)} \cap (\mathcal{L}_{V|Y_{(1)}}^{(n)})^{\mathrm{C}}\big], \tag{4.27}$$

$$\Upsilon_{(2)}^{(V)} \triangleq \tilde{A}_L\big[\mathcal{H}_V^{(n)} \cap (\mathcal{L}_{V|Y_{(2)}}^{(n)})^{\mathrm{C}}\big]. \tag{4.28}$$

The sequence $\Upsilon_{(k)}^{(V)}$ is required by legitimate Receiver $k \in [1,2]$ to initialize the decoding process. Therefore, the transmitter additionally sends $\big(\Upsilon_{(k)}^{(V)}, \Phi_{(k),i}^{(V)}\big) \oplus \kappa_{\Upsilon\Phi_{(k)}}^{(V)}$ to legitimate Receiver k, where $\kappa_{\Upsilon\Phi_{(k)}}^{(V)}$ is a uniformly distributed key with size

$$L\Big|\big(\mathcal{H}_V^{(n)}\big)^{\mathrm{C}} \cap \big(\mathcal{L}_{V|Y_{(k)}}^{(n)}\big)^{\mathrm{C}}\Big| + \Big|\mathcal{H}_V^{(n)} \cap \big(\mathcal{L}_{V|Y_{(k)}}^{(n)}\big)^{\mathrm{C}}\Big|$$

that is privately shared between transmitter and the corresponding receiver. In Section 4.3.1 we show that the length of $\kappa_{\Upsilon\Phi_{(1)}}^{(V)}$ and $\kappa_{\Upsilon\Phi_{(2)}}^{(V)}$ is asymptotically negligible in terms of rate.

4.2.2 Function `form_A_G`

The function `form_A_G` encodes the confidential messages $S_{1:L}$ and builds the chaining construction. Based on the sets in (4.10)–(4.19), let $\mathcal{R}_1^{(n)} \subseteq \mathcal{G}_0^{(n)} \cup \mathcal{G}_2^{(n)}$, $\mathcal{R}_1'^{(n)} \subseteq \mathcal{G}_2^{(n)}$, $\mathcal{R}_2^{(n)} \subseteq \mathcal{G}_1^{(n)}$, $\mathcal{R}_2'^{(n)} \subseteq \mathcal{G}_1^{(n)}$, $\mathcal{R}_{1,2}^{(n)} \subseteq \mathcal{G}_0^{(n)}$, $\mathcal{R}_{1,2}'^{(n)} \subseteq \mathcal{G}_0^{(n)}$, $\mathcal{I}^{(n)} \subseteq \mathcal{G}_0^{(n)} \cup \mathcal{G}_2^{(n)}$, $\mathcal{R}_{\mathrm{S}}^{(n)} \subseteq \mathcal{G}_1^{(n)}$ and $\mathcal{R}_{\Lambda}^{(n)} \subseteq \mathcal{G}_1^{(n)}$ form an additional partition of $\mathcal{G}^{(n)}$. The definition of $\mathcal{R}_1^{(n)}$, $\mathcal{R}_1'^{(n)}$, $\mathcal{R}_2^{(n)}$, $\mathcal{R}_2'^{(n)}$, $\mathcal{R}_{1,2}^{(n)}$ and $\mathcal{R}_{1,2}'^{(n)}$ will depend on the particular case (among A to D), while

$$\mathcal{I}^{(n)} \triangleq \big(\mathcal{G}_0^{(n)} \cup \mathcal{G}_2^{(n)}\big) \setminus \big(\mathcal{R}_1^{(n)} \cup \mathcal{R}_1'^{(n)} \cup \mathcal{R}_{1,2}^{(n)} \cup \mathcal{R}_{1,2}'^{(n)}\big), \tag{4.29}$$

$$\mathcal{R}_{\mathrm{S}}^{(n)} \triangleq \text{any subset of } \mathcal{G}_1^{(n)} \setminus \big(\mathcal{R}_2^{(n)} \cup \mathcal{R}_2'^{(n)}\big) \text{ with size } \big|\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)}\big|, \tag{4.30}$$

$$\mathcal{R}_{\Lambda}^{(n)} \triangleq \mathcal{G}_{1,2}^{(n)} \cup \big(\mathcal{G}_1^{(n)} \setminus \big(\mathcal{R}_2^{(n)} \cup \mathcal{R}_2'^{(n)} \cup \mathcal{R}_{\mathrm{S}}^{(n)}\big)\big). \tag{4.31}$$

For $i \in [1,L]$, let S_i denote a uniformly distributed vector that represents the confidential message. The message S_1 has size $\big|\mathcal{I}^{(n)} \cup \mathcal{G}_1^{(n)} \cup \mathcal{G}_{1,2}^{(n)}\big|$; for $i \in [2, L-1]$, S_i has size $\big|\mathcal{I}^{(n)}\big|$; and S_L has size $\big|\mathcal{I}^{(n)} \cup \mathcal{G}_2^{(n)}\big|$. Also, for $i \in [1,L]$, we write $\Psi_i^{(V)} \triangleq \big[\Psi_{1,i}^{(V)}, \Psi_{2,i}^{(V)}\big]$, $\Gamma_i^{(V)} \triangleq \big[\Gamma_{1,i}^{(V)}, \Gamma_{2,i}^{(V)}\big]$, $\bar{\Theta}_i^{(V)} \triangleq \big[\bar{\Theta}_{1,i}^{(V)}, \bar{\Theta}_{2,i}^{(V)}\big]$ and $\bar{\Gamma}_i^{(V)} \triangleq \big[\bar{\Gamma}_{1,i}^{(V)}, \bar{\Gamma}_{2,i}^{(V)}\big]$, where we define $\Psi_{p,i}$, $\Gamma_{p,i}$, $\bar{\Theta}_{p,i}$ and $\bar{\Gamma}_{p,i}$, for any $p \in [1,2]$, accordingly in each case.

This function, which is used in Case A to Case D, is described in Algorithm 4.2.

Algorithm 4.2 Function `form_A_G`

Require: i, S_i, $\bar{\Theta}_{i+1}^{(V)}$, $\bar{\Gamma}_{i+1}^{(V)}$, $\Psi_{i-1}^{(V)}$, $\Gamma_{i-1}^{(V)}$, $\Pi_{i-1}^{(V)}$, $\Lambda_{i-1}^{(V)}$

Define $\mathcal{R}_1^{(n)}$, $\mathcal{R}_1'^{(n)}$, $\mathcal{R}_2^{(n)}$, $\mathcal{R}_2'^{(n)}$, $\mathcal{R}_{1,2}^{(n)}$, $\mathcal{R}_{1,2}'^{(n)}$, $\mathcal{I}^{(n)}$, $\mathcal{R}_{\mathrm{S}}^{(n)}$, $\mathcal{R}_{\Lambda}^{(n)}$ (depending on the case)
if $i = 1$ **then** $\tilde{A}_1[\mathcal{I}^{(n)} \cup \mathcal{G}_1^{(n)} \cup \mathcal{G}_{1,2}^{(n)}] \leftarrow S_1$
if $i \in [2, L-1]$ **then** $\tilde{A}_i[\mathcal{I}^{(n)}] \leftarrow S_i$
if $i = L$ **then** $\tilde{A}_L[\mathcal{I}^{(n)} \cup \mathcal{G}_2^{(n)}] \leftarrow S_L$
$\Psi_{1,i-1}^{(V)}$, $\Psi_{2,i-1}^{(V)} \leftarrow \Psi_{i-1}^{(V)}$ (depending on the case)
$\Gamma_{1,i-1}^{(V)}$, $\Gamma_{2,i-1}^{(V)} \leftarrow \Gamma_{i-1}^{(V)}$ (depending on the case)
$\bar{\Theta}_{1,i+1}^{(V)}$, $\bar{\Theta}_{2,i+1}^{(V)} \leftarrow \bar{\Theta}_{i+1}^{(V)}$ (depending on the case)
$\bar{\Gamma}_{1,i+1}^{(V)}$, $\bar{\Gamma}_{2,i+1}^{(V)} \leftarrow \bar{\Gamma}_{i+1}^{(V)}$ (depending on the case)
$\tilde{A}_i[\mathcal{R}_{1,2}^{(n)}] \leftarrow \Gamma_{1,i-1}^{(V)} \oplus \bar{\Gamma}_{1,i+1}^{(V)}$
$\tilde{A}_i[\mathcal{R}_{1,2}'^{(n)}] \leftarrow \Psi_{2,i-1}^{(V)} \oplus \bar{\Theta}_{2,i+1}^{(V)}$
if $i \in [1, L-1]$ **then**
    $\tilde{A}_i[\mathcal{R}_1^{(n)}] \leftarrow \bar{\Theta}_{1,i+1}^{(V)}$
    $\tilde{A}_i[\mathcal{R}_1'^{(n)}] \leftarrow \bar{\Gamma}_{2,i+1}^{(V)}$
end if
if $i \in [2, L]$ **then**
    $\tilde{A}_i[\mathcal{R}_2^{(n)}] \leftarrow \Psi_{1,i-1}^{(V)}$
    $\tilde{A}_i[\mathcal{R}_2'^{(n)}] \leftarrow \Gamma_{2,i-1}^{(V)}$
    $\tilde{A}_i[\mathcal{R}_{\mathrm{S}}^{(n)}] \leftarrow \Pi_{i-1}^{(V)}$
    $\tilde{A}_i[\mathcal{R}_{\Lambda}^{(n)}] \leftarrow \Lambda_{i-1}^{(V)}$
end if
$\Pi_i^{(V)} \leftarrow \tilde{A}_i[\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)}]$
$\Lambda_i^{(V)} \leftarrow \tilde{A}_i[\mathcal{R}_{\Lambda}^{(n)}]$
return the sequences $\tilde{A}_i\big[\mathcal{G}^{(n)}\big]$, $\Pi_i^{(V)}$ and $\Lambda_i^{(V)}$

Case A

In this case, recall that $|\mathcal{G}_1^{(n)}| > |\mathcal{C}_2^{(n)}|$, $|\mathcal{G}_2^{(n)}| > |\mathcal{C}_1^{(n)}|$ and $|\mathcal{G}_0^{(n)}| \geq |\mathcal{C}_{1,2}^{(n)}|$. We define

$$\mathcal{R}_1^{(n)} \triangleq \text{any subset of } \mathcal{G}_2^{(n)} \text{ with size } \big|\mathcal{C}_1^{(n)}\big|, \tag{4.32}$$

$$\mathcal{R}_2^{(n)} \triangleq \text{any subset of } \mathcal{G}_1^{(n)} \text{ with size } \big|\mathcal{C}_2^{(n)}\big|, \tag{4.33}$$

$$\mathcal{R}_{1,2}^{(n)} \triangleq \text{any subset of } \mathcal{G}_0^{(n)} \text{ with size } \big|\mathcal{C}_{1,2}^{(n)}\big|, \tag{4.34}$$

and $\mathcal{R}_1'^{(n)} = \mathcal{R}_2'^{(n)} = \mathcal{R}_{1,2}'^{(n)} \triangleq \emptyset$. By the assumption of Case A, it is clear that $\mathcal{R}_1^{(n)}$, $\mathcal{R}_2^{(n)}$ and $\mathcal{R}_{1,2}^{(n)}$ exist. Also, by (4.20), the set $\mathcal{I}^{(n)}$ exists, and so will $\mathcal{R}_{\mathrm{S}}^{(n)}$ because

$$\begin{aligned}\big|\mathcal{G}_1^{(n)} \setminus \big(\mathcal{R}_2^{(n)} \cup \mathcal{R}_2'^{(n)}\big)\big| - \big|\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)}\big| &= \big|\mathcal{G}_1^{(n)} \setminus \big(\mathcal{R}_2^{(n)} \cup \mathcal{R}_2'^{(n)}\big)\big| - \big|\big(\mathcal{G}_2^{(n)} \setminus \mathcal{R}_1^{(n)} \cup \mathcal{R}_1'^{(n)}\big)\big| \\ &= |\mathcal{G}_1^{(n)}| - |\mathcal{C}_2^{(n)}| - |\mathcal{G}_2^{(n)}| - |\mathcal{C}_1^{(n)}| \geq 0.\end{aligned}$$

These sets that form the partition of $\mathcal{G}^{(n)}$ in Case A can be seen in Figure 4.3, which also displays the encoding process that aims to construct $\tilde{A}_{1:L}\big[\mathcal{H}_V^{(n)}\big] = \tilde{A}_{1:L}\big[\mathcal{C}^{(n)} \cup \mathcal{G}^{(n)}\big]$.

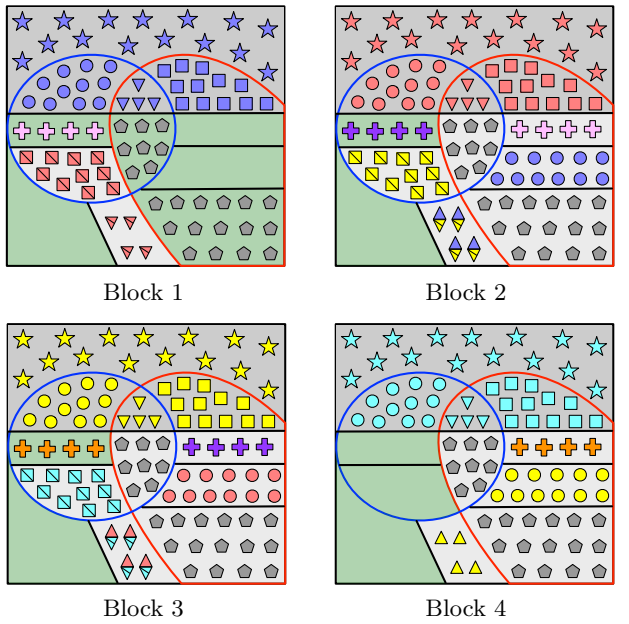

Figure 4.3: For Case A, graphical representation of the encoding that leads to the construction of $\tilde{A}_{1:L}[\mathcal{H}_V^{(n)}]$ when $L = 4$. Consider the Block 2: $\mathcal{R}_1^{(n)}$, $\mathcal{R}_2^{(n)}$, $\mathcal{R}_{1,2}^{(n)}$, $\mathcal{R}_{\mathrm{S}}^{(n)}$ and $\mathcal{R}_{\Lambda}^{(n)}$ are those areas filled with yellow squares, blue circles, blue and yellow diamonds, pink crosses, and gray pentagons, respectively, and the set $\mathcal{I}^{(n)}$ is the green filled area. At Block $i \in [1, L]$, W_i is represented by symbols of the same color (e.g., red symbols at Block 2), and $\Theta_i^{(V)}$, $\Psi_i^{(V)}$ and $\Gamma_i^{(V)}$ are represented by squares, circles and triangles respectively. Also, $\bar{\Theta}_i^{(V)}$ and $\bar{\Gamma}_i^{(V)}$ are denoted by squares and triangles, respectively, with a line through them. At Block $i \in [2, L-1]$, the diamonds denote $\Gamma_{1,i-1}^{(V)} \oplus \bar{\Gamma}_{1,i+1}^{(V)}$. In Block $i \in [1, L]$, S_i is stored into those entries whose indices belong to the green area. For $i \in [1, L-1]$, $\Pi_i^{(V)}$ is denoted by crosses (e.g., purple crosses at Block 2), and is repeated in $\tilde{A}_{i+1}[\mathcal{R}_{\mathrm{S}}^{(n)}]$. The sequence $\Lambda_1^{(V)}$ is represented by gray pentagons and is replicated in all blocks. The sequences $\Upsilon_{(1)}^{(V)}$ and $\Upsilon_{(2)}^{(V)}$ are those entries inside the red at Block 1 and the blue curve at Block L, respectively.

For $i \in [1, L]$, we define $\Psi_{1,i}^{(V)} \triangleq \Psi_i^{(V)}$, $\Gamma_{1,i}^{(V)} \triangleq \Gamma_i^{(V)}$, $\bar{\Theta}_{1,i}^{(V)} \triangleq \bar{\Theta}_i^{(V)}$, $\bar{\Gamma}_{1,i}^{(V)} \triangleq \bar{\Gamma}_i^{(V)}$ and, therefore, we have $\Psi_{2,i}^{(V)} = \Gamma_{2,i}^{(V)} = \bar{\Theta}_{2,i}^{(V)} = \bar{\Gamma}_{2,i}^{(V)} \triangleq \varnothing$.

From (4.18), we have $\mathcal{C}_2^{(n)} \subseteq \mathcal{L}_{V|Y_{(1)}}^{(n)} \setminus \mathcal{L}_{V|Y_{(2)}}^{(n)}$. Thus, the sequence $\Psi_{1,i-1}^{(V)} = \tilde{A}_{i-1}\big[\mathcal{C}_2^{(n)}\big]$ is needed by legitimate Receiver 2 to reliably reconstruct $\tilde{A}_{i-1}^n$, but can be reliably inferred by legitimate Receiver 1 given $\tilde{A}_{i-1}\big[(\mathcal{L}_{V|Y_{(1)}}^{(n)})^{\mathrm{C}}\big]$. Hence, according to Algorithm 4.2, the encoder repeats the entire sequence $\Psi_{1,i-1}^{(V)}$ in $\tilde{A}_i\big[\mathcal{R}_2^{(n)}\big] \subseteq \tilde{A}_i[\mathcal{L}_{V|Y_{(2)}}^{(n)} \setminus \mathcal{L}_{V|Y_{(1)}}^{(n)}\big]$.

Similarly, from (4.17), we have $\mathcal{C}_1^{(n)} \subseteq \mathcal{L}_{V|Y_{(2)}}^{(n)} \setminus \mathcal{L}_{V|Y_{(1)}}^{(n)}$. Thus, $\Theta_{1,i+1}^{(V)} = \tilde{A}_{i+1}\big[\mathcal{C}_1^{(n)}\big]$ is needed by Receiver 1 to form $\tilde{A}_{i+1}^n$ but can be inferred by Receiver 2 given $\tilde{A}_{i+1}\big[(\mathcal{L}_{V|Y_{(2)}}^{(n)})^{\mathrm{C}}\big]$.

Hence, the encoder repeats the sequence $\bar{\Theta}_{1,i+1}^{(V)}$ in $\tilde{A}_i[\mathcal{R}_1^{(n)}] \subseteq \tilde{A}_i\big[\mathcal{L}_{V|Y_{(1)}}^{(n)} \setminus \mathcal{L}_{V|Y_{(2)}}^{(n)}\big]$.

Finally, from (4.19), $\mathcal{C}_{1,2}^{(n)} \subseteq (\mathcal{L}_{V|Y_{(2)}}^{(n)})^{\mathrm{C}} \cap (\mathcal{L}_{V|Y_{(1)}}^{(n)})^{\mathrm{C}}$. Thus, sequences $\Gamma_{1,i-1}^{(V)} = \tilde{A}_{i-1}\big[\mathcal{C}_{1,2}^{(n)}\big]$ and $\Gamma_{1,i+1}^{(V)} = \tilde{A}_{i+1}\big[\mathcal{C}_{1,2}^{(n)}\big]$ are needed by both receivers to form $\tilde{A}_{i-1}^n$ and $\tilde{A}_{i+1}^n$ respectively. Hence, the encoder repeats $\Gamma_{1,i-1}^{(V)}$ and $\bar{\Gamma}_{1,i+1}^{(V)}$ in $\tilde{A}_i\big[\mathcal{R}_{1,2}^{(n)}\big] \subseteq \tilde{A}_i\big[\mathcal{L}_{V|Y_{(1)}}^{(n)} \cap \mathcal{L}_{V|Y_{(2)}}^{(n)}\big]$. Indeed, both sequences are repeated in the same entries of $\tilde{A}_i[\mathcal{G}_0^{(n)}]$ by performing $\Gamma_{1,i-1}^{(V)} \oplus \bar{\Gamma}_{1,i+1}^{(V)}$. Since $\Gamma_{1,0}^{(V)} = \bar{\Gamma}_{1,L+1}^{(V)} = \varnothing$, only $\bar{\Gamma}_{1,2}^{(V)}$ is repeated at Block 1 and $\Gamma_{1,L-1}^{(V)}$ at Block L.

Moreover, part of secret message S_i, $i \in [1, L]$, is stored into some entries of $\tilde{A}_i^n$ whose indices belong to $\mathcal{G}_2^{(n)}$. Thus, in any Block $i \in [2, L]$, the encoder repeats

$$\Pi_{i-1}^{(V)} \triangleq \tilde{A}_{i-1}\big[\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)}\big] \tag{4.35}$$

in $\tilde{A}_i[\mathcal{R}_{\mathrm{S}}^{(n)}] \subseteq \tilde{A}_i[\mathcal{L}_{V|Y_{(2)}}^{(n)} \setminus \mathcal{L}_{V|Y_{(1)}}^{(n)}]$. Also, it repeats

$$\Lambda_{i-1}^{(V)} \triangleq \tilde{A}_{i-1}\big[\mathcal{R}_{\Lambda}^{(n)}\big] \tag{4.36}$$

in $\tilde{A}_i[\mathcal{R}_{\Lambda}^{(n)}]$. Hence, notice that $\Lambda_1^{(V)}$ is replicated in all blocks.

Case B

In this case, $\big|\mathcal{G}_1^{(n)}\big| > \big|\mathcal{C}_2^{(n)}\big|$, $\big|\mathcal{G}_2^{(n)}\big| > \big|\mathcal{C}_1^{(n)}\big|$ and $\big|\mathcal{G}_0^{(n)}\big| < \big|\mathcal{C}_{1,2}^{(n)}\big|$. We define $\mathcal{R}_1^{(n)}$ and $\mathcal{R}_2^{(n)}$ as in (4.32) and (4.33) respectively, and $\mathcal{R}_{1,2}^{\prime(n)} \triangleq \emptyset$. Now, since $\big|\mathcal{G}_0^{(n)}\big| < \big|\mathcal{C}_{1,2}^{(n)}\big|$, only a part of $\Gamma_{i-1}^{(V)}$ and $\bar{\Gamma}_{i+1}^{(V)}$, $i \in [1, L]$, can be repeated in $\tilde{A}_i\big[\mathcal{G}_0^{(n)}\big]$. Thus, we define $\mathcal{R}_{1,2}^{(n)} \triangleq \mathcal{G}_0^{(n)}$ and

$$\mathcal{R}_1^{\prime(n)} \triangleq \text{any subset of } \mathcal{G}_2^{(n)} \setminus \mathcal{R}_1^{(n)} \text{ with size } \big|\mathcal{C}_{1,2}^{(n)}\big| - \big|\mathcal{G}_0^{(n)}\big|, \tag{4.37}$$

$$\mathcal{R}_2^{\prime(n)} \triangleq \text{any subset of } \mathcal{G}_1^{(n)} \setminus \mathcal{R}_2^{(n)} \text{ with size } \big|\mathcal{C}_{1,2}^{(n)}\big| - \big|\mathcal{G}_0^{(n)}\big|. \tag{4.38}$$

Obviously, $\mathcal{R}_{1,2}^{(n)}$ exists and, by the assumption of Case B, so do $\mathcal{R}_1^{(n)}$ and $\mathcal{R}_2^{(n)}$. By (4.20), $\mathcal{R}_1^{\prime(n)}$ exists and so does $\mathcal{I}^{(n)}$. Indeed, since $\mathcal{G}_0^{(n)} \setminus \mathcal{R}_{1,2}^{(n)} = \emptyset$, then $\mathcal{I}^{(n)} \subseteq \mathcal{G}_2^{(n)}$. Again by the property in (4.20), $\mathcal{R}_2^{\prime(n)}$ exists and so does $\mathcal{R}_{\mathrm{S}}^{(n)}$ because

$$\begin{aligned}
&\big|\mathcal{G}_1^{(n)} \setminus \big(\mathcal{R}_2^{(n)} \cup \mathcal{R}_2^{\prime(n)}\big)\big| - \big|\big(\mathcal{G}_2^{(n)} \setminus \mathcal{R}_1^{(n)} \cup \mathcal{R}_1^{\prime(n)}\big)\big| \\
&\quad = \big|\mathcal{G}_1^{(n)}\big| - \big|\mathcal{C}_2^{(n)}\big| - \big(\big|\mathcal{C}_{1,2}^{(n)}\big| - \big|\mathcal{G}_0^{(n)}\big|\big) - \Big(\big|\mathcal{G}_2^{(n)}\big| - \big|\mathcal{C}_1^{(n)}\big| - \big(\big|\mathcal{C}_{1,2}^{(n)}\big| - \big|\mathcal{G}_0^{(n)}\big|\big)\Big) \\
&\quad = \big|\mathcal{G}_1^{(n)}\big| - \big|\mathcal{C}_2^{(n)}\big| - \big|\mathcal{G}_2^{(n)}\big| + \big|\mathcal{C}_1^{(n)}\big| \geq 0.
\end{aligned}$$

Indeed, since $\mathcal{I}^{(n)} \subseteq \mathcal{G}_2^{(n)}$, notice that $\big|\mathcal{R}_{\mathrm{S}}^{(n)}\big| = \big|\mathcal{I}^{(n)}\big|$. These sets that form the partition of $\mathcal{G}^{(n)}$ in Case B can be seen in Figure 4.4, which also displays the encoding process that aims to construct $\tilde{A}_{1:L}\big[\mathcal{H}_V^{(n)}\big] = \tilde{A}_{1:L}\big[\mathcal{C}^{(n)} \cup \mathcal{G}^{(n)}\big]$.

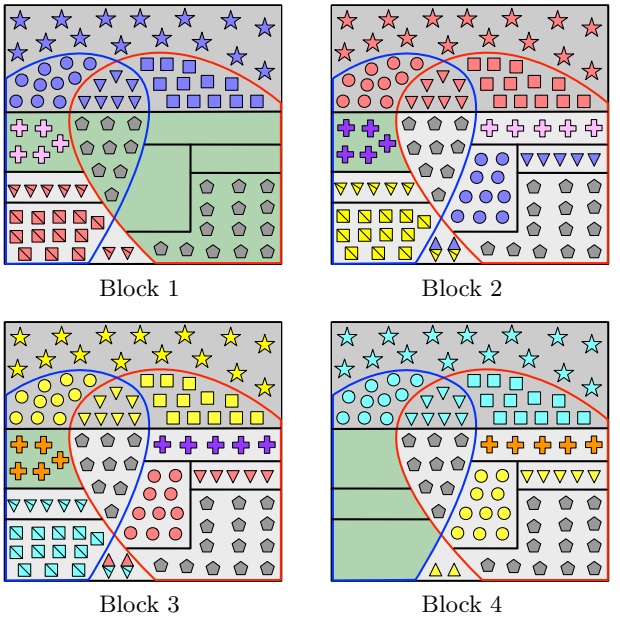

Figure 4.4: For Case B, graphically representation of the encoding that leads to the construction of $\tilde{A}_{1:L}[\mathcal{H}_V^{(n)}]$ when $L = 4$. Consider the Block 2: the sets $\mathcal{R}_1^{(n)}$, $\mathcal{R}_1'^{(n)}$, $\mathcal{R}_2^{(n)}$, $\mathcal{R}_2'^{(n)}$, $\mathcal{R}_{1,2}^{(n)}$, $\mathcal{R}_{\mathrm{S}}^{(n)}$ and $\mathcal{R}_{\Lambda}^{(n)}$ are those areas filled with yellow squares, yellow triangles, blue circles, blue triangles, blue and yellow diamonds, pink crosses, and gray pentagons, respectively, and $\mathcal{I}^{(n)}$ is the green filled area with purple crosses. At Block $i \in [1, L]$, W_i is represented by symbols of the same color (e.g., red symbols at Block 2), and $\Theta_i^{(V)}$, $\Psi_i^{(V)}$ and $\Gamma_i^{(V)}$ are represented by squares, circles and triangles respectively. Also, $\bar{\Theta}_i^{(V)}$ and $\bar{\Gamma}_i^{(V)}$ are denoted by squares and triangles, respectively, with a line through them. At Block $i \in [2, L-1]$, the diamonds denote $\Gamma_{1,i-1}^{(V)} \oplus \bar{\Gamma}_{1,i+1}^{(V)}$. In Block $i \in [1, L]$, S_i is stored into those entries whose indices belong to the green area. For $i \in [2, L-1]$, $\Pi_i^{(V)} = S_i$ and, therefore, S_i is repeated entirely into $\tilde{A}_{i+1}[\mathcal{R}_{\mathrm{S}}^{(n)}]$. The sequence $\Lambda_1^{(V)}$ from S_1 is represented by gray pentagons and is repeated in all blocks. The sequences $\Upsilon_{(1)}^{(V)}$ and $\Upsilon_{(2)}^{(V)}$ are the entries inside the red curve at Block 1 and the blue curve at Block L, respectively.

In this case, for any $i \in [1, L]$, $\Psi_{1,i}^{(V)} \triangleq \Psi_i^{(V)}$, $\bar{\Theta}_{1,i}^{(V)} \triangleq \bar{\Theta}_i^{(V)}$ and $\Psi_{2,i}^{(V)} = \bar{\Theta}_{2,i}^{(V)} \triangleq \varnothing$; and we define $\Gamma_{1,i}^{(V)}$ and $\bar{\Gamma}_{1,i}^{(V)}$ as any part of $\Gamma_i^{(V)}$ and $\bar{\Gamma}_i^{(V)}$, respectively, with size $\left|\mathcal{G}_0^{(n)}\right|$, and $\Gamma_{2,i}^{(V)}$ and $\bar{\Gamma}_{2,i}^{(V)}$ as the remaining parts with size $\left|\mathcal{C}_{1,2}^{(n)}\right| - \left|\mathcal{G}_0^{(n)}\right|$. Now, the encoder copies $\Gamma_{1,i-1}^{(V)} \oplus \bar{\Gamma}_{1,i+1}^{(V)}$ into $\tilde{A}_i\left[\mathcal{R}_{1,2}^{(n)}\right]$, and $\Gamma_{2,i-1}^{(V)}$ and $\bar{\Gamma}_{2,i+1}^{(V)}$ into $\tilde{A}_i\left[\mathcal{R}_2'^{(n)}\right]$ and $\tilde{A}_i\left[\mathcal{R}_1'^{(n)}\right]$ respectively. Moreover, since $\mathcal{I}^{(n)} \subseteq \mathcal{G}_2^{(n)}$, notice that $\Pi_i^{(V)} = S_i$ for any $i \in [2, L-1]$.

Case C

In this case, recall that $\left|\mathcal{G}_1^{(n)}\right| \geq \left|\mathcal{C}_2^{(n)}\right|$, $\left|\mathcal{G}_2^{(n)}\right| \leq \left|\mathcal{C}_1^{(n)}\right|$ and $\left|\mathcal{G}_0^{(n)}\right| > \left|\mathcal{C}_{1,2}^{(n)}\right|$. Hence, we define $\mathcal{R}_2^{(n)}$ and $\mathcal{R}_{1,2}^{(n)}$ as in (4.33) and (4.34) respectively, and $\mathcal{R}_1'^{(n)} = \mathcal{R}_2'^{(n)} = \mathcal{R}_{1,2}'^{(n)} \triangleq \emptyset$. On the other hand, since $\left|\mathcal{G}_2^{(n)}\right| \leq \left|\mathcal{C}_1^{(n)}\right|$, now for $i \in [1, L-1]$ only a part of $\bar{\Theta}_{i+1}^{(V)}$ can be repeated

entirely in $\tilde{A}_i\big[\mathcal{G}_2^{(n)}\big]$. Consequently, we define

$$\mathcal{R}_1^{(n)} \triangleq \text{the union of } \mathcal{G}_2^{(n)} \text{ with any subset of } \mathcal{G}_0^{(n)} \setminus \mathcal{R}_{1,2}^{(n)} \text{ with size } \big|\mathcal{C}_1^{(n)}\big| - \big|\mathcal{G}_2^{(n)}\big|. \quad (4.39)$$

It is clear that $\mathcal{R}_2^{(n)}$ and $\mathcal{R}_{1,2}^{(n)}$ exist. By (4.20), $\mathcal{R}_1^{(n)}$ also exists and so does $\mathcal{I}^{(n)}$. Since $\mathcal{R}_1^{(n)} \supseteq \mathcal{G}_2^{(n)}$, then $\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)} = \emptyset$ and $\mathcal{R}_{\mathrm{S}}^{(n)} = \emptyset$. These sets that form $\mathcal{G}^{(n)}$ are represented in Figure 4.5, which also displays the part of the encoding that aims to construct $\tilde{A}_{1:L}\big[\mathcal{H}_V^{(n)}\big]$.

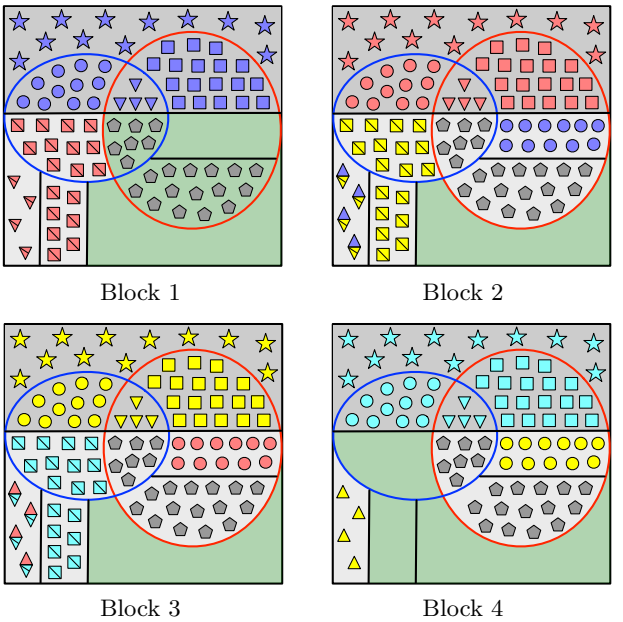

Figure 4.5: For Case C, graphically representation of the encoding that leads to the construction of $\tilde{A}_{1:L}[\mathcal{H}_V^{(n)}]$ when $L = 4$. Consider the Bloc 2: $\mathcal{R}_1^{(n)}$, $\mathcal{R}_2^{(n)}$, $\mathcal{R}_{1,2}^{(n)}$ and $\mathcal{R}_{\Lambda}^{(n)}$ are those areas filled with yellow squares, blue circles, blue and yellow diamonds, and gray pentagons, respectively, and $\mathcal{I}^{(n)}$ is the green filled area. At Block $i \in [1, L]$, W_i is represented by symbols of the same color (e.g., red symbols at Block 2), and $\Theta_i^{(V)}$, $\Psi_i^{(V)}$ and $\Gamma_i^{(V)}$ are represented by squares, circles and triangles respectively. Also, $\bar{\Theta}_i^{(V)}$ and $\bar{\Gamma}_i^{(V)}$ are denoted by squares and triangles, respectively, with a line through them. At Block $i \in [2, L-1]$, the diamonds denote $\Gamma_{1,i-1}^{(V)} \oplus \bar{\Gamma}_{1,i+1}^{(V)}$. For $i \in [1, L]$, S_i is stored into those entries belonging to the green area. The sequence $\Lambda_1^{(V)}$ is represented by gray pentagons and is repeated in all blocks. The sequences $\Upsilon_{(1)}^{(V)}$ and $\Upsilon_{(2)}^{(V)}$ are the entries inside the red curve at Block 1 and the blue curve at Block L, respectively.

In this case, for $i \in [1, L]$, we define $\Psi_{1,i}^{(V)} \triangleq \Psi_i^{(V)}$, $\Gamma_{1,i}^{(V)} \triangleq \Gamma_i^{(V)}$, $\bar{\Theta}_{1,i}^{(V)} \triangleq \bar{\Theta}_i^{(V)}$, $\bar{\Gamma}_{1,i}^{(V)} \triangleq \bar{\Gamma}_i^{(V)}$, and $\Psi_{2,i}^{(V)} = \Gamma_{2,i}^{(V)} = \bar{\Theta}_{2,i}^{(V)} = \bar{\Gamma}_{2,i}^{(V)} \triangleq \varnothing$. Moreover, note that $\Pi_i^{(V)} = \varnothing$ because $\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)} = \emptyset$.

Case D

In this case, recall that $\big|\mathcal{G}_1^{(n)}\big| < \big|\mathcal{C}_2^{(n)}\big|$, $\big|\mathcal{G}_2^{(n)}\big| < \big|\mathcal{C}_1^{(n)}\big|$ and $\big|\mathcal{G}_0^{(n)}\big| > \big|\mathcal{C}_{1,2}^{(n)}\big|$. The sets that form the partition of $\mathcal{G}^{(n)}$ in Case D are defined below and can be seen in Figure 4.6, which

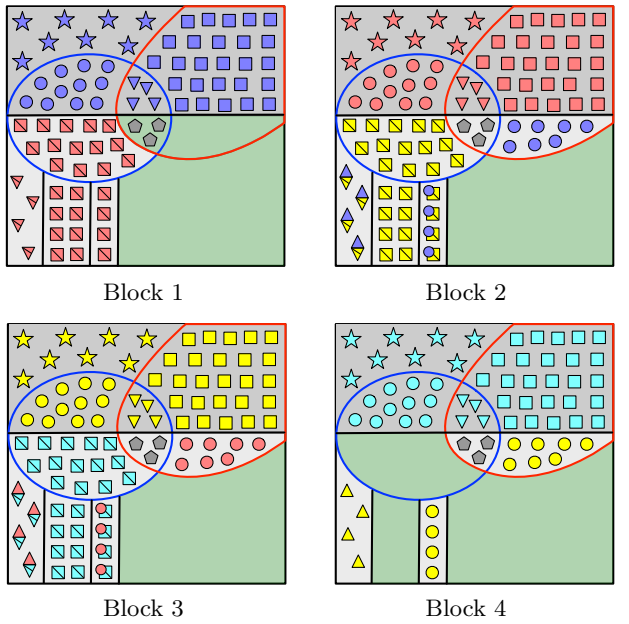

Figure 4.6: For Case D, graphically representation of the encoding that leads to the construction of $\tilde{A}_{1:L}\left[\mathcal{H}_V^{(n)}\right]$ when $L = 4$. Consider the Block 2: $\mathcal{R}_1^{(n)}$, $\mathcal{R}_2^{(n)}$, $\mathcal{R}_{1,2}^{(n)}$, $\mathcal{R}_{1,2}^{\prime(n)}$ and $\mathcal{R}_{\Lambda}^{(n)}$ are those areas filled with yellow squares, blue circles, blue and yellow diamonds, yellow squares overlapped by blue circles, and gray pentagons, respectively, and the set $\mathcal{I}^{(n)}$ is the green filled area. At Block $i \in [1, L]$, W_i is represented by symbols of the same color (e.g., red symbols at Block 2), and $\Theta_i^{(V)}$, $\Psi_i^{(V)}$ and $\Gamma_i^{(V)}$ are represented by squares, circles and triangles respectively. Also, $\bar{\Theta}_i^{(V)}$ and $\bar{\Gamma}_i^{(V)}$ are denoted by squares and triangles, respectively, with a line through them. At Block $i \in [2, L-1]$, $\Gamma_{1,i-1}^{(V)} \oplus \bar{\Gamma}_{1,i+1}^{(V)}$ is represented by diamonds, and $\Psi_{2,i-1}^{(V)} \oplus \bar{\Theta}_{2,i+1}^{(V)}$ by squares overlapped by circles. At Block $i \in [1, L]$, S_i is stored into those entries that belong to the green area. Sequence $\Lambda_1^{(V)}$ is denoted by gray pentagons and is repeated in all blocks. Sequences $\Upsilon_{(1)}^{(V)}$ and $\Upsilon_{(2)}^{(V)}$ are the entries inside the red curve at Block 1 and the blue curve at Block L, respectively.

also displays the encoding process that aims to construct of $\tilde{A}_{1:L}\left[\mathcal{H}_V^{(n)}\right]$.

As in Case A and Case C, since $\left|\mathcal{G}_0^{(n)}\right| > \left|\mathcal{C}_{1,2}^{(n)}\right|$ then we define the set $\mathcal{R}_{1,2}^{(n)}$ as in (4.34) and $\mathcal{R}_1^{\prime(n)} = \mathcal{R}_2^{\prime(n)} \triangleq \emptyset$. On the other hand, since $|\mathcal{G}_1^{(n)}| < |\mathcal{C}_2^{(n)}|$, now for $i \in [2, L]$ only a part of $\Psi_{i-1}^{(V)}$ can be repeated entirely in $\tilde{A}_i[\mathcal{G}_1^{(n)}]$. Consequently, we define $\mathcal{R}_2^{(n)} \triangleq \mathcal{G}_1^{(n)}$ and

$$\mathcal{R}_{1,2}^{\prime(n)} \triangleq \text{any subset of } \mathcal{G}_0^{(n)} \setminus \mathcal{R}_{1,2}^{(n)} \text{ with size } \left|\mathcal{C}_2^{(n)}\right| - \left|\mathcal{G}_1^{(n)}\right|. \tag{4.40}$$

By (4.20), it is clear that $\mathcal{R}_{1,2}^{\prime(n)}$ exists. Now, despite $\left|\mathcal{G}_2^{(n)}\right| < \left|\mathcal{C}_1^{(n)}\right|$ as in Case C, the set $\mathcal{R}_1^{(n)}$ is not defined as in (4.39), but

$$\begin{aligned}\mathcal{R}_1^{(n)} \triangleq{}& \text{the union of } \mathcal{G}_2^{(n)} \text{ with any subset} \\ & \text{of } \mathcal{G}_0^{(n)} \setminus \left(\mathcal{R}_{1,2}^{(n)} \cup \mathcal{R}_{1,2}^{\prime(n)}\right) \text{ with size } \left|\mathcal{C}_1^{(n)}\right| - \left|\mathcal{G}_2^{(n)}\right| - \left(\left|\mathcal{C}_2^{(n)}\right| - \left|\mathcal{G}_1^{(n)}\right|\right),\end{aligned} \tag{4.41}$$

which exists because, by the assumption in (4.20), we have

$$\begin{aligned}
&\left|\mathcal{G}_0^{(n)} \setminus \left(\mathcal{R}_{1,2}^{(n)} \cup \mathcal{R}_{1,2}^{\prime(n)}\right)\right| - \left|\mathcal{R}_1^{(n)}\right| \\
&\quad = \left|\mathcal{G}_0^{(n)}\right| - \left|\mathcal{C}_{1,2}^{(n)}\right| - \left|\mathcal{C}_2^{(n)}\right| + \left|\mathcal{G}_1^{(n)}\right| - \left(\left|\mathcal{C}_1^{(n)}\right| - \left|\mathcal{G}_2^{(n)}\right| - \left|\mathcal{C}_2^{(n)}\right| + \left|\mathcal{G}_1^{(n)}\right|\right) \\
&\quad = \left|\mathcal{G}_0^{(n)}\right| - \left|\mathcal{C}_{1,2}^{(n)}\right| - \left|\mathcal{C}_1^{(n)}\right| + \left|\mathcal{G}_2^{(n)}\right| \geq 0.
\end{aligned}$$

In this case, for $i \in [1, L]$, we set $\Gamma_{1,i}^{(V)} \triangleq \Gamma_i^{(V)}$, $\bar{\Gamma}_{1,i}^{(V)} \triangleq \bar{\Gamma}_i^{(V)}$ and $\bar{\Gamma}_{2,i}^{(V)} = \Gamma_{2,i}^{(V)} \triangleq \varnothing$. Also, we define $\Psi_{1,i}^{(V)}$ as any part of $\Psi_i^{(V)}$ with size $\left|\mathcal{G}_1^{(n)}\right|$, and $\Psi_{2,i}^{(V)}$ as the remaining part with size $\left|\mathcal{C}_2^{(n)}\right| - \left|\mathcal{G}_1^{(n)}\right|$. Lastly, we define $\bar{\Theta}_{1,i}^{(V)}$ as any part $\bar{\Theta}_i^{(V)}$ with size $\left|\mathcal{C}_1^{(n)}\right| - \left(\left|\mathcal{C}_2^{(n)}\right| - \left|\mathcal{G}_1^{(n)}\right|\right)$, and $\bar{\Theta}_{2,i}^{(V)}$ as the remaining part with size $\left|\mathcal{C}_2^{(n)}\right| - \left|\mathcal{G}_1^{(n)}\right|$.

Thus, according to Algorithm 4.2, instead of repeating $\Psi_{2,i-1}^{(V)}$, that is, the part of $\Psi_{i-1}^{(V)}$ that does not fit in $\tilde{A}_i^n\left[\mathcal{G}_1^{(n)}\right]$, in a specific part of $\tilde{A}_i\left[\mathcal{G}_0^{(n)}\right]$, the encoder stores $\Psi_{2,i-1}^{(V)} \oplus \bar{\Theta}_{2,i+1}^{(V)}$ into $\tilde{A}_i\left[\mathcal{R}_{1,2}^{\prime(n)}\right] \subseteq \tilde{A}_i\left[\mathcal{G}_0^{(n)}\right]$, where $\bar{\Theta}_{2,i+1}^{(V)}$ denotes part of those elements of $\bar{\Theta}_{i+1}^{(V)}$ that do not fit in $\tilde{A}_i\left[\mathcal{G}_2^{(n)}\right]$. Furthermore, as in Case C, since $\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)} = \emptyset$, we have $\Pi_i^{(V)} = \varnothing$.

4.2.3 Channel prefixing

For $i \in [1, L]$, let R_i be a uniformly distributed vector of length $\left|\mathcal{H}_{X|V}^{(n)} \setminus \mathcal{H}_{X|VZ}^{(n)}\right|$ that represents the randomization sequence. Also, let $\Lambda_0^{(X)}$ be a uniformly distributed random sequence of size $\left|\mathcal{H}_{X|VZ}^{(n)}\right|$. The channel prefixing aims to construct $\tilde{X}_i^n = \tilde{T}_i^n G_n$ and is summarized in Algorithm 4.3.

Algorithm 4.3 Function `pb_ch_pref`

Require: $\tilde{V}_i^n$, R_i, $\Lambda_{i-1}^{(X)}$
1: $\tilde{T}_i\left[\mathcal{H}_{X|VZ}^{(n)}\right] \leftarrow \Lambda_{i-1}^{(X)}$
2: $\tilde{T}_i\left[\mathcal{H}_{X|V}^{(n)} \setminus \mathcal{H}_{X|VZ}^{(n)}\right] \leftarrow R_i$
3: **for** $j \in \left(\mathcal{H}_{X|V}^{(n)}\right)^{\mathrm{C}}$ **do**
4: **if** $j \in \left(\mathcal{H}_{X|V}^{(n)}\right)^{\mathrm{C}} \setminus \mathcal{L}_{X|V}^{(n)}$ **then**
5: $\tilde{T}_i(j) \leftarrow p_{T(j)|T^{1:j-1}V^n}\left(\tilde{T}_i(j) \middle| \tilde{T}_i^{1:j-1}\tilde{V}_i^n\right)$
6: **else if** $j \in \mathcal{L}_{X|V}^{(n)}$ **then**
7: $\tilde{T}_i(j) \leftarrow \arg\max_{t \in \mathcal{X}} p_{T(j)|T^{1:j-1}V^n}\left(t \middle| \tilde{T}_i^{1:j-1}\tilde{V}_i^n\right)$
8: **end if**
9: **end for**
10: $\tilde{X}_i^n \leftarrow \tilde{T}_i^n G_n$
11: $\Lambda_i^{(X)} \leftarrow \tilde{T}_i\left[\mathcal{H}_{X|V}^{(n)} \setminus \mathcal{H}_{X|VZ}^{(n)}\right]$
12: **return** $\tilde{X}_i^n$ and $\Lambda_i^{(X)}$

Notice that the sequence $\Lambda_0^{(X)}$ is copied in $\tilde{T}_i\big[\mathcal{H}_{X|VZ}^{(n)}\big]$ at any Block $i \in [1, L]$, while R_i is stored into $\tilde{T}_i\big[\mathcal{H}_{X|V}^{(n)} \setminus \mathcal{H}_{X|VZ}^{(n)}\big]$. After forming $\tilde{T}_i\big[\mathcal{H}_{X|V}^{(n)}\big]$, and given the sequence $\tilde{V}_i^n \triangleq \tilde{A}_i^n G_n$, the encoder forms the remaining entries of $\tilde{T}_i^n$, that is, $\tilde{T}_i\big[\big(\mathcal{H}_{X|V}^{(n)}\big)^{\mathrm{C}}\big]$ as follows. If $j \in \mathcal{L}_{X|V}^{(n)}$, where $\mathcal{L}_{V|X}^{(n)} \triangleq \big\{j \in [1, n] : H\big(T(j)\big|T^{1:j-1}V^n\big) \leq \delta_n\big\}$, it constructs $\tilde{T}_i(j)$ deterministically by using SC encoding. Otherwise, if $j \in \big(\mathcal{H}_{X|V}^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{L}_{X|V}^{(n)}$, the encoder randomly draws $\tilde{T}_i(j)$ from distribution $p_{T(j)|T^{1:j-1}V^n}$.

4.2.4 Decoding

Consider that $\big(\Upsilon_{(k)}^{(V)}, \Phi_{(k),1:L}^{(V)}\big)$, for all $k \in [1, 2]$, is available to the k-th legitimate receiver. In the decoding process, both legitimate receivers form the estimates $\hat{A}_{1:L}^n$ of $\tilde{A}_{1:L}^n$ and then obtain the messages $\big(\hat{W}_{1:L}, \hat{S}_{1:L}\big)$.

Legitimate Receiver 1

This receiver forms the estimates $\hat{A}_{1:L}^n$ by going forward, i.e., from $\hat{A}_1^n$ to $\hat{A}_L^n$, and this process is summarized in Algorithm 4.4.

Algorithm 4.4 Decoding at legitimate Receiver 1

Require: $\Upsilon_{(1)}^{(V)}$, $\Phi_{(1),1:L}^{(V)}$, $\kappa_{\Theta}^{(V)}$ and $\kappa_{\Gamma}^{(V)}$, and $\tilde{Y}_{(1),1:L}^n$.

$\hat{A}_1^n \leftarrow \big(\Upsilon_{(1)}^{(V)}, \Phi_{(1),1}^{(V)}, \tilde{Y}_{(1),1}^n\big)$
$\hat{\Lambda}_{2:L}^{(V)} \leftarrow \hat{A}_1\big[\mathcal{R}_{\Lambda}^{(n)}\big]$
for $i = 1$ to $L - 1$ **do**
  $\hat{\Psi}_i^{(V)} \leftarrow \hat{A}_i[\mathcal{C}_2^{(n)}]$
  $\hat{\Gamma}_i^{(V)} \leftarrow \hat{A}_i[\mathcal{C}_{1,2}^{(n)}]$
  $\hat{\tilde{\Theta}}_{i+1}^{(V)} \leftarrow \big(\hat{A}_i[\mathcal{R}_1^{(n)}], \hat{A}_i[\mathcal{R}_{1,2}^{\prime(n)}] \oplus \hat{\Psi}_{2,i-1}^{(V)}\big)$
  $\hat{\Theta}_{i+1}^{(V)} \leftarrow \hat{\tilde{\Theta}}_{i+1}^{(V)} \oplus \kappa_{\Theta}^{(V)}$
  $\hat{\tilde{\Gamma}}_{i+1}^{(V)} \leftarrow \big(\hat{A}_i[\mathcal{R}_{1,2}^{(n)}] \oplus \hat{\Gamma}_{1,i-1}^{(V)}, \hat{A}_i[\mathcal{R}_1^{\prime(n)}]\big)$
  $\hat{\Gamma}_{i+1}^{(V)} \leftarrow \hat{\tilde{\Gamma}}_{i+1}^{(V)} \oplus \kappa_{\Gamma}^{(V)}$
  $\hat{\Pi}_i^{(V)} \leftarrow \hat{A}_i[\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)}]$
  $\hat{\Upsilon}_{(1),i+1}^{\prime(V)} \leftarrow \big(\hat{\Psi}_{1,i}^{(V)}, \hat{\Gamma}_{2,i}^{(V)}, \hat{\Theta}_{i+1}^{(V)}, \hat{\Gamma}_{i+1}^{(V)}, \hat{\Pi}_i^{(V)}, \hat{\Lambda}_i^{(V)}\big)$
  $\hat{A}_{i+1}^n \leftarrow \big(\hat{\Upsilon}_{(1),i+1}^{\prime(V)}, \Phi_{(1),i+1}^{(V)}, \tilde{Y}_{(1),i+1}^n\big)$
end for

In all cases (among Case A to Case D), Receiver 1 constructs $\hat{A}_1^n$ as follows. Given $\Upsilon_{(1)}^{(V)}$ (all the elements inside the red curve at Block 1 in Figures 4.3–4.6) and $\Phi_{(1),1}^{(V)}$, notice that Receiver 1 knows $\tilde{A}_1\big[\big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}}\big]$. Therefore, from $\big(\Upsilon_{(1)}^{(V)}, \Phi_{(1),1}^{(V)}\big)$ and channel observations

$\tilde{Y}^n_{(1),1}$, Receiver 1 performs SC decoding to form $\hat{A}^n_1$. Moreover, since $\Lambda^{(V)}_1$ has been replicated in all blocks, legitimate Receiver 1 obtains $\hat{\Lambda}^{(V)}_{2:L} = \hat{A}_1\big[\mathcal{R}^{(n)}_\Lambda\big]$ (gray pentagons in all blocks).

For $i \in [1, L-1]$, consider the construction of $\hat{A}^n_{i+1}$. First, since $\hat{A}^n_{1:i}$ have already been estimated, from $\hat{A}^n_i$ Receiver 1 obtains $\hat{\Psi}^{(V)}_i = \hat{A}_i\big[\mathcal{C}^{(n)}_2\big]$ (e.g., red circles at Block 2 in Figures 4.3–4.6) and $\hat{\Gamma}^{(V)}_i = \hat{A}_i\big[\mathcal{C}^{(n)}_{1,2}\big]$ (red triangles).

Also, from $\hat{A}^n_i$, Receiver 1 obtains $\hat{\Theta}^{(V)}_{i+1}$ as follows. At Block 1, in all cases it gets $\hat{\tilde{\Theta}}^{(V)}_2 = \tilde{A}_1\big[\mathcal{R}^{(n)}_1 \cup \mathcal{R}'^{(n)}_{1,2}\big]$ (all the red squares with a line through them at Block 1 in Figures 4.3–4.6). At Block $i \in [2, L-1]$, we distinguish two situations:

- In Case D, Receiver 1 gets $\hat{\tilde{\Theta}}^{(V)}_{1,i+1} = \hat{A}_i\big[\mathcal{R}^{(V)}_1\big]$ (e.g., yellow squares with a line through them at Block 2 in Figure 4.6) and $\hat{\Psi}^{(V)}_{2,i-1} \oplus \hat{\tilde{\Theta}}^{(V)}_{2,i+1} = \hat{A}_i\big[\mathcal{R}'^{(V)}_{1,2}\big]$ (yellow squares with a line through them overlapped by blue circles). Since $\hat{\Psi}^{(V)}_{2,i-1} \subset \hat{A}^n_{i-1}$ (blue circles) has already been estimated, Receiver 1 obtains $\hat{\tilde{\Theta}}^{(V)}_{2,i+1} = \hat{\Psi}^{(V)}_{2,i-1} \oplus \hat{A}_i\big[\mathcal{R}'^{(V)}_{1,2}\big]$ (yellow squares with a line through them).

- Otherwise, in other cases, Receiver 1 obtains $\hat{\tilde{\Theta}}^{(V)}_{i+1} = \hat{A}_i\big[\mathcal{R}^{(n)}_1\big]$ directly (yellow squares with a line through them at Block 2 in Figures 4.3–4.5).

Then, given $\hat{\tilde{\Theta}}^{(V)}_{i+1} = \big[\hat{\tilde{\Theta}}^{(V)}_{1,i+1}, \hat{\tilde{\Theta}}^{(V)}_{2,i+1}\big]$, in all cases Receiver 1 recovers $\hat{\Theta}^{(V)}_{i+1} = \hat{\tilde{\Theta}}^{(V)}_{i+1} \oplus \kappa^{(V)}_\Theta$.

From $\hat{A}^n_i$, Receiver 1 also obtains $\hat{\Gamma}^{(V)}_{i+1}$ as follows. At Block 1, in all cases it gets $\hat{\tilde{\Gamma}}^{(V)}_2 = \tilde{A}_1\big[\mathcal{R}^{(n)}_{1,2} \cup \mathcal{R}'^{(n)}_1\big]$ directly (e.g., all red triangles with a line through them at Block 1 in Figures 4.3–4.6). At Block $i \in [2, L-1]$, in all cases it obtains $\hat{\Gamma}^{(V)}_{1,i-1} \oplus \hat{\tilde{\Gamma}}^{(V)}_{1,i+1} = \hat{A}_i\big[\mathcal{R}^{(n)}_{1,2}\big]$ (e.g., blue and yellow diamonds with a line through them at Block 2). Since $\hat{\Gamma}^{(V)}_{1,i-1} \subset \hat{A}^n_{i-1}$ (blue triangles) has already been estimated, Receiver 1 obtains $\hat{\tilde{\Gamma}}^{(V)}_{1,i+1} = \hat{A}_i\big[\mathcal{R}^{(n)}_{1,2}\big] \oplus \hat{\Gamma}^{(V)}_{1,i-1}$ (yellow triangles with a line through them). Only in Case B, Receiver 1 obtains $\hat{\tilde{\Gamma}}^{(V)}_{2,i+1} = \hat{A}_i\big[\mathcal{R}'^{(n)}_1\big]$ (remaining yellow triangles with a line through them at Block 2 in Figure 4.4). Then, given $\hat{\tilde{\Gamma}}^{(V)}_{i+1} = \big[\hat{\tilde{\Gamma}}^{(V)}_{1,i+1}, \hat{\tilde{\Gamma}}^{(V)}_{2,i+1}\big]$, in all cases Receiver 1 recovers $\hat{\Gamma}^{(V)}_{i+1} = \hat{\tilde{\Gamma}}^{(V)}_{i+1} \oplus \kappa^{(V)}_\Gamma$.

Lastly, only in Case A and Case B, Receiver 1 obtains $\hat{\Pi}^{(V)}_i = \hat{A}_i\big[\mathcal{I}^{(n)} \cap \mathcal{G}^{(n)}_2\big]$ (e.g. purple crosses at Block 2 in Figure 4.3 and Figure 4.4).

Finally, define the sequence $\hat{\Upsilon}'^{(V)}_{(1),i+1} \triangleq \big[\hat{\Psi}^{(V)}_{1,i}, \hat{\Gamma}^{(V)}_{2,i}, \hat{\Theta}^{(V)}_{i+1}, \hat{\Gamma}^{(V)}_{i+1}, \hat{\Pi}^{(V)}_i, \hat{\Lambda}^{(V)}_i\big]$. Notice that $\hat{\Upsilon}'^{(V)}_{(1),i+1} \supseteq \hat{A}_{i+1}\big[\mathcal{H}^{(n)}_V \setminus \mathcal{L}^{(n)}_{V|Y_{(1)}}\big]$ (elements inside red curve at Block $i+1$ in Figures 4.3–4.6). Therefore, Receiver 1 performs SC decoding to form $\hat{A}^n_{i+1}$ by using $\hat{\Upsilon}'^{(V)}_{(1),i+1}$, $\Phi^{(V)}_{(1),i+1}$ and the channel output observations $\tilde{Y}^n_{(1),i+1}$.

Legitimate receiver 2

This receiver forms the estimates $\hat{A}^n_{1:L}$ by going backward, i.e., from $\hat{A}^n_L$ to $\hat{A}^n_1$, and this process is summarized in Algorithm 4.5.

Algorithm 4.5 Decoding at legitimate Receiver 2

Require: $\Upsilon_{(2)}^{(V)}$, $\Phi_{(2),1:L}^{(V)}$, $\kappa_{\Theta}^{(V)}$ and $\kappa_{\Gamma}^{(V)}$, and $\tilde{Y}_{(2),1:L}^{n}$.

$\hat{A}_L^n \leftarrow \big(\Upsilon_{(2)}^{(V)}, \Phi_{(2),L}^{(V)}, \tilde{Y}_{(2),L}^{n}\big)$
$\hat{\Lambda}_{1:L-1}^{(V)} \leftarrow \hat{A}_L\big[\mathcal{R}_{\Lambda}^{(n)}\big]$
for $i = L$ to 2 **do**
  $\hat{\tilde{\Theta}}_i^{(V)} \leftarrow \hat{A}_i[\mathcal{C}_1^{(n)}] \oplus \kappa_{\Theta}^{(V)}$
  $\hat{\tilde{\Gamma}}_i^{(V)} \leftarrow \hat{A}_i[\mathcal{C}_{1,2}^{(n)}] \oplus \kappa_{\Gamma}^{(V)}$
  $\hat{\Psi}_{i-1}^{(V)} \leftarrow \big(\hat{A}_i[\mathcal{R}_2^{(n)}], \hat{A}_i[\mathcal{R}_{1,2}^{\prime(n)}] \oplus \hat{\tilde{\Theta}}_{2,i+1}^{(V)}\big)$
  $\hat{\Gamma}_{i-1}^{(V)} \leftarrow \big(\hat{A}_i[\mathcal{R}_{1,2}^{(n)}] \oplus \hat{\tilde{\Gamma}}_{1,i+1}^{(V)}, \hat{A}_i[\mathcal{R}_2^{\prime(n)}]\big)$
  $\hat{\Pi}_{i-1}^{(V)} \leftarrow \hat{A}_i[\mathcal{R}_{\mathrm{S}}^{(n)}]$
  $\Upsilon_{(2),i-1}^{\prime(V)} \leftarrow \big(\hat{\tilde{\Theta}}_{1,i}^{(V)}, \hat{\tilde{\Gamma}}_{2,i}^{(V)}, \hat{\Psi}_{i-1}^{(V)}, \hat{\Gamma}_{i-1}^{(V)}, \hat{\Pi}_{i-1}^{(V)}, \hat{\Lambda}_{i-1}^{(V)}\big)$
  $\hat{A}_{i-1}^{n} \leftarrow \big(\Upsilon_{(2),i-1}^{\prime(V)}, \Phi_{(2),i-1}^{(V)}, \tilde{Y}_{(2),i-1}^{n}\big)$
end for

In all cases (among Case A to Case D), Receiver 2 constructs $\hat{A}_L^n$ as follows. Given $\Upsilon_{(2)}^{(V)}$ (all the elements inside blue curve at Block 4 in Figures 4.3–4.6) and $\Phi_{(2),L}^{(V)}$, notice that Receiver 2 knows $\tilde{A}_L\big[\big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}}\big]$. Hence, from $\big(\Upsilon_{(2)}^{(V)}, \Phi_{(2),L}^{(V)}\big)$ and channel output observations $\tilde{Y}_{(2),L}^{n}$, Receiver 2 performs SC decoding to form $\hat{A}_L^n$. Since $\Lambda_1^{(V)}$ has been replicated in all blocks, from $\hat{A}_L^n$ it obtains $\hat{\Lambda}_{1:L-1}^{(V)} = \hat{A}_L\big[\mathcal{R}_{\Lambda}^{(n)}\big]$ (gray pentagons at all blocks).

For $i \in [2, L]$, consider the construction of $\hat{A}_{i-1}^n$. First, since $\hat{A}_{i:L}^n$ have already been estimated, from $\hat{A}_i^n$ Receiver 2 obtains the sequence $\hat{\Theta}_i^{(V)} = \hat{A}_i\big[\mathcal{C}_1^{(n)}\big]$ (e.g., yellow squares at Block 3 in Figures 4.3–4.6). Given $\hat{\Theta}_i^{(V)}$, it computes $\hat{\tilde{\Theta}}_i^{(V)} = \hat{\Theta}_i^{(V)} \oplus \kappa_{\Theta}^{(V)}$ (yellow squares with a line through them). Also, Receiver 2 obtains $\hat{\Gamma}_i^{(V)} = \hat{A}_i\big[\mathcal{C}_{1,2}^{(n)}\big]$ (yellow triangles at Block 3 in Figures 4.3–4.6). Given this sequence, it computes $\hat{\tilde{\Gamma}}_i^{(V)} = \hat{\Gamma}_i^{(V)} \oplus \kappa_{\Gamma}^{(V)}$ (yellow triangles with a line through them).

Also, from $\hat{A}_i^n$, Receiver 2 obtains $\hat{\Psi}_{i-1}^{(V)}$ as follows. At block L, in all cases it gets $\hat{\Psi}_{L-1}^{(V)} = \hat{A}_i\big[\mathcal{R}_2^{(n)} \cup \mathcal{R}_{1,2}^{\prime(n)}\big]$ directly (all yellow circles at Block L in Figures 4.3–4.6). At Block $i \in [2, L-1]$, we distinguish two situations:

- In Case D, Receiver 2 obtains $\hat{\Psi}_{1,i-1}^{(V)} = \hat{A}_i\big[\mathcal{R}_2^{(n)}\big]$ (e.g., red circles at Block 3 in Figure 4.6) and $\hat{\Psi}_{2,i-1}^{(V)} \oplus \hat{\tilde{\Theta}}_{2,i+1}^{(V)} = \hat{A}_i\big[\mathcal{R}_{1,2}^{\prime(n)}\big]$ (cyan squares with a line through them overlapped by red circles). Since $\hat{\tilde{\Theta}}_{2,i+1}^{(V)}$ (cyan squares with a line through them) has already been estimated, it obtains $\hat{\Psi}_{2,i-1}^{(V)} = \hat{A}_i\big[\mathcal{R}_{1,2}^{\prime(n)}\big] \oplus \hat{\tilde{\Theta}}_{2,i+1}^{(V)}$ (red circles).

- Otherwise, in other cases, Receiver 2 obtains directly $\hat{\Psi}_{i-1}^{(V)} = \hat{A}_i\big[\mathcal{R}_2^{(n)}\big]$ (e.g., red circles at Block 3 in Figures 4.3–4.5).

From $\hat{A}_i^n$, Receiver 2 also obtains $\hat{\Gamma}_{i-1}^{(V)}$ as follows. At block L, in all cases it gets $\hat{\tilde{\Gamma}}_{L-1}^{(V)} = \hat{A}_L\big[\mathcal{R}_{1,2}^{(n)} \cup \mathcal{R}_2^{\prime(n)}\big]$ (e.g., all yellow triangles at Block L in Figures 4.3–4.6). At Block $i \in [2, L-1]$, in all cases Receiver 2 obtains $\hat{\Gamma}_{1,i-1}^{(V)} \oplus \hat{\tilde{\Gamma}}_{1,i+1}^{(V)} = \hat{A}_i\big[\mathcal{R}_{1,2}^{(n)}\big]$ (e.g., red and cyan diamonds with a line through them at Block 3). Since $\hat{\tilde{\Gamma}}_{1,i+1}^{(V)}$ (cyan triangles with a line through them) has already been estimated, Receiver 2 obtains $\hat{\Gamma}_{1,i-1}^{(V)} = \hat{A}_i\big[\mathcal{R}_{1,2}^{(n)}\big] \oplus \hat{\tilde{\Gamma}}_{1,i+1}^{(V)}$ (red triangles). Also, only in Case B, Receiver 2 obtains the sequence $\hat{\Gamma}_{2,i-1}^{(V)} = \hat{A}_i\big[\mathcal{R}_2^{\prime(n)}\big]$ (remaining red triangles at Block 3 in Figure 4.4).

Lastly, only in Case A and Case B, Receiver 2 obtains the sequence $\hat{\Pi}_{i-1}^{(V)} = \hat{A}_i\big[\mathcal{R}_{\mathrm{S}}^{(n)}\big]$ (e.g., purple crosses at Block 3 in Figure 4.3 and Figure 4.4).

Finally, define the sequence $\Upsilon_{(2),i-1}^{\prime(V)} \triangleq \big[\hat{\tilde{\Theta}}_{1,i}^{(V)}, \hat{\tilde{\Gamma}}_{2,i}^{(V)}, \hat{\Psi}_{i-1}^{(V)}, \hat{\Gamma}_{i-1}^{(V)}, \hat{\Pi}_{i-1}^{(V)}, \hat{\Lambda}_{i-1}^{(V)}\big]$. Notice that $\Upsilon_{(2),i-1}^{\prime(V)} \supseteq \hat{A}_{i-1}\big[\mathcal{H}_V^{(n)} \setminus \mathcal{L}_{V|Y_{(2)}}^{(n)}\big]$ (elements inside blue curve at Block $i-1$ in Figures 4.3–4.6). Thus, Receiver 2 performs SC decoding to form $\hat{A}_{i-1}^n$ by using $\Upsilon_{(2),i-1}^{\prime(V)}$, $\Phi_{(2),i-1}^{(V)}$ and $\tilde{Y}_{(2),i-1}^n$.

4.3 Performance of the polar coding scheme

The analysis of the polar coding scheme of Section 4.2 leads to the following theorem.

Theorem 4.1. *Let $(\mathcal{X}, p_{Y_{(1)}Y_{(2)}Z|X}, \mathcal{Y}_{(1)} \times \mathcal{Y}_{(2)} \times \mathcal{Z})$ be an arbitrary WTBC such that $\mathcal{X} \in \{0,1\}$. The PCS described in Section 4.2 achieves the corner point in Equation (4.4) of the region $\mathfrak{R}_{\text{CI-WTBC}}$ defined in Proposition 4.1.*

The proof of Theorem 4.1 follows in four steps and is provided in the following subsections. In Section 4.3.1 we show that the PCS approaches the rate tuple in (4.4). In Section 4.3.2 we prove that the joint distribution of $(\tilde{V}_i^n, \tilde{X}_i^n, \tilde{Y}_{(1),i}^n, \tilde{Y}_{(2),i}^n, \tilde{Z}_i^n)$, for all $i \in [1, L]$, is asymptotically indistinguishable of the one of the original DMS that is used for the polar code construction. Finally, in Section 4.3.3 and Section 4.3.4 we show that the polar coding scheme satisfies the reliability and the secrecy conditions (4.1) and (4.2) respectively.

4.3.1 Transmission rates

We prove that the polar coding scheme described in Section 4.2 approaches the rate tuple in Equation (4.4). Also, we show that the overall length of the secret keys $\kappa_{\Theta}^{(V)}$, $\kappa_{\Gamma}^{(V)}$, $\kappa_{\Upsilon\Phi_{(1)}}^{(V)}$ and $\kappa_{\Upsilon\Phi_{(2)}}^{(V)}$, and the additional randomness used in the encoding (besides the randomization sequences) are asymptotically negligible in terms of rate.

Private message rate

For $i \in [1, L]$, we have $W_i = \tilde{A}_i\big[\mathcal{C}^{(n)}\big]$. According to the definition of $\mathcal{C}^{(n)}$ in (4.11), and since $\mathcal{H}_{V|Z}^{(n)} \subseteq \mathcal{H}_V^{(n)}$, the rate of $W_{1:L}$ is

$$\frac{1}{nL}\sum_{i=1}^{L}|W_i| = \frac{1}{n}\big|\mathcal{H}_V^{(n)} \cap \big(\mathcal{H}_{V|Z}^{(n)}\big)^{\mathrm{C}}\big| = \frac{1}{n}\big|\mathcal{H}_V^{(n)}\big| - \frac{1}{n}\big|\mathcal{H}_{V|Z}^{(n)}\big| \xrightarrow{n\to\infty} H(V) - H(V|Z)$$

where the limit holds by Theorem 2.1. Therefore, the private message rate achieved by the polar coding scheme is $R_W = I(V;Z)$ as in (4.4).

Confidential message rate

From Section 4.2.2, in all cases we have $S_1 = \tilde{A}_1\big[\mathcal{I}^{(n)} \cup \mathcal{G}_1^{(n)} \cup \mathcal{G}_{1,2}^{(n)}\big]$; for $i \in [2, L-1]$, we have $S_i = \tilde{A}_i\big[\mathcal{I}^{(n)}\big]$; and $S_L = \tilde{A}_L\big[\mathcal{I}^{(n)} \cup \mathcal{G}_2^{(n)}\big]$. Thus, we have

$$\begin{aligned}
&\frac{1}{nL}\sum_{i=1}^{L}|S_i| \\
&= \frac{(L-2)}{nL}\big|\mathcal{I}^{(n)}\big| + \frac{1}{nL}\Big(\big|\mathcal{I}^{(n)} \cup \mathcal{G}_1^{(n)} \cup \mathcal{G}_{1,2}^{(n)}\big| + \big|\mathcal{I}^{(n)} \cup \mathcal{G}_2^{(n)}\big|\Big) \\
&= \frac{1}{n}\big|\mathcal{I}^{(n)}\big| + \frac{1}{nL}\Big(\big|\mathcal{G}_1^{(n)}\big| + \big|\mathcal{G}_2^{(n)}\big| + \big|\mathcal{G}_{1,2}^{(n)}\big|\Big) \\
&= \frac{1}{n}\big|\mathcal{I}^{(n)}\big| + \frac{1}{nL}\big|\mathcal{G}^{(n)} \setminus \mathcal{G}_0^{(n)}\big| \\
&\overset{(a)}{=} \frac{1}{n}\Big(\big|\mathcal{G}_0^{(n)}\big| + \big|\mathcal{G}_2^{(n)}\big| - \big|\mathcal{R}_{1,2}^{(n)}\big| - \big|\mathcal{R}_{1,2}^{\prime(n)}\big| - \big|\mathcal{R}_1^{(n)}\big| - \big|\mathcal{R}_1^{\prime(n)}\big|\Big) + \frac{1}{nL}\big|\mathcal{G}^{(n)} \setminus \mathcal{G}_0^{(n)}\big| \\
&\overset{(b)}{=} \frac{1}{n}\Big(\big|\mathcal{G}_0^{(n)}\big| + \big|\mathcal{G}_2^{(n)}\big| - \big|\mathcal{C}_1^{(n)}\big| - \big|\mathcal{C}_{1,2}^{(n)}\big|\Big) + \frac{\big|\mathcal{G}^{(n)} \setminus \mathcal{G}_0^{(n)}\big|}{nL} \\
&\overset{(c)}{\geq} \frac{1}{n}\Big(\big|\mathcal{H}_{V|Z}^{(n)} \cap \mathcal{L}_{V|Y_{(1)}}^{(n)}\big| - \big|\big(\mathcal{H}_{V|Z}^{(n)}\big)^{\mathrm{C}} \cap \big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}}\big|\Big) + \frac{1}{nL}\Big|\mathcal{H}_{V|Z}^{(n)} \cap \Big(\mathcal{L}_{V|Y_{(1)}}^{(n)} \cap \mathcal{L}_{V|Y_{(2)}}^{(n)}\Big)^{\mathrm{C}}\Big| \\
&\overset{(d)}{\geq} \frac{1}{n}\Big(\big|\mathcal{H}_{V|Z}^{(n)} \cap \mathcal{L}_{V|Y_{(1)}}^{(n)}\big| - \big|\big(\mathcal{H}_{V|Z}^{(n)}\big)^{\mathrm{C}} \cap \big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}}\big|\Big) + \frac{1}{nL}\big|\mathcal{H}_{V|Z}^{(n)}\big| - \frac{1}{nL}\Big|\big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}}\Big| \\
&= \frac{1}{n}\big|\mathcal{H}_{V|Z}^{(n)}\big| - \frac{1}{n}\big|\big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}}\big| + \frac{1}{nL}\big|\mathcal{H}_{V|Z}^{(n)}\big| - \frac{1}{nL}\big|\big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}}\big| \\
&\xrightarrow{n\to\infty} H(V|Z) - H(V|Y_{(1)}) + \frac{1}{L}\big(H(V|Z) - H(V|Y_{(1)})\big) \\
&\xrightarrow{L\to\infty} H(V|Z) - H(V|Y_{(1)})
\end{aligned}$$

where (a) holds by the definition of $\mathcal{I}^{(n)}$ in (4.29); (b) holds because, in all cases, we have $\big|\mathcal{R}_{1,2}^{(n)}\big| + \big|\mathcal{R}_1^{\prime(n)}\big| = \big|\mathcal{C}_{1,2}^{(n)}\big|$ and $\big|\mathcal{R}_1^{(n)}\big| + \big|\mathcal{R}_{1,2}^{\prime(n)}\big| = \big|\mathcal{C}_1^{(n)}\big|$; (c) follows from the partition of $\mathcal{H}_V^{(n)}$ defined in (4.12)–(4.19); (d) follows from applying elementary set operations and because,

by assumption, $H(V|Y_{(1)}) \geq H(V|Y_{(2)})$, which means that $\big|\big(\mathcal{L}^{(n)}_{V|Y_{(1)}}\big)^{\mathrm{C}}\big| \geq \big|\big(\mathcal{L}^{(n)}_{V|Y_{(2)}}\big)^{\mathrm{C}}\big|$ (by Theorem 2.1); and the limit when n goes to infinity holds also by Theorem 2.1. Hence, the PCS operates as close to the rate R_S in (4.4) as desired by choosing a sufficiently large L.

Randomization sequence rate

For $i \in [1, L]$, we have $R_i = \tilde{T}_i\big[\mathcal{H}^{(n)}_{X|V} \cap (\mathcal{H}^{(n)}_{X|VZ})^{\mathrm{C}}\big]$. Since $\mathcal{H}^{(n)}_{X|VZ} \supseteq \mathcal{H}^{(n)}_{X|V}$, we have

$$\frac{1}{nL}\sum_{i=1}^{L}|R_i| = \frac{1}{n}\Big|\mathcal{H}^{(n)}_{X|V} \cap \big(\mathcal{H}^{(n)}_{X|VZ}\big)^{\mathrm{C}}\Big| = \frac{1}{n}\big|\mathcal{H}^{(n)}_{X|V}\big| - \frac{1}{n}\big|\mathcal{H}^{(n)}_{X|VZ}\big| \xrightarrow{n\to\infty} H(X|Z) - H(X|VZ)$$

where the limit holds by Theorem 2.1. Thus, the randomization sequence rate used by the PCS is $R_R = I(X;Z|V)$ as in (4.4).

Private-shared sequence rate

Transmitter and legitimate Receiver $k \in [1, 2]$ must privately share the keys $\kappa^{(V)}_{\Theta}$, $\kappa^{(V)}_{\Gamma}$ and $\kappa^{(V)}_{\Upsilon\Phi_{(k)}}$. Hence, the overall rate is

$$\begin{aligned}
&\frac{1}{nL}\Big(\big|\kappa^{(V)}_{\Theta}\big| + \big|\kappa^{(V)}_{\Gamma}\big| + \sum_{k=1}^{2}\big|\kappa^{(V)}_{\Upsilon\Phi_{(k)}}\big|\Big) \\
&\quad= \frac{1}{nL}\Big(\big|\mathcal{C}^{(n)}_{1}\big| + \big|\mathcal{C}^{(n)}_{1,2}\big|\Big) + \frac{1}{nL}\sum_{k=1}^{2}\Big(L\big|\big(\mathcal{H}^{(n)}_{V}\big)^{\mathrm{C}} \cap \big(\mathcal{L}^{(n)}_{V|Y_{(k)}}\big)^{\mathrm{C}}\big| + \big|\mathcal{H}^{(n)}_{V} \cap \big(\mathcal{L}^{(n)}_{V|Y_{(k)}}\big)^{\mathrm{C}}\big|\Big) \\
&\quad\overset{(a)}{=} \frac{1}{nL}\Big(\big|\mathcal{H}^{(n)}_{V} \cap \big(\mathcal{H}^{(n)}_{V|Z}\big)^{\mathrm{C}} \cap \big(\mathcal{L}^{(n)}_{V|Y_{(1)}}\big)^{\mathrm{C}}\big|\Big) \\
&\qquad+ \frac{1}{nL}\sum_{k=1}^{2}\Big(L\big|\big(\mathcal{H}^{(n)}_{V}\big)^{\mathrm{C}} \cap \big(\mathcal{L}^{(n)}_{V|Y_{(k)}}\big)^{\mathrm{C}}\big| + \big|\mathcal{H}^{(n)}_{V} \cap \big(\mathcal{L}^{(n)}_{V|Y_{(k)}}\big)^{\mathrm{C}}\big|\Big) \\
&\quad\overset{(b)}{\leq} \frac{1}{nL}\big|\big(\mathcal{L}^{(n)}_{V|Y_{(1)}}\big)^{\mathrm{C}}\big| + \frac{1}{nL}\sum_{k=1}^{2}\Big(L\big|\big(\mathcal{H}^{(n)}_{V|Y_{(k)}}\big)^{\mathrm{C}} \cap \big(\mathcal{L}^{(n)}_{V|Y_{(k)}}\big)^{\mathrm{C}}\big| + \big|\big(\mathcal{L}^{(n)}_{V|Y_{(k)}}\big)^{\mathrm{C}}\big|\Big) \\
&\quad\xrightarrow{n\to\infty} \frac{1}{L}\big(2H(V|Y_{(1)}) + H(V|Y_{(2)})\big) \\
&\quad\xrightarrow{L\to\infty} 0,
\end{aligned}$$

where (a) follows from the definition of $\mathcal{C}^{(n)}_{1}$ and $\mathcal{C}^{(n)}_{1,2}$ in (4.17) and (4.19) respectively; (b) follows from standard set properties and because $\big(\mathcal{H}^{(n)}_{V|Z}\big)^{\mathrm{C}} \subseteq \big(\mathcal{H}^{(n)}_{V|Y_{(k)}}\big)^{\mathrm{C}}$ for any $k \in [1, 2]$; and the limit when n goes to infinity holds by Theorem 2.1.

Rate of the additional randomness

Besides the randomization sequences $R_{1:L}$, the encoder uses the random sequence $\Lambda_0^{(X)}$, with size $\left|\mathcal{H}_{X|V}^{(n)}\right|$, for the polar-based channel prefixing. Moreover, for $i \in [1, L]$, the encoder randomly draws those elements $\tilde{A}_i(j)$ such that $j \in \left(\mathcal{H}_V^{(n)}\right)^{\mathrm{C}} \setminus \mathcal{L}_V^{(n)}$, and those elements $\tilde{T}_i(j)$ such that $j \in \left(\mathcal{H}_{X|V}^{(n)}\right)^{\mathrm{C}} \setminus \mathcal{L}_{X|V}^{(n)}$. Nevertheless, we have

$$\begin{aligned}
&\frac{1}{nL}\Big(\left|\mathcal{H}_{X|V}^{(n)}\right| + L\left|\left(\mathcal{H}_V^{(n)}\right)^{\mathrm{C}} \setminus \mathcal{L}_V^{(n)}\right| + L\left|\left(\mathcal{H}_{X|V}^{(n)}\right)^{\mathrm{C}} \setminus \mathcal{L}_{X|V}^{(n)}\right|\Big) \\
&\quad \xrightarrow{n\to\infty} \frac{1}{L} H(X|V) \\
&\quad \xrightarrow{L\to\infty} 0,
\end{aligned}$$

where the limit when n approaches to infinity follows from applying Theorem 2.1.

4.3.2 Distribution of the DMS after the polar encoding

For $i \in [1, L]$, let $\tilde{q}_{A_i^n T_i^n}$ denote the distribution of $(\tilde{A}_i^n, \tilde{T}_i^n)$ after the encoding. The following lemma proves that $\tilde{q}_{A_i^n T_i^n}$ and the marginal distribution $p_{A^n T^n}$ of the original DMS are nearly statistically indistinguishable for sufficiently large n and, consequently, so are $\tilde{q}_{V_i^n X_i^n Y_{(1),i}^n Y_{(2),i}^n Z_i^n}$ and $p_{V^n X^n Y_{(1)}^n Y_{(2)}^n Z^n}$. This result is crucial for the reliability and secrecy performance of the polar coding scheme.

Lemma 4.1. *For any $i \in [1, L]$, we obtain*

$$\begin{aligned}
\mathbb{V}(\tilde{q}_{A_i^n T_i^n}, p_{A^n T^n}) &\le \delta_n^{(*)}, \\
\mathbb{V}(\tilde{q}_{V_i^n X_i^n Y_{(1),i}^n Y_{(2),i}^n Z_i^n}, p_{V^n X^n Y_{(1)}^n Y_{(2)}^n Z^n}) &\le \delta_n^{(*)},
\end{aligned}$$

where $\delta_n^{(*)} \triangleq 2n\sqrt{4\sqrt{n\delta_n \ln 2}\left(2n - \log\left(2\sqrt{n\delta_n \ln 2}\right)\right) + \delta_n} + 2\sqrt{n\delta_n \ln 2}$.

Proof. For the first claim, see Lemma 2.3 taking $T_{\mathrm{V}} \triangleq 2$. The second holds by Corollary 2.2 due to the invertibility of G_n and $\tilde{q}_{X^n Y_K^n \ldots Y_1^n Z_M^n \ldots Z_1^n} \equiv \tilde{q}_{V_i^n X_i^n} p_{Y_{(1),i}^n Y_{(2),i}^n Z_i^n | X_i^n}$. □

4.3.3 Reliability analysis

In this section we prove that both legitimate receivers can reliably reconstruct the private and the confidential messages $(W_{1:L}, S_{1:L})$ with arbitrary small error probability.

For $i \in [1, L]$ and $k \in [1, 2]$, let $\tilde{q}_{V_i^n Y_{(k),i}^n}$ and $p_{V^n Y_{(k)}^n}$ be marginals of $\tilde{q}_{V_i^n X_i^n Y_{(1),i}^n Y_{(2),i}^n Z_i^n}$ and $p_{V^n X^n Y_{(1)}^n Y_{(2)}^n Z^n}$ respectively, and define an optimal coupling [LPW09] (Proposition 4.7) between $\tilde{q}_{V_i^n Y_{(k),i}^n}$ and $p_{V^n Y_{(k)}^n}$ such that $\mathbb{P}\left[\mathcal{E}_{V_i^n Y_{(k),i}^n}\right] = \mathbb{V}\left(\tilde{q}_{V_i^n Y_{(k),i}^n}, p_{V^n Y_{(k)}^n}\right)$, where

$\mathcal{E}_{V_i^n Y_{(k),i}^n} \triangleq \big\{\big(\tilde{V}_i^n, \tilde{Y}_{(k),i}^n\big) \neq \big(V^n, Y_{(k)}^n\big)\big\}$. Additionally, define the error event

$$\mathcal{E}_{(k),i} \triangleq \Big\{\hat{A}_i\big[\big(\mathcal{L}_{V|Y_{(k)}}^{(n)}\big)^{\mathrm{C}}\big] \neq \tilde{A}_i\big[\big(\mathcal{L}_{V|Y_{(k)}}^{(n)}\big)^{\mathrm{C}}\big]\Big\}.$$

Recall that $(\Upsilon_{(k)}^{(V)}, \Phi_{(k),1:L}^{(V)})$ is available to Receiver $k \in [1,2]$. Thus, $\mathbb{P}[\mathcal{E}_{(1),1}] = \mathbb{P}[\mathcal{E}_{(2),L}] = 0$ because given $\Upsilon_{(1)}^{(V)}$ and $\Phi_{(1),1}^{(V)}$ legitimate Receiver 1 knows $\tilde{A}_1\big[\big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}}\big]$, and given $\Upsilon_{(2)}^{(V)}$ and $\Phi_{(2),L}^{(V)}$ legitimate Receiver 2 knows $\tilde{A}_L\big[\big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}}\big]$. Moreover, due to the chaining structure, in Section 4.2.4 we have seen that $\tilde{A}_i\big[\mathcal{H}_V^{(n)} \cap \big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}}\big]$ is repeated in $\tilde{A}_{i-1}^n$ for $i \in [2, L]$. Therefore, at legitimate Receiver 1, for $i \in [2, L]$ we have

$$\mathbb{P}[\mathcal{E}_{(1),i}] \leq \mathbb{P}\big[\hat{A}_{i-1}^n \neq \tilde{A}_{i-1}^n\big]. \tag{4.42}$$

Similarly, due to the chaining construction, we have seen that $\tilde{A}_i\big[\mathcal{H}_V^{(n)} \cap \big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}}\big]$ is repeated in $\tilde{A}_{i+1}^n$ for $i \in [1, L-1]$. Thus, at legitimate Receiver 2, for $i \in [1, L-1]$ we obtain

$$\mathbb{P}[\mathcal{E}_{(2),i}] \leq \mathbb{P}\big[\hat{A}_{i+1}^n \neq \tilde{A}_{i+1}^n\big]. \tag{4.43}$$

Hence, the probability of incorrectly decoding (W_i, S_i) at the Receiver $k \in [1,2]$ is

$$\begin{aligned}
\mathbb{P}\big[(W_i, S_i) \neq (\hat{W}_i, \hat{S}_i)\big] &\leq \mathbb{P}\big[\hat{A}_i^n \neq \tilde{A}_i^n\big] \\
&= \mathbb{P}\big[\hat{A}_i^n \neq \tilde{A}_i^n \big| \mathcal{E}_{V_i^n Y_{(k),i}^n}^{\mathrm{C}} \cap \mathcal{E}_{(k),i}^{\mathrm{C}}\big]\mathbb{P}\big[\mathcal{E}_{V_i^n Y_{(k),i}^n}^{\mathrm{C}} \cap \mathcal{E}_{(k),i}^{\mathrm{C}}\big] \\
&\quad + \mathbb{P}\big[\hat{A}_i^n \neq \tilde{A}_i^n \big| \mathcal{E}_{V_i^n Y_{(k),i}^n} \cup \mathcal{E}_{(k),i}\big]\mathbb{P}\big[\mathcal{E}_{V_i^n Y_{(k),i}^n} \cup \mathcal{E}_{(k),i}\big] \\
&\leq \mathbb{P}\big[\hat{A}_i^n \neq \tilde{A}_i^n \big| \mathcal{E}_{V_i^n Y_{(k),i}^n}^{\mathrm{C}} \cap \mathcal{E}_{(k),i}^{\mathrm{C}}\big] + \mathbb{P}\big[\mathcal{E}_{V_i^n Y_{(k),i}^n}\big] + \mathbb{P}\big[\mathcal{E}_{(k),i}\big] \\
&\overset{(a)}{\leq} n\delta_n + \mathbb{P}\big[\mathcal{E}_{V_i^n Y_{(k),i}^n}\big] + \mathbb{P}\big[\mathcal{E}_{(k),i}\big] \\
&\overset{(b)}{\leq} n\delta_n + \delta_n^{(*)} + \mathbb{P}\big[\mathcal{E}_{(k),i}\big] \\
&\overset{(c)}{\leq} i\big(n\delta_n + \delta_n^{(*)}\big),
\end{aligned}$$

where (a) holds by Theorem 2.1; (b) follows from the optimal coupling and Lemma 4.1; and (c) holds by induction and Equations (4.42) and (4.43). Therefore, by the union bound we obtain

$$\mathbb{P}\big[(W_{1:L}, S_{1:L}) \neq (\hat{W}_{1:L}, \hat{S}_{1:L})\big] \leq \sum_{i=1}^{L} \mathbb{P}\big[\tilde{A}_i^n \neq \hat{A}_i^n\big] \leq \frac{L(L+1)}{2}\big(n\delta_n + 2\delta_n^{(*)}\big),$$

and for sufficiently large n the PCS satisfies the reliability condition in (4.1).

4.3.4 Secrecy analysis

Since encoding in Section 4.2 takes place over L blocks of size n, we need to prove that

$$\lim_{n\to\infty} I(S_{1:L}, \tilde{Z}^n_{1:L}) = 0.$$

For clarity and with slight abuse of notation, for any Block $i \in [1, L]$ let

$$\Xi_i^{(V)} \triangleq \left[\Pi_i^{(V)}, \Lambda_i^{(V)}, \Psi_i^{(V)}, \Gamma_i^{(V)}\right], \tag{4.44}$$

which denotes the entire sequence depending on $\tilde{A}_i^n$ that is repeated at Block $i+1$. Also, let

$$\bar{\Omega}_i^{(V)} \triangleq [\bar{\Theta}_i^{(V)}, \bar{\Gamma}_i^{(V)}], \tag{4.45}$$

which represents the sequence depending on $\tilde{A}_i^n$ that is repeated at Block $i-1$. Furthermore, we define $\kappa_\Omega^{(V)} \triangleq [\kappa_\Theta^{(V)}, \kappa_\Gamma^{(V)}]$. Then, a Bayesian graph describing the dependencies between all the variables involved in the PCS of Section 4.2 is given in Figure 4.7.

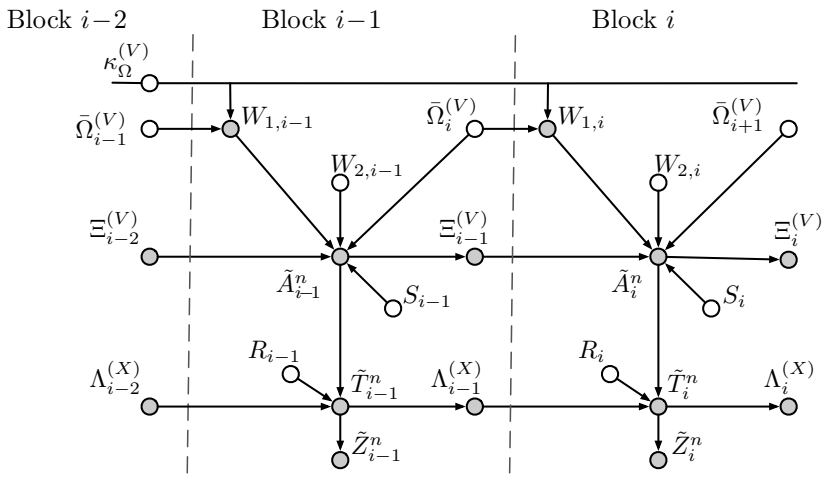

Figure 4.7: Graphical representation (Bayesian graph) of the dependencies between random variables involved in the PCS. Independent random variables are indicated by white nodes, whereas those that are dependent are indicated by gray nodes.

Despite $\Gamma_i^{(V)} \subseteq \Xi_i^{(V)}$ and $\bar{\Gamma}_i^{(V)} = \Gamma_i^{(V)} \oplus \kappa_\Gamma^{(V)} \subseteq \bar{\Omega}_i^{(V)}$, we represent $\Xi_i^{(V)}$ and $\bar{\Omega}_i^{(V)}$ as two separate nodes in the Bayesian graph because, by *crypto lemma* [G.D03], $\Gamma_i^{(V)}$ and $\bar{\Gamma}_i^{(V)}$ are statistically independent. Furthermore, for convenience, we have considered that dependencies only take place forward (from Block i to Block $i+1$), which is possible by

reformulating the encoding as follows. According to Section 4.2.1, for any $i \in [1, L]$ we have $\tilde{A}_i\big[\mathcal{C}^{(n)}\big] = W_i$. Consequently, we can write $W_i \triangleq [W_{1,i}, W_{2,i}]$, where $W_{1,i} \triangleq \tilde{A}_i[\mathcal{C}_1^{(n)} \cup \mathcal{C}_{1,2}^{(n)}]$ and $W_{2,i} \triangleq \tilde{A}_i[\mathcal{C}_2^{(n)} \cup \mathcal{C}_0^{(n)}]$. Since $\bar{\Theta}_i^{(V)} = \tilde{A}_i\big[\mathcal{C}_1^{(n)}\big] \oplus \kappa_\Theta^{(V)}$ and $\bar{\Gamma}_i^{(V)} = \tilde{A}_i\big[\mathcal{C}_{1,2}^{(n)}\big] \oplus \kappa_\Gamma^{(V)}$, we regard $\bar{\Omega}_i^{(V)}$ as an independent random sequence generated at Block $i-1$ that is stored properly into some part of $\tilde{A}_{i-1}[\mathcal{G}^{(n)}]$. Then, we consider that the encoder obtains $W_{1,i} \triangleq \bar{\Omega}_i^{(V)} \oplus \kappa_\Omega^{(V)}$, which is stored into $\tilde{A}_i[\mathcal{C}_1^{(n)} \cup \mathcal{C}_{1,2}^{(n)}]$ at Block i. On the other hand, the remaining part $W_{2,i}$ is independently generated at Block i. Recall that the *secret-key* $\kappa_\Omega^{(V)}$ is reused in all blocks.

The following lemma shows that strong secrecy holds for any Block $i \in [1, L]$.

Lemma 4.2. *For any $i \in [1, L]$ and sufficiently large n,*

$$I\big(S_i \Xi_{i-1}^{(V)} \Lambda_{i-1}^{(X)}; \tilde{Z}_i^n\big) \le \delta_n^{(\mathrm{S})},$$

where $\delta_n^{(\mathrm{S})} \triangleq 2n\delta_n + 2\delta_n^{(*)}\big(2n - \log \delta_n^{(*)}\big)$ and $\delta_n^{(*)}$ defined as in Lemma 4.1.

Proof. For n sufficiently large, we have

$$\begin{aligned}
&I\big(S_i \Xi_{i-1}^{(V)} \Lambda_{i-1}^{(X)}; \tilde{Z}_i^n\big) \\
&\quad \overset{(a)}{=} I\big(\tilde{A}_i\big[\mathcal{H}_{V|Z}^{(n)}\big]\tilde{T}_i\big[\mathcal{H}_{X|VZ}^{(n)}\big]; \tilde{Z}_i^n\big) \\
&\quad \overset{(b)}{=} \big|\mathcal{H}_{V|Z}^{(n)}\big| + \big|\mathcal{H}_{X|VZ}^{(n)}\big| - H\big(\tilde{A}_i\big[\mathcal{H}_{V|Z}^{(n)}\big]\tilde{T}_i\big[\mathcal{H}_{X|VZ}^{(n)}\big]\big|\tilde{Z}_i^n\big) \\
&\quad \overset{(c)}{\le} \big|\mathcal{H}_{V|Z}^{(n)}\big| + \big|\mathcal{H}_{X|VZ}^{(n)}\big| - H\big(A\big[\mathcal{H}_{V|Z}^{(n)}\big]T\big[\mathcal{H}_{X|VZ}^{(n)}\big]\big|Z_i^n\big) + 4n\delta_n^{(*)} - 2\delta_n^{(*)} \log \delta_n^{(*)} \\
&\quad \overset{(d)}{\le} 2n\delta_n + 4n\delta_n^{(*)} - 2\delta_n^{(*)} \log \delta_n^{(*)}
\end{aligned}$$

where (a) holds by the encoding described in Section 4.2; (b) holds by the uniformity of $\tilde{A}_i\big[\mathcal{H}_{V|Z}^{(n)}\big]$ and $\tilde{A}_i\big[\mathcal{H}_{X|VZ}^{(n)}\big]$; (c) follows from applying Lemma 2.4 (where $T_{\mathrm{V}} \triangleq 2$ and $T_{\mathrm{O}} \triangleq 1$) and Lemma 4.1; and (d) holds because

$$\begin{aligned}
&H\big(A\big[\mathcal{H}_{V|Z}^{(n)}\big]T\big[\mathcal{H}_{X|VZ}^{(n)}\big]\big|Z^n\big) \\
&\quad \ge H\big(A\big[\mathcal{H}_{V|Z}^{(n)}\big]\big|Z^n\big) + H\big(T\big[\mathcal{H}_{X|VZ}^{(n)}\big]\big|A^n Z^n\big) \\
&\quad \ge \sum_{j \in \mathcal{H}_{V|Z}^{(n)}} H\big(A(j)\big|A^{1:j-1} Z^n\big) + \sum_{j \in \mathcal{H}_{X|VZ}^{(n)}} H\big(T(j)\big|T^{1:j-1} V^n Z^n\big) \\
&\quad \ge \big|\mathcal{H}_{V|Z}^{(n)}\big|(1-\delta_n) + \big|\mathcal{H}_{X|VZ}^{(n)}\big|(1-\delta_n)
\end{aligned}$$

where we have used the fact that conditioning does not increase entropy, the invertibility of G_n, and the definition of $\mathcal{H}_{V|Z}^{(n)}$ and $\mathcal{H}_{X|VZ}^{(n)}$ in (4.6) and (4.9) respectively. □

Next, the following lemma shows that eavesdropper observations $\tilde{Z}_i^n$ are asymptotically statistically independent of observations $\tilde{Z}_{1:i-1}^n$ from previous blocks.

Lemma 4.3. *For any $i \in [2, L]$ and sufficiently large n,*

$$I\big(S_{1:L}\tilde{Z}_{1:i-1}^n; \tilde{Z}_i^n\big) \leq \delta_n^{(\mathrm{S})},$$

where $\delta_n^{(\mathrm{S})}$ is defined as in Lemma 4.2.

Proof. For any $i \in [2, L]$ and sufficiently large n, we have

$$\begin{aligned}
&I\big(S_{1:L}\tilde{Z}_{1:i-1}^n; \tilde{Z}_i^n\big) \\
&\quad= I\big(S_{1:i}\tilde{Z}_{1:i-1}^n; \tilde{Z}_i^n\big) + I\big(S_{i+1:L}; \tilde{Z}_i^n \big| S_{1:i}\tilde{Z}_{1:i-1}^n\big) \\
&\quad\overset{(a)}{=} I\big(S_{1:i}\tilde{Z}_{1:i-1}^n; \tilde{Z}_i^n\big) \\
&\quad\leq I\big(S_{1:i}\tilde{Z}_{1:i-1}^n \Xi_{i-1}^{(V)}\Lambda_{i-1}^{(X)}; \tilde{Z}_i^n\big) \\
&\quad= I\big(S_i\Xi_{i-1}^{(V)}\Lambda_{i-1}^{(X)}; \tilde{Z}_i^n\big) + I\big(S_{1:i-1}\tilde{Z}_{1:i-1}^n; \tilde{Z}_i^n \big| S_i\Xi_{i-1}^{(V)}\Lambda_{i-1}^{(X)}\big) \\
&\quad\overset{(b)}{\leq} \delta_n^{(\mathrm{S})} + I\big(S_{1:i-1}\tilde{Z}_{1:i-1}^n; \tilde{Z}_i^n \big| S_i\Xi_{i-1}^{(V)}\Lambda_{i-1}^{(X)}\big) \\
&\quad\leq \delta_n^{(\mathrm{S})} + I\big(S_{1:i-1}\tilde{Z}_{1:i-1}^n; \tilde{Z}_i^n W_{1,i} \big| S_i\Xi_{i-1}^{(V)}\Lambda_{i-1}^{(X)}\big) \\
&\quad= \delta_n^{(\mathrm{S})} + I\big(S_{1:i-1}\tilde{Z}_{1:i-1}^n; W_{1,i} \big| S_i\Xi_{i-1}^{(V)}\Lambda_{i-1}^{(X)}\big) + I\big(S_{1:i-1}\tilde{Z}_{1:i-1}^n; \tilde{Z}_i^n \big| S_i\Xi_{i-1}^{(V)}\Lambda_{i-1}^{(X)}W_{1,i}\big) \\
&\quad\overset{(c)}{=} \delta_n^{(\mathrm{S})} + I\big(S_{1:i-1}\tilde{Z}_{1:i-1}^n; W_{1,i} \big| S_i\Xi_{i-1}^{(V)}\Lambda_{i-1}^{(X)}\big) \\
&\quad\leq \delta_n^{(\mathrm{S})} + I\big(\tilde{A}_{1:i-1}^n\tilde{Z}_{1:i-1}^n; W_{1,i} \big| S_i\Xi_{i-1}^{(V)}\Lambda_{i-1}^{(X)}\big) \\
&\quad= \delta_n^{(\mathrm{S})} + I\big(\tilde{A}_{1:i-1}^n; W_{1,i} \big| S_i\Xi_{i-1}^{(V)}\Lambda_{i-1}^{(X)}\big) + I\big(\tilde{Z}_{1:i-1}^n; W_{1,i} \big| \tilde{A}_{1:i-1}^n S_i\Xi_{i-1}^{(V)}\Lambda_{i-1}^{(X)}\big) \\
&\quad\overset{(d)}{=} \delta_n^{(\mathrm{S})} + I\big(\tilde{A}_{1:i-1}^n; W_{1,i} \big| S_i\Xi_{i-1}^{(V)}\Lambda_{i-1}^{(X)}\big) \\
&\quad\overset{(e)}{=} \delta_n^{(\mathrm{S})} + I\big(\tilde{A}_{1:i-1}^n; \bar{\Omega}_i^{(V)} \oplus \kappa_{\Omega}^{(V)} \big| S_i\Xi_{i-1}^{(V)}\Lambda_{i-1}^{(X)}\big) \\
&\quad\overset{(f)}{=} \delta_n^{(\mathrm{S})}
\end{aligned}$$

where (a) holds by independence between $S_{i+1:L}$ and any random variable from Blocks 1 to i; (b) holds by Lemma 4.2; (c) follows from applying d-separation [Pea09] over the Bayesian graph in Figure 4.7 to obtain that $\tilde{Z}_i^n$ and $(S_{1:i-1}, \tilde{Z}_{1:i-1}^n)$ are conditionally independent given $(S_i, \Xi_{i-1}^{(V)}, \Lambda_{i-1}^{(X)}, W_{1,i})$; (d) also follows from applying *d-separation* to obtain that $W_{1,i}$ and $\tilde{Z}_{1:i-1}^n$ are conditionally independent given $(\tilde{A}_{1:i-1}^n, S_i, \Xi_{i-1}^{(V)}, \Lambda_{i-1}^{(X)})$; (e) holds by definition; and (f) holds because $\bar{\Omega}_i^{(V)}$ is independent of $(S_i, \Xi_{i-1}^{(V)}, \Lambda_{i-1}^{(X)})$ and any random variable from Block 1 to $(i-2)$, and because from applying crypto-lemma [G.D03] we obtain that $\bar{\Omega}_i^{(V)} \oplus \kappa_{\Omega}^{(V)}$ is independent of $\tilde{A}_{i-1}^n$. □

Therefore, we obtain

$$\begin{aligned} I\big(S_{1:L};\tilde{Z}_{1:L}^n\big) &\overset{(a)}{=} I\big(S_{1:L};\tilde{Z}_1^n\big) + \sum_{i=2}^{L} I\big(S_{1:L};\tilde{Z}_i^n\big|\tilde{Z}_{1:i-1}^n\big) \\ &\overset{(b)}{\leq} I\big(S_{1:L};\tilde{Z}_1^n\big) + (L-1)\delta_n^{(\mathrm{S})} \\ &= I\big(S_1;\tilde{Z}_1^n\big) + I\big(S_{2:L};\tilde{Z}_1^n\big|S_1\big) + (L-1)\delta_n^{(\mathrm{S})} \\ &\overset{(c)}{=} I\big(S_1;\tilde{Z}_1^n\big) + (L-1)\delta_n^{(\mathrm{S})} \\ &\overset{(d)}{\leq} L\delta_n^{(\mathrm{S})} \end{aligned}$$

where (a) follows from applying the chain rule; (b) holds by Lemma 4.3; (c) holds by independence between $S_{2:L}$ and any random variable from Block 1; and (d) holds by Lemma 4.2. Thus, for sufficiently large n the PCS satisfies the strong secrecy condition in (4.2).

Remark 4.1. *We conjecture that the use $\kappa_\Omega^{(V)}$ is not needed for the PCS to satisfy the strong secrecy condition. However, the key is required in order to prove this condition by means of analyzing a causal Bayesian graph similar to the one in Figure 4.7.*

Remark 4.2. *Although backward dependencies between random variables of different blocks appear in [CY18], a secret seed as $\kappa_\Omega^{(V)}$ is not necessary for the PCS to provide strong secrecy. This is because random sequences that are repeated in adjacent blocks are stored only into those corresponding entries whose indices belong to the "high entropy set given eavesdropper observations", i.e., the equivalent sets of $\mathcal{H}_{V|Z}^{(n)}$ and $\mathcal{H}_{X|VZ}^{(n)}$ in our PCS. By contrast, notice that our PCS repeats $\big[\Theta_i^{(V)},\Gamma_i^{(V)}\big] \subseteq \tilde{A}_i\big[(\mathcal{H}_{V|Z}^{(n)})^{\mathrm{C}}\big]$.*

Remark 4.3. *Another possibility for the PCS is to repeat at Block $i+1$ the modulo-2 addition between $\big[\Psi_i^{(V)},\Gamma_i^{(V)}\big]$ and a particular secret-key, instead of repeating an* encrypted *version of $\big[\Theta_i^{(V)},\Gamma_i^{(V)}\big]$ at Block $i-1$. Then, it is not difficult to prove that $I\big(S_{1:L}\tilde{Z}_{i+1:L}^n;\tilde{Z}_i^n\big) \leq \delta_n^{(\mathrm{S})}$ (similar to Lemma 4.3). Thus, one can minimize the length of this secret-key depending on whether $\big|\mathcal{C}_1^{(n)}\big| < \big|\mathcal{C}_2^{(n)}\big|$ or vice versa.*

4.4 Concluding remarks

A strongly secure PCS has been proposed for the WTBC with two legitimate receivers and one eavesdropper. This polar code achieves the best known inner-bound on the achievable region of the CI-WTBC model, where transmitter wants to send common information (private and confidential) to both receivers. Due to the non-degradedness assumption of the channel,

the encoder builds a chaining construction that induces bidirectional dependencies between adjacent blocks, which need to be taken carefully into account in the secrecy analysis.

These bidirectional dependencies involve elements from adjacent blocks whose indices belong to the "low entropy sets given eavesdropper observations". Consequently, in order to prove that the PCS satisfies the strong secrecy condition, we have introduced a secret-key whose length becomes negligible in terms of rate as the number of blocks grows indefinitely. In the proposed PCS, this key has been used to randomize part of these elements from any block that are repeated in the previous (or next) one. In this way, we can analyze the dependencies between all random variables involved in the secrecy analysis by means of a causal Bayesian graph and apply d-separation to prove that the PCS induces eavesdropper's observations that are statistically independent of one another.

Despite the good performance of the PCSs, some issues still persist. As we have concluded in Chapter 3 (Section 3.5), how to avoid the additional secret transmission (that is negligible in terms of rate) required by the legitimate receivers as well as how to replace the random decisions entirely by deterministic ones in SC encoding are problems that still remains unsolved. Additionally, we conjecture that the previous secret-keys that are used to prove independence between blocks are not necessary. However, how to prove these independence without using them seems a difficult problem to address at this point.

5

Polar coding for the wiretap broadcast channel with multiple messages

This chapter focuses on a channel model over the WTBC where transmitter wants to reliably send different confidential (and non-confidential) messages to different legitimate receivers with the presence of an eavesdropper. This model generalizes the one described in Chapter 4, where only common information is intended for both receivers.

There are two different inner-bounds on the achievable region of this model in the literature. On the one hand, the inner-bound found in [BP15] considers confidential information only, while the one in [EU13] consider confidential and non-confidential messages. The random coding techniques used in [BP15] and [EU13] are Marton's coding and rate splitting in conjunction with superposition coding and binning. The only difference between them is that the first uses joint decoding, while the second uses successive decoding. Indeed, if we consider confidential information transmission only, the inner-bound in [BP15] includes the one in [EU13], but is not straightforward to show that whether the first inner-bound is strictly larger or not: for a given input distribution, the inner-bound in [BP15] is strictly larger; nevertheless, we do not know if the rate points that are only included in this inner-bound for a particular distribution may be in the inner-bound found in [EU13] under another distribution.

We provide a PCS that achieves the inner-bound in [BP15] and, additionally, allows transmitting different non-confidential messages to both legitimate receivers. Our PCS is based in part on the one described in [MHSU15] that achieves Marton's region of broadcast channels without secrecy constraints, and the one described in Chapter 4 for the CI-WTBC. In Marton's coding we have three different layers: one inner-layer that must be reliably decoded by both legitimate receivers, and two outer-layers such that each one conveys

information intended only for one receiver. Due to the non-degradedness condition of the channels, the PCS requires the use of a chaining construction which induces bidirectional dependencies between adjacent blocks. Moreover, we show that joint and successive decoding have their counterpart in polar coding, and jointly decoding allows to enlarge the achievable region for a particular input distribution. Indeed, due to the polar-based jointly decoding, our PCS needs to build a chaining construction that introduces dependencies between different encoding layers of adjacent blocks.

The remaining of this chapter is organized as follows. Section 5.1 introduces the channel model formally as well as an enlarged version of the inner-bound found in [BP15] that considers the transmission of private messages. In Section 5.2 we describe a PCS that achieves this inner-bound. Then, Section 5.3 evaluates the performance of this PCS. Finally, the concluding remarks are presented in Section 5.4.

5.1 Channel model and achievable region

A WTBC $(\mathcal{X}, p_{Y_{(1)}Y_{(2)}Z|X}, \mathcal{Y}_{(1)} \times \mathcal{Y}_{(2)} \times \mathcal{Z})$ with 2 legitimate receivers and an external eavesdropper, as we have seen in the previous chapter, is characterized by the probability transition function $p_{Y_{(1)}Y_{(2)}Z|X}$, where $X \in \mathcal{X}$ denotes the channel input, $Y_{(k)} \in \mathcal{Y}_{(k)}$ denotes the channel output corresponding to the legitimate receiver $k \in [1,2]$, and $Z \in \mathcal{Z}$ denotes the channel output corresponding to the eavesdropper. Now, we consider a model, namely Multiple Information over the Wiretap Broadcast Channel (MI-WTBC), in which the transmitter wishes to send two private messages W_1 and W_2, and two confidential messages S_1 and S_2, where W_1 and S_1 are intended to legitimate Receiver 1, and W_2 and S_2 are intended to legitimate Receiver 2. A code $\left(\lceil 2^{nR_{W_{(1)}}} \rceil, \lceil 2^{nR_{S_{(1)}}} \rceil, \lceil 2^{nR_{W_{(2)}}} \rceil, \lceil 2^{nR_{S_{(2)}}} \rceil, n\right)$ for the MI-WTBC consists of two private message sets $\mathcal{W}_{(1)}$ and $\mathcal{W}_{(2)}$ where $\mathcal{W}_{(k)} \triangleq \left[1, \lceil 2^{nR_{W_{(k)}}} \rceil\right]$ for $k \in [1,2]$, two confidential message sets $\mathcal{S}_{(1)}$ and $\mathcal{S}_{(2)}$ where $\mathcal{S}_{(k)} \triangleq \left[1, \lceil 2^{nR_{S_{(k)}}} \rceil\right]$ for $k \in [1,2]$, an encoding function $f : \mathcal{W}_{(1)} \times \mathcal{S}_{(1)} \times \mathcal{W}_{(2)} \times \mathcal{S}_{(2)} \to \mathcal{X}^n$ that maps $(w_{(1)}, w_{(2)}, s_{(1)}, s_{(2)})$ to a codeword x^n, and two decoding functions $g_{(1)}$ and $g_{(2)}$ such that $g_{(k)} : \mathcal{Y}_{(k)}^n \to \mathcal{W}_{(k)} \times \mathcal{S}_{(k)}$ $(k \in [1,2])$ maps the k-th legitimate receiver observations $y_{(k)}^n$ to the estimates $(\hat{w}_{(k)}, \hat{s}_{(k)})$. The reliability condition to be satisfied by this code is given by

$$\lim_{n\to\infty} \mathbb{P}\left[(W_{(k)}, S_{(k)}) \neq (\hat{W}_{(k)}, \hat{S}_{(k)})\right] = 0, \quad k \in [1,2]. \tag{5.1}$$

The *strong* secrecy condition is measured in terms of the information leakage and is given by

$$\lim_{n\to\infty} I\left(S_{(1)}S_{(2)}; Z^n\right) = 0. \tag{5.2}$$

This model is plotted in Figure 5.1. A tuple of rates $(R_{W_{(1)}}, R_{S_{(1)}}, R_{W_{(2)}}, R_{S_{(2)}}) \in \mathbb{R}_+^4$ is achievable for the MI-WTBC if a sequence of $\left(\lceil 2^{nR_{W_{(1)}}} \rceil, \lceil 2^{nR_{S_{(1)}}} \rceil, \lceil 2^{nR_{W_{(2)}}} \rceil, \lceil 2^{nR_{S_{(2)}}} \rceil, n\right)$ codes that satisfy the reliability and secrecy conditions (5.1) and (5.2) respectively exists.

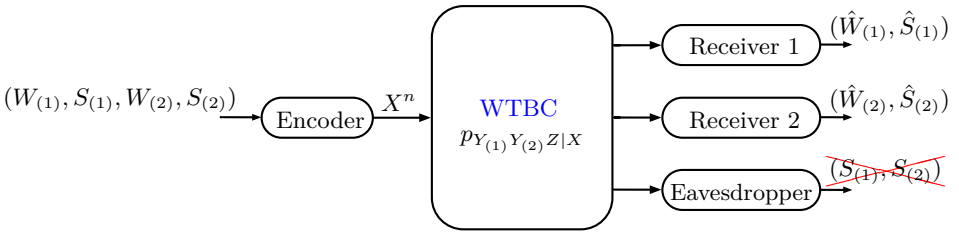

Figure 5.1: Channel model: MI-WTBC.

References [BP15] and [EU13] define two different inner-bounds on the capacity region of this model. Indeed, the inner-bound in [BP15] only consider the case where $R_{W_{(1)}} = R_{W_{(2)}} \triangleq 0$, that is, when only confidential messages are transmitted over the broadcast channel. In this situation, [BP15] (Remark 3) points out that this inner-bound includes the one defined in [EU13], but it does not specify whether this bound is strictly larger or not.

Definition 5.1 (Adapted from [BP15]). *The region $\mathfrak{R}_{\text{MI-WTBC}}^{(\text{S})}$ defined by the union over all the pairs of rates $(R_{S_{(1)}}, R_{S_{(2)}}) \in \mathbb{R}_+^2$ satisfying*

$$\begin{aligned} R_{S_{(1)}} &\leq I(VU_{(1)}; Y_{(1)}) - I(VU_{(1)}; Z) \\ R_{S_{(2)}} &\leq I(VU_{(2)}; Y_{(2)}) - I(VU_{(2)}; Z) \\ R_{S_{(1)}} + R_{S_{(2)}} &\leq I(VU_{(1)}; Y_{(1)}) + I(VU_{(2)}; Y_{(2)}) - I(U_{(1)}; U_{(2)}|V) \\ &\quad - I(VU_{(1)}U_{(2)}; Z) - \max\{I(V; Y_{(1)}), I(V; Y_{(2)}), I(V; Z)\} \end{aligned}$$

for some distribution $p_{VU_{(1)}U_{(2)}XY_{(1)}Y_{(2)}Z}$ such that $(VU_{(1)}U_{(2)}) - X - (Y_{(1)}, Y_{(2)}, Z)$ forms a Markov chain and $I(U_{(1)}; Y_{(1)}|V) + I(U_{(2)}; Y_{(2)}|V) \geq I(U_{(1)}; U_{(2)}|V)$, defines an inner-bound on the achievable region of the MI-WTBC when $R_{W_{(1)}} = R_{W_{(2)}} \triangleq 0$.

Remark 5.1. *Since the previous inner-bound on the achievable region of the MI-WTBC cannot be enlarged by considering general distributions $p_{X|VU_{(1)}U_{(2)}}$, the channel input X can be restricted to be any deterministic function of random variables $(VU_{(1)}U_{(2)})$.*

Remark 5.2. *If $Z \triangleq \varnothing$ then region $\mathfrak{R}_{\text{MI-WTBC}}^{(\text{S})}$ reduces to well-known Marton's region for the broadcast channel without secrecy constraints [Mar79].*

Proposition 5.1. *When $R_{W_{(1)}} = R_{W_{(2)}} \triangleq 0$, for a particular distribution $p_{VU_{(1)}U_{(2)}XY_{(1)}Y_{(2)}Z}$, $\mathfrak{R}_{\text{MI-WTBC}}^{(\text{S})}$ in Proposition 5.1 is strictly larger than the inner-bound in [EU13] (Theorem 1).*

Proof. Consider $\mathfrak{R}^{(\mathrm{S})}_{\text{MI-WTBC}}$ when $p_{VU_{(1)}U_{(2)}XY_{(1)}Y_{(2)}Z}$ is such that $I(V;Y_{(1)}) < I(V;Y_{(2)})$. In this case, it is easy to check that the inner-bound in [EU13] (Theorem 1) imposes that $R_{S_{(2)}} \leq I(V;Y_{(1)}) + I(U_{(2)};Y_{(2)}|V) - I(VU_{(2)};Z)$, which is strictly less than the bound on $R_{S_{(2)}}$ in Proposition 5.1. Similarly, the upper-bound on $R_{S_{(1)}}$ in Proposition 5.1 is also strictly larger than the one in [EU13] (Theorem 1) when $I(V;Y_{(2)}) < I(V;Y_{(1)})$. □

Remark 5.3. *In general, we cannot affirm that the inner-bound in Proposition 5.1 is strictly larger than the one in [EU13]: the rate tuples that are included only in Proposition 5.1 for a particular distribution may be in the inner-bound of [EU13] under another distribution.*

Remark 5.4. *The region in [EU13] imposes that $I(V;Z) \leq I(V;Y_{(k)})$ for any $k \in [1,2]$. Nevertheless, Proposition 5.1 does not restrict $p_{VU_{(1)}U_{(2)}XY_{(1)}Y_{(2)}Z}$ to satisfy this condition.*

Remark 5.5. *As mentioned in [BP15] (Remark 3), the coding techniques used in [BP15] and [EU13] to obtain the inner-bounds are almost the same and the only difference are the decoding strategies: joint decoding in [BP15] and successive decoding for [EU13]. Indeed, we will see that these strategies have a connection on the PCS that is described in Section 5.2 and joint decoding enlarges the inner-bound on the achievable region for a particular distribution.*

For compactness of notation, let $k \in [1,2]$, and $\bar{k} \triangleq [1,2] \setminus k$. The following proposition defines an inner-bound on the achievable region for the MI-WTBC when considering also the transmission of the private messages $W_{(1)}$ and $W_{(2)}$.

Proposition 5.2. *The region $\mathfrak{R}_{\text{MI-WTBC}} \triangleq Conv\big(\mathfrak{R}^{(1)}_{\text{MI-WTBC}} \cup \mathfrak{R}^{(2)}_{\text{MI-WTBC}}\big)$ defines an inner-bound on the achievable region of the MI-WTBC, where $Conv(\cdot)$ denotes the convex hull of a set of rate-tuples, for $k \in [1,2]$ we have*

$$\mathfrak{R}^{(k)}_{\text{MI-WTBC}} \triangleq \bigcup_{\mathcal{P}} \left\{ \begin{array}{r} R_{S_{(k)}} \leq I(VU_{(k)};Y_{(k)}) - I(VU_{(k)};Z) \\ R_{S_{(\bar{k})}} \leq I(VU_{(\bar{k})};Y_{(\bar{k})}) - I(U_{(\bar{k})};U_{(k)}|V) - I(U_{(\bar{k})};Z|VU_{(k)}) \\ - \max\{I(V;Y_{(1)}), I(V;Y_{(2)}), I(V;Z)\} \\ R_{S_{(k)}} + R_{W_{(k)}} \leq I(VU_{(k)};Y_{(k)}) \\ R_{S_{(\bar{k})}} + R_{W_{(\bar{k})}} \leq I(VU_{(\bar{k})};Y_{(\bar{k})}) - I(U_{(\bar{k})};U_{(k)}|V) \\ - \max\{I(V;Y_{(1)}), I(V;Y_{(2)}), I(V;Z)\} + I(V;Z), \end{array} \right\},$$

and $\mathcal{P}$ contains all distributions $p_{VU_{(1)}U_{(2)}XY_{(1)}Y_{(2)}Z}$ such that $(VU_{(1)}U_{(2)}) - X - (Y_{(1)},Y_{(2)},Z)$ forms a Markov chain and $I(U_{(1)};Y_{(1)}|V) + I(U_{(2)};Y_{(2)}|V) \geq I(U_{(1)};U_{(2)}|V)$.

In Section 5.2 we describe a PCS that achieves the corner point of $\mathfrak{R}^{(k)}_{\text{MI-WTBC}}$, where $k \in [1,2]$, and then we discuss how to achieve any rate tuple of the entire region $\mathfrak{R}_{\text{MI-WTBC}}$.

5.2 Polar coding scheme

Notice that $\mathfrak{R}_{\text{MI-WTBC}}$ of Proposition 5.2 is not affected by switching subindices 1 and 2.Thus, we can assume without loss of generality that $I(V;Y_{(1)}) \leq I(V;Y_{(2)})$. Otherwise, the coding scheme that is described later will also be suitable by simply exchanging the roles of Receiver 1 and Receiver 2. Consequently, the PCS must contemplate three different situations:

Situation 1: when $I(V;Z) \leq I(V;Y_{(1)}) \leq I(V;Y_{(2)})$,

Situation 2: when $I(V;Y_{(1)}) < I(V;Z) \leq I(V;Y_{(2)})$,

Situation 3: when $I(V;Y_{(1)}) \leq I(V;Y_{(2)}) < I(V;Z)$.

Under the previous assumption, in order to proof that $\mathfrak{R}_{\text{MI-WTBC}}$ is entirely achievable by using polar codes for any of the situations mentioned before, it suffices to provide a PCS that achieves the corner points $(R^{\star 1}_{S_{(1)}}, R^{\star 1}_{S_{(2)}}, R^{\star 1}_{W_{(1)}}, R^{\star 1}_{W_{(2)}}) \subset \mathfrak{R}^{(1)}_{\text{MI-WTBC}}$ and $(R^{\star 2}_{S_{(1)}}, R^{\star 2}_{S_{(2)}}, R^{\star 2}_{W_{(1)}}, R^{\star 2}_{W_{(2)}}) \subset \mathfrak{R}^{(2)}_{\text{MI-WTBC}}$, where

$$R^{\star k}_{S_{(k)}} \triangleq H(VU_{(k)}|Z) - H(VU_{(k)}|Y_{(k)}), \tag{5.3}$$

$$\begin{aligned} R^{\star k}_{S_{(\bar{k})}} \triangleq\ & H(U_{(\bar{k})}|VU_{(k)}Z) - H(U_{(\bar{k})}|VY_{(\bar{k})}) \\ & - \big(H(V|Y_{(\bar{k})}) - \min\{H(V|Y_{(1)}), H(V|Z)\}\big), \end{aligned} \tag{5.4}$$

$$R^{\star k}_{W_{(k)}} \triangleq H(VU_{(k)}) - H(VU_{(k)}|Z), \tag{5.5}$$

$$R^{\star k}_{W_{(\bar{k})}} \triangleq H(U_{(\bar{k})}|VU_{(k)}) - H(U_{(\bar{k})}|VU_{(k)}Z). \tag{5.6}$$

for any $k \in [1,2]$, and recall that $\bar{k} = [1,2] \setminus k$. We have expressed $(R^{\star k}_{S_{(1)}}, R^{\star k}_{S_{(2)}}, R^{\star k}_{W_{(1)}}, R^{\star k}_{W_{(2)}})$ in terms of entropies for convenience. Indeed, $(R^{\star k}_{S_{(1)}}, R^{\star k}_{S_{(2)}}, R^{\star k}_{W_{(1)}}, R^{\star k}_{W_{(2)}})$ corresponds to the case where, for a given distribution $p_{VU_{(1)}U_{(2)}XY_{(1)}Y_{(2)}Z}$, we set the maximum rate for the confidential and private messages intended for Receiver k, and then we set the maximum possible rates of the remaining messages associated to Receiver $\bar{k}$.

Remark 5.6. *For distributions such that $I(V;Y_{(1)}) < I(V;Y_{(2)})$, the inner-bound in [EU13] does not include the corner point $(R^{\star 2}_{S_{(1)}}, R^{\star 2}_{S_{(2)}}, R^{\star 2}_{W_{(1)}}, R^{\star 2}_{W_{(2)}})$. In this section we will see that polar-based joint decoding is necessary for the PCS to approach this rate tuple.*

Moreover, distributions $p_{VU_{(1)}U_{(2)}XY_{(1)}Y_{(2)}Z}$ such that satisfy Situations 2 and 3, that is when $I(V;Y_{(k)}) < I(V;Z)$ for some $k \in [1,2]$, are not considered in the definition of the inner-bound in [EU13]. We will see that polar-based joint decoding is also needed in these situations for the PCS to approach $(R^{\star k}_{S_{(1)}}, R^{\star k}_{S_{(2)}}, R^{\star k}_{W_{(1)}}, R^{\star k}_{W_{(2)}})$ for any $k \in [1,2]$.

Let $(\mathcal{V} \times \mathcal{U}_{(1)} \times \mathcal{U}_{(2)} \times \mathcal{X} \times \mathcal{Y}_{(1)} \times \mathcal{Y}_{(2)} \times \mathcal{Z}, p_{VU_{(1)}U_{(2)}XY_{(1)}Y_{(2)}Z})$ denote the DMS that represents the input $(V, U_{(1)}, U_{(2)}, X)$ and output $(Y_{(1)}, Y_{(2)}, Z)$ random variables of the

MI-WTBC, where $|\mathcal{V}| = |\mathcal{U}_{(1)}| = |\mathcal{U}_{(2)}| = |\mathcal{X}| \triangleq 2$. For the input random variable V, we define the polar transform $A^n \triangleq V^n G_n$ and the associated sets

$$\mathcal{H}_V^{(n)} \triangleq \big\{j \in [1,n] : H\big(A(j)\big|A^{1:j-1}\big) \geq 1-\delta_n\big\}, \tag{5.7}$$

$$\mathcal{L}_V^{(n)} \triangleq \big\{j \in [1,n] : H\big(A(j)\big|A^{1:j-1}\big) \leq \delta_n\big\}, \tag{5.8}$$

$$\mathcal{H}_{V|Z}^{(n)} \triangleq \big\{j \in [1,n] : H\big(A(j)\big|A^{1:j-1}Z^n\big) \geq 1-\delta_n\big\}, \tag{5.9}$$

$$\mathcal{L}_{V|Y_{(k)}}^{(n)} \triangleq \big\{j \in [1,n] : H\big(A(j)\big|A^{1:j-1}Y_{(k)}^n\big) \leq \delta_n\big\}, \quad k=1,2. \tag{5.10}$$

For the random variable $U_{(k)}$, where $k \in [1,2]$, we define the polar transform $T_{(k)}^n \triangleq U_{(k)}^n G_n$. In this model, due to the polar-based Marton's coding strategy similar to the one in [MHSU15], the polar code constructions corresponding to $T_{(1)}^n$ and $T_{(2)}^n$ are different depending on the corner point that the PCS must approach. To achieve $(R_{S_{(1)}}^{\star 1}, R_{S_{(2)}}^{\star 1}, R_{W_{(1)}}^{\star 1}, R_{W_{(2)}}^{\star 1})$, the construction of $T_{(1)}^n$ only depends on V^n, while $T_{(2)}^n$ depends on V^n and $T_{(1)}^n$. Otherwise, to achieve $(R_{S_{(1)}}^{\star 2}, R_{S_{(2)}}^{\star 2}, R_{W_{(1)}}^{\star 2}, R_{W_{(2)}}^{\star 2})$, the construction of $T_{(2)}^n$ only depends on V^n, while the one of $T_{(1)}^n$ depends on V^n and $T_{(2)}^n$. Therefore, consider that the PCS must achieve $(R_{S_{(1)}}^{\star k}, R_{S_{(2)}}^{\star k}, R_{W_{(1)}}^{\star k}, R_{W_{(2)}}^{\star k}) \subseteq \mathfrak{R}_{\text{MI-WTBC}}^{(k)}$, where $k \in [1,2]$. Associated to $U_{(k)}$, define

$$\mathcal{H}_{U_{(k)}|V}^{(n)} \triangleq \big\{j \in [1,n] : H\big(T_{(k)}(j)\big|T_{(k)}^{1:j-1}V^n\big) \geq 1-\delta_n\big\}, \tag{5.11}$$

$$\mathcal{L}_{U_{(k)}|V}^{(n)} \triangleq \big\{j \in [1,n] : H\big(T_{(k)}(j)\big|T_{(k)}^{1:j-1}V^n\big) \leq \delta_n\big\}, \tag{5.12}$$

$$\mathcal{H}_{U_{(k)}|VZ}^{(n)} \triangleq \big\{j \in [1,n] : H\big(T_{(k)}(j)\big|T_{(k)}^{1:j-1}V^nZ^n\big) \geq 1-\delta_n\big\}, \tag{5.13}$$

$$\mathcal{L}_{U_{(k)}|VY_{(k)}}^{(n)} \triangleq \big\{j \in [1,n] : H\big(T_{(k)}(j)\big|T_{(k)}^{1:j-1}V^nY_{(k)}^n\big) \leq \delta_n\big\}. \tag{5.14}$$

Also, define the following sets associated to the polar transform $U_{(\bar{k})}$:

$$\mathcal{H}_{U_{(\bar{k})}|VU_{(k)}}^{(n)} \triangleq \big\{j \in [1,n] : H\big(T_{(\bar{k})}(j)\big|T_{(\bar{k})}^{1:j-1}V^nU_{(k)}^n\big) \geq 1-\delta_n\big\}, \tag{5.15}$$

$$\mathcal{L}_{U_{(\bar{k})}|VU_{(k)}}^{(n)} \triangleq \big\{j \in [1,n] : H\big(T_{(\bar{k})}(j)\big|T_{(\bar{k})}^{1:j-1}V^nU_{(k)}^n\big) \leq \delta_n\big\}, \tag{5.16}$$

$$\mathcal{H}_{U_{(\bar{k})}|VU_{(k)}Z}^{(n)} \triangleq \big\{j \in [1,n] : H\big(T_{(\bar{k})}(j)\big|T_{(\bar{k})}^{1:j-1}V^nU_{(k)}^nZ^n\big) \geq 1-\delta_n\big\}, \tag{5.17}$$

$$\mathcal{L}_{U_{(\bar{k})}|VY_{(\bar{k})}}^{(n)} \triangleq \big\{j \in [1,n] : H\big(T_{(\bar{k})}(j)\big|T_{(\bar{k})}^{1:j-1}V^nY_{(\bar{k})}^n\big) \leq \delta_n\big\}. \tag{5.18}$$

Consider that the encoding takes place over L blocks indexed by $i \in [1,L]$. In order to approach the corner point $(R_{S_{(1)}}^{\star k}, R_{S_{(2)}}^{\star k}, R_{W_{(1)}}^{\star k}, R_{W_{(2)}}^{\star k})$, where $k \in [1,2]$, at Block $i \in [1,L]$ the encoder will construct $\tilde{A}_i^n$, which will carry part of the confidential and private message that is intended for legitimate Receiver k. Additionally, the encoder will store into $\tilde{A}_i^n$ some elements from $\tilde{A}_{i-1}^n$ (if $i \in [2,L]$) and $\tilde{A}_{i+1}^n$ (if $i \in [1,L-1]$) so that both legitimate receivers are able

to reliably reconstruct $\tilde{A}_{1:L}^n$ (chaining construction). Then, the encoder first constructs $\tilde{T}_{(k),i}^n$, which will depend on $\tilde{V}_i^n = \tilde{A}_i^n G_n$ and will carry the remaining parts of the confidential and private messages intended for Receiver k. Indeed, it could also depend on $\tilde{V}_{i-1}^n$ and/or $\tilde{V}_{i+1}^n$ if polar-based jointly decoding is considered because some elements of $\tilde{V}_{i-1}^n$ and/or $\tilde{V}_{i+1}^n$ may be stored in $\tilde{T}_{(k),i}^n$. Then, the encoder forms $\tilde{T}_{(\bar{k}),i}^n$, which depends on $\big(\tilde{V}_i^n, \tilde{T}_{(k),i}^n\big)$. In fact, as before, if polar-based jointly decoding is considered then the chaining construction may store some elements of $\tilde{V}_{i-1}^n$ and/or $\tilde{V}_{i+1}^n$ in $\tilde{T}_{(\bar{k}),i}^n$. Finally, it will obtain $\tilde{U}_{(k),i}^n = \tilde{T}_{(k),i}^n G_n$ for $k \in [1,2]$ and deterministically form $\tilde{X}_i^n$ (see Remark 5.1). The codeword $\tilde{X}^n$ then is transmitted over the WTBC inducing the channel outputs $(\tilde{Y}_{(1),i}^n, \tilde{Y}_{(2),i}^n, \tilde{Z}_i^n)$.

For better readability and understanding, the methods of constructing the *inner-layer* $\tilde{A}_{1:L}^n$ and the *outer-layers* $\tilde{T}_{(1),1:L}^n$ and $\tilde{T}_{(2),1:L}^n$ are described independently in the following subsections. Nevertheless, if we consider the encoding moving from Block 1 to Block L, and since dependencies only occur between adjacent blocks, the encoder is able to form $\tilde{T}_{(1),i}^n$ and $\tilde{T}_{(2),i}^n$ once $\tilde{A}_{i+1}^n$ ($i \in [1, L-1]$) is constructed.

5.2.1 Construction of the inner-layer

The method of forming $\tilde{A}_{1:L}^n$ is very similar to the one described in Chapter 4. Besides the sets in (5.7)–(5.10), we define $\mathcal{G}^{(n)} \triangleq \mathcal{H}_{V|Z}^{(n)}$ and $\mathcal{C}^{(n)} \triangleq \mathcal{H}_V^{(n)} \cap \big(\mathcal{H}_{V|Z}^{(n)}\big)^{\mathrm{C}}$, which form a partition of $\mathcal{H}_V^{(n)}$. Moreover, we also define the following partition of the set $\mathcal{G}^{(n)}$:

$$\mathcal{G}_0^{(n)} \triangleq \mathcal{G}^{(n)} \cap \mathcal{L}_{V|Y_{(1)}}^{(n)} \cap \mathcal{L}_{V|Y_{(2)}}^{(n)}, \tag{5.19}$$

$$\mathcal{G}_1^{(n)} \triangleq \mathcal{G}^{(n)} \cap \big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}} \cap \mathcal{L}_{V|Y_{(2)}}^{(n)}, \tag{5.20}$$

$$\mathcal{G}_2^{(n)} \triangleq \mathcal{G}^{(n)} \cap \mathcal{L}_{V|Y_{(1)}}^{(n)} \cap \big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}}, \tag{5.21}$$

$$\mathcal{G}_{1,2}^{(n)} \triangleq \mathcal{G}^{(n)} \cap \big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}} \cap \big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}}, \tag{5.22}$$

and the following partition of the set $\mathcal{C}^{(n)}$:

$$\mathcal{C}_0^{(n)} \triangleq \mathcal{C}^{(n)} \cap \mathcal{L}_{V|Y_{(1)}}^{(n)} \cap \mathcal{L}_{V|Y_{(2)}}^{(n)}, \tag{5.23}$$

$$\mathcal{C}_1^{(n)} \triangleq \mathcal{C}^{(n)} \cap \big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}} \cap \mathcal{L}_{V|Y_{(2)}}^{(n)}, \tag{5.24}$$

$$\mathcal{C}_2^{(n)} \triangleq \mathcal{C}^{(n)} \cap \mathcal{L}_{V|Y_{(1)}}^{(n)} \cap \big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}}, \tag{5.25}$$

$$\mathcal{C}_{1,2}^{(n)} \triangleq \mathcal{C}^{(n)} \cap \big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}} \cap \big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}}. \tag{5.26}$$

These sets are graphically represented in Chapter 4 (Figure 4.2).

Recall that $\tilde{A}_i[\mathcal{H}_V^{(n)}]$, $i \in [1, L]$, is suitable for storing uniformly distributed random sequences, and $\tilde{A}_i[\mathcal{G}^{(n)}]$ is suitable for storing information to be secured from the eavesdropper.

Moreover, sets in (5.19)–(5.26) with subscript $k \in [1,2]$ form $\mathcal{H}_V^{(n)} \cap \big(\mathcal{L}_{V|Y_{(k)}}^{(n)}\big)^{\mathrm{C}}$, and the elements of $\tilde{A}_i^n$ corresponding to this set of indices are required by Receiver k to reliably reconstruct $\tilde{A}_i^n$ entirely by performing SC decoding.

As mentioned before, the PCS must consider three different situations. In Situation 1 we have the condition $I(V;Z) \leq I(V;Y_1) \leq I(V;Y_2)$. As seen in Chapter 4, for n sufficiently large this condition imposes the following restriction on the size of previous sets:

$$\big|\mathcal{G}_1^{(n)}\big| - \big|\mathcal{C}_2^{(n)}\big| \geq \big|\mathcal{G}_2^{(n)}\big| - \big|\mathcal{C}_1^{(n)}\big| \geq \big|\mathcal{C}_{1,2}^{(n)}\big| - \big|\mathcal{G}_0^{(n)}\big|; \tag{5.27}$$

Similarly, Situation 2, where $I(V;Y_{(1)}) < I(V;Z) \leq I(V;Y_2)$, imposes that

$$\big|\mathcal{G}_1^{(n)}\big| - \big|\mathcal{C}_2^{(n)}\big| \geq \big|\mathcal{C}_{1,2}^{(n)}\big| - \big|\mathcal{G}_0^{(n)}\big| > \big|\mathcal{G}_2^{(n)}\big| - \big|\mathcal{C}_1^{(n)}\big|; \tag{5.28}$$

and Situation 3, where $I(V;Y_{(1)}) \leq I(V;Y_2) < I(V;Z)$, imposes that

$$\big|\mathcal{C}_{1,2}^{(n)}\big| - \big|\mathcal{G}_0^{(n)}\big| > \big|\mathcal{G}_1^{(n)}\big| - \big|\mathcal{C}_2^{(n)}\big| \geq \big|\mathcal{G}_2^{(n)}\big| - \big|\mathcal{C}_1^{(n)}\big|. \tag{5.29}$$

Thus, according to (5.27)–(5.29), we must consider six different cases:

A. $|\mathcal{G}_1^{(n)}| > |\mathcal{C}_2^{(n)}|$, $|\mathcal{G}_2^{(n)}| > |\mathcal{C}_1^{(n)}|$ and $|\mathcal{G}_0^{(n)}| \geq |\mathcal{C}_{1,2}^{(n)}|$ (only for Situation 1),

B. $|\mathcal{G}_1^{(n)}| > |\mathcal{C}_2^{(n)}|$, $|\mathcal{G}_2^{(n)}| > |\mathcal{C}_1^{(n)}|$ and $|\mathcal{G}_0^{(n)}| < |\mathcal{C}_{1,2}^{(n)}|$ (for all situations),

C. $|\mathcal{G}_1^{(n)}| \geq |\mathcal{C}_2^{(n)}|$, $|\mathcal{G}_2^{(n)}| \leq |\mathcal{C}_1^{(n)}|$ and $|\mathcal{G}_0^{(n)}| > |\mathcal{C}_{1,2}^{(n)}|$ (only for Situations 1 and 2),

D. $|\mathcal{G}_1^{(n)}| < |\mathcal{C}_2^{(n)}|$, $|\mathcal{G}_2^{(n)}| < |\mathcal{C}_1^{(n)}|$ and $|\mathcal{G}_0^{(n)}| > |\mathcal{C}_{1,2}^{(n)}|$ (for all situations),

E. $|\mathcal{G}_1^{(n)}| > |\mathcal{C}_2^{(n)}|$, $|\mathcal{G}_2^{(n)}| < |\mathcal{C}_1^{(n)}|$ and $|\mathcal{G}_0^{(n)}| < |\mathcal{C}_{1,2}^{(n)}|$ (only for Situations 2 and 3),

F. $|\mathcal{G}_1^{(n)}| < |\mathcal{C}_2^{(n)}|$, $|\mathcal{G}_2^{(n)}| < |\mathcal{C}_1^{(n)}|$ and $|\mathcal{G}_0^{(n)}| < |\mathcal{C}_{1,2}^{(n)}|$ (only for Situation 3).

The inner-layer encoding process to achieve $(R_{S_{(1)}}^{\star k}, R_{S_{(2)}}^{\star k}, R_{W_{(1)}}^{\star k}, R_{W_{(2)}}^{\star k})$, for any $k \in [1,2]$, in all cases is summarized in Algorithm 5.1. For $i \in [1,L]$, let $W_{(k),i}^{(V)}$ be a uniformly distributed vector of length $|\mathcal{C}^{(n)}|$ that represents part of the private message intended to legitimate Receiver k. The encoder forms $\tilde{A}_i\big[\mathcal{C}^{(n)}\big]$ by simply storing $W_{(k),i}^{(V)}$. Then, from $\tilde{A}_i\big[\mathcal{C}^{(n)}\big]$, we define $\Psi_i^{(V)} \triangleq \tilde{A}_i\big[\mathcal{C}_2^{(n)}\big]$, $\Gamma_i^{(V)} \triangleq \tilde{A}_i\big[\mathcal{C}_{1,2}^{(n)}\big]$ and $\Theta_i^{(V)} \triangleq \tilde{A}_i\big[\mathcal{C}_1^{(n)}\big]$.

The function `form2_Ag` in Algorithm 5.1 constructs $\tilde{A}_{1:L}\big[\mathcal{G}^{(n)}\big]$ and is explained in detail below. Then, given $\tilde{A}_i\big[\mathcal{C}^{(n)} \cup \mathcal{G}^{(n)}\big]$, $i \in [1,L]$, the encoder forms the remaining entries of $\tilde{A}_i^n$ by using SC encoding: deterministic for $\tilde{A}_i\big[\mathcal{L}_V^{(n)}\big]$, and random for $\tilde{A}_i\big[(\mathcal{H}_V^{(n)})^{\mathrm{C}} \setminus \mathcal{L}_V^{(n)}\big]$.

Also, from $\tilde{A}_i^n$, where $i \in [1,L]$, the encoder obtains $\Phi_{(k),i}^{(V)} \triangleq \tilde{A}_i\big[\big(\mathcal{H}_V^{(n)}\big)^{\mathrm{C}} \cap \big(\mathcal{L}_{V|Y_{(k)}}^{(n)}\big)^{\mathrm{C}}\big]$ for any $k \in [1,2]$. Moreover, from $\tilde{A}_1^n$ and $\tilde{A}_L^n$, it obtains $\Upsilon_{(1)}^{(V)} \triangleq \tilde{A}_1\big[\mathcal{H}_V^{(n)} \cap (\mathcal{L}_{V|Y_{(1)}}^{(n)})^{\mathrm{C}}\big]$ and $\Upsilon_{(2)}^{(V)} \triangleq \tilde{A}_L\big[\mathcal{H}_V^{(n)} \cap (\mathcal{L}_{V|Y_{(2)}}^{(n)})^{\mathrm{C}}\big]$, respectively. Recall that $\big(\Upsilon_{(k)}^{(V)}, \Phi_{(k),i}^{(V)}\big)$ is required by

Algorithm 5.1 Inner-layer encoding to achieve $(R^{\star k}_{S_{(1)}}, R^{\star k}_{S_{(2)}}, R^{\star k}_{W_{(1)}}, R^{\star k}_{W_{(2)}}) \subseteq \mathfrak{R}^{(k)}_{\text{MI-WTBC}}$

Require: Parts $W^{(V)}_{(k),1:L}$ and $S^{(V)}_{(k),1:L}$ of messages; and secret-key $\{\kappa^{(V)}_{\Upsilon\Phi_{(k)}}\}_{k=1}^{2}$

$\Psi^{(V)}_0$, $\Gamma^{(V)}_0$, $\bar{\Psi}^{(V)}_0$, $\Pi^{(V)}_{(2),0}$, $\Lambda^{(V)}_0$, $\bar{\Theta}^{(V)}_{L+1}$, $\bar{\Gamma}^{(V)}_{L+1} \leftarrow \varnothing$ ▷ For notation purposes
$\tilde{A}_1[\mathcal{C}^{(n)}] \leftarrow W^{(V)}_{(k),1}$
$\Psi^{(V)}_1 \leftarrow \tilde{A}_1[\mathcal{C}^{(n)}_2]$ **and** $\Gamma^{(V)}_1 \leftarrow \tilde{A}_1[\mathcal{C}^{(n)}_{1,2}]$
for $i = 1$ **to** L **do**
  if $i \neq L$ **then**
    $\tilde{A}_{i+1}[\mathcal{C}^{(n)}] \leftarrow W^{(V)}_{(k),i+1}$
    $\Psi^{(V)}_{i+1} \leftarrow \tilde{A}_{i+1}[\mathcal{C}^{(n)}_2]$ **and** $\Theta^{(V)}_{i+1} \leftarrow \tilde{A}_{i+1}[\mathcal{C}^{(n)}_1]$ **and** $\Gamma^{(V)}_{i+1} \leftarrow \tilde{A}_{i+1}[\mathcal{C}^{(n)}_{1,2}]$
  end if
  $\tilde{A}_i\big[\mathcal{G}^{(n)}\big]$, $\Pi^{(V)}_{(1),i}$, $\Pi^{(V)}_{(2),i}$, $\Lambda^{(V)}_i, \ldots$
    $\ldots \Delta^{(V)}_{(1),i+1}, \Delta^{(V)}_{(2),i-1} \leftarrow \texttt{form2\_A}_{\texttt{G}}\big(i, S^{(V)}_{(k),i}, \Theta^{(V)}_{i+1}, \Gamma^{(V)}_{i+1}, \Psi^{(V)}_{i-1}, \Gamma^{(V)}_{i-1}, \Pi^{(V)}_{(2),i-1}, \Lambda^{(V)}_{i-1}\big)$
  for $j \in \big(\mathcal{H}^{(n)}_V\big)^{\mathrm{C}}$ **do**
    if $j \in \big(\mathcal{H}^{(n)}_V\big)^{\mathrm{C}} \setminus \mathcal{L}^{(n)}_V$ **then**
      $\tilde{A}_i(j) \leftarrow p_{A(j)|A^{1:j-1}}\big(\tilde{A}_i(j)\big|\tilde{A}_i^{1:j-1}\big)$
    else if $j \in \mathcal{L}^{(n)}_V$ **then**
      $\tilde{A}_i(j) \leftarrow \arg\max_{a\in\mathcal{V}} p_{A(j)|A^{1:j-1}}\big(a\big|\tilde{A}_i^{1:j-1}\big)$
    end if
  end for
  $\tilde{V}^n_i = \tilde{A}^n_i G_n$
  $\Phi^{(V)}_{(k),i} \leftarrow \tilde{A}_i\big[\big(\mathcal{H}^{(n)}_V\big)^{\mathrm{C}} \cap \big(\mathcal{L}^{(n)}_{V|Y_{(k)}}\big)^{\mathrm{C}}\big]$ for $k \in [1,2]$
  if $i = 1$ **then** $\Upsilon^{(V)}_{(1)} \leftarrow \tilde{A}_1\big[\mathcal{H}^{(n)}_V \cap \big(\mathcal{L}^{(n)}_{V|Y_{(1)}}\big)^{\mathrm{C}}\big]$
  if $i = L$ **then** $\Upsilon^{(V)}_{(2)} \leftarrow \tilde{A}_L\big[\mathcal{H}^{(n)}_V \cap \big(\mathcal{L}^{(n)}_{V|Y_{(2)}}\big)^{\mathrm{C}}\big]$
end for
Send $\Pi_{(1),1:L}$ and $\Delta^{(V)}_{(1),1:L}$ to the encoding responsible for the construction of $\tilde{T}^n_{(1)}$
Send $\Delta^{(V)}_{(2),1:L}$ to the encoding responsible for the construction of $\tilde{T}^n_{(2)}$
Send $\big(\Phi^{(V)}_{(k),i}, \Upsilon^{(V)}_{(k)}\big) \oplus \kappa^{(V)}_{\Upsilon\Phi_{(k)}}$ to Receiver $k \in [1,2]$
return $\tilde{V}^n_{1:L}$

legitimate Receiver k to reliably estimate $\tilde{A}^n_{1:L}$. Hence, the transmitter additionally sends $\big(\Upsilon^{(V)}_{(k)}, \Phi^{(V)}_{(k),i}\big) \oplus \kappa^{(V)}_{\Upsilon\Phi_{(k)}}$ to legitimate Receiver k, where $\kappa^{(V)}_{\Upsilon\Phi_{(k)}}$ is a uniformly distributed key with size $L\big|\big(\mathcal{H}^{(n)}_V\big)^{\mathrm{C}} \cap \big(\mathcal{L}^{(n)}_{V|Y_{(k)}}\big)^{\mathrm{C}}\big| + \big|\mathcal{H}^{(n)}_V \cap \big(\mathcal{L}^{(n)}_{V|Y_{(k)}}\big)^{\mathrm{C}}\big|$.

The function $\texttt{form2\_A}_{\texttt{G}}$ is summarized in Algorithm 5.2. For any $i \in [1,L]$, this function stores part of the confidential message intended for Receiver $k \in [1,2]$, namely $S^{(V)}_{(k),i}$, into $\tilde{A}_i\big[\mathcal{G}^{(n)}\big]$, as well as different elements of $\tilde{A}^n_{i-1}$ ($i \in [2,L]$) and $\tilde{A}^n_{i+1}$ ($i \in [1,L-1]$) due to the chaining construction: recall that $\big[\Psi^{(V)}_i, \Gamma^{(V)}_i\big] = \tilde{A}_i\big[\mathcal{C}^{(n)}_2 \cup \mathcal{C}^{(n)}_{1,2}\big]$ is required by Receiver 2 to

reliably estimate $\tilde{A}_i^n$, while $\left[\Theta_i^{(V)}, \Gamma_i^{(V)}\right] = \tilde{A}_i\left[\mathcal{C}_1^{(n)} \cup \mathcal{C}_{1,2}^{(n)}\right]$ is required by Receiver 1.

Notice in Algorithm 5.2 that if the PCS operates to achieve the corner point of $\mathfrak{R}_{\text{MI-WTBC}}^{(1)}$ then, for $i \in [1, L-1]$, sequences $\Theta_{i+1}^{(V)}$ and $\Gamma_{i+1}^{(V)}$ are not repeated directly in $\tilde{A}_i\left[\mathcal{G}^{(n)}\right]$. Instead, the encoder repeats $\bar{\Theta}_{i+1}^{(V)} \triangleq \Theta_{i+1}^{(V)} \oplus \kappa_{\Theta}^{(V)}$ and $\bar{\Gamma}_{i+1}^{(V)} \triangleq \Gamma_{i+1}^{(V)} \oplus \kappa_{\Gamma}^{(V)}$, where $\kappa_{\Theta}^{(V)}$ and $\kappa_{\Gamma}^{(V)}$ are uniformly distributed keys with length $|\mathcal{C}_1^{(n)}|$ and $|\mathcal{C}_{1,2}^{(n)}|$ respectively that are privately shared between transmitter and both receivers. Otherwise, to achieve the corner point of $\mathfrak{R}_{\text{MI-WTBC}}^{(2)}$, instead of $\Psi_{i-1}^{(V)}$ and $\Gamma_{i-1}^{(V)}$, $i \in [2, L]$, the encoder repeats $\bar{\Psi}_{i-1}^{(V)} \triangleq \Psi_{i-1}^{(V)} \oplus \kappa_{\Psi}^{(V)}$ and $\bar{\Gamma}_{i-1}^{(V)} \triangleq \Gamma_{i-1}^{(V)} \oplus \kappa_{\Gamma}^{(V)}$, where $\kappa_{\Psi}^{(V)}$ is a distributed key with length $|\mathcal{C}_2^{(n)}|$. Since these keys are reused in all blocks, clearly their size become negligible in terms of rate for L large enough.

As in Chapter 4, based on the sets in (5.19)–(5.26), let $\mathcal{R}_1^{(n)}$, $\mathcal{R}_1'^{(n)}$, $\mathcal{R}_2^{(n)}$, $\mathcal{R}_2'^{(n)}$, $\mathcal{R}_{1,2}^{(n)}$, $\mathcal{R}_{1,2}'^{(n)}$, $\mathcal{I}^{(n)}$, $\mathcal{R}_{\text{S}}^{(n)}$ and $\mathcal{R}_{\Lambda}^{(n)}$ form an additional partition of $\mathcal{G}^{(n)}$. The definition of $\mathcal{R}_1^{(n)}$, $\mathcal{R}_1'^{(n)}$, $\mathcal{R}_2^{(n)}$, $\mathcal{R}_2'^{(n)}$, $\mathcal{R}_{1,2}^{(n)}$ and $\mathcal{R}_{1,2}'^{(n)}$ will depend on the particular case (among A to F) and situation (among 1 to 3), as well as on the corner point the PCS must approach. Then, we define

$$\mathcal{R}_{\text{S}}^{(n)} \triangleq \text{any subset of } \mathcal{G}_1^{(n)} \setminus \left(\mathcal{R}_2^{(n)} \cup \mathcal{R}_2'^{(n)}\right) \text{ with size } \left|\mathcal{G}_2^{(n)} \setminus \left(\mathcal{R}_1^{(n)} \cup \mathcal{R}_1'^{(n)}\right)\right|. \tag{5.30}$$

Finally, the definition of $\mathcal{I}^{(n)}$ and $\mathcal{R}_{\Lambda}^{(n)}$ depend on the corner point the PCS must achieve: if $(R_{S_{(1)}}^{\star 1}, R_{S_{(2)}}^{\star 1}, R_{W_{(1)}}^{\star 1}, R_{W_{(2)}}^{\star 1}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(1)}$ then

$$\mathcal{I}^{(n)} \triangleq \left(\mathcal{G}_0^{(n)} \cup \mathcal{G}_2^{(n)}\right) \setminus \left(\mathcal{R}_1^{(n)} \cup \mathcal{R}_1'^{(n)} \cup \mathcal{R}_{1,2}^{(n)} \cup \mathcal{R}_{1,2}'^{(n)}\right), \tag{5.31}$$

$$\mathcal{R}_{\Lambda}^{(n)} \triangleq \mathcal{G}_{1,2}^{(n)} \cup \left(\mathcal{G}_1^{(n)} \setminus \left(\mathcal{R}_2^{(n)} \cup \mathcal{R}_2'^{(n)} \cup \mathcal{R}_{\text{S}}^{(n)}\right)\right); \tag{5.32}$$

and if $(R_{S_{(1)}}^{\star 2}, R_{S_{(2)}}^{\star 2}, R_{W_{(1)}}^{\star 2}, R_{W_{(2)}}^{\star 2}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(2)}$ then we define

$$\mathcal{I}^{(n)} \triangleq \left(\mathcal{G}_0^{(n)} \cup \mathcal{G}_1^{(n)} \cup \mathcal{G}_2^{(n)}\right) \setminus \left(\mathcal{R}_1^{(n)} \cup \mathcal{R}_1'^{(n)} \cup \mathcal{R}_{1,2}^{(n)} \cup \mathcal{R}_{1,2}'^{(n)} \cup \mathcal{R}_2^{(n)} \cup \mathcal{R}_2'^{(n)} \cup \mathcal{R}_{\text{S}}^{(n)}\right), \tag{5.33}$$

$$\mathcal{R}_{\Lambda}^{(n)} \triangleq \mathcal{G}_{1,2}^{(n)}. \tag{5.34}$$

Note that $\mathcal{G}_1^{(n)} \setminus \left(\mathcal{R}_2^{(n)} \cup \mathcal{R}_2'^{(n)} \cup \mathcal{R}_{\text{S}}^{(n)}\right)$ will belong to $\mathcal{I}^{(n)}$ or $\mathcal{R}_{\Lambda}^{(n)}$ depending on whether the PCS approaches the first or the second corner point, respectively. Based on these sets, define

$$\Lambda_i^{(V)} \triangleq \tilde{A}_i\left[\mathcal{R}_{\Lambda}^{(n)}\right], \tag{5.35}$$

$$\Pi_{(2),i}^{(V)} \triangleq \tilde{A}_i\left[\mathcal{G}_2^{(n)} \cap \mathcal{I}^{(n)}\right], \tag{5.36}$$

$$\Pi_{(1),i}^{(V)} \triangleq \tilde{A}_i\left[\mathcal{G}_1^{(n)} \cap \mathcal{I}^{(n)}\right]. \tag{5.37}$$

Indeed, note that $\Pi_{(1),i}^{(V)} \neq \varnothing$ only when the PCS must approach the corner point of $\mathfrak{R}_{\text{MI-WTBC}}^{(2)}$.

Also, let $S_{(k),i}^{(V)}$ be a uniform random sequence representing the part of the confidential message intended for Receiver $k \in [1, 2]$ that is carried in the inner-layer. Then, $S_{(k),1}^{(V)}$ has size $\left|\mathcal{I}^{(n)} \cup \mathcal{G}_{1,2}^{(n)} \cup \mathcal{G}_1^{(n)}\right|$; for $i \in [2, L-1]$, $S_{(k),i}^{(V)}$ has size $\left|\mathcal{I}^{(n)}\right|$; and $S_{(k),L}^{(V)}$ has size $\left|\mathcal{I}^{(n)} \cup \mathcal{G}_2^{(n)}\right|$.

Moreover, for $i \in [1, L]$ we write $\Psi_i^{(V)} \triangleq \left[\Psi_{1,i}^{(V)}, \Psi_{2,i}^{(V)}, \Psi_{3,i}^{(V)}\right]$, $\bar{\Psi}_i^{(V)} \triangleq \left[\bar{\Psi}_{1,i}^{(V)}, \bar{\Psi}_{2,i}^{(V)}, \bar{\Psi}_{3,i}^{(V)}\right]$, $\Theta_i^{(V)} \triangleq \left[\Theta_{1,i}^{(V)}, \Theta_{2,i}^{(V)}, \Theta_{3,i}^{(V)}\right]$, $\bar{\Theta}_i^{(V)} \triangleq \left[\bar{\Theta}_{1,i}^{(V)}, \bar{\Theta}_{2,i}^{(V)}, \bar{\Theta}_{3,i}^{(V)}\right]$, $\Gamma_i^{(V)} \triangleq \left[\Gamma_{1,i}^{(V)}, \Gamma_{2,i}^{(V)}, \Gamma_{3,i}^{(V)}\right]$ and, lastly, $\bar{\Gamma}_i^{(V)} \triangleq \left[\bar{\Gamma}_{1,i}^{(V)}, \bar{\Gamma}_{2,i}^{(V)}, \bar{\Gamma}_{3,i}^{(V)}\right]$, where we will define $\Psi_{p,i}^{(V)}$, $\bar{\Psi}_{p,i}^{(V)}$, $\Theta_{p,i}^{(V)}$, $\bar{\Theta}_{p,i}^{(V)}$, $\Gamma_{p,i}^{(V)}$ and $\bar{\Gamma}_{p,i}^{(V)}$, for any $p \in [1, 2, 3]$, accordingly in each case. For notation purposes, let

$$\Delta_{(1),i}^{(V)} \triangleq \left[\bar{\Theta}_{3,i}^{(V)}, \bar{\Gamma}_{3,i}^{(V)}\right] \quad \text{and} \quad \Delta_{(2),i}^{(V)} \triangleq \left[\Psi_{3,i}^{(V)}, \Gamma_{3,i}^{(V)}\right] \quad (\text{if } k = 1), \tag{5.38}$$

$$\Delta_{(1),i}^{(V)} \triangleq \left[\Theta_{3,i}^{(V)}, \Gamma_{3,i}^{(V)}\right] \quad \text{and} \quad \Delta_{(2),i}^{(V)} \triangleq \left[\bar{\Psi}_{3,i}^{(V)}, \bar{\Gamma}_{3,i}^{(V)}\right] \quad (\text{if } k = 2). \tag{5.39}$$

According to Algorithm 5.1, recall that $\Pi_{(1),1:L}^{(V)}$ and $\Delta_{(1),1:L}^{(V)}$ are sent to the outer-layer associated to Receiver 1, while $\Delta_{(2),1:L}^{(V)}$ is sent to the outer-layer associated to Receiver 2.

Algorithm 5.2 Function `form2_Ac` to achieve $(R_{S_{(1)}}^{\star k}, R_{S_{(2)}}^{\star k}, R_{W_{(1)}}^{\star k}, R_{W_{(2)}}^{\star k}) \subseteq \mathfrak{R}_{\text{MI-WTBC}}^{(k)}$

Require: i, $S_{(k),i}^{(V)}$, $\Theta_{i+1}^{(V)}$, $\Gamma_{i+1}^{(V)}$, $\Psi_{i-1}^{(V)}$, $\Gamma_{i-1}^{(V)}$, $\Pi_{(2),i-1}^{(V)}$, $\Lambda_{i-1}^{(V)}$; secret-keys $\kappa_\Theta^{(V)}$, $\kappa_\Psi^{(V)}$ and $\kappa_\Gamma^{(V)}$

Define $\mathcal{R}_1^{(n)}$, $\mathcal{R}_1'^{(n)}$, $\mathcal{R}_2^{(n)}$, $\mathcal{R}_2'^{(n)}$, $\mathcal{R}_{1,2}^{(n)}$, $\mathcal{R}_{1,2}'^{(n)}$, $\mathcal{I}^{(n)}$, $\mathcal{R}_{\text{S}}^{(n)}$, $\mathcal{R}_\Lambda^{(n)}$
if $i = 1$ **then** $\tilde{A}_1[\mathcal{I}^{(n)} \cup \mathcal{G}_1^{(n)} \cup \mathcal{G}_{1,2}^{(n)}] \leftarrow S_{(k),1}^{(V)}$
if $i \in [2, L-1]$ **then** $\tilde{A}_i[\mathcal{I}^{(n)}] \leftarrow S_{(k),i}^{(V)}$
if $i = L$ **then** $\tilde{A}_L[\mathcal{I}^{(n)} \cup \mathcal{G}_2^{(n)}] \leftarrow S_{(k),L}^{(V)}$
$\bar{\Psi}_{i-1}^{(V)} \leftarrow \Psi_{i-1}^{(V)} \oplus \kappa_\Psi^{(V)}$ **and** $\bar{\Gamma}_{i-1}^{(V)} \leftarrow \Gamma_{i-1}^{(V)} \oplus \kappa_\Gamma^{(V)}$
$\bar{\Theta}_{i+1}^{(V)} \leftarrow \Theta_{i+1}^{(V)} \oplus \kappa_\Theta^{(V)}$ **and** $\bar{\Gamma}_{i+1}^{(V)} \leftarrow \Gamma_{i+1}^{(V)} \oplus \kappa_\Gamma^{(V)}$
if $k = 1$ **then** $\tilde{A}_i[\mathcal{R}_{1,2}^{(n)}] \leftarrow \Gamma_{1,i-1}^{(V)} \oplus \bar{\Gamma}_{1,i+1}^{(V)}$ **else** $\tilde{A}_i[\mathcal{R}_{1,2}^{(n)}] \leftarrow \bar{\Gamma}_{1,i-1}^{(V)} \oplus \Gamma_{1,i+1}^{(V)}$
if $k = 1$ **then** $\tilde{A}_i[\mathcal{R}_{1,2}'^{(n)}] \leftarrow \Psi_{2,i-1}^{(V)} \oplus \bar{\Theta}_{2,i+1}^{(V)}$ **else** $\tilde{A}_i[\mathcal{R}_{1,2}'^{(n)}] \leftarrow \bar{\Psi}_{2,i-1}^{(V)} \oplus \Theta_{2,i+1}^{(V)}$
if $i \in [1, L-1]$ **then**
    if $k = 1$ **then** $\tilde{A}_i[\mathcal{R}_1^{(n)}] \leftarrow \bar{\Theta}_{1,i+1}^{(V)}$ **else** $\tilde{A}_i[\mathcal{R}_1^{(n)}] \leftarrow \Theta_{1,i+1}^{(V)}$
    if $k = 1$ **then** $\tilde{A}_i[\mathcal{R}_1'^{(n)}] \leftarrow \bar{\Gamma}_{2,i+1}^{(V)}$ **else** $\tilde{A}_i[\mathcal{R}_1'^{(n)}] \leftarrow \Gamma_{2,i+1}^{(V)}$
end if
if $i \in [2, L]$ **then**
    if $k = 1$ **then** $\tilde{A}_i[\mathcal{R}_2^{(n)}] \leftarrow \Psi_{1,i-1}^{(V)}$ **else** $\tilde{A}_i[\mathcal{R}_2^{(n)}] \leftarrow \bar{\Psi}_{1,i-1}^{(V)}$
    if $k = 1$ **then** $\tilde{A}_i[\mathcal{R}_2'^{(n)}] \leftarrow \Gamma_{2,i-1}^{(V)}$ **else** $\tilde{A}_i[\mathcal{R}_2'^{(n)}] \leftarrow \bar{\Gamma}_{2,i-1}^{(V)}$
    $\tilde{A}_i[\mathcal{R}_{\text{S}}^{(n)}] \leftarrow \Pi_{(2),i-1}^{(V)}$
    $\tilde{A}_i[\mathcal{R}_\Lambda^{(n)}] \leftarrow \Lambda_{i-1}^{(V)}$
end if
$\Pi_{(1),i}^{(V)} \leftarrow \tilde{A}_i[\mathcal{I}^{(n)} \cap \mathcal{G}_1^{(n)}]$ **and** $\Pi_{(2),i}^{(V)} \leftarrow \tilde{A}_i[\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)}]$
$\Lambda_i^{(V)} \leftarrow \tilde{A}_i[\mathcal{R}_\Lambda^{(n)}]$
if $k = 1$ **then** $\Delta_{(1),i}^{(V)} \leftarrow \left(\bar{\Theta}_{3,i}^{(V)}, \bar{\Gamma}_{3,i}^{(V)}\right)$ **else** $\Delta_{(1),i}^{(V)} \leftarrow \left(\Theta_{3,i}^{(V)}, \Gamma_{3,i}^{(V)}\right)$
if $k = 1$ **then** $\Delta_{(2),i}^{(V)} \leftarrow \left(\Psi_{3,i}^{(V)}, \Gamma_{3,i}^{(V)}\right)$ **else** $\Delta_{(2),i}^{(V)} \leftarrow \left(\bar{\Psi}_{3,i}^{(V)}, \bar{\Gamma}_{3,i}^{(V)}\right)$
return $\tilde{A}_i\left[\mathcal{G}^{(n)}\right]$, $\Pi_{(1),i}^{(V)}$, $\Pi_{(2),i}^{(V)}$, $\Lambda_i^{(V)}$, $\Delta_{(1),i}^{(V)}$ and $\Delta_{(2),i}^{(V)}$

Case A when $I(V;Z) \leq I(V;Y_{(1)}) \leq I(V;Y_{(2)})$

In Case A, we have $|\mathcal{G}_1^{(n)}| > |\mathcal{C}_2^{(n)}|$, $|\mathcal{G}_2^{(n)}| > |\mathcal{C}_1^{(n)}|$ and $|\mathcal{G}_0^{(n)}| \geq |\mathcal{C}_{1,2}^{(n)}|$.

1. *Achievability of* $(R_{S_{(1)}}^{\star 1}, R_{S_{(2)}}^{\star 1}, R_{W_{(1)}}^{\star 1}, R_{W_{(2)}}^{\star 1}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(1)}$. In this case, the construction of $\tilde{A}_{1:L}\big[\mathcal{G}^{(n)}\big]$ is the same as the one in Chapter 4 (Section 4.2.2, Case A). Hence, define

$$\begin{aligned}
\mathcal{R}_1^{(n)} &\triangleq \text{any subset of } \mathcal{G}_2^{(n)} \text{ with size } \big|\mathcal{C}_1^{(n)}\big|,\\
\mathcal{R}_2^{(n)} &\triangleq \text{any subset of } \mathcal{G}_1^{(n)} \text{ with size } \big|\mathcal{C}_2^{(n)}\big|,\\
\mathcal{R}_{1,2}^{(n)} &\triangleq \text{any subset of } \mathcal{G}_0^{(n)} \text{ with size } \big|\mathcal{C}_{1,2}^{(n)}\big|,
\end{aligned}$$

and $\mathcal{R}_1^{\prime(n)} = \mathcal{R}_2^{\prime(n)} = \mathcal{R}_{1,2}^{\prime(n)} \triangleq \emptyset$. Therefore, according to (5.30)–(5.32), we have

$$\begin{aligned}
\mathcal{R}_{\text{S}}^{(n)} &= \text{any subset of } \mathcal{G}_1^{(n)} \setminus \mathcal{R}_2^{(n)} \text{ with size } \big|\mathcal{G}_2^{(n)}\big| - \big|\mathcal{C}_1^{(n)}\big|,\\
\mathcal{I}^{(n)} &= \big(\mathcal{G}_0^{(n)} \cup \mathcal{G}_2^{(n)}\big) \setminus \big(\mathcal{R}_1^{(n)} \cup \mathcal{R}_{1,2}^{(n)}\big),\\
\mathcal{R}_{\Lambda}^{(n)} &= \mathcal{G}_{1,2}^{(n)} \cup \big(\mathcal{G}_1^{(n)} \setminus \big(\mathcal{R}_2^{(n)} \cup \mathcal{R}_{\text{S}}^{(n)}\big)\big).
\end{aligned}$$

From condition (5.27), all previous sets exist. Also, for $i \in [1, L]$, define $\Psi_{1,i}^{(V)} \triangleq \Psi_i^{(V)}$, $\Gamma_{1,i}^{(V)} \triangleq \Gamma_i^{(V)}$, $\bar{\Theta}_{1,i}^{(V)} \triangleq \bar{\Theta}_i^{(V)}$, $\bar{\Gamma}_{1,i}^{(V)} \triangleq \bar{\Gamma}_i^{(V)}$ and $\Psi_{p,i}^{(V)} = \Gamma_{p,i}^{(V)} = \bar{\Theta}_{p,i}^{(V)} = \bar{\Gamma}_{p,i}^{(V)} \triangleq \varnothing$, where $p \in [2, 3]$. Then, according to (5.36)–(5.39), for $i \in [1, L]$ we have $\Pi_{(2),i}^{(V)} = \tilde{A}_i\big[\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)}\big]$ with size $\big|\mathcal{G}_2^{(n)}\big| - \big|\mathcal{C}_1^{(n)}\big|$, $\Pi_{(1),i}^{(V)} = \tilde{A}_i\big[\mathcal{I}^{(n)} \cap \mathcal{G}_1^{(n)}\big] = \varnothing$, and $\Delta_{(1),i}^{(V)} = \Delta_{(2),i}^{(V)} = \varnothing$.

According to Algorithm 5.2, recall that, for $i \in [2, L]$, the chaining construction repeats $\Psi_{i-1}^{(V)}$ and $\Gamma_{i-1}^{(V)}$ entirely in $\tilde{A}_i\big[\mathcal{R}_2^{(n)}\big] \subseteq \tilde{A}_i\big[\mathcal{G}_1^{(n)}\big]$ and $\tilde{A}_i\big[\mathcal{R}_{1,2}^{(n)}\big] \subseteq \tilde{A}_i\big[\mathcal{G}_0^{(n)}\big]$ respectively. Also, for $i \in [1, L-1]$, it repeats the sequences $\bar{\Theta}_{i+1}^{(V)}$ and $\bar{\Gamma}_{i+1}^{(V)}$ in $\tilde{A}_i\big[\mathcal{R}_1^{(n)}\big] \subseteq \tilde{A}_i\big[\mathcal{G}_2^{(n)}\big]$ and $\tilde{A}_i\big[\mathcal{G}_0^{(n)}\big]$ respectively. Indeed, for $i \in [2, L-1]$, recall that the encoder stores $\Gamma_{i-1}^{(V)} \oplus \bar{\Gamma}_{i+1}^{(V)}$ in $\tilde{A}_i\big[\mathcal{R}_{1,2}^{(n)}\big]$. The inner-layer carries confidential information $S_{(1),1:L}^{(V)}$ intended for Receiver 1, and for $i \in [2, L]$ the encoder repeats $\Pi_{(2),i-1}^{(V)}$ in $\tilde{A}_i[\mathcal{R}_{\text{S}}^{(n)}]$. Finally, for $i \in [2, L]$, it repeats $\Lambda_{i-1}^{(V)}$ in $\tilde{A}_i[\mathcal{R}_{\Lambda}^{(n)}]$ and, therefore, notice that $\Lambda_1^{(V)}$ is replicated in all blocks. This particular encoding procedure is graphically represented in Chapter 4 (Figure 4.3).

2. *Achievability of* $(R_{S_{(1)}}^{\star 2}, R_{S_{(2)}}^{\star 2}, R_{W_{(1)}}^{\star 2}, R_{W_{(2)}}^{\star 2}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(2)}$. Define $\mathcal{R}_1^{(n)}$, $\mathcal{R}_2^{(n)}$, $\mathcal{R}_{1,2}^{(n)}$, $\mathcal{R}_1^{\prime(n)}$, $\mathcal{R}_2^{\prime(n)}$ and $\mathcal{R}_{1,2}^{\prime(n)}$ as for the previous corner point. According to (5.30), (5.33) and (5.34):

$$\begin{aligned}
\mathcal{R}_{\text{S}}^{(n)} &= \text{any subset of } \mathcal{G}_1^{(n)} \setminus \mathcal{R}_2^{(n)} \text{ with size } \big|\mathcal{G}_2^{(n)}\big| - \big|\mathcal{C}_1^{(n)}\big|,\\
\mathcal{I}^{(n)} &= \big(\mathcal{G}_0^{(n)} \cup \mathcal{G}_1^{(n)} \cup \mathcal{G}_2^{(n)}\big) \setminus \big(\mathcal{R}_1^{(n)} \cup \mathcal{R}_2^{(n)} \cup \mathcal{R}_{1,2}^{(n)} \cup \mathcal{R}_{\text{S}}^{(n)}\big),\\
\mathcal{R}_{\Lambda}^{(n)} &= \mathcal{G}_{1,2}^{(n)}.
\end{aligned}$$

Also, for $i \in [1, L]$, we define $\bar{\Psi}_{1,i}^{(V)} \triangleq \bar{\Psi}_i^{(V)}$, $\bar{\Gamma}_{1,i}^{(V)} \triangleq \bar{\Gamma}_i^{(V)}$, $\Theta_{1,i}^{(V)} \triangleq \Theta_i^{(V)}$, $\Gamma_{1,i}^{(V)} \triangleq \Gamma_i^{(V)}$

and, therefore, $\bar{\Psi}_{p,i}^{(V)} = \bar{\Gamma}_{p,i}^{(V)} = \Theta_{p,i}^{(V)} = \Gamma_{p,i}^{(V)} \triangleq \varnothing$, where $p \in [2,3]$. Then, according to (5.36)–(5.39), for $i \in [1, L]$ we have $\Pi_{(2),i}^{(V)} = \tilde{A}_i\big[\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)}\big]$ with size $\big|\mathcal{G}_2^{(n)}\big| - \big|\mathcal{C}_1^{(n)}\big|$, $\Pi_{(1),i}^{(V)} = \tilde{A}_i\big[\mathcal{I}^{(n)} \cap \mathcal{G}_1^{(n)}\big]$ with size $\big|\mathcal{G}_1^{(n)}\big| - \big|\mathcal{C}_2^{(n)}\big| - \big(\big|\mathcal{G}_2^{(n)}\big| - \big|\mathcal{C}_1^{(n)}\big|\big)$, and $\Delta_{(1),i}^{(V)} = \Delta_{(2),i}^{(V)} = \varnothing$. According to Algorithm 5.2, now the inner-layer carries confidential information $S_{(2),1:L}^{(V)}$ intended for Receiver 2. Indeed, for $i \in [1, L]$, $\tilde{A}_i\big[\mathcal{G}_1^{(n)} \setminus \big(\mathcal{R}_2^{(n)} \cup \mathcal{R}_{\mathrm{S}}^{(n)}\big)\big]$, which previously contained part of $\Lambda_i^{(V)}$, now store part of $S_{(2),i}^{(V)}$. As before, for $i \in [2, L]$, $\Pi_{(2),i-1}^{(V)}$ is repeated in $\tilde{A}_i[\mathcal{R}_{\mathrm{S}}^{(n)}]$ and $\Lambda_{i-1}^{(V)}$ in $\tilde{A}_i[\mathcal{R}_{\Lambda}^{(n)}]$. Now, as will be seen in Section 5.2.2, for $i \in [1, L-1]$ the sequence $\Pi_{(1),i+1}^{(V)}$ will be repeated in the outer-layer $\tilde{T}_{(1),i}$ associated to Receiver 1. This particular encoding procedure is graphically represented in Figure 5.2.

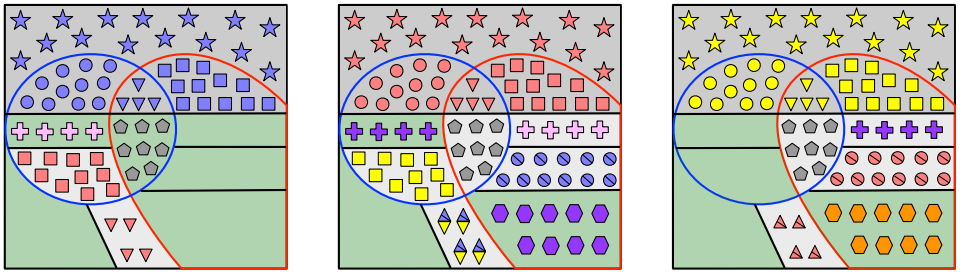

Figure 5.2: Case A when $I(V;Z) \leq I(V;Y_{(1)}) \leq I(V;Y_{(2)})$: inner-layer encoding to achieve the corner point of $\mathfrak{R}_{\text{MI-WTBC}}^{(2)}$ that leads to the construction of $\tilde{A}_{1:L}[\mathcal{H}_V^{(n)}]$ when $L = 3$. Consider Block 2: the sets $\mathcal{R}_1^{(n)}$, $\mathcal{R}_2^{(n)}$, $\mathcal{R}_{1,2}^{(n)}$, $\mathcal{R}_{\mathrm{S}}^{(n)}$ and $\mathcal{R}_{\Lambda}^{(n)}$ are those areas filled with yellow squares, blue circles, blue and yellow diamonds, pink crosses, and gray pentagons, respectively; and $\mathcal{I}^{(n)}$ is the green filled area. At Block $i \in [1, L]$, $W_{(2),i}^{(V)}$ is represented by symbols of the same color (e.g., red symbols at Block 2), and $\Theta_i^{(V)}$, $\Psi_i^{(V)}$ and $\Gamma_i^{(V)}$ are represented by squares, circles and triangles respectively. Also, $\bar{\Psi}_i^{(V)}$ and $\bar{\Gamma}_i^{(V)}$ are denoted by circles and triangles, respectively, with a line through them. At Block $i \in [2, L-1]$, the diamonds denote $\bar{\Gamma}_{i-1}^{(V)} \oplus \Gamma_{i+1}^{(V)}$. In Block $i \in [1, L]$, $S_{(2),i}^{(V)}$ is stored into those entries whose indices belong to the green filled area. For $i \in [2, L]$, $\Pi_{(2),i-1}^{(V)}$ is denoted by crosses (e.g., purple crosses at Block 2), and is repeated in $\tilde{A}_i[\mathcal{R}_{\mathrm{S}}^{(n)}]$. For $i \in [1, L-1]$, the sequence $\Pi_{(1),i+1}^{(V)}$ is denoted by hexagons, and it will be send to the outer-layer $\tilde{T}_{(1),i}$ associated to Receiver 1. At Block 1, $\Lambda_1^{(V)}$ is denoted by gray pentagons, and is repeated in all blocks. Finally, $\Upsilon_{(1)}^{(V)}$ and $\Upsilon_{(2)}^{(V)}$ are those entries inside the red curve at Block 1 and the blue curve at Block L, respectively.

Case B when $I(V;Z) \leq I(V;Y_{(1)}) \leq I(V;Y_{(2)})$

In Case B, we have $|\mathcal{G}_1^{(n)}| > |\mathcal{C}_2^{(n)}|$, $|\mathcal{G}_2^{(n)}| > |\mathcal{C}_1^{(n)}|$ and $|\mathcal{G}_0^{(n)}| < |\mathcal{C}_{1,2}^{(n)}|$.

1. *Achievability of* $(R_{S_{(1)}}^{\star 1}, R_{S_{(2)}}^{\star 1}, R_{W_{(1)}}^{\star 1}, R_{W_{(2)}}^{\star 1}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(1)}$. In this case, the construction of $\tilde{A}_{1:L}\big[\mathcal{G}^{(n)}\big]$ is the same as the one described in Chapter 4 (Section 4.2.2, Case B). Now, since $\big|\mathcal{G}_0^{(n)}\big| < \big|\mathcal{C}_{1,2}^{(n)}\big|$, only a part of $\Gamma_{i-1}^{(V)}$ ($i \in [2, L]$) and $\bar{\Gamma}_{i+1}^{(V)}$ ($i \in [1, L-1]$) can be

repeated in $\tilde{A}_i\big[\mathcal{G}_0^{(n)}\big]$. Thus, define

$$\begin{aligned}
\mathcal{R}_1^{(n)} &\triangleq \text{any subset of } \mathcal{G}_2^{(n)} \text{ with size } \big|\mathcal{C}_1^{(n)}\big|,\\
\mathcal{R}_2^{(n)} &\triangleq \text{any subset of } \mathcal{G}_1^{(n)} \text{ with size } \big|\mathcal{C}_2^{(n)}\big|,\\
\mathcal{R}_{1,2}^{(n)} &\triangleq \mathcal{G}_0^{(n)},\\
\mathcal{R}_1'^{(n)} &\triangleq \text{any subset of } \mathcal{G}_2^{(n)} \setminus \mathcal{R}_1^{(n)} \text{ with size } \big|\mathcal{C}_{1,2}^{(n)}\big| - \big|\mathcal{G}_0^{(n)}\big|,\\
\mathcal{R}_2'^{(n)} &\triangleq \text{any subset of } \mathcal{G}_1^{(n)} \setminus \mathcal{R}_2^{(n)} \text{ with size } \big|\mathcal{C}_{1,2}^{(n)}\big| - \big|\mathcal{G}_0^{(n)}\big|,
\end{aligned}$$

and $\mathcal{R}_{1,2}'^{(n)} \triangleq \emptyset$. Therefore, according to (5.30)–(5.32), we have

$$\begin{aligned}
\mathcal{R}_{\mathrm{S}}^{(n)} &= \text{any subset of } \mathcal{G}_1^{(n)} \setminus \big(\mathcal{R}_2^{(n)} \cup \mathcal{R}_2'^{(n)}\big)\\
&\qquad \text{with size } \big|\mathcal{G}_2^{(n)}\big| - \big|\mathcal{C}_1^{(n)}\big| - \big(\big|\mathcal{C}_{1,2}^{(n)}\big| - \big|\mathcal{G}_0^{(n)}\big|\big),\\
\mathcal{I}^{(n)} &= \mathcal{G}_2^{(n)} \setminus \big(\mathcal{R}_1^{(n)} \cup \mathcal{R}_1'^{(n)}\big),\\
\mathcal{R}_{\Lambda}^{(n)} &\triangleq \mathcal{G}_{1,2}^{(n)} \cup \big(\mathcal{G}_1^{(n)} \setminus \big(\mathcal{R}_2^{(n)} \cup \mathcal{R}_2'^{(n)} \cup \mathcal{R}_{\mathrm{S}}^{(n)}\big)\big).
\end{aligned}$$

From (5.27), all previous sets exist. For $i \in [1, L]$, we define $\Psi_{1,i}^{(V)} \triangleq \Psi_i^{(V)}$, $\bar{\Theta}_{1,i}^{(V)} \triangleq \bar{\Theta}_i^{(V)}$ and $\Psi_{p,i}^{(V)} = \bar{\Theta}_{p,i}^{(V)} \triangleq \varnothing$ for $p \in [2, 3]$; and $\Gamma_{1,i}^{(V)}$ and $\bar{\Gamma}_{1,i}^{(V)}$ as any part of $\Gamma_i^{(V)}$ and $\bar{\Gamma}_i^{(V)}$, respectively, with size $\big|\mathcal{G}_0^{(n)}\big|$, $\Gamma_{2,i}^{(V)}$ and $\bar{\Gamma}_{2,i}^{(V)}$ as the remaining parts with size $\big|\mathcal{C}_{1,2}^{(n)}\big| - \big|\mathcal{G}_0^{(n)}\big|$, and $\Gamma_{3,i}^{(V)} = \bar{\Gamma}_{3,i}^{(V)} \triangleq \varnothing$. From (5.36)–(5.39), for $i \in [1, L]$ we have $\Pi_{(2),i}^{(V)} = \tilde{A}_i\big[\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)}\big]$ with size $\big|\mathcal{G}_2^{(n)}\big| - \big|\mathcal{C}_1^{(n)}\big| - \big(\big|\mathcal{C}_{1,2}^{(n)}\big| - \big|\mathcal{G}_0^{(n)}\big|\big)$, $\Pi_{(1),i}^{(V)} = \tilde{A}_i\big[\mathcal{I}^{(n)} \cap \mathcal{G}_1^{(n)}\big] = \varnothing$, and we have $\Delta_{(1),i}^{(V)} = \Delta_{(2),i}^{(V)} = \varnothing$.

According to Algorithm 5.2, for $i \in [1, L]$, $\Gamma_{1,i-1}^{(V)} \oplus \bar{\Gamma}_{1,i+1}^{(V)}$ is repeated in $\tilde{A}_i\big[\mathcal{R}_{1,2}^{(n)}\big]$, where $\Gamma_{1,0}^{(V)} = \bar{\Gamma}_{1,L}^{(V)} = \varnothing$. On the other hand, now $\Gamma_{2,i-1}^{(V)}$ ($i \in [2, L]$) and $\bar{\Gamma}_{2,i+1}^{(V)}$ ($i \in [1, L-1]$) are repeated in $\tilde{A}_i\big[\mathcal{R}_2'^{(n)}\big]$ and $\tilde{A}_i\big[\mathcal{R}_1'^{(n)}\big]$ respectively. The inner-layer carries confidential information $S_{(1),1:L}^{(V)}$ intended for Receiver 1, and for $i \in [2, L]$ the encoder repeats $\Pi_{(2),i-1}^{(V)}$ in $\tilde{A}_i[\mathcal{R}_{\mathrm{S}}^{(n)}]$. Indeed, since $\mathcal{I}^{(n)} \subseteq \mathcal{G}_2^{(n)}$, we have $\Pi_{(2),i}^{(V)} = S_{(1),i}^{(V)}$ for $i \in [1, L]$. Finally, for $i \in [2, L]$, the encoder repeats $\Lambda_{i-1}^{(V)}$ in $\tilde{A}_i[\mathcal{R}_{\Lambda}^{(n)}]$ and, hence, $\Lambda_1^{(V)}$ is replicated in all blocks. This particular encoding procedure is graphically represented in Chapter 4 (Figure 4.4).

2. *Achievability of* $(R_{S_{(1)}}^{\star 2}, R_{S_{(2)}}^{\star 2}, R_{W_{(1)}}^{\star 2}, R_{W_{(2)}}^{\star 2}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(2)}$. Define $\mathcal{R}_1^{(n)}$, $\mathcal{R}_2^{(n)}$, $\mathcal{R}_{1,2}^{(n)}$, $\mathcal{R}_2'^{(n)}$ and $\mathcal{R}_{1,2}'^{(n)}$ as for the previous corner point, and $\mathcal{R}_1'^{(n)} \triangleq \emptyset$. From (5.30), (5.33) and (5.34):

$$\begin{aligned}
\mathcal{R}_{\mathrm{S}}^{(n)} &= \text{any subset of } \mathcal{G}_1^{(n)} \setminus \big(\mathcal{R}_2^{(n)} \cup \mathcal{R}_2'^{(n)}\big) \text{ with size } \big|\mathcal{G}_2^{(n)}\big| - \big|\mathcal{C}_1^{(n)}\big|,\\
\mathcal{I}^{(n)} &= \big(\mathcal{G}_1^{(n)} \cup \mathcal{G}_2^{(n)}\big) \setminus \big(\mathcal{R}_1^{(n)} \cup \mathcal{R}_2^{(n)} \cup \mathcal{R}_2'^{(n)} \cup \mathcal{R}_{\mathrm{S}}^{(n)}\big),\\
\mathcal{R}_{\Lambda}^{(n)} &= \mathcal{G}_{1,2}^{(n)}.
\end{aligned}$$

For $i \in [1, L]$, define $\bar{\Psi}_{1,i}^{(V)} \triangleq \bar{\Psi}_i^{(V)}$, $\Theta_{1,i}^{(V)} \triangleq \Theta_i^{(V)}$ and $\bar{\Psi}_{p,i}^{(V)} = \Theta_{p,i}^{(V)} \triangleq \varnothing$ for $p \in [2, 3]$. Also, we define $\bar{\Gamma}_{1,i}^{(V)}$ as any part of $\bar{\Gamma}_i^{(V)}$ with size $\left|\mathcal{G}_0^{(n)}\right|$, $\bar{\Gamma}_{2,i}^{(V)}$ as the remaining part with size $\left|\mathcal{C}_{1,2}^{(n)}\right| - \left|\mathcal{G}_0^{(n)}\right|$, and $\Gamma_{3,i}^{(V)} \triangleq \varnothing$. On the other hand, now we define $\Gamma_{1,i}^{(V)}$ as any part of $\Gamma_i^{(V)}$ with size $\left|\mathcal{G}_0^{(n)}\right|$, $\Gamma_{2,i}^{(V)} \triangleq \varnothing$ and $\Gamma_{3,i}^{(V)}$ as the remaining part with size $\left|\mathcal{C}_{1,2}^{(n)}\right| - \left|\mathcal{G}_0^{(n)}\right|$. According to (5.36)–(5.39), for $i \in [1, L]$ we have $\Pi_{(2),i}^{(V)} = \tilde{A}_i\left[\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)}\right]$ with size $\left|\mathcal{G}_2^{(n)}\right| - \left|\mathcal{C}_1^{(n)}\right| - \left(\left|\mathcal{C}_{1,2}^{(n)}\right| - \left|\mathcal{G}_0^{(n)}\right|\right)$, sequence $\Pi_{(1),i}^{(V)} = \tilde{A}_i\left[\mathcal{I}^{(n)} \cap \mathcal{G}_1^{(n)}\right]$ with size $\left|\mathcal{G}_1^{(n)}\right| - \left|\mathcal{C}_2^{(n)}\right| - \left(\left|\mathcal{G}_2^{(n)}\right| - \left|\mathcal{C}_1^{(n)}\right|\right)$, $\Delta_{(1),i}^{(V)} = \Gamma_{3,i}^{(V)}$ with size $\left|\mathcal{C}_{1,2}^{(n)}\right| - \left|\mathcal{G}_0^{(n)}\right|$ and $\Delta_{(2),i}^{(V)} = \varnothing$. According to Algorithm 5.2, the inner-layer carries confidential information $S_{(2),1:L}^{(V)}$ intended for Receiver 2. For $i \in [2, L]$, $\Pi_{(2),i-1}^{(V)}$ is repeated in $\tilde{A}_i[\mathcal{R}_{\mathrm{S}}^{(n)}]$ and $\Lambda_{i-1}^{(V)}$ in $\tilde{A}_i[\mathcal{R}_{\Lambda}^{(n)}]$. Now, for $i \in [1, L-1]$ both $\Pi_{(1),i+1}^{(V)}$ and $\Delta_{(1),i+1}^{(V)}$ will be repeated in outer-layer $\tilde{T}_{(1),i}$ associated to Receiver 1. This particular encoding is represented in Figure 5.3.

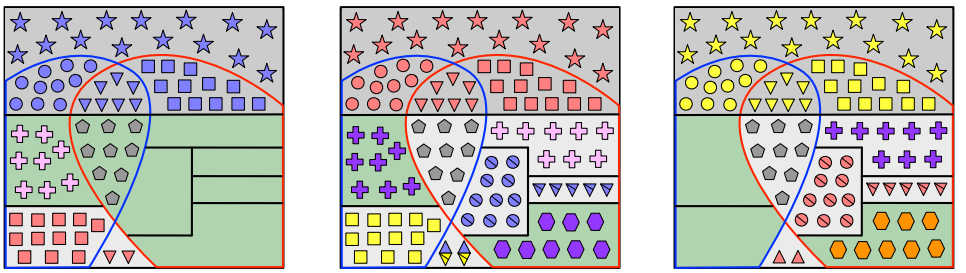

Figure 5.3: Case B when $I(V;Z) \leq I(V;Y_{(1)}) \leq I(V;Y_{(2)})$: inner-layer encoding to achieve the corner point of $\mathfrak{R}_{\text{MI-WTBC}}^{(2)}$ that leads to the construction of $\tilde{A}_{1:L}[\mathcal{H}_V^{(n)}]$ when $L = 3$. Consider Block 2: the sets $\mathcal{R}_1^{(n)}$, $\mathcal{R}_2^{(n)}$, $\mathcal{R}_2'^{(n)}$, $\mathcal{R}_{1,2}^{(n)}$, $\mathcal{R}_{\mathrm{S}}^{(n)}$ and $\mathcal{R}_{\Lambda}^{(n)}$ are those areas filled with yellow squares, blue circles, blue triangles, blue and yellow diamonds, pink crosses, and gray pentagons, respectively; and $\mathcal{I}^{(n)}$ is the green filled area. At Block $i \in [1, L]$, $W_{(2),i}^{(V)}$ is represented by symbols of the same color (e.g., red symbols at Block 2), and $\Theta_i^{(V)}$, $\Psi_i^{(V)}$ and $\Gamma_i^{(V)}$ are represented by squares, circles and triangles respectively. Also, $\bar{\Psi}_i^{(V)}$ and $\bar{\Gamma}_i^{(V)}$ are denoted by circles and triangles, respectively, with a line through them. At Block $i \in [2, L-1]$, the diamonds denote $\bar{\Gamma}_{1,i-1}^{(V)} \oplus \Gamma_{1,i+1}^{(V)}$. For $i \in [1, L-1]$, the elements of $\Gamma_{i+1}^{(V)}$ that do not belong to $\Gamma_{1,i+1}^{(V)}$ are not repeated in $\tilde{A}_i[\mathcal{G}^{(n)}]$, but $\Delta_{(1),i+1}^{(V)} = \Gamma_{3,i+1}^{(V)}$ will be sent to the outer-layer $\tilde{T}_{(1),i}$. In Block $i \in [1, L]$, $S_{(2),i}^{(V)}$ is stored into those entries whose indices belong to the green filled area. For $i \in [2, L]$, $\Pi_{(2),i-1}^{(V)}$ is denoted by crosses and is repeated in $\tilde{A}_i[\mathcal{R}_{\mathrm{S}}^{(n)}]$. For $i \in [1, L-1]$, the sequence $\Pi_{(1),i+1}^{(V)}$ is denoted by hexagons, and it will be send also to $\tilde{T}_{(1),i}$. At Block 1, $\Lambda_1^{(V)}$ is denoted by gray pentagons and is repeated in all blocks. Finally, $\Upsilon_{(1)}^{(V)}$ and $\Upsilon_{(2)}^{(V)}$ are those entries inside the red curve at Block 1 and the blue curve at Block L, respectively.

Case B when $I(V;Y_{(1)}) < I(V;Z) \leq I(V;Y_{(2)})$

1. *Achievability of* $(R_{S_{(1)}}^{\star 1}, R_{S_{(2)}}^{\star 1}, R_{W_{(1)}}^{\star 1}, R_{W_{(2)}}^{\star 1}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(1)}$. In this situation, according to condition (5.28), $\left|\mathcal{G}_2^{(n)}\right| - \left|\mathcal{C}_1^{(n)}\right| < \left|\mathcal{C}_{1,2}^{(n)}\right| - \left|\mathcal{G}_0^{(n)}\right|$. Therefore, for $i \in [1, L-1]$, sequence

$\bar{\Gamma}_{i+1}^{(V)}$ cannot be repeated entirely in $\tilde{A}_i\big[\mathcal{G}_0^{(n)} \cup \big(\mathcal{G}_2^{(n)} \setminus \mathcal{R}_1^{(n)}\big)\big]$. Thus, we define

$$\begin{aligned}
\mathcal{R}_1^{(n)} &\triangleq \text{any subset of } \mathcal{G}_2^{(n)} \text{ with size } \big|\mathcal{C}_1^{(n)}\big|,\\
\mathcal{R}_2^{(n)} &\triangleq \text{any subset of } \mathcal{G}_1^{(n)} \text{ with size } \big|\mathcal{C}_2^{(n)}\big|,\\
\mathcal{R}_{1,2}^{(n)} &\triangleq \mathcal{G}_0^{(n)},\\
\mathcal{R}_1'^{(n)} &\triangleq \mathcal{G}_2^{(n)} \setminus \mathcal{R}_1^{(n)},\\
\mathcal{R}_2'^{(n)} &\triangleq \text{any subset of } \mathcal{G}_1^{(n)} \setminus \mathcal{R}_2^{(n)} \text{ with size } \big|\mathcal{C}_{1,2}^{(n)}\big| - \big|\mathcal{G}_0^{(n)}\big|,
\end{aligned}$$

and $\mathcal{R}_{1,2}'^{(n)} \triangleq \emptyset$. Therefore, according to (5.30)–(5.32), we have $\mathcal{R}_{\mathrm{S}}^{(n)} = \mathcal{I}^{(n)} = \emptyset$ and

$$\mathcal{R}_{\Lambda}^{(n)} \triangleq \mathcal{G}_{1,2}^{(n)} \cup \big(\mathcal{G}_1^{(n)} \setminus \big(\mathcal{R}_2^{(n)} \cup \mathcal{R}_2'^{(n)}\big)\big).$$

For $i \in [1, L]$, we define $\Psi_{1,i}^{(V)} \triangleq \Psi_i^{(V)}$, $\bar{\Theta}_{1,i}^{(V)} \triangleq \bar{\Theta}_i^{(V)}$ and $\Psi_{p,i}^{(V)} = \bar{\Theta}_{p,i}^{(V)} \triangleq \varnothing$ for $p \in [2, 3]$. Also, we define $\Gamma_{1,i}^{(V)}$ as any part of $\Gamma_i^{(V)}$ with size $\big|\mathcal{G}_0^{(n)}\big|$, $\Gamma_{2,i}^{(V)}$ as the remaining part with size $\big|\mathcal{C}_{1,2}^{(n)}\big| - \big|\mathcal{G}_0^{(n)}\big|$ and $\Gamma_{3,i}^{(V)} \triangleq \varnothing$; and $\bar{\Gamma}_{1,i}^{(V)}$ as any part of $\bar{\Gamma}_i^{(V)}$ with size $\big|\mathcal{G}_0^{(n)}\big|$, $\bar{\Gamma}_{2,i}^{(V)}$ as any part of $\bar{\Gamma}_i^{(V)}$ that is not included in $\bar{\Gamma}_{1,i}^{(V)}$ with size $\big|\mathcal{G}_2^{(n)}\big| - \big|\mathcal{C}_1^{(n)}\big|$, and $\bar{\Gamma}_{3,i}^{(V)}$ as the remaining part of $\bar{\Gamma}_i^{(V)}$ with size $\big|\mathcal{C}_{1,2}^{(n)}\big| - \big|\mathcal{G}_0^{(n)}\big| - \big(\big|\mathcal{G}_2^{(n)}\big| - \big|\mathcal{C}_1^{(n)}\big|\big)$. Thus, according to (5.36)–(5.39), for $i \in [1, L]$ we have $\Pi_{(2),i}^{(V)} = \tilde{A}_i\big[\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)}\big] = \varnothing$, $\Pi_{(1),i}^{(V)} = \tilde{A}_i\big[\mathcal{I}^{(n)} \cap \mathcal{G}_1^{(n)}\big] = \varnothing$, $\Delta_{(1),i}^{(V)} = \bar{\Gamma}_{3,i}^{(V)}$ and $\Delta_{(2),i}^{(V)} = \varnothing$. According to Algorithm 5.2, since $\mathcal{I}^{(n)} = \emptyset$ then $\tilde{A}_{2:L-1}^{n}\big[\mathcal{G}^{(n)}\big]$ does not carry confidential information $S_{(1),2:L-1}^{(V)}$. For $i \in [1, L-1]$, $\Delta_{(1),i+1}^{(V)}$ will be repeated in outer-layer $\tilde{T}_{(1),i}^{n}$. This particular encoding is graphically represented in Figure 5.4.

2. *Achievability of* $(R_{S_{(1)}}^{\star 2}, R_{S_{(2)}}^{\star 2}, R_{W_{(1)}}^{\star 2}, R_{W_{(2)}}^{\star 2}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(2)}$. Construction of $\tilde{A}_{1:L}\big[\mathcal{G}^{(n)}\big]$ is the same as the one to achieve this rate tuple when $I(V;Z) \leq I(V;Y_{(1)}) \leq I(V;Y_{(2)})$.

Case B when $I(V;Y_{(1)}) \leq I(V;Y_{(2)}) < I(V;Z)$

1. *Achievability of* $(R_{S_{(1)}}^{\star 1}, R_{S_{(2)}}^{\star 1}, R_{W_{(1)}}^{\star 1}, R_{W_{(2)}}^{\star 1}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(1)}$. In this situation, define

$$\begin{aligned}
\mathcal{R}_1^{(n)} &\triangleq \text{any subset of } \mathcal{G}_2^{(n)} \text{ with size } \big|\mathcal{C}_1^{(n)}\big|,\\
\mathcal{R}_2^{(n)} &\triangleq \text{any subset of } \mathcal{G}_1^{(n)} \text{ with size } \big|\mathcal{C}_2^{(n)}\big|,\\
\mathcal{R}_{1,2}^{(n)} &\triangleq \mathcal{G}_0^{(n)},\\
\mathcal{R}_1'^{(n)} &\triangleq \mathcal{G}_2^{(n)} \setminus \mathcal{R}_1^{(n)},\\
\mathcal{R}_2'^{(n)} &\triangleq \mathcal{G}_1^{(n)} \setminus \mathcal{R}_2^{(n)},
\end{aligned}$$

and $\mathcal{R}_{1,2}'^{(n)} \triangleq \emptyset$. Thus, according to (5.30)–(5.32), $\mathcal{R}_{\mathrm{S}}^{(n)} = \mathcal{I}^{(n)} = \emptyset$ and $\mathcal{R}_{\Lambda}^{(n)} = \mathcal{G}_{1,2}^{(n)}$. In this situation we have defined $\mathcal{R}_1'^{(n)}$ and $\mathcal{R}_2'^{(n)}$ as above because, according to

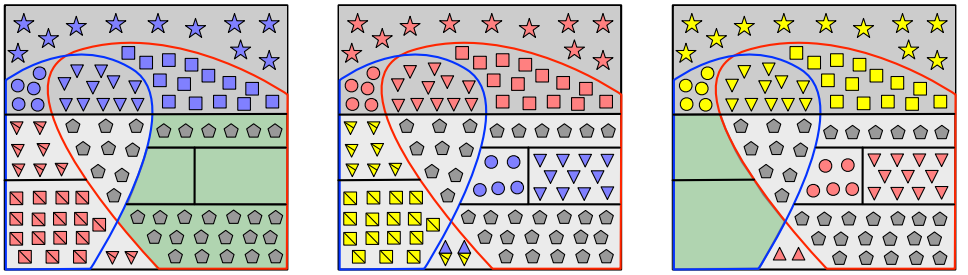

Figure 5.4: Case B when $I(V;Y_{(1)}) < I(V;Z) \leq I(V;Y_{(2)})$: inner-layer encoding to achieve the corner point of $\mathfrak{R}^{(1)}_{\text{MI-WTBC}}$ that leads to the construction of $\tilde{A}_{1:L}[\mathcal{H}_V^{(n)}]$ when $L=3$. Consider Block 2: the sets $\mathcal{R}_1^{(n)}$, $\mathcal{R}_1^{\prime(n)}$, $\mathcal{R}_2^{(n)}$, $\mathcal{R}_2^{\prime(n)}$, $\mathcal{R}_{1,2}^{(n)}$ and $\mathcal{R}_{\Lambda}^{(n)}$ are those areas filled with yellow squares, yellow triangles, blue circles, blue triangles, blue and yellow diamonds, and gray pentagons, respectively. At Block $i \in [1,L]$, $W^{(V)}_{(1),i}$ is represented by symbols of the same color (e.g., red symbols at Block 2), and $\Theta_i^{(V)}$, $\Psi_i^{(V)}$ and $\Gamma_i^{(V)}$ are represented by squares, circles and triangles respectively. Also, $\bar{\Theta}_i^{(V)}$ and $\bar{\Gamma}_i^{(V)}$ are denoted by squares and triangles, respectively, with a line through them. At Block $i \in [2, L-1]$, the diamonds denote $\Gamma_{i-1}^{(V)} \oplus \bar{\Gamma}_{i+1}^{(V)}$. For $i \in [2, L-1]$, $\tilde{A}_i[\mathcal{G}^{(n)}]$ does not carry confidential information $S^{(V)}_{(1),i}$, but only $\tilde{A}_1[\mathcal{G}^{(n)}]$ and $\tilde{A}_L[\mathcal{G}^{(n)}]$ does (into the green area). The elements of $\bar{\Gamma}^{(V)}_{2,i+1}$ that do not fit in $\tilde{A}_i[\mathcal{R}_1^{\prime(n)}]$ will be sent to outer-layer $\tilde{T}^n_{(1),i}$. At Block 1, $\Lambda_1^{(V)}$ is denoted by gray pentagons, and is repeated in all blocks. Finally, sequences $\Upsilon^{(V)}_{(1)}$ and $\Upsilon^{(V)}_{(2)}$ are those entries inside the red curve at Block 1 and the blue curve at Block L, respectively.

condition (5.29), $\left|\mathcal{G}_2^{(n)}\right| - \left|\mathcal{C}_1^{(n)}\right| < \left|\mathcal{C}_{1,2}^{(n)}\right| - \left|\mathcal{G}_0^{(n)}\right|$ and $\left|\mathcal{G}_1^{(n)}\right| - \left|\mathcal{C}_2^{(n)}\right| < \left|\mathcal{C}_{1,2}^{(n)}\right| - \left|\mathcal{G}_0^{(n)}\right|$. Therefore, neither $\Gamma_{i-1}^{(V)}$ (for $i \in [2,L]$) nor $\bar{\Gamma}_{i+1}^{(V)}$ (for $i \in [1, L-1]$) can be repeated entirely in $\tilde{A}_i\big[\mathcal{G}_0^{(n)} \cup \big(\mathcal{G}_1^{(n)} \setminus \mathcal{R}_2^{(n)}\big)\big]$ or $\tilde{A}_i\big[\big(\mathcal{G}_0^{(n)} \cup \big(\mathcal{G}_2^{(n)} \setminus \mathcal{R}_1^{(n)}\big)\big)\big]$, respectively.

For $i \in [1,L]$, we define $\Psi_{1,i}^{(V)} \triangleq \Psi_i^{(V)}$, $\bar{\Theta}_{1,i}^{(V)} \triangleq \bar{\Theta}_i^{(V)}$ and $\Psi_{p,i}^{(V)} = \bar{\Theta}_{p,i}^{(V)} \triangleq \varnothing$ for $p \in [2,3]$; we define $\Gamma_{1,i}^{(V)}$ as any part of $\Gamma_i^{(V)}$ with size $\left|\mathcal{G}_0^{(n)}\right|$, $\Gamma_{2,i}^{(V)}$ as any part of $\Gamma_i^{(V)}$ that is not included in $\Gamma_{1,i}^{(V)}$ with size $\left|\mathcal{G}_1^{(n)}\right| - \left|\mathcal{C}_2^{(n)}\right|$, and $\Gamma_{3,i}^{(V)}$ as the remaining part of $\Gamma_i^{(V)}$ with size $\left|\mathcal{C}_{1,2}^{(n)}\right| - \left|\mathcal{G}_0^{(n)}\right| - \left(\left|\mathcal{G}_1^{(n)}\right| - \left|\mathcal{C}_2^{(n)}\right|\right)$; and we define $\bar{\Gamma}_{1,i}^{(V)}$ as any part of $\bar{\Gamma}_i^{(V)}$ with size $\left|\mathcal{G}_0^{(n)}\right|$, $\bar{\Gamma}_{2,i}^{(V)}$ as any part of $\bar{\Gamma}_i^{(V)}$ that is not included in $\bar{\Gamma}_{1,i}^{(V)}$ with size $\left|\mathcal{G}_2^{(n)}\right| - \left|\mathcal{C}_1^{(n)}\right|$, and $\bar{\Gamma}_{3,i}^{(V)}$ as the remaining part with size $\left|\mathcal{C}_{1,2}^{(n)}\right| - \left|\mathcal{G}_0^{(n)}\right| - \left(\left|\mathcal{G}_2^{(n)}\right| - \left|\mathcal{C}_1^{(n)}\right|\right)$. Hence, according to (5.36)–(5.39), for $i \in [1,L]$ we have $\Pi_{(2),i}^{(V)} = \tilde{A}_i\big[\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)}\big] = \varnothing$, $\Pi_{(1),i}^{(V)} = \tilde{A}_i\big[\mathcal{I}^{(n)} \cap \mathcal{G}_1^{(n)}\big] = \varnothing$, and we have $\Delta_{(1),i}^{(V)} = \bar{\Gamma}_{3,i}^{(V)}$ and $\Delta_{(2),i}^{(V)} = \Gamma_{3,i}^{(V)}$. According to Algorithm 5.2, since $\mathcal{I}^{(n)} = \emptyset$ then $\tilde{A}^n_{2:L-1}\big[\mathcal{G}^{(n)}\big]$ does not carry confidential information $S^{(V)}_{(1),2:L-1}$. For $i \in [1, L-1]$, $\Delta^{(V)}_{(1),i+1}$ will be repeated in $\tilde{T}^n_{(1),i}$, while $\Delta^{(V)}_{(2),i-1}$, for $i \in [2,L]$, will be repeated in $\tilde{T}^n_{(2),i}$. This particular encoding is represented in Figure 5.5.

2. *Achievability of* $(R^{\star 2}_{S_{(1)}}, R^{\star 2}_{S_{(2)}}, R^{\star 2}_{W_{(1)}}, R^{\star 2}_{W_{(2)}}) \subset \mathfrak{R}^{(2)}_{\text{MI-WTBC}}$. Construction of $\tilde{A}_{1:L}\big[\mathcal{G}^{(n)}\big]$ is almost the same as that to achieve the previous corner point of region $\mathfrak{R}^{(1)}_{\text{MI-WTBC}}$: to approach this rate tuple the encoder repeats $\big[\bar{\Psi}_{i-1}^{(V)}, \bar{\Gamma}_{i-1}^{(V)}\big]$ and $\big[\Theta_{i+1}^{(V)}, \Gamma_{i+1}^{(V)}\big]$ in Block i.

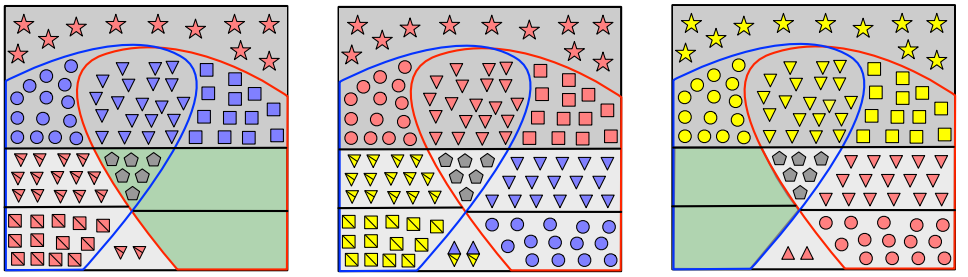

Figure 5.5: Case B when $I(V;Y_{(1)}) \leq I(V;Y_{(2)}) < I(V;Z)$: inner-layer encoding to achieve the corner point of $\mathfrak{R}^{(1)}_{\text{MI-WTBC}}$ that leads to the construction of $\tilde{A}_{1:L}[\mathcal{H}_V^{(n)}]$ when $L=3$. Consider Block 2: the sets $\mathcal{R}_1^{(n)}$, $\mathcal{R}_1^{\prime(n)}$, $\mathcal{R}_2^{(n)}$, $\mathcal{R}_2^{\prime(n)}$, $\mathcal{R}_{1,2}^{(n)}$ and $\mathcal{R}_\Lambda^{(n)}$ are those areas filled with yellow squares, yellow triangles, blue circles, blue triangles, blue and yellow diamonds, and gray pentagons, respectively. At Block $i \in [1,L]$, $W_{(1),i}^{(V)}$ is represented by symbols of the same color (e.g., red symbols at Block 2), and $\Theta_i^{(V)}$, $\Psi_i^{(V)}$ and $\Gamma_i^{(V)}$ are represented by squares, circles and triangles respectively. Also, $\bar{\Theta}_i^{(V)}$ and $\bar{\Gamma}_i^{(V)}$ are denoted by squares and triangles, respectively, with a line through them. The diamonds at Block $i \in [2, L-1]$ denote $\Gamma_{1,i-1}^{(V)} \oplus \bar{\Gamma}_{1,i+1}^{(V)}$. For $i \in [2, L-1]$, $\tilde{A}_i[\mathcal{G}^{(n)}]$ does not carry confidential information $S_{(1),i}^{(V)}$, but only $\tilde{A}_1[\mathcal{G}^{(n)}]$ and $\tilde{A}_L[\mathcal{G}^{(n)}]$ does (into the green area). The elements of $\Gamma_{i-1}^{(V)}$, or $\bar{\Gamma}_{i+1}^{(V)}$, which do not fit in $\tilde{A}_i[\mathcal{R}_{1,2}^{(n)} \cup \mathcal{R}_2^{\prime(n)}]$, or $\tilde{A}_i[\mathcal{R}_{1,2}^{(n)} \cup \mathcal{R}_1^{\prime(n)}]$, will be sent to the outer-layer $\tilde{T}_{(2),i}^n$, or $\tilde{T}_{(1),i}^n$, respectively. At Block 1, $\Lambda_1^{(V)}$ is denoted by gray pentagons and is replicated in all blocks. Finally, sequences $\Upsilon_{(1)}^{(V)}$ and $\Upsilon_{(2)}^{(V)}$ are those entries inside the red curve at Block 1 and the blue curve at Block L, respectively.

Case C when $I(V;Z) \leq I(V;Y_{(1)}) \leq I(V;Y_{(2)})$

In Case C, we have $|\mathcal{G}_1^{(n)}| \geq |\mathcal{C}_2^{(n)}|$, $|\mathcal{G}_2^{(n)}| \leq |\mathcal{C}_1^{(n)}|$ and $|\mathcal{G}_0^{(n)}| > |\mathcal{C}_{1,2}^{(n)}|$.

1. *Achievability of* $(R_{S_{(1)}}^{\star 1}, R_{S_{(2)}}^{\star 1}, R_{W_{(1)}}^{\star 1}, R_{W_{(2)}}^{\star 1}) \subset \mathfrak{R}^{(1)}_{\text{MI-WTBC}}$. The construction of $\tilde{A}_{1:L}\left[\mathcal{G}^{(n)}\right]$ in this case is the same as that in Chapter 4 (Section 4.2.2, Case C). Since $\left|\mathcal{G}_2^{(n)}\right| \leq \left|\mathcal{C}_1^{(n)}\right|$, now for $i \in [1, L-1]$ we have that $\bar{\Theta}_{i+1}^{(V)}$ fills all the elements of $\tilde{A}_i\left[\mathcal{G}_2^{(n)}\right]$. Therefore:

$$\begin{aligned}
&\mathcal{R}_{1,2}^{(n)} \triangleq \text{any subset of } \mathcal{G}_0^{(n)} \text{ with size } \left|\mathcal{C}_{1,2}^{(n)}\right|,\\
&\mathcal{R}_1^{(n)} \triangleq \text{the union of } \mathcal{G}_2^{(n)} \text{ with any subset of } \mathcal{G}_0^{(n)} \setminus \mathcal{R}_{1,2}^{(n)} \text{ with size } \left|\mathcal{C}_1^{(n)}\right| - \left|\mathcal{G}_2^{(n)}\right|,\\
&\mathcal{R}_2^{(n)} \triangleq \text{any subset of } \mathcal{G}_1^{(n)} \text{ with size } \left|\mathcal{C}_2^{(n)}\right|,
\end{aligned}$$

and $\mathcal{R}_1^{\prime(n)} = \mathcal{R}_2^{\prime(n)} = \mathcal{R}_{1,2}^{\prime(n)} \triangleq \emptyset$. Hence, according to (5.30)–(5.32), we have $\mathcal{R}_{\text{S}}^{(n)} = \emptyset$ and

$$\begin{aligned}
\mathcal{I}^{(n)} &= \mathcal{G}_0^{(n)} \setminus \mathcal{R}_{1,2}^{(n)},\\
\mathcal{R}_\Lambda^{(n)} &= \mathcal{G}_{1,2}^{(n)} \cup \left(\mathcal{G}_1^{(n)} \setminus \mathcal{R}_2^{(n)}\right).
\end{aligned}$$

From condition (5.27), all previous sets exist. For $i \in [1, L]$, we define $\Psi_{1,i}^{(V)} \triangleq \Psi_i^{(V)}$,

$\Gamma_{1,i}^{(V)} \triangleq \Gamma_i^{(V)}$, $\bar{\Theta}_{1,i}^{(V)} \triangleq \bar{\Theta}_i^{(V)}$, $\bar{\Gamma}_{1,i}^{(V)} \triangleq \bar{\Gamma}_i^{(V)}$, and $\Psi_{p,i}^{(V)} = \Gamma_{p,i}^{(V)} = \bar{\Theta}_{p,i}^{(V)} = \bar{\Gamma}_{p,i}^{(V)} \triangleq \varnothing$ for $p \in [2,3]$. According to (5.36)–(5.39), for $i \in [1, L]$ we have $\Pi_{(2),i}^{(V)} = \tilde{A}_i\big[\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)}\big] = \varnothing$, $\Pi_{(1),i}^{(V)} = \tilde{A}_i\big[\mathcal{I}^{(n)} \cap \mathcal{G}_1^{(n)}\big] = \varnothing$, and $\Delta_{(1),i}^{(V)} = \Delta_{(2),i}^{(V)} = \varnothing$. According to Algorithm 5.2, the inner-layer carries confidential information $S_{(1),1:L}^{(V)}$ intended for Receiver 1. For $i \in [2, L]$, the encoder repeats $\Lambda_{i-1}^{(V)}$ in $\tilde{A}_i[\mathcal{R}_\Lambda^{(n)}]$ and, therefore, $\Lambda_1^{(V)}$ is replicated in all blocks. This particular encoding procedure is graphically represented in Chapter 4 (Figure 4.5).

2. *Achievability of* $(R_{S_{(1)}}^{\star 2}, R_{S_{(2)}}^{\star 2}, R_{W_{(1)}}^{\star 2}, R_{W_{(2)}}^{\star 2}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(2)}$. Define $\mathcal{R}_2^{(n)}$, $\mathcal{R}_{1,2}^{(n)}$, $\mathcal{R}_1^{\prime(n)}$, $\mathcal{R}_2^{\prime(n)}$ and $\mathcal{R}_{1,2}^{\prime(n)}$ as for the previous corner point, and define $\mathcal{R}_1^{(n)} \triangleq \mathcal{G}_2^{(n)}$. Thus, according to (5.30), (5.33) and (5.34), we have $\mathcal{R}_{\text{S}}^{(n)} = \emptyset$ and

$$\begin{aligned}\mathcal{I}^{(n)} &= \big(\mathcal{G}_0^{(n)} \cup \mathcal{G}_1^{(n)}\big) \setminus \big(\mathcal{R}_2^{(n)} \cup \mathcal{R}_{1,2}^{(n)}\big),\\ \mathcal{R}_\Lambda^{(n)} &= \mathcal{G}_{1,2}^{(n)}.\end{aligned}$$

For $i \in [1, L]$, let $\bar{\Psi}_{1,i}^{(V)} \triangleq \bar{\Psi}_i^{(V)}$, $\Gamma_{1,i}^{(V)} \triangleq \Gamma_i^{(V)}$, $\bar{\Gamma}_{1,i}^{(V)} \triangleq \bar{\Gamma}_i^{(V)}$, and $\bar{\Psi}_{p,i}^{(V)} = \Gamma_{p,i}^{(V)} = \bar{\Gamma}_{p,i}^{(V)} \triangleq \varnothing$ for $p \in [2,3]$. Now, we define $\Theta_{1,i}^{(V)}$ as any part of $\Theta_i^{(V)}$ with size $\big|\mathcal{G}_2^{(n)}\big|$, $\Theta_{2,i}^{(V)} \triangleq \varnothing$, and $\Theta_{3,i}^{(V)}$ as the remaining part of $\Theta_i^{(V)}$ with size $\big|\mathcal{C}_1^{(n)}\big| - \big|\mathcal{G}_2^{(n)}\big|$. According to (5.36)–(5.39), for $i \in [1, L]$ we have $\Pi_{(2),i}^{(V)} = \tilde{A}_i\big[\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)}\big] = \varnothing$, $\Pi_{(1),i}^{(V)} = \tilde{A}_i\big[\mathcal{I}^{(n)} \cap \mathcal{G}_1^{(n)}\big]$ with size $\big|\mathcal{G}_1^{(n)}\big| - \big|\mathcal{C}_2^{(n)}\big|$, $\Delta_{(1),i}^{(V)} = \Theta_{3,i}^{(V)}$, and $\Delta_{(2),i}^{(V)} = \varnothing$. Now, the inner-layer carries confidential information $S_{(2),1:L}^{(V)}$ intended for Receiver 2. For $i \in [1, L-1]$, both $\Delta_{(1),i+1}^{(V)}$ and $\Pi_{(1),i+1}^{(V)}$ will be repeated in outer-layer $\tilde{T}_{(1),i}^n$. This particular encoding is represented in Figure 5.6.

Case C when $I(V; Y_{(1)}) < I(V; Z) \leq I(V; Y_{(2)})$

1. *Achievability of* $(R_{S_{(1)}}^{\star 1}, R_{S_{(2)}}^{\star 1}, R_{W_{(1)}}^{\star 1}, R_{W_{(2)}}^{\star 1}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(1)}$. In this situation, according to (5.28), $\big|\mathcal{G}_2^{(n)}\big| - \big|\mathcal{C}_1^{(n)}\big| < \big|\mathcal{C}_{1,2}^{(n)}\big| - \big|\mathcal{G}_0^{(n)}\big|$. Hence, for $i \in [1, L-1]$, $\bar{\Theta}_{i+1}^{(V)}$ cannot be repeated entirely in $\tilde{A}_i\big[\mathcal{G}_2^{(n)} \cup \big(\mathcal{G}_0^{(n)} \setminus \mathcal{R}_{1,2}^{(n)}\big)\big]$. Therefore, define

$$\begin{aligned}\mathcal{R}_{1,2}^{(n)} &\triangleq \text{any subset of } \mathcal{G}_0^{(n)} \text{ with size } \big|\mathcal{C}_{1,2}^{(n)}\big|,\\ \mathcal{R}_1^{(n)} &\triangleq \mathcal{G}_2^{(n)} \cup \big(\mathcal{G}_0^{(n)} \setminus \mathcal{R}_{1,2}^{(n)}\big),\\ \mathcal{R}_2^{(n)} &\triangleq \text{any subset of } \mathcal{G}_1^{(n)} \text{ with size } \big|\mathcal{C}_2^{(n)}\big|,\end{aligned}$$

and $\mathcal{R}_1^{\prime(n)} = \mathcal{R}_2^{\prime(n)} = \mathcal{R}_{1,2}^{\prime(n)} \triangleq \emptyset$. Then, according to (5.30)–(5.32), $\mathcal{R}_{\text{S}}^{(n)} = \mathcal{I}^{(n)} = \emptyset$ and

$$\mathcal{R}_\Lambda^{(n)} = \mathcal{G}_{1,2}^{(n)} \cup \big(\mathcal{G}_1^{(n)} \setminus \mathcal{R}_2^{(n)}\big).$$

For $i \in [1, L]$, let $\Psi_{1,i}^{(V)} \triangleq \Psi_i^{(V)}$, $\Gamma_{1,i}^{(V)} \triangleq \Gamma_i^{(V)}$, $\bar{\Gamma}_{1,i}^{(V)} \triangleq \bar{\Gamma}_i^{(V)}$, and $\Psi_{p,i}^{(V)} = \Gamma_{p,i}^{(V)} = \bar{\Gamma}_{p,i}^{(V)} \triangleq \varnothing$ for $p \in [2,3]$. Also, we define $\bar{\Theta}_{1,i}^{(V)}$ as any part of $\bar{\Theta}_i^{(V)}$ with size $\big|\mathcal{G}_2^{(n)}\big| + \big(\big|\mathcal{G}_0^{(n)}\big| - \big|\mathcal{C}_{1,2}^{(n)}\big|\big)$,

$\bar{\Theta}_{2,i}^{(V)} = \varnothing$ and $\bar{\Theta}_{3,i}^{(V)}$ as the remaining part with size $\big|\mathcal{C}_1^{(n)}\big| - \big|\mathcal{G}_2^{(n)}\big| - \big(\big|\mathcal{G}_0^{(n)}\big| - \big|\mathcal{C}_{1,2}^{(n)}\big|\big)$. According to (5.36)–(5.39), for $i \in [1, L]$ we have $\Pi_{(2),i}^{(V)} = \tilde{A}_i\big[\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)}\big] = \varnothing$, $\Pi_{(1),i}^{(V)} = \tilde{A}_i\big[\mathcal{I}^{(n)} \cap \mathcal{G}_1^{(n)}\big] = \varnothing$, $\Delta_{(1),i}^{(V)} = \bar{\Theta}_{3,i}^{(V)}$, and $\Delta_{(2),i}^{(V)} = \varnothing$. Since $\mathcal{I}^{(n)} = \emptyset$ then $\tilde{A}_{2:L-1}^{n}\big[\mathcal{G}^{(n)}\big]$ does not carry confidential information $S_{(1),2:L-1}^{(V)}$. For $i \in [1, L-1]$, sequence $\Delta_{(1),i+1}^{(V)}$ will be repeated in outer-layer $\tilde{T}_{(1),i}^{n}$ associated to Receiver 1.

2. *Achievability of* $(R_{S_{(1)}}^{\star 2}, R_{S_{(2)}}^{\star 2}, R_{W_{(1)}}^{\star 2}, R_{W_{(2)}}^{\star 2}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(2)}$. Construction of $\tilde{A}_{1:L}\big[\mathcal{G}^{(n)}\big]$ is the same as that to achieve this rate tuple when $I(V;Z) \leq I(V;Y_{(1)}) \leq I(V;Y_{(2)})$.

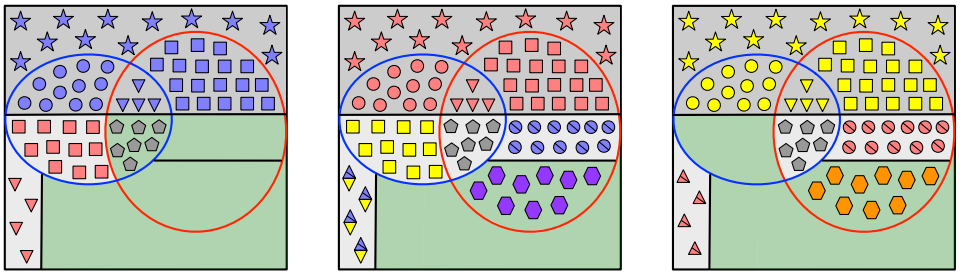

Figure 5.6: Case C when $I(V;Z) \leq I(V;Y_{(1)}) \leq I(V;Y_{(2)})$: inner-layer encoding to achieve the corner point of $\mathfrak{R}_{\text{MI-WTBC}}^{(2)}$ that leads to the construction of $\tilde{A}_{1:L}[\mathcal{H}_V^{(n)}]$ when $L = 3$. Consider the Block 2: $\mathcal{R}_1^{(n)}$, $\mathcal{R}_2^{(n)}$, $\mathcal{R}_{1,2}^{(n)}$ and $\mathcal{R}_{\Lambda}^{(n)}$ are those areas filled with yellow squares, blue circles, blue and yellow diamonds, and gray pentagons, respectively, and $\mathcal{I}^{(n)}$ is the green filled area. At Block $i \in [1, L]$, $W_{(2),i}^{(V)}$ is represented by symbols of the same color (e.g., red symbols at Block 2), and $\Theta_i^{(V)}$, $\Psi_i^{(V)}$ and $\Gamma_i^{(V)}$ are represented by squares, circles and triangles respectively. Also, $\bar{\Psi}_i^{(V)}$ and $\bar{\Gamma}_i^{(V)}$ are denoted by circles and triangles, respectively, with a line through them. At Block $i \in [2, L-1]$, the diamonds denote $\bar{\Gamma}_{1,i-1}^{(V)} \oplus \Gamma_{1,i+1}^{(V)}$. For $i \in [1, L-1]$, the elements of $\Theta_{i+1}^{(V)}$ that do not belong to $\Theta_{1,i+1}^{(V)}$ are not repeated in $\tilde{A}_i[\mathcal{G}^{(n)}]$, but $\Delta_{(1),i+1}^{(V)} = \Theta_{3,i+1}^{(V)}$ will be sent to the outer-layer $\tilde{T}_{(1),i}$. For $i \in [1, L]$, confidential information $S_{(2),i}^{(V)}$ is stored into those entries belonging to the green area. For $i \in [1, L-1]$, sequence $\Pi_{(1),i+1}^{(V)}$ is denoted by hexagons, and it will be send also to $\tilde{T}_{(1),i}$. At Block 1, $\Lambda_1^{(V)}$ is denoted by gray pentagons and is replicated in all blocks. Finally, $\Upsilon_{(1)}^{(V)}$ and $\Upsilon_{(2)}^{(V)}$ are those entries inside the red curve at Block 1 and the blue curve at Block L, respectively.

Case D when $I(V;Z) \leq I(V;Y_{(1)}) \leq I(V;Y_{(2)})$

In Case D, we have $|\mathcal{G}_1^{(n)}| < |\mathcal{C}_2^{(n)}|$, $|\mathcal{G}_2^{(n)}| < |\mathcal{C}_1^{(n)}|$ and $|\mathcal{G}_0^{(n)}| > |\mathcal{C}_{1,2}^{(n)}|$.

1. *Achievability of* $(R_{S_{(1)}}^{\star 1}, R_{S_{(2)}}^{\star 1}, R_{W_{(1)}}^{\star 1}, R_{W_{(2)}}^{\star 1}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(1)}$. In this case, the construction of $\tilde{A}_{1:L}\big[\mathcal{G}^{(n)}\big]$ is the same as the one described in Chapter 4 (Section 4.2.2, Case D). Since $|\mathcal{G}_1^{(n)}| < |\mathcal{C}_2^{(n)}|$, now for $i \in [2, L]$ only a part of $\Psi_{i-1}^{(V)}$ can be repeated entirely in

$\tilde{A}_i[\mathcal{G}_1^{(n)}]$. Consequently, we define $\mathcal{R}_2^{(n)} \triangleq \mathcal{G}_1^{(n)}$,

$$\begin{aligned}
\mathcal{R}_{1,2}^{(n)} &\triangleq \text{any subset of } \mathcal{G}_0^{(n)} \text{ with size } \left|\mathcal{C}_{1,2}^{(n)}\right|,\\
\mathcal{R}_{1,2}^{\prime(n)} &\triangleq \text{any subset of } \mathcal{G}_0^{(n)} \setminus \mathcal{R}_{1,2}^{(n)} \text{ with size } \left|\mathcal{C}_2^{(n)}\right| - \left|\mathcal{G}_1^{(n)}\right|,\\
\mathcal{R}_1^{(n)} &\triangleq \text{the union of } \mathcal{G}_2^{(n)} \text{ with any subset of}\\
&\qquad \mathcal{G}_0^{(n)} \setminus \left(\mathcal{R}_{1,2}^{(n)} \cup \mathcal{R}_{1,2}^{\prime(n)}\right) \text{ with size } \left|\mathcal{C}_1^{(n)}\right| - \left|\mathcal{G}_2^{(n)}\right| - \left(\left|\mathcal{C}_2^{(n)}\right| - \left|\mathcal{G}_1^{(n)}\right|\right);
\end{aligned}$$

and $\mathcal{R}_1^{\prime(n)} = \mathcal{R}_2^{\prime(n)} \triangleq \emptyset$. Hence, according to (5.30)–(5.32), we have $\mathcal{R}_{\mathrm{S}}^{(n)} = \emptyset$ and

$$\begin{aligned}
\mathcal{I}^{(n)} &= \mathcal{G}_0^{(n)} \setminus \left(\mathcal{R}_{1,2}^{(n)} \cup \mathcal{R}_{1,2}^{\prime(n)}\right),\\
\mathcal{R}_{\Lambda}^{(n)} &= \mathcal{G}_{1,2}^{(n)}.
\end{aligned}$$

From condition (5.27), all previous sets exist. For $i \in [1, L]$, let $\Gamma_{1,i}^{(V)} \triangleq \Gamma_i^{(V)}$, $\bar{\Gamma}_{1,i}^{(V)} \triangleq \bar{\Gamma}_i^{(V)}$ and $\bar{\Gamma}_{p,i}^{(V)} = \Gamma_{p,i}^{(V)} \triangleq \varnothing$ for $p \in [2, 3]$. On the other hand, define $\Psi_{1,i}^{(V)}$ as any part $\Psi_i^{(V)}$ with size $\left|\mathcal{G}_1^{(n)}\right|$, $\Psi_{2,i}^{(V)}$ as the remaining part with size $\left|\mathcal{C}_2^{(n)}\right| - \left|\mathcal{G}_1^{(n)}\right|$, and $\Psi_{3,i}^{(V)} \triangleq \varnothing$; and $\bar{\Theta}_{1,i}^{(V)}$ as any part of $\bar{\Theta}_i^{(V)}$ with size $\left|\mathcal{C}_1^{(n)}\right| - \left(\left|\mathcal{C}_2^{(n)}\right| - \left|\mathcal{G}_1^{(n)}\right|\right)$, $\bar{\Theta}_{2,i}^{(V)}$ as the remaining part with size $\left|\mathcal{C}_2^{(n)}\right| - \left|\mathcal{G}_1^{(n)}\right|$, and $\bar{\Theta}_{3,i}^{(V)} \triangleq \varnothing$. Thus, from (5.36)–(5.39), for $i \in [1, L]$ we have $\Pi_{(2),i}^{(V)} = \tilde{A}_i\left[\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)}\right] = \varnothing$, $\Pi_{(1),i}^{(V)} = \tilde{A}_i\left[\mathcal{I}^{(n)} \cap \mathcal{G}_1^{(n)}\right] = \varnothing$, and $\Delta_{(1),i}^{(V)} = \Delta_{(2),i}^{(V)} = \varnothing$.

According to Algorithm 5.2, the inner-layer carries confidential information $S_{(1),1:L}^{(V)}$ intended for Receiver 1. Also, instead of repeating $\Psi_{2,i-1}^{(V)}$ (the part of $\Psi_{i-1}^{(V)}$ that does not fit in $\tilde{A}_i^n\left[\mathcal{G}_1^{(n)}\right]$) in a specific part of $\tilde{A}_i\left[\mathcal{G}_0^{(n)}\right]$, the encoder stores $\Psi_{2,i-1}^{(V)} \oplus \bar{\Theta}_{2,i+1}^{(V)}$ into $\tilde{A}_i\left[\mathcal{R}_{1,2}^{\prime(n)}\right] \subseteq \tilde{A}_i\left[\mathcal{G}_0^{(n)}\right]$, where $\bar{\Theta}_{2,i+1}^{(V)}$ denotes the elements of $\bar{\Theta}_{i+1}^{(V)}$ that do not fit in $\tilde{A}_i\left[\mathcal{G}_2^{(n)}\right]$. Finally, for $i \in [2, L]$, $\Lambda_{i-1}^{(V)}$ is repeated in $\tilde{A}_i[\mathcal{R}_{\Lambda}^{(n)}]$ and, hence, $\Lambda_1^{(V)}$ is replicated in all blocks. This particular encoding is represented in Chapter 4 (Figure 4.6).

2. *Achievability of* $(R_{S_{(1)}}^{\star 2}, R_{S_{(2)}}^{\star 2}, R_{W_{(1)}}^{\star 2}, R_{W_{(2)}}^{\star 2}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(2)}$. Define $\mathcal{R}_2^{(n)}$, $\mathcal{R}_{1,2}^{(n)}$, $\mathcal{R}_1^{\prime(n)}$, $\mathcal{R}_2^{\prime(n)}$ and $\mathcal{R}_{1,2}^{\prime(n)}$ as for the previous corner point, and define $\mathcal{R}_1^{(n)} \triangleq \mathcal{G}_2^{(n)}$. Thus, according to (5.30), (5.33) and (5.34), we have $\mathcal{R}_{\mathrm{S}}^{(n)} = \emptyset$ and

$$\begin{aligned}
\mathcal{I}^{(n)} &= \mathcal{G}_0^{(n)} \setminus \left(\mathcal{R}_{1,2}^{(n)} \cup \mathcal{R}_{1,2}^{\prime(n)}\right),\\
\mathcal{R}_{\Lambda}^{(n)} &= \mathcal{G}_{1,2}^{(n)}.
\end{aligned}$$

For $i \in [1, L]$, let $\Gamma_{1,i}^{(V)} \triangleq \Gamma_i^{(V)}$, $\bar{\Gamma}_{1,i}^{(V)} \triangleq \bar{\Gamma}_i^{(V)}$ and $\bar{\Gamma}_{p,i}^{(V)} = \Gamma_{p,i}^{(V)} \triangleq \varnothing$ for $p \in [2, 3]$; and define $\bar{\Psi}_{1,i}^{(V)}$ as any part $\bar{\Psi}_i^{(V)}$ with size $\left|\mathcal{G}_1^{(n)}\right|$, $\bar{\Psi}_{2,i}^{(V)}$ as the remaining part with size $\left|\mathcal{C}_2^{(n)}\right| - \left|\mathcal{G}_1^{(n)}\right|$, and $\bar{\Psi}_{3,i}^{(V)} \triangleq \varnothing$. On the other hand, define $\Theta_{1,i}^{(V)}$ as any part of $\Theta_i^{(V)}$ with size $\left|\mathcal{G}_2^{(n)}\right|$, $\Theta_{2,i}^{(V)}$ as any part of $\Theta_i^{(V)}$ that is not included in $\Theta_{1,i}^{(V)}$ with size $\left|\mathcal{C}_2^{(n)}\right| - \left|\mathcal{G}_1^{(n)}\right|$, and $\Theta_{3,i}^{(V)}$ as the remaining part of $\Theta_i^{(V)}$ with size $\left|\mathcal{C}_1^{(n)}\right| - \left|\mathcal{G}_2^{(n)}\right| - \left(\left|\mathcal{C}_2^{(n)}\right| - \left|\mathcal{G}_1^{(n)}\right|\right)$.

Therefore, according to (5.36)–(5.39), for $i \in [1, L]$ we have $\Pi^{(V)}_{(2),i} = \tilde{A}_i\big[\mathcal{I}^{(n)} \cap \mathcal{G}^{(n)}_2\big] = \varnothing$, $\Pi^{(V)}_{(1),i} = \tilde{A}_i\big[\mathcal{I}^{(n)} \cap \mathcal{G}^{(n)}_1\big] = \varnothing$, $\Delta^{(V)}_{(1),i} = \Theta^{(V)}_{3,i}$, and $\Delta^{(V)}_{(2),i} = \varnothing$. Now, the inner-layer carries confidential information $S^{(V)}_{(2),1:L}$ intended for Receiver 2. For $i \in [1, L-1]$, sequence $\Delta^{(V)}_{(1),i+1}$ will be repeated in outer-layer $\tilde{T}^{n}_{(1),i}$. This particular encoding procedure is graphically represented in Figure 5.7.

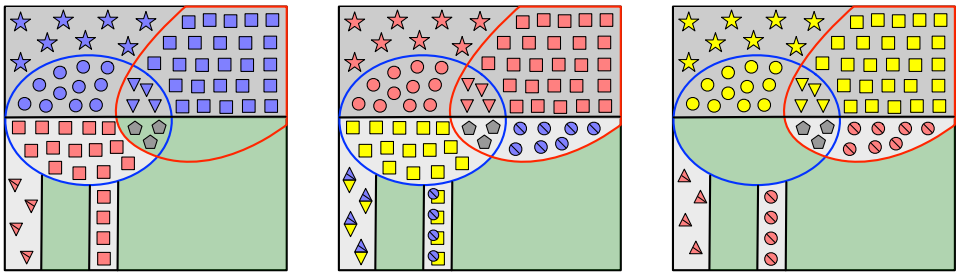

Figure 5.7: Case D when $I(V;Z) \leq I(V;Y_{(1)}) \leq I(V;Y_{(2)})$: inner-layer encoding to achieve the corner point of $\mathfrak{R}^{(2)}_{\text{MI-WTBC}}$ that leads to the construction of $\tilde{A}_{1:L}[\mathcal{H}^{(n)}_V]$ when $L = 3$. Consider Block 2: $\mathcal{R}^{(n)}_1$, $\mathcal{R}^{(n)}_2$, $\mathcal{R}^{(n)}_{1,2}$, $\mathcal{R}'^{(n)}_{1,2}$ and $\mathcal{R}^{(n)}_{\Lambda}$ are those areas filled with yellow squares, blue circles, blue and yellow diamonds, yellow squares overlapped by blue circles, and gray pentagons, respectively, and $\mathcal{I}^{(n)}$ is the green filled area. At Block $i \in [1, L]$, $W^{(V)}_{(2),i}$ is represented by symbols of the same color, and $\Theta^{(V)}_i$, $\Psi^{(V)}_i$ and $\Gamma^{(V)}_i$ are represented by squares, circles and triangles respectively. Also, $\bar{\Psi}^{(V)}_i$ and $\bar{\Gamma}^{(V)}_i$ are denoted by circles and triangles, respectively, with a line through them. At Block $i \in [2, L-1]$, the diamonds denote $\bar{\Gamma}^{(V)}_{1,i-1} \oplus \Gamma^{(V)}_{1,i+1}$, while the yellow squares overlapped by blue circles denote $\bar{\Psi}^{(V)}_{2,i-1} \oplus \Theta^{(V)}_{2,i+1}$. For $i \in [1, L-1]$, the elements of $\Theta^{(V)}_{i+1}$ that are included neither in $\Theta^{(V)}_{1,i+1}$ nor $\Theta^{(V)}_{2,i+1}$ are not repeated in $\tilde{A}_i[\mathcal{G}^{(n)}]$, but $\Delta^{(V)}_{(1),i+1} = \Theta^{(V)}_{3,i+1}$ will be sent to outer-layer $\tilde{T}_{(1),i}$. For $i \in [1, L]$, $S^{(V)}_{(2),i}$ is stored into those entries belonging to the green area. At Block 1, sequence $\Lambda^{(V)}_1$ is denoted by gray pentagons and is replicated in all blocks. Finally, $\Upsilon^{(V)}_{(1)}$ and $\Upsilon^{(V)}_{(2)}$ are those entries inside the red curve at Block 1 and the blue curve at Block L, respectively.

Case D when $I(V;Y_{(1)}) < I(V;Z) \leq I(V;Y_{(2)})$

1. *Achievability of* $(R^{\star 1}_{S_{(1)}}, R^{\star 1}_{S_{(2)}}, R^{\star 1}_{W_{(1)}}, R^{\star 1}_{W_{(2)}}) \subset \mathfrak{R}^{(1)}_{\text{MI-WTBC}}$. In this situation, according to (5.28), $\big|\mathcal{G}^{(n)}_2\big| - \big|\mathcal{C}^{(n)}_1\big| < \big|\mathcal{C}^{(n)}_{1,2}\big| - \big|\mathcal{G}^{(n)}_0\big|$. Hence, for $i \in [1, L-1]$, $\bar{\Theta}^{(V)}_{i+1}$ cannot be repeated entirely in $\tilde{A}_i\big[\mathcal{G}^{(n)}_2 \cup \big(\mathcal{G}^{(n)}_0 \setminus \mathcal{R}^{(n)}_{1,2}\big)\big]$. Therefore, define $\mathcal{R}^{(n)}_2 \triangleq \mathcal{G}^{(n)}_1$,

$$\begin{aligned}
\mathcal{R}^{(n)}_{1,2} &\triangleq \text{any subset of } \mathcal{G}^{(n)}_0 \text{ with size } \big|\mathcal{C}^{(n)}_{1,2}\big|,\\
\mathcal{R}'^{(n)}_{1,2} &\triangleq \text{any subset of } \mathcal{G}^{(n)}_0 \setminus \mathcal{R}^{(n)}_{1,2} \text{ with size } \big|\mathcal{C}^{(n)}_2\big| - \big|\mathcal{G}^{(n)}_1\big|,\\
\mathcal{R}^{(n)}_1 &\triangleq \mathcal{G}^{(n)}_2 \cup \big(\mathcal{G}^{(n)}_0 \setminus \big(\mathcal{R}^{(n)}_{1,2} \cup \mathcal{R}'^{(n)}_{1,2}\big)\big),
\end{aligned}$$

and $\mathcal{R}_1'^{(n)} = \mathcal{R}_2'^{(n)} \triangleq \emptyset$. Then, from (5.30)–(5.32), $\mathcal{R}_{\mathrm{S}}^{(n)} = \mathcal{I}^{(n)} = \emptyset$ and $\mathcal{R}_{\Lambda}^{(n)} = \mathcal{G}_{1,2}^{(n)}$. For $i \in [1, L]$, let $\Gamma_{1,i}^{(V)} \triangleq \Gamma_i^{(V)}$, $\bar{\Gamma}_{1,i}^{(V)} \triangleq \bar{\Gamma}_i^{(V)}$ and $\bar{\Gamma}_{p,i}^{(V)} = \Gamma_{p,i}^{(V)} \triangleq \varnothing$ for $p \in [2, 3]$; and define $\Psi_{1,i}^{(V)}$ as any part $\Psi_i^{(V)}$ with size $\left|\mathcal{G}_1^{(n)}\right|$, $\Psi_{2,i}^{(V)}$ as the remaining part with size $\left|\mathcal{C}_2^{(n)}\right| - \left|\mathcal{G}_1^{(n)}\right|$, and $\Psi_{3,i}^{(V)} \triangleq \varnothing$. On the other hand, we define $\bar{\Theta}_{1,i}^{(V)}$ as any part of $\bar{\Theta}_i^{(V)}$ with size $\left|\mathcal{G}_2^{(n)}\right| + \left|\mathcal{G}_0^{(n)}\right| - \left|\mathcal{C}_{1,2}^{(n)}\right| - \left(\left|\mathcal{C}_2^{(n)}\right| + \left|\mathcal{G}_1^{(n)}\right|\right)$, $\bar{\Theta}_{2,i}^{(V)}$ as any part of $\bar{\Theta}_i^{(V)}$ that is not included in $\bar{\Theta}_{1,i}^{(V)}$ with size $\left|\mathcal{C}_2^{(n)}\right| - \left|\mathcal{G}_1^{(n)}\right|$, and $\bar{\Theta}_{3,i}^{(V)}$ as the remaining part with size $\left|\mathcal{C}_1^{(n)}\right| - \left(\left|\mathcal{G}_2^{(n)}\right| + \left|\mathcal{G}_0^{(n)}\right| - \left|\mathcal{C}_{1,2}^{(n)}\right|\right)$. According to (5.36)–(5.39), for $i \in [1, L]$ we have $\Pi_{(2),i}^{(V)} = \tilde{A}_i\left[\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)}\right] = \varnothing$, $\Pi_{(1),i}^{(V)} = \tilde{A}_i\left[\mathcal{I}^{(n)} \cap \mathcal{G}_1^{(n)}\right] = \varnothing$, $\Delta_{(1),i}^{(V)} = \bar{\Theta}_{3,i}^{(V)}$, and $\Delta_{(2),i}^{(V)} = \varnothing$. Since $\mathcal{I}^{(n)} = \emptyset$, $\tilde{A}_{2:L-1}^n\left[\mathcal{G}^{(n)}\right]$ does not carry confidential information $S_{(1),2:L-1}^{(V)}$. For $i \in [1, L-1]$, sequence $\Delta_{(1),i+1}^{(V)}$ will be repeated in outer-layer $\tilde{T}_{(1),i}^n$.

2. *Achievability of* $(R_{S_{(1)}}^{\star 2}, R_{S_{(2)}}^{\star 2}, R_{W_{(1)}}^{\star 2}, R_{W_{(2)}}^{\star 2}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(2)}$. Construction of $\tilde{A}_{1:L}\left[\mathcal{G}^{(n)}\right]$ is the same as that to achieve this rate tuple when $I(V;Z) \leq I(V;Y_{(1)}) \leq I(V;Y_{(2)})$.

Case D when $I(V;Y_{(1)}) \leq I(V;Y_{(2)}) < I(V;Z)$

1. *Achievability of* $(R_{S_{(1)}}^{\star 1}, R_{S_{(2)}}^{\star 1}, R_{W_{(1)}}^{\star 1}, R_{W_{(2)}}^{\star 1}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(1)}$. In this situation, from (5.29), we have $\left|\mathcal{G}_0^{(n)}\right| - \left|\mathcal{C}_{1,2}^{(n)}\right| < \left|\mathcal{C}_1^{(n)}\right| - \left|\mathcal{G}_2^{(n)}\right|$ and $\left|\mathcal{G}_0^{(n)}\right| - \left|\mathcal{C}_{1,2}^{(n)}\right| < \left|\mathcal{C}_2^{(n)}\right| - \left|\mathcal{G}_1^{(n)}\right|$. Therefore:

$$\begin{aligned}\mathcal{R}_{1,2}^{(n)} &\triangleq \text{any subset of } \mathcal{G}_0^{(n)} \text{ with size } \left|\mathcal{C}_{1,2}^{(n)}\right|,\\ \mathcal{R}_{1,2}'^{(n)} &\triangleq \mathcal{G}_0^{(n)} \setminus \mathcal{R}_{1,2}^{(n)},\end{aligned}$$

$\mathcal{R}_1^{(n)} \triangleq \mathcal{G}_2^{(n)}$, $\mathcal{R}_2^{(n)} \triangleq \mathcal{G}_1^{(n)}$ and $\mathcal{R}_1'^{(n)} = \mathcal{R}_2'^{(n)} \triangleq \emptyset$. Then, from (5.30)–(5.32), we have $\mathcal{R}_{\mathrm{S}}^{(n)} = \mathcal{I}^{(n)} = \emptyset$ and $\mathcal{R}_{\Lambda}^{(n)} = \mathcal{G}_{1,2}^{(n)}$. For $i \in [1, L]$, let $\Gamma_{1,i}^{(V)} \triangleq \Gamma_i^{(V)}$, $\bar{\Gamma}_{1,i}^{(V)} \triangleq \bar{\Gamma}_i^{(V)}$ and $\bar{\Gamma}_{p,i}^{(V)} = \Gamma_{p,i}^{(V)} \triangleq \varnothing$ for $p \in [2, 3]$. Also, we define $\bar{\Theta}_{1,i}^{(V)}$ as any part of $\bar{\Theta}_i^{(V)}$ with size $\left|\mathcal{G}_2^{(n)}\right|$, $\bar{\Theta}_{2,i}^{(V)}$ as any part of $\bar{\Theta}_i^{(V)}$ that is not included in $\bar{\Theta}_{1,i}^{(V)}$ with size $\left|\mathcal{G}_0^{(n)}\right| - \left|\mathcal{C}_{1,2}^{(n)}\right|$, and $\bar{\Theta}_{3,i}^{(V)}$ as the remaining part of $\bar{\Theta}_i^{(V)}$ with size $\left|\mathcal{C}_1^{(n)}\right| - \left|\mathcal{G}_2^{(n)}\right| - \left(\left|\mathcal{G}_0^{(n)}\right| - \left|\mathcal{C}_{1,2}^{(n)}\right|\right)$. On the other hand, define $\Psi_{1,i}^{(V)}$ as any part of $\Psi_i^{(V)}$ with size $\left|\mathcal{G}_1^{(n)}\right|$, $\Psi_{2,i}^{(V)}$ as any part of $\Psi_i^{(V)}$ that is not included in $\Psi_{1,i}^{(V)}$ with size $\left|\mathcal{G}_0^{(n)}\right| - \left|\mathcal{C}_{1,2}^{(n)}\right|$, and $\Psi_{3,i}^{(V)}$ as the remaining part with size $\left|\mathcal{C}_2^{(n)}\right| - \left|\mathcal{G}_1^{(n)}\right| - \left(\left|\mathcal{G}_0^{(n)}\right| - \left|\mathcal{C}_{1,2}^{(n)}\right|\right)$. According to (5.36)–(5.39), for $i \in [1, L]$ we have $\Pi_{(2),i}^{(V)} = \tilde{A}_i\left[\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)}\right] = \varnothing$, $\Pi_{(1),i}^{(V)} = \tilde{A}_i\left[\mathcal{I}^{(n)} \cap \mathcal{G}_1^{(n)}\right] = \varnothing$, $\Delta_{(1),i}^{(V)} = \bar{\Theta}_{3,i}^{(V)}$, and $\Delta_{(2),i}^{(V)} = \Psi_{3,i}^{(V)}$. The sequence $\Delta_{(1),i+1}^{(V)}$ $(i \in [1, L-1])$ will be repeated in $\tilde{T}_{(1),i}^n$, while $\Delta_{(2),i-1}^{(V)}$ $(i \in [2, L])$ will be stored in $\tilde{T}_{(2),i}^n$. Since $\mathcal{I}^{(n)} = \emptyset$, then $\tilde{A}_{2:L-1}^n\left[\mathcal{G}^{(n)}\right]$ does not carry confidential information. This particular encoding is represented in Figure 5.8.

2. *Achievability of* $(R_{S_{(1)}}^{\star 2}, R_{S_{(2)}}^{\star 2}, R_{W_{(1)}}^{\star 2}, R_{W_{(2)}}^{\star 2}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(2)}$. Construction of $\tilde{A}_{1:L}\left[\mathcal{G}^{(n)}\right]$ is almost the same as that to achieve the previous corner point of region $\mathfrak{R}_{\text{MI-WTBC}}^{(1)}$: to approach this rate tuple the encoder repeats $\left[\bar{\Psi}_{i-1}^{(V)}, \bar{\Gamma}_{i-1}^{(V)}\right]$ and $\left[\Theta_{i+1}^{(V)}, \Gamma_{i+1}^{(V)}\right]$ in Block i.

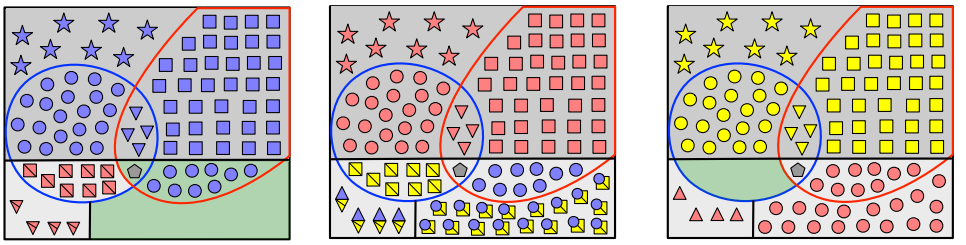

Figure 5.8: Case D when $I(V;Y_{(1)}) \leq I(V;Y_{(2)}) < I(V;Z)$: inner-layer encoding to achieve the corner point of $\mathfrak{R}^{(1)}_{\text{MI-WTBC}}$ that leads to the construction of $\tilde{A}_{1:L}[\mathcal{H}_V^{(n)}]$ when $L=3$. Consider Block 2: the sets $\mathcal{R}_1^{(n)}$, $\mathcal{R}_2^{(n)}$, $\mathcal{R}_{1,2}^{(n)}$, $\mathcal{R}_{1,2}^{\prime(n)}$ and $\mathcal{R}_\Lambda^{(n)}$ are those areas filled with yellow squares, blue circles, blue and yellow diamonds, yellow squares overlapped by blue circles, and gray pentagons, respectively. At Block $i \in [1,L]$, $W_{(1),i}^{(V)}$ is represented by symbols of the same color (red symbols at Block 2), and $\Theta_i^{(V)}$, $\Psi_i^{(V)}$ and $\Gamma_i^{(V)}$ are represented by squares, circles and triangles respectively. Also, $\bar{\Theta}_i^{(V)}$ and $\bar{\Gamma}_i^{(V)}$ are denoted by squares and triangles, respectively, with a line through them. The diamonds at Block $i \in [2, L-1]$ represent $\Gamma_{1,i-1}^{(V)} \oplus \bar{\Gamma}_{1,i+1}^{(V)}$, while the squares overlapped by circles denote $\Psi_{2,i-1}^{(V)} \oplus \bar{\Theta}_{2,i+1}^{(V)}$. For $i \in [2, L-1]$, $\tilde{A}_i[\mathcal{G}^{(n)}]$ does not carry confidential information $S_{(1),i}^{(V)}$, but only $\tilde{A}_1[\mathcal{G}^{(n)}]$ and $\tilde{A}_L[\mathcal{G}^{(n)}]$ does (into the green area). The elements of $\Psi_{i-1}^{(V)}$, or $\bar{\Theta}_{i+1}^{(V)}$, which do not fit in $\tilde{A}_i[\mathcal{R}_{1,2}^{\prime(n)} \cup \mathcal{R}_2^{(n)}]$, or $\tilde{A}_i[\mathcal{R}_{1,2}^{\prime(n)} \cup \mathcal{R}_1^{(n)}]$, will be sent to $\tilde{T}_{(2),i}^n$, or $\tilde{T}_{(1),i}^n$, respectively. At Block 1, $\Lambda_1^{(V)}$ is denoted by gray pentagons and is repeated in all blocks. Finally, sequences $\Upsilon_{(1)}^{(V)}$ and $\Upsilon_{(2)}^{(V)}$ are those entries inside the red curve at Block 1 and the blue curve at Block L, respectively.

Case E when $I(V;Y_{(1)}) < I(V;Z) \leq I(V;Y_{(2)})$

In Case E, we have $|\mathcal{G}_1^{(n)}| > |\mathcal{C}_2^{(n)}|$, $|\mathcal{G}_2^{(n)}| < |\mathcal{C}_1^{(n)}|$ and $|\mathcal{G}_0^{(n)}| < |\mathcal{C}_{1,2}^{(n)}|$.

1. *Achievability of* $(R_{S_{(1)}}^{\star 1}, R_{S_{(2)}}^{\star 1}, R_{W_{(1)}}^{\star 1}, R_{W_{(2)}}^{\star 1}) \subset \mathfrak{R}^{(1)}_{\text{MI-WTBC}}$. In this case, we define

$$\begin{aligned}
\mathcal{R}_1^{(n)} &\triangleq \mathcal{G}_2^{(n)},\\
\mathcal{R}_2^{(n)} &\triangleq \text{any subset of } \mathcal{G}_1^{(n)} \text{ with size } \left|\mathcal{C}_2^{(n)}\right|,\\
\mathcal{R}_{1,2}^{(n)} &\triangleq \mathcal{G}_0^{(n)},\\
\mathcal{R}_2^{\prime(n)} &\triangleq \text{any subset of } \mathcal{G}_1^{(n)} \setminus \mathcal{R}_2^{(n)} \text{ with size } \left|\mathcal{C}_{1,2}^{(n)}\right| - \left|\mathcal{G}_0^{(n)}\right|,
\end{aligned}$$

and $\mathcal{R}_1^{\prime(n)} = \mathcal{R}_{1,2}^{\prime(n)} \triangleq \varnothing$. Then, from (5.30)–(5.32), we have $\mathcal{R}_{\text{S}}^{(n)} = \mathcal{I}^{(n)} = \emptyset$ and

$$\mathcal{R}_\Lambda^{(n)} = \mathcal{G}_{1,2}^{(n)} \cup \left(\mathcal{G}_1^{(n)} \setminus \mathcal{R}_2^{(n)}\right).$$

From condition (5.28), all previous sets exist. For $i \in [1,L]$, we define $\Psi_{1,i}^{(V)} \triangleq \Psi_i^{(V)}$ and $\Psi_{p,i}^{(V)} \triangleq \varnothing$ for $p \in [2,3]$. Also, we define $\bar{\Theta}_{1,i}^{(V)}$ as any part of $\bar{\Theta}_i^{(V)}$ with size $\left|\mathcal{G}_2^{(n)}\right|$, $\bar{\Theta}_{2,i}^{(V)} \triangleq \varnothing$, and $\bar{\Theta}_{3,i}^{(V)}$ as the remaining part with size $\left|\mathcal{C}_1^{(n)}\right| - \left|\mathcal{G}_2^{(n)}\right|$. We define $\Gamma_{1,i}^{(V)}$ as any part of $\Gamma_i^{(V)}$ with size $\left|\mathcal{G}_0^{(n)}\right|$, $\Gamma_{2,i}^{(V)}$ as the remaining part with size $\left|\mathcal{C}_{1,2}^{(n)}\right| - \left|\mathcal{G}_0^{(n)}\right|$, and

$\Gamma_{3,i}^{(V)} \triangleq \varnothing$. Finally, $\bar{\Gamma}_{1,i}^{(V)}$ is defined as any part of $\bar{\Gamma}_i^{(V)}$ with size $\left|\mathcal{G}_0^{(n)}\right|$, $\bar{\Gamma}_{2,i}^{(V)} \triangleq \varnothing$, and $\bar{\Gamma}_{3,i}^{(V)}$ as the remaining part of $\bar{\Gamma}_i^{(V)}$ with size $\left|\mathcal{C}_{1,2}^{(n)}\right| - \left|\mathcal{G}_0^{(n)}\right|$. According to (5.36)–(5.39), for $i \in [1, L]$ we have $\Pi_{(2),i}^{(V)} = \tilde{A}_i\big[\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)}\big] = \varnothing$, $\Pi_{(1),i}^{(V)} = \tilde{A}_i\big[\mathcal{I}^{(n)} \cap \mathcal{G}_1^{(n)}\big] = \varnothing$, $\Delta_{(1),i}^{(V)} = \big[\bar{\Theta}_{3,i}^{(V)}, \bar{\Gamma}_{3,i}^{(V)}\big]$ with size $\left|\mathcal{C}_1^{(n)}\right| - \left|\mathcal{G}_2^{(n)}\right| + \left|\mathcal{C}_{1,2}^{(n)}\right| - \left|\mathcal{G}_0^{(n)}\right|$, and $\Delta_{(2),i}^{(V)} = \varnothing$. Since $\mathcal{I}^{(n)} = \emptyset$, $\tilde{A}_{2:L-1}^n\big[\mathcal{G}^{(n)}\big]$ does not carry confidential information $S_{(1),2:L-1}^{(V)}$. For $i \in [1, L-1]$, sequence $\Delta_{(1),i+1}^{(V)}$ will be repeated in outer-layer $\tilde{T}_{(1),i}^n$.

2. *Achievability of* $(R_{S_{(1)}}^{\star 2}, R_{S_{(2)}}^{\star 2}, R_{W_{(1)}}^{\star 2}, R_{W_{(2)}}^{\star 2}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(2)}$. Construction of $\tilde{A}_{1:L}\big[\mathcal{G}^{(n)}\big]$ is similar to the previous one to achieve the previous corner point of region $\mathfrak{R}_{\text{MI-WTBC}}^{(1)}$. We define $\mathcal{R}_1^{(n)}$, $\mathcal{R}_2^{(n)}$, $\mathcal{R}_{1,2}^{(n)}$, $\mathcal{R}_1^{\prime(n)}$, $\mathcal{R}_2^{\prime(n)}$ and $\mathcal{R}_{1,2}^{\prime(n)}$ as for the previous corner point. Thus, according to (5.30), (5.33) and (5.34), we have $\mathcal{R}_{\text{S}}^{(n)} = \emptyset$ and

$$\begin{aligned}\mathcal{I}^{(n)} &= \mathcal{G}_1^{(n)} \setminus \big(\mathcal{R}_2^{(n)} \cup \mathcal{R}_2^{\prime(n)}\big),\\ \mathcal{R}_{\Lambda}^{(n)} &= \mathcal{G}_{1,2}^{(n)}.\end{aligned}$$

Now, for $i \in [1, L]$ we define $\bar{\Psi}_{1,i}^{(V)} \triangleq \bar{\Psi}_i^{(V)}$ and $\bar{\Psi}_{p,i}^{(V)} \triangleq \varnothing$ for $p \in [2, 3]$. Also, $\Theta_{1,i}^{(V)}$ is defined as any part of $\Theta_i^{(V)}$ with size $\left|\mathcal{G}_2^{(n)}\right|$, $\Theta_{2,i}^{(V)} \triangleq \varnothing$, and $\Theta_{3,i}^{(V)}$ as the remaining part with size $\left|\mathcal{C}_1^{(n)}\right| - \left|\mathcal{G}_2^{(n)}\right|$. We define $\bar{\Gamma}_{1,i}^{(V)}$ as any part of $\bar{\Gamma}_i^{(V)}$ with size $\left|\mathcal{G}_0^{(n)}\right|$, $\bar{\Gamma}_{2,i}^{(V)}$ as the remaining part with size $\left|\mathcal{C}_{1,2}^{(n)}\right| - \left|\mathcal{G}_0^{(n)}\right|$, and $\bar{\Gamma}_{3,i}^{(V)} \triangleq \varnothing$. Finally, we define $\Gamma_{1,i}^{(V)}$ as any part of $\Gamma_i^{(V)}$ with size $\left|\mathcal{G}_0^{(n)}\right|$, $\bar{\Gamma}_{2,i}^{(V)} \triangleq \varnothing$, and $\Gamma_{3,i}^{(V)}$ as the remaining part with size $\left|\mathcal{C}_{1,2}^{(n)}\right| - \left|\mathcal{G}_0^{(n)}\right|$. From (5.36)–(5.39), for $i \in [1, L]$ we have $\Pi_{(2),i}^{(V)} = \tilde{A}_i\big[\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)}\big] = \varnothing$, $\Pi_{(1),i}^{(V)} = \tilde{A}_i\big[\mathcal{I}^{(n)} \cap \mathcal{G}_1^{(n)}\big]$ with size $\left|\mathcal{G}_1^{(n)}\right| - \left|\mathcal{C}_2^{(n)}\right| - \big(\left|\mathcal{C}_{1,2}^{(n)}\right| - \left|\mathcal{G}_0^{(n)}\right|\big)$, $\Delta_{(2),i}^{(V)} = \varnothing$ and $\Delta_{(1),i}^{(V)} = \big[\Theta_{3,i}^{(V)}, \Gamma_{3,i}^{(V)}\big]$ with size $\left|\mathcal{C}_1^{(n)}\right| - \left|\mathcal{G}_2^{(n)}\right| + \left|\mathcal{C}_{1,2}^{(n)}\right| - \left|\mathcal{G}_0^{(n)}\right|$. According to Algorithm 5.2, now $\tilde{A}_{1:L}^n\big[\mathcal{G}^{(n)}\big]$ carries confidential information $S_{(2),1:L}^{(V)}$. For $i \in [1, L-1]$, $\Delta_{(1),i+1}^{(V)}$ will be repeated in $\tilde{T}_{(1),i}^n$.

Case E when $I(V; Y_{(1)}) \leq I(V; Y_{(2)}) < I(V; Z)$

1. *Achievability of* $(R_{S_{(1)}}^{\star 1}, R_{S_{(2)}}^{\star 1}, R_{W_{(1)}}^{\star 1}, R_{W_{(2)}}^{\star 1}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(1)}$. According to condition (5.29), now we have $\left|\mathcal{G}_1^{(n)}\right| - \left|\mathcal{C}_2^{(n)}\right| < \left|\mathcal{C}_{1,2}^{(n)}\right| - \left|\mathcal{G}_0^{(n)}\right|$ and $\left|\mathcal{G}_2^{(n)}\right| - \left|\mathcal{C}_1^{(n)}\right| < \left|\mathcal{C}_{1,2}^{(n)}\right| - \left|\mathcal{G}_0^{(n)}\right|$. Now, all the elements of $\Gamma_{i-1}^{(V)}$, $i \in [2, L]$, cannot be repeated in $\tilde{A}_i\big[\mathcal{G}_1^{(n)} \setminus \mathcal{R}_2^{(n)}\big]$ as before. Thus:

$$\begin{aligned}&\mathcal{R}_1^{(n)} \triangleq \mathcal{G}_2^{(n)},\\ &\mathcal{R}_2^{(n)} \triangleq \text{any subset of } \mathcal{G}_1^{(n)} \text{ with size } \left|\mathcal{C}_2^{(n)}\right|,\\ &\mathcal{R}_{1,2}^{(n)} \triangleq \mathcal{G}_0^{(n)},\\ &\mathcal{R}_2^{\prime(n)} \triangleq \mathcal{G}_1^{(n)} \setminus \mathcal{R}_2^{(n)},\end{aligned}$$

and $\mathcal{R}_1^{\prime(n)} = \mathcal{R}_{1,2}^{\prime(n)} \triangleq \varnothing$. Then, from (5.30)–(5.32), we have $\mathcal{R}_{\mathrm{S}}^{(n)} = \mathcal{I}^{(n)} = \emptyset$ and $\mathcal{R}_{\Lambda}^{(n)} = \mathcal{G}_{1,2}^{(n)}$. For $i \in [1, L]$ we define $\Psi_{1,i}^{(V)} \triangleq \Psi_i^{(V)}$ and $\Psi_{p,i}^{(V)} \triangleq \varnothing$ for $p \in [2, 3]$. Also, $\bar{\Theta}_{1,i}^{(V)}$ is defined as any part of $\bar{\Theta}_i^{(V)}$ with size $\left|\mathcal{G}_2^{(n)}\right|$, $\bar{\Theta}_{2,i}^{(V)} \triangleq \varnothing$, and $\bar{\Theta}_{3,i}^{(V)}$ as the remaining part with size $\left|\mathcal{C}_1^{(n)}\right| - \left|\mathcal{G}_2^{(n)}\right|$. We define $\bar{\Gamma}_{1,i}^{(V)}$ as any part of $\bar{\Gamma}_i^{(V)}$ with size $\left|\mathcal{G}_0^{(n)}\right|$, $\bar{\Gamma}_{2,i}^{(V)} \triangleq \varnothing$, and $\bar{\Gamma}_{3,i}^{(V)}$ as the remaining part with size $\left|\mathcal{C}_{1,2}^{(n)}\right| - \left|\mathcal{G}_0^{(n)}\right|$. Finally, we define $\Gamma_{1,i}^{(V)}$ as any part of $\Gamma_i^{(V)}$ with size $\left|\mathcal{G}_0^{(n)}\right|$, $\Gamma_{2,i}^{(V)}$ as any part of $\Gamma_i^{(V)}$ that is not included in $\Gamma_{1,i}^{(V)}$ with size $\left|\mathcal{G}_1^{(n)}\right| - \left|\mathcal{C}_2^{(n)}\right|$, and $\Gamma_{3,i}^{(V)}$ as the remaining part with size $\left|\mathcal{C}_{1,2}^{(n)}\right| - \left|\mathcal{G}_0^{(n)}\right| - \left(\left|\mathcal{G}_1^{(n)}\right| - \left|\mathcal{C}_2^{(n)}\right|\right)$. According to (5.36)–(5.39), for $i \in [1, L]$ we have $\Pi_{(2),i}^{(V)} = \tilde{A}_i\left[\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)}\right] = \varnothing$, $\Pi_{(1),i}^{(V)} = \tilde{A}_i\left[\mathcal{I}^{(n)} \cap \mathcal{G}_1^{(n)}\right] = \varnothing$, $\Delta_{(1),i}^{(V)} = \left[\bar{\Theta}_{3,i}^{(V)}, \bar{\Gamma}_{3,i}^{(V)}\right]$ with size $\left|\mathcal{C}_1^{(n)}\right| - \left|\mathcal{G}_2^{(n)}\right| + \left|\mathcal{C}_{1,2}^{(n)}\right| - \left|\mathcal{G}_0^{(n)}\right|$, and $\Delta_{(2),i}^{(V)} = \Gamma_{3,i}^{(V)}$ with size $\left|\mathcal{C}_{1,2}^{(n)}\right| - \left|\mathcal{G}_0^{(n)}\right| - \left|\mathcal{G}_1^{(n)}\right| + \left|\mathcal{C}_2^{(n)}\right|$. Since $\mathcal{I}^{(n)} = \emptyset$, $\tilde{A}_{2:L-1}^n$ does not carry confidential information $S_{(1),2:L-1}^{(V)}$. Lastly, $\Delta_{(1),i+1}^{(V)}$ ($i \in [1, L-1]$) will be repeated in $\tilde{T}_{(1),i}^n$, and $\Delta_{(2),i-1}^{(V)}$ ($i \in [2, L]$) will be repeated in $\tilde{T}_{(2),i}^n$.

2. *Achievability of* $(R_{S_{(1)}}^{\star 2}, R_{S_{(2)}}^{\star 2}, R_{W_{(1)}}^{\star 2}, R_{W_{(2)}}^{\star 2}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(2)}$. Construction of $\tilde{A}_{1:L}\left[\mathcal{G}^{(n)}\right]$ is exactly the same as the one to achieve the previous corner point of region $\mathfrak{R}_{\text{MI-WTBC}}^{(1)}$.

Case F when $I(V; Y_{(1)}) \leq I(V; Y_{(2)}) < I(V; Z)$

In Case F, we have $|\mathcal{G}_1^{(n)}| < |\mathcal{C}_2^{(n)}|$, $|\mathcal{G}_2^{(n)}| < |\mathcal{C}_1^{(n)}|$ and $|\mathcal{G}_0^{(n)}| < |\mathcal{C}_{1,2}^{(n)}|$.

1. *Achievability of* $(R_{S_{(1)}}^{\star 1}, R_{S_{(2)}}^{\star 1}, R_{W_{(1)}}^{\star 1}, R_{W_{(2)}}^{\star 1}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(1)}$. In this case, for $i \in [2, L]$ the PCS can repeat entirely neither $\Gamma_{i-1}^{(V)}$ in $\tilde{A}_i\left[\mathcal{G}_0^{(n)}\right]$ nor $\Psi_{i-1}^{(V)}$ in $\tilde{A}_i\left[\mathcal{G}_1^{(n)}\right]$. Also, for $i \in [1, L-1]$, it can repeat entirely neither $\bar{\Gamma}_{i+1}^{(V)}$ in $\tilde{A}_i\left[\mathcal{G}_0^{(n)}\right]$ nor $\bar{\Theta}_{i+1}^{(V)}$ in $\tilde{A}_i\left[\mathcal{G}_2^{(n)}\right]$. Thus, we define $\mathcal{R}_{1,2}^{(n)} \triangleq \mathcal{G}_0^{(n)}$, $\mathcal{R}_1^{(n)} \triangleq \mathcal{G}_2^{(n)}$, $\mathcal{R}_2^{(n)} \triangleq \mathcal{G}_1^{(n)}$, and $\mathcal{R}_1^{\prime(n)} = \mathcal{R}_2^{\prime(n)} = \mathcal{R}_{1,2}^{\prime(n)} \triangleq \varnothing$. For $i \in [1, L]$, we define $\Psi_{1,i}^{(V)}$ as any part of $\Psi_i^{(V)}$ with size $\left|\mathcal{G}_1^{(n)}\right|$, $\Psi_{1,i}^{(V)} \triangleq \varnothing$, and $\Psi_{3,i}^{(V)}$ as the remaining part with size $\left|\mathcal{C}_2^{(n)}\right| - \left|\mathcal{G}_1^{(n)}\right|$. Also, we define $\bar{\Theta}_{1,i}^{(V)}$ as any part of $\bar{\Theta}_i^{(V)}$ with size $\left|\mathcal{G}_2^{(n)}\right|$, $\bar{\Theta}_{2,i}^{(V)} \triangleq \varnothing$, and $\bar{\Theta}_{3,i}^{(V)}$ as the remaining part with size $\left|\mathcal{C}_1^{(n)}\right| - \left|\mathcal{G}_2^{(n)}\right|$. Finally, we define $\Gamma_{1,i}^{(V)}$ and $\bar{\Gamma}_{1,i}^{(V)}$ as any part of $\Gamma_i^{(V)}$ and $\bar{\Gamma}_i^{(V)}$, respectively, with size $\left|\mathcal{G}_0^{(n)}\right|$, $\Gamma_{2,i}^{(V)} = \bar{\Gamma}_{2,i}^{(V)} \triangleq \varnothing$, and $\Gamma_{3,i}^{(V)}$ and $\bar{\Gamma}_{3,i}^{(V)}$ as the remaining parts with size $\left|\mathcal{C}_{1,2}^{(n)}\right| - \left|\mathcal{G}_0^{(n)}\right|$. According to (5.36)–(5.39), for $i \in [1, L]$ we have $\Pi_{(2),i}^{(V)} = \tilde{A}_i\left[\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)}\right] = \varnothing$, $\Pi_{(1),i}^{(V)} = \tilde{A}_i\left[\mathcal{I}^{(n)} \cap \mathcal{G}_1^{(n)}\right] = \varnothing$, $\Delta_{(1),i}^{(V)} = \left[\bar{\Theta}_{3,i}^{(V)}, \bar{\Gamma}_{3,i}^{(V)}\right]$ with size $\left|\mathcal{C}_1^{(n)}\right| - \left|\mathcal{G}_2^{(n)}\right| + \left|\mathcal{C}_{1,2}^{(n)}\right| - \left|\mathcal{G}_0^{(n)}\right|$, and $\Delta_{(2),i}^{(V)} = \left[\Psi_{3,i}^{(V)}, \Gamma_{3,i}^{(V)}\right]$ with size $\left|\mathcal{C}_2^{(n)}\right| - \left|\mathcal{G}_1^{(n)}\right| + \left|\mathcal{C}_{1,2}^{(n)}\right| - \left|\mathcal{G}_0^{(n)}\right|$. Since $\mathcal{I}^{(n)} = \emptyset$, $\tilde{A}_{2:L-1}^n$ does not carry confidential information $S_{(1),2:L-1}^{(V)}$. Lastly, $\Delta_{(1),i+1}^{(V)}$ ($i \in [1, L-1]$) will be repeated in $\tilde{T}_{(1),i}^n$, and $\Delta_{(2),i-1}^{(V)}$ ($i \in [2, L]$) will be repeated in $\tilde{T}_{(2),i}^n$.

2. *Achievability of* $(R_{S_{(1)}}^{\star 2}, R_{S_{(2)}}^{\star 2}, R_{W_{(1)}}^{\star 2}, R_{W_{(2)}}^{\star 2}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(2)}$. Construction of $\tilde{A}_{1:L}\left[\mathcal{G}^{(n)}\right]$ is almost the same as that to achieve the previous corner point of region $\mathfrak{R}_{\text{MI-WTBC}}^{(1)}$: to approach this rate tuple the encoder repeats $\left[\bar{\Psi}_{i-1}^{(V)}, \bar{\Gamma}_{i-1}^{(V)}\right]$ and $\left[\Theta_{i+1}^{(V)}, \Gamma_{i+1}^{(V)}\right]$ in Block i.

Summary of the construction of $\tilde{\boldsymbol{A}}_{1:L}\big[\mathcal{G}^{(n)}\big]$

From (5.30)–(5.39); and from the definition of $\mathcal{R}_1^{(n)}$, $\mathcal{R}_2^{(n)}$, $\mathcal{R}_{1,2}^{(n)}$, $\mathcal{R}_1'^{(n)}$, $\mathcal{R}_2'^{(n)}$ and $\mathcal{R}_{1,2}'^{(n)}$, and $\Psi_{p,i}^{(V)}$, $\bar{\Psi}_{p,i}^{(V)}$, $\Gamma_{p,i}^{(V)}$, $\bar{\Gamma}_{p,i}^{(V)}$, $\Theta_{p,i}^{(V)}$ and $\bar{\Theta}_{p,i}^{(V)}$ for $p \in [1,3]$ and $i \in [1,L]$ in each case, we have:

1. when $I(V;Z) \leq I(V;Y_{(1)}) \leq I(V;Y_{(2)})$,
   - if the PCS operates to achieve $(R_{S_{(1)}}^{\star 1}, R_{S_{(2)}}^{\star 1}, R_{W_{(1)}}^{\star 1}, R_{W_{(2)}}^{\star 1}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(1)}$:
     - the inner-layer carries $S_{(1),1:L}^{(V)}$, and $\big|\mathcal{I}^{(n)}\big| = \big|\mathcal{G}_0^{(n)}\big| + \big|\mathcal{G}_2^{(n)}\big| - \big|\mathcal{C}_1^{(n)}\big| - \big|\mathcal{C}_{1,2}^{(n)}\big|$;
     - we have $\Pi_{(1),i}^{(V)} = \varnothing$ and $\Delta_{(1),i}^{(V)} = \varnothing$;
     - we have $\Delta_{(2),i}^{(V)} = \varnothing$.
   - if the PCS operates to achieve $(R_{S_{(1)}}^{\star 2}, R_{S_{(2)}}^{\star 2}, R_{W_{(1)}}^{\star 2}, R_{W_{(2)}}^{\star 2}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(2)}$:
     - the inner-layer carries $S_{(2),1:L}^{(V)}$, and $\big|\mathcal{I}^{(n)}\big| = \big|\mathcal{G}_0^{(n)}\big| + \big|\mathcal{G}_1^{(n)}\big| - \big|\mathcal{C}_2^{(n)}\big| - \big|\mathcal{C}_{1,2}^{(n)}\big|$;
     - the overall size of $\big[\Pi_{(1),i}^{(V)}, \Delta_{(1),i}^{(V)}\big]$ is $\big|\mathcal{G}_1^{(n)}\big| + \big|\mathcal{C}_1^{(n)}\big| - \big|\mathcal{G}_2^{(n)}\big| - \big|\mathcal{C}_2^{(n)}\big|$;
     - we have $\Delta_{(2),i}^{(V)} = \varnothing$.
2. when $I(V;Y_{(1)}) < I(V;Z) \leq I(V;Y_{(2)})$,
   - if the PCS operates to achieve $(R_{S_{(1)}}^{\star 1}, R_{S_{(2)}}^{\star 1}, R_{W_{(1)}}^{\star 1}, R_{W_{(2)}}^{\star 1}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(1)}$:
     - the inner-layer carries $S_{(1),1:L}^{(V)}$, but $\big|\mathcal{I}^{(n)}\big| = 0$;
     - we have $\Pi_{(1),i}^{(V)} = \varnothing$, and the size of $\Delta_{(1),i}^{(V)}$ is $\big|\mathcal{C}_1^{(n)}\big| + \big|\mathcal{C}_{1,2}^{(n)}\big| - \big|\mathcal{G}_0^{(n)}\big| - \big|\mathcal{G}_2^{(n)}\big|$;
     - we have $\Delta_{(2),i}^{(V)} = \varnothing$.
   - if the PCS operates to achieve $(R_{S_{(1)}}^{\star 2}, R_{S_{(2)}}^{\star 2}, R_{W_{(1)}}^{\star 2}, R_{W_{(2)}}^{\star 2}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(2)}$:
     - the inner-layer carries $S_{(2),1:L}^{(V)}$, and $\big|\mathcal{I}^{(n)}\big| = \big|\mathcal{G}_0^{(n)}\big| + \big|\mathcal{G}_1^{(n)}\big| - \big|\mathcal{C}_2^{(n)}\big| - \big|\mathcal{C}_{1,2}^{(n)}\big|$;
     - the overall size of $\big[\Pi_{(1),i}^{(V)}, \Delta_{(1),i}^{(V)}\big]$ is $\big|\mathcal{G}_1^{(n)}\big| + \big|\mathcal{C}_1^{(n)}\big| - \big|\mathcal{G}_2^{(n)}\big| - \big|\mathcal{C}_2^{(n)}\big|$;
     - we have $\Delta_{(2),i}^{(V)} = \varnothing$.
3. when $I(V;Y_{(1)}) \leq I(V;Y_{(2)}) < I(V;Z)$,
   - if the PCS operates to achieve $(R_{S_{(1)}}^{\star 1}, R_{S_{(2)}}^{\star 1}, R_{W_{(1)}}^{\star 1}, R_{W_{(2)}}^{\star 1}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(1)}$:
     - the inner-layer carries $S_{(1),1:L}^{(V)}$, but $\big|\mathcal{I}^{(n)}\big| = 0$;
     - we have $\Pi_{(1),i}^{(V)} = \varnothing$, and the size of $\Delta_{(1),i}^{(V)}$ is $\big|\mathcal{C}_1^{(n)}\big| + \big|\mathcal{C}_{1,2}^{(n)}\big| - \big|\mathcal{G}_0^{(n)}\big| - \big|\mathcal{G}_2^{(n)}\big|$;
     - the length of $\Delta_{(2),i}^{(V)}$ is $\big|\mathcal{C}_2^{(n)}\big| + \big|\mathcal{C}_{1,2}^{(n)}\big| - \big|\mathcal{G}_0^{(n)}\big| - \big|\mathcal{G}_1^{(n)}\big|$.
   - if the PCS operates to achieve $(R_{S_{(1)}}^{\star 2}, R_{S_{(2)}}^{\star 2}, R_{W_{(1)}}^{\star 2}, R_{W_{(2)}}^{\star 2}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(2)}$:
     - the inner-layer carries $S_{(2),1:L}^{(V)}$, but $\big|\mathcal{I}^{(n)}\big| = 0$;
     - we have $\Pi_{(1),i}^{(V)} = \varnothing$, and the size of $\Delta_{(1),i}^{(V)}$ is $\big|\mathcal{C}_1^{(n)}\big| + \big|\mathcal{C}_{1,2}^{(n)}\big| - \big|\mathcal{G}_0^{(n)}\big| - \big|\mathcal{G}_2^{(n)}\big|$;
     - the length of $\Delta_{(2),i}^{(V)}$ is $\big|\mathcal{C}_2^{(n)}\big| + \big|\mathcal{C}_{1,2}^{(n)}\big| - \big|\mathcal{G}_0^{(n)}\big| - \big|\mathcal{G}_1^{(n)}\big|$.

5.2.2 Construction of the outer-layers

Consider that the PCS must achieve $(R^{\star k}_{S_{(1)}}, R^{\star k}_{S_{(2)}}, R^{\star k}_{W_{(1)}}, R^{\star k}_{W_{(2)}}) \subseteq \mathfrak{R}^{(k)}_{\text{MI-WTBC}}$, where $k \in [1,2]$. In order to achieve this corner point, for $i \in [1, L]$ the PCS first constructs $\tilde{T}^n_{(k),i}$ associated to Receiver k, and then forms $\tilde{T}^n_{(\bar{k}),i}$ associated to Receiver $\bar{k}$, where recall that $\bar{k} = [1,2] \setminus k$.

1. New sets associated to $T^n_{(k),1:L}$. The sets $\mathcal{H}^{(n)}_{U_{(k)}|V}$, $\mathcal{L}^{(n)}_{U_{(k)}|V}$, $\mathcal{H}^{(n)}_{U_{(k)}|VZ}$ and $\mathcal{L}^{(n)}_{U_{(k)}|VY_{(k)}}$ associated to outer-layer $T^n_{(k)} = U^n_{(k)} G_n$ are defined as in (5.11)–(5.14). Besides the previous sets, define the following partition of $\mathcal{H}^{(n)}_{U_{(k)}|V}$:

$$\mathcal{F}^{(n)}_0 \triangleq \mathcal{H}^{(n)}_{U_{(k)}|VZ} \cap \mathcal{L}^{(n)}_{U_{(k)}|VY_{(k)}}, \tag{5.40}$$

$$\mathcal{F}^{(n)}_k \triangleq \mathcal{H}^{(n)}_{U_{(k)}|VZ} \setminus \mathcal{L}^{(n)}_{U_{(k)}|VY_{(k)}}, \tag{5.41}$$

$$\mathcal{J}^{(n)}_0 \triangleq \mathcal{H}^{(n)}_{U_{(k)}|V} \cap \big(\mathcal{H}^{(n)}_{U_{(k)}|VZ}\big)^{\mathrm{C}} \cap \mathcal{L}^{(n)}_{U_{(k)}|VY_{(k)}}, \tag{5.42}$$

$$\mathcal{J}^{(n)}_k \triangleq \mathcal{H}^{(n)}_{U_{(k)}|V} \cap \big(\mathcal{H}^{(n)}_{U_{(k)}|VZ}\big)^{\mathrm{C}} \setminus \mathcal{L}^{(n)}_{U_{(k)}|VY_{(k)}}. \tag{5.43}$$

For $i \in [1, L]$, $\tilde{T}_{(k),i}\big[\mathcal{H}^{(n)}_{U_{(k)}|V}\big]$ will be suitable for storing uniformly distributed random sequences that are independent of $\tilde{V}^n_i$, and $\tilde{T}_{(k),i}\big[\mathcal{F}^{(n)}_0 \cup \mathcal{F}^{(n)}_k\big] = \tilde{T}_{(k),i}\big[\mathcal{H}^{(n)}_{U_{(k)}|VZ}\big]$ is suitable for storing information to be secured from the eavesdropper. Moreover, $\tilde{T}_{(k),i}\big[\mathcal{F}^{(n)}_k \cup \mathcal{J}^{(n)}_k\big] = \tilde{T}_{(k),i}\big[\mathcal{H}^{(n)}_{U_{(k)}|V} \setminus \mathcal{L}^{(n)}_{U_{(k)}|VY_{(k)}}\big]$ is the uniformly distributed part independent of $\tilde{V}^n_i$ that is needed by Receiver k to reliably reconstruct $\tilde{T}^n_{(k),i}$ from observations $\tilde{Y}^n_{(k),i}$ and sequence $\tilde{V}^n_i$ by performing SC decoding.

We consider that $I(U_{(k)}; Y_{(k)}|V) \geq I(U_{(k)}; Z|V)$ (see Remark 5.8 and Remark 5.9). Therefore, besides the partition defined in (5.40)–(5.43), we define

$$\mathcal{D}^{(n)}_k \triangleq \text{ any subset of } \mathcal{F}^{(n)}_0 \text{ with size } \big|\mathcal{J}^{(n)}_k\big|, \tag{5.44}$$

$$\mathcal{L}^{(n)}_k \triangleq \text{ any subset of } \mathcal{F}^{(n)}_0 \setminus \mathcal{D}^{(n)}_k \text{ with size } \big\{\big|\mathcal{C}^{(n)}_k\big| + \big|\mathcal{C}^{(n)}_{1,2}\big| - \big|\mathcal{G}^{(n)}_0\big| - \big|\mathcal{G}^{(n)}_{\bar{k}}\big|\big\}^+. \tag{5.45}$$

The set $\mathcal{D}^{(n)}_k$ exists because we have

$$\begin{aligned}
\big|\mathcal{F}^{(n)}_0\big| - \big|\mathcal{J}^{(n)}_k\big| &= \Big|\mathcal{H}^{(n)}_{U_{(k)}|VZ} \cap \mathcal{L}^{(n)}_{U_{(k)}|VY_{(k)}}\Big| - \Big|\mathcal{H}^{(n)}_{U_{(k)}|V} \cap \big(\mathcal{H}^{(n)}_{U_{(k)}|VZ}\big)^{\mathrm{C}} \setminus \mathcal{L}^{(n)}_{U_{(k)}|VY_{(k)}}\Big| \\
&\geq \Big|\mathcal{H}^{(n)}_{U_{(k)}|VZ} \cap \mathcal{L}^{(n)}_{U_{(k)}|VY_{(k)}}\Big| - \Big|\big(\mathcal{H}^{(n)}_{U_{(k)}|VZ}\big)^{\mathrm{C}} \setminus \mathcal{L}^{(n)}_{U_{(k)}|VY_{(k)}}\Big| \\
&= \Big|\mathcal{H}^{(n)}_{U_{(k)}|VZ}\Big| - \Big|\big(\mathcal{L}^{(n)}_{U_{(k)}|VY_{(k)}}\big)^{\mathrm{C}}\Big| \geq 0,
\end{aligned} \tag{5.46}$$

where the positivity holds by assumption and from applying Theorem 2.1 because

$$\frac{1}{n}\Big(\Big|\mathcal{H}^{(n)}_{U_{(k)}|VZ}\Big| - \Big|\big(\mathcal{L}^{(n)}_{U_{(k)}|VY_{(k)}}\big)^{\mathrm{C}}\Big|\Big) \xrightarrow{n\to\infty} H(U_{(k)}|VZ) - H(U_{(k)}|VY_{(k)}). \tag{5.47}$$

On the other hand, according to (5.27)–(5.29), if $k=1$ and $\bar{k}=2$ then $\mathcal{L}_k^{(n)}=\emptyset$ in Situation 1, where $I(V;Z)\le I(V;Y_{(1)})\le I(V;Y_{(2)})$; and $\mathcal{L}_k^{(n)}\neq\emptyset$ in Situation 2, where $I(V;Y_{(1)})<I(V;Z)\le I(V;Y_{(2)})$, and Situation 3, where $I(V;Y_{(1)})\le I(V;Y_{(2)})<I(V;Z)$. Otherwise, if $k=2$ and $\bar{k}=1$, then we have $\mathcal{L}_k^{(n)}=\emptyset$ in Situation 1 and Situation 2, while $\mathcal{L}_k^{(n)}\neq\emptyset$ in Situation 3. In situations where $\mathcal{L}_k^{(n)}\neq\emptyset$, if we consider only input distributions that imply $(R^{\star k}_{S_{(1)}},R^{\star k}_{S_{(2)}},R^{\star k}_{W_{(1)}},R^{\star k}_{W_{(2)}})\in\mathbb{R}_+^4$, set $\mathcal{L}_k^{(n)}$ exists because for $i\in[1,L]$ the entries $\tilde{A}_i(j)$ such that $j\in\mathcal{F}_0^{(n)}\setminus\big(\mathcal{D}_k^{(n)}\cup\mathcal{J}_k^{(n)}\big)$ will be intended for storing $S_{(k)}$, and the rate of $S_{(k)}$ carried in the inner-layer is is negligible (see Section 5.3.1).

2. New sets associated to $T^n_{(\bar{k}),1:L}$. Sets $\mathcal{H}^{(n)}_{U_{(\bar{k})}|VU_{(k)}}$, $\mathcal{L}^{(n)}_{U_{(\bar{k})}|VU_{(k)}}$, $\mathcal{H}^{(n)}_{U_{(\bar{k})}|VU_{(k)}Z}$ and $\mathcal{L}^{(n)}_{U_{(\bar{k})}|VY_{(k)}}$ associated to $T^n_{(\bar{k})}=U^n_{(\bar{k})}G_n$ are defined in (5.15)–(5.18). Besides the previous sets, define:

$$\mathcal{Q}_0^{(n)}\triangleq\mathcal{H}^{(n)}_{U_{(\bar{k})}|VU_{(k)}Z}\cap\mathcal{L}^{(n)}_{U_{(\bar{k})}|VY_{(\bar{k})}},\tag{5.48}$$

$$\mathcal{Q}_{\bar{k}}^{(n)}\triangleq\mathcal{H}^{(n)}_{U_{(\bar{k})}|VU_{(k)}Z}\setminus\mathcal{L}^{(n)}_{U_{(\bar{k})}|VY_{(\bar{k})}},\tag{5.49}$$

$$\mathcal{B}_0^{(n)}\triangleq\mathcal{H}^{(n)}_{U_{(\bar{k})}|VU_{(k)}}\cap\big(\mathcal{H}^{(n)}_{U_{(\bar{k})}|VU_{(k)}Z}\big)^{\mathrm{C}}\cap\mathcal{L}^{(n)}_{U_{(\bar{k})}|VY_{(\bar{k})}},\tag{5.50}$$

$$\mathcal{B}_{\bar{k}}^{(n)}\triangleq\mathcal{H}^{(n)}_{U_{(\bar{k})}|VU_{(k)}}\cap\big(\mathcal{H}^{(n)}_{U_{(\bar{k})}|VU_{(k)}Z}\big)^{\mathrm{C}}\setminus\mathcal{L}^{(n)}_{U_{(\bar{k})}|VY_{(\bar{k})}}.\tag{5.51}$$

For $i\in[1,L]$, the entries of $\tilde{T}_{(\bar{k}),i}\big[\mathcal{H}^{(n)}_{U_{(\bar{k})}|VU_{(k)}}\big]$ will be suitable for storing uniformly distributed random sequences that are independent of $(\tilde{V}_i^n,\tilde{U}^n_{(k),i})$, and $\tilde{T}_{(\bar{k}),i}\big[\mathcal{Q}_0^{(n)}\cup\mathcal{Q}_{\bar{k}}^{(n)}\big]$ will be suitable for storing information to be secured from the eavesdropper. Moreover, the elements of $\tilde{T}_{(\bar{k}),i}\big[\mathcal{B}_{\bar{k}}^{(n)}\cup\mathcal{Q}_{\bar{k}}^{(n)}\big]$ are required by Receiver $\bar{k}$ to reliably construct the entire sequence $\tilde{T}^n_{(\bar{k}),i}$ from $(\tilde{V}_i^n,\tilde{Y}^n_{(\bar{k}),i})$ by using SC decoding. Additionally, define

$$\mathcal{O}_{\bar{k}}^{(n)}\triangleq\text{ any subset of }\mathcal{Q}_0^{(n)}\text{ with size }\Big|\big(\mathcal{H}^{(n)}_{U_{(\bar{k})}|VU_{(k)}}\big)^{\mathrm{C}}\cap\mathcal{H}^{(n)}_{U_{(\bar{k})}|V}\setminus\mathcal{L}^{(n)}_{U_{(\bar{k})}|VY_{(\bar{k})}}\Big|,\tag{5.52}$$

$$\mathcal{N}_{\bar{k}}^{(n)}\triangleq\text{ any subset of }\mathcal{Q}_0^{(n)}\setminus\mathcal{O}_{\bar{k}}^{(n)}\text{ with size }\big|\mathcal{B}_{\bar{k}}^{(n)}\big|,\tag{5.53}$$

and $\mathcal{M}_{\bar{k}}^{(n)}$, which is defined as follows. If $k=1$ and $\bar{k}=2$, then

$$\mathcal{M}_2^{(n)}\triangleq\text{ any subset of }\mathcal{Q}_0^{(n)}\setminus(\mathcal{O}_2^{(n)}\cup\mathcal{N}_2^{(n)})\text{ with size }\big\{|\mathcal{C}_2^{(n)}|+|\mathcal{C}_{1,2}^{(n)}|-|\mathcal{G}_0^{(n)}|-|\mathcal{G}_1^{(n)}|\big\}^+.\tag{5.54}$$

Consequently, $\mathcal{M}_2^{(n)}\neq\emptyset$ only in Situation 3, where $I(V;Y_{(1)})\le I(V;Y_{(2)})<I(V;Z)$. On the other hand, if $k=2$ and $\bar{k}=1$, then

$$\mathcal{M}_1^{(n)}\triangleq\text{ any subset of }\mathcal{Q}_0^{(n)}\setminus(\mathcal{O}_1^{(n)}\cup\mathcal{N}_1^{(n)})\quad\text{with size}\begin{cases}|\mathcal{G}_1^{(n)}|+|\mathcal{C}_1^{(n)}|-|\mathcal{G}_2^{(n)}|-|\mathcal{C}_2^{(n)}| & \text{if } I(V;Z)\le I(V;Y_{(2)}),\\ |\mathcal{C}_1^{(n)}|+|\mathcal{C}_{1,2}^{(n)}|-|\mathcal{G}_0^{(n)}|-|\mathcal{G}_2^{(n)}| & \text{otherwise.}\end{cases}\tag{5.55}$$

Recall that $I(V;Z) \leq I(V;Y_{(2)})$ in Situation 1, where $I(V;Z) < I(V;Y_{(1)}) \leq I(V;Y_{(2)})$, and in Situation 2, where $I(V;Y_{(1)}) < I(V;Z) \leq I(V;Y_{(2)})$.

If we consider only distributions implying $(R^{\star k}_{S_{(1)}}, R^{\star k}_{S_{(2)}}, R^{\star k}_{W_{(1)}}, R^{\star k}_{W_{(2)}}) \in \mathbb{R}^4_+$, then $\mathcal{O}^{(n)}_{\bar{k}}$, $\mathcal{N}^{(n)}_{\bar{k}}$ and $\mathcal{M}^{(n)}_{\bar{k}}$ must exist because, for $i \in [1,L]$, $\tilde{T}_{(\bar{k}),i}\big[\mathcal{Q}^{(n)}_0 \setminus \big(\mathcal{O}^{(n)}_{\bar{k}} \cup \mathcal{N}^{(n)}_{\bar{k}} \cup \mathcal{M}^{(n)}_{\bar{k}}\big)\big]$ is the only part that will be intended for storing confidential information $S_{(\bar{k})}$.

Construction of $\tilde{T}^n_{(1),1:L}$ and $\tilde{T}^n_{(2),1:L}$ for $(R^{\star 1}_{S_{(1)}}, R^{\star 1}_{S_{(2)}}, R^{\star 1}_{W_{(1)}}, R^{\star 1}_{W_{(2)}}) \in \mathfrak{R}^{(1)}_{\text{MI-WTBC}}$

In this case ($k = 1$ and $\bar{k} = 2$), given $\tilde{V}^n_i$, for $i \in [1,L]$ the encoder first constructs $\tilde{T}^n_{(1),i}$ associated to Receiver 1. Then, given $\tilde{V}^n_i$ and $\tilde{T}^n_{(1),i}$, it forms $\tilde{T}^n_{(2),i}$ associated to Receiver 2.

1. Construction of $\tilde{T}^n_{(1),i}$. Associated to $\tilde{T}^n_{(1),i}$, we have defined the sets $\mathcal{F}^{(n)}_0$, $\mathcal{F}^{(n)}_1$, $\mathcal{J}^{(n)}_0$ and $\mathcal{J}^{(n)}_1$ as in (5.40)–(5.43), and $\mathcal{D}^{(n)}_1$ and $\mathcal{L}^{(n)}_1$ as in (5.44) and (5.45) respectively.

   For $i \in [1,L]$, let $W^{(U)}_{(1),i}$ be a uniformly distributed vector of length $\big|\mathcal{J}^{(n)}_0 \cup \mathcal{J}^{(n)}_1\big|$ that represents part of the private message intended for Receiver 1. The encoder forms $\tilde{T}_{(1),i}\big[\mathcal{J}^{(n)}_0 \cup \mathcal{J}^{(n)}_1\big]$ by simply storing $W^{(U)}_{(1),i}$. We define $\Theta^{(U)}_{(1),i} \triangleq \tilde{T}_{(1),i}\big[\mathcal{J}^{(n)}_1\big]$, which is required by Receiver 1 to reliably estimate $\tilde{T}^n_{(1),i}$. Hence, for $i \in [1, L-1]$, sequence $\Theta^{(U)}_{(1),i+1}$ is repeated in $\tilde{T}_{(1),i}\big[\mathcal{D}^{(n)}_1\big] \subseteq \tilde{T}_{(1),i}\big[\mathcal{F}^{(n)}_0\big]$. This sequence is not repeated directly, but the encoder copies instead $\bar{\Theta}^{(U)}_{(1),i+1}$ that is obtained as follows. Let $\kappa^{(U)}_{\Theta}$ be a uniformly distributed key with length $\big|\mathcal{J}^{(n)}_1\big|$ that is privately shared between transmitter and Receiver 1. Then, for $i \in [1,L]$, we obtain $\bar{\Theta}^{(U)}_{(1),i} \triangleq \Theta^{(U)}_{(1),i} \oplus \kappa^{(U)}_{\Theta}$. Since $\kappa^{(U)}_{\Theta}$ is reused in all blocks, it is clear that its size becomes negligible in terms of rate for L large enough.

   For $i \in [1,L]$, let $S^{(U)}_{(1),i}$ be a uniformly distributed vector that represents part of the confidential message intended for legitimate Receiver 1. At Block 1, $S^{(U)}_{(1),1}$ has size $\big|\big(\mathcal{F}^{(n)}_0 \cup \mathcal{F}^{(n)}_1\big) \setminus \big(\mathcal{D}^{(n)}_1 \cup \mathcal{L}^{(n)}_1\big)\big|$ and is stored in $\tilde{T}_{(1),1}\big[\big(\mathcal{F}^{(n)}_0 \cup \mathcal{F}^{(n)}_1\big) \setminus \big(\mathcal{D}^{(n)}_1 \cup \mathcal{L}^{(n)}_1\big)\big]$; for $i \in [2, L-1]$, $S^{(U)}_{(1),i}$ has size $\big|\mathcal{F}^{(n)}_0 \setminus \big(\mathcal{D}^{(n)}_1 \cup \mathcal{L}^{(n)}_1\big)\big|$ and is stored in $\tilde{T}_{(1),i}\big[\mathcal{F}^{(n)}_0 \setminus \big(\mathcal{D}^{(n)}_1 \cup \mathcal{L}^{(n)}_1\big)\big]$; and at Block L, $S^{(U)}_{(1),L}$ has size $\big|\mathcal{F}^{(n)}_0\big|$ and is stored into $\tilde{T}_{(1),L}\big[\mathcal{F}^{(n)}_0\big]$. Moreover, for $i \in [1,L]$, we define $\Lambda^{(U)}_{(1),i} \triangleq \tilde{T}_{(1),i}\big[\mathcal{F}^{(n)}_1\big]$. For $i \in [2,L]$, $\Lambda^{(U)}_{(1),i-1}$ is repeated in $\tilde{T}_{(1),i}\big[\mathcal{F}^{(n)}_1\big]$ and, therefore, $\Lambda^{(U)}_{(1),1}$, which contains part of $S^{(U)}_{(1),1}$, is replicated in all blocks.

   Furthermore, for $i \in [1, L-1]$, the encoder repeats[1] $\big[\Pi^{(V)}_{(1),i+1}\Delta^{(V)}_{(1),i+1}\big]$, which contain part of $\tilde{A}^n_{i+1}$, in $\tilde{T}_{(1),i}\big[\mathcal{L}^{(n)}_1\big]$. According to the summary of the construction of $\tilde{A}_{1:L}\big[\mathcal{G}^{(n)}\big]$ in the last part of Section 5.2.1, notice that the length of $\Delta^{(V)}_{(1),i+1}$ is $\big|\mathcal{L}^{(n)}_1\big|$.

   Then, for $i \in [1,L]$, given $\tilde{T}_{(1),i}\big[\mathcal{H}^{(n)}_{U_{(1)}|V}\big]$ and $\tilde{V}^n_i$ the encoder forms the remaining entries of $\tilde{T}^n_{(1),i}$ by using SC encoding: deterministic SC encoding for the elements of

[1] From Section 5.2.1, $\hat{\Pi}^{(V)}_{(1),1:L} = \varnothing$ when the PCS operates to achieve the corner point of $\mathfrak{R}^{(1)}_{\text{MI-WTBC}}$.

$\tilde{T}_{(1),i}\big[\mathcal{L}^{(n)}_{U_{(1)}|V}\big]$ and random SC encoding for the entries of $\tilde{T}_{(1),i}\big[\big(\mathcal{H}^{(n)}_{U_{(1)}|V}\big)^{\mathrm{C}} \setminus \mathcal{L}^{(n)}_{U_{(1)}|V}\big]$.

For $i \in [1, L]$, the encoder obtains $\Phi^{(U)}_{(1),i} \triangleq \tilde{T}_{(1),i}\big[\big(\mathcal{H}^{(n)}_{U_{(1)}|V}\big)^{\mathrm{C}} \setminus \mathcal{L}^{(n)}_{U_{(1)}|VY_{(1)}}\big]$. Also, it obtains $\Upsilon^{(U)}_{(1)} \triangleq \tilde{T}_{(1),1}\big[\mathcal{H}^{(n)}_{U_{(1)}|V} \setminus \mathcal{L}^{(n)}_{U_{(1)}|VY_{(1)}}\big]$ from Block 1. The transmitter additionally sends $\big(\Upsilon^{(U)}_{(1)}, \Phi^{(U)}_{(1),1:L}\big) \oplus \kappa^{(U)}_{\Upsilon\Phi_{(1)}}$ to Receiver 1, where $\kappa^{(U)}_{\Upsilon\Phi_{(1)}}$ is a uniformly distributed key with size $L\big|\big(\mathcal{H}^{(n)}_{U_{(1)}|V}\big)^{\mathrm{C}} \setminus \mathcal{L}^{(n)}_{U_{(1)}|VY_{(1)}}\big| + \big|\mathcal{H}^{(n)}_{U_{(1)}|V} \setminus \mathcal{L}^{(n)}_{U_{(1)}|VY_{(1)}}\big|$ that is privately shared between transmitter and Receiver 1.

Figure 5.10 graphically represents this construction of $\tilde{T}^n_{(1),1:L}$ if we do the following substitutions: $\mathcal{F}^{(n)}_0 \leftarrow \mathcal{Q}^{(n)}_0$, $\mathcal{F}^{(n)}_1 \leftarrow \mathcal{Q}^{(n)}_1$, $\mathcal{J}^{(n)}_0 \leftarrow \mathcal{B}^{(n)}_0$, $\mathcal{J}^{(n)}_1 \leftarrow \mathcal{B}^{(n)}_1$, $\mathcal{D}^{(n)}_1 \leftarrow \mathcal{N}^{(n)}_1$, $\mathcal{L}^{(n)}_1 \leftarrow \mathcal{M}^{(n)}_1$, $\emptyset \leftarrow \mathcal{O}^{(n)}_1$, $\big(\mathcal{H}^{(n)}_{U_{(1)}|V}\big)^{\mathrm{C}} \leftarrow \big(\mathcal{H}^{(n)}_{U_{(1)}|VU_{(2)}}\big)^{\mathrm{C}}$, $O^{(U)}_{(1),1:L} \leftarrow \varnothing$. Moreover, at Block $i \in [1, L-1]$, the encoder repeats $\Theta^{(U)}_{(1),i+1} \oplus \kappa^{(U)}_{\Theta}$ instead of $\Theta^{(U)}_{(1),i+1}$.

2. Construction of $\tilde{T}^n_{(2),i}$. Associated to $\tilde{T}^n_{(2),i}$, we have defined the sets $\mathcal{Q}^{(n)}_0$, $\mathcal{Q}^{(n)}_2$, $\mathcal{B}^{(n)}_0$ and $\mathcal{B}^{(n)}_2$ as in (5.48)–(5.51), and $\mathcal{O}^{(n)}_2$, $\mathcal{N}^{(n)}_2$ and $\mathcal{M}^{(n)}_2$ as in (5.52)–(5.54) respectively.

   The construction of $\tilde{T}^n_{(2),1:L}$ is graphically summarized in Figure 5.9. For $i \in [1, L]$, let $W^{(U)}_{(2),i}$ be a uniformly distributed vector of length $\big|\mathcal{B}^{(n)}_0 \cup \mathcal{B}^{(n)}_2\big|$ that represents the entire private message intended for Receiver 2. The encoder forms $\tilde{T}_{(2),i}\big[\mathcal{B}^{(n)}_0 \cup \mathcal{B}^{(n)}_2\big]$ by simply storing $W^{(U)}_{(2),i}$. We define $\Psi^{(U)}_{(2),i} \triangleq \tilde{T}_{(2),i}\big[\mathcal{B}^{(n)}_2\big]$, which is required by Receiver 2 to reliably estimate $\tilde{T}^n_{(2),i}$. Thus, for $i \in [2, L]$, $\Psi^{(U)}_{(2),i-1}$ is repeated in $\tilde{T}_{(2),i}\big[\mathcal{N}^{(n)}_2\big] \subseteq \tilde{T}_{(2),i}\big[\mathcal{Q}^{(n)}_0\big]$.

   For $i \in [1, L]$, let $S^{(U)}_{(2),i}$ be a uniformly distributed vector that represents part of the confidential message intended for legitimate Receiver 2. At Block 1, $S^{(U)}_{(2),1}$ has size $\big|\mathcal{Q}^{(n)}_0 \cup \mathcal{Q}^{(n)}_2\big|$ and is stored in $\tilde{T}_{(2),1}\big[\mathcal{Q}^{(n)}_0 \cup \mathcal{Q}^{(n)}_2\big]$; and for $i \in [2, L]$, $S^{(U)}_{(2),i}$ has size $\big|\mathcal{Q}^{(n)}_0 \setminus \big(\mathcal{O}^{(n)}_2 \cup \mathcal{N}^{(n)}_2 \cup \mathcal{M}^{(n)}_2\big)\big|$ and is stored in $\tilde{T}_{(2),i}\big[\mathcal{Q}^{(n)}_0 \setminus \big(\mathcal{O}^{(n)}_2 \cup \mathcal{N}^{(n)}_2 \cup \mathcal{M}^{(n)}_2\big)\big]$. Moreover, for $i \in [1, L]$ we define $\Lambda^{(U)}_{(2),i} \triangleq \tilde{T}_{(2),i}\big[\mathcal{Q}^{(n)}_2\big]$. For $i \in [2, L]$, $\Lambda^{(U)}_{(2),i-1}$ is repeated in $\tilde{T}_{(2),i}\big[\mathcal{Q}^{(n)}_2\big]$ and, hence, $\Lambda^{(U)}_{(2),1}$, which contains part of $S^{(U)}_{(2),1}$, is replicated in all blocks.

   Furthermore, for $i \in [2, L]$ the encoder repeats $\Delta^{(V)}_{(2),i-1}$, which recall that contains part of $\tilde{A}^n_{i-1}$, in $\tilde{T}_{(2),i}\big[\mathcal{M}^{(n)}_2\big]$. According to the summary of the construction of $\tilde{A}_{1:L}\big[\mathcal{G}^{(n)}\big]$ in the last part of Section 5.2.1, the length of $\Delta^{(V)}_{(2),i-1}$ matches with $\big|\mathcal{M}^{(n)}_2\big|$.

   Then, for $i \in [1, L]$, given $\tilde{T}_{(2),i}\big[\mathcal{H}^{(n)}_{U_{(2)}|VU_{(1)}}\big]$, $\tilde{V}^n_i$ and $\tilde{T}^n_{(1),i}$, the encoder forms the remaining entries of $\tilde{T}^n_{(2),i}$ by using SC encoding. Now, notice that $\tilde{T}_{(2),i}\big[\big(\mathcal{H}^{(n)}_{U_{(2)}|VU_{(1)}}\big)^{\mathrm{C}}\big]$ must depend not only on sequence $\tilde{V}^n_i$, but also on sequence $\tilde{U}^n_{(1),i}$ that was constructed before. Moreover, $\tilde{T}_{(2),i}\big[\mathcal{L}^{(n)}_{U_{(2)}|VU_{(1)}}\big]$ is formed by performing deterministic SC encoding, while $\tilde{T}_{(2),i}\big[\big(\mathcal{H}^{(n)}_{U_{(2)}|VU_{(1)}}\big)^{\mathrm{C}} \setminus \mathcal{L}^{(n)}_{U_{(2)}|VU_{(1)}}\big]$ is drawn randomly.

   For $i \in [1, L]$, we define sequences $O^{(U)}_{(2),i} \triangleq \tilde{T}_{(2),i}\big[\big(\mathcal{H}^{(n)}_{U_{(2)}|VU_{(1)}}\big)^{\mathrm{C}} \cap \mathcal{H}^{(n)}_{U_{(2)}|V} \setminus \mathcal{L}^{(n)}_{U_{(2)}|VY_{(2)}}\big]$ and $\Phi^{(U)}_{(2),i} \triangleq \tilde{T}_{(2),i}\big[\big(\mathcal{H}^{(n)}_{U_{(2)}|V}\big)^{\mathrm{C}} \setminus \mathcal{L}^{(n)}_{U_{(2)}|VY_{(2)}}\big]$, where notice that $\big[O^{(U)}_{(2),i}, \Phi^{(U)}_{(2),i}\big]$ contains

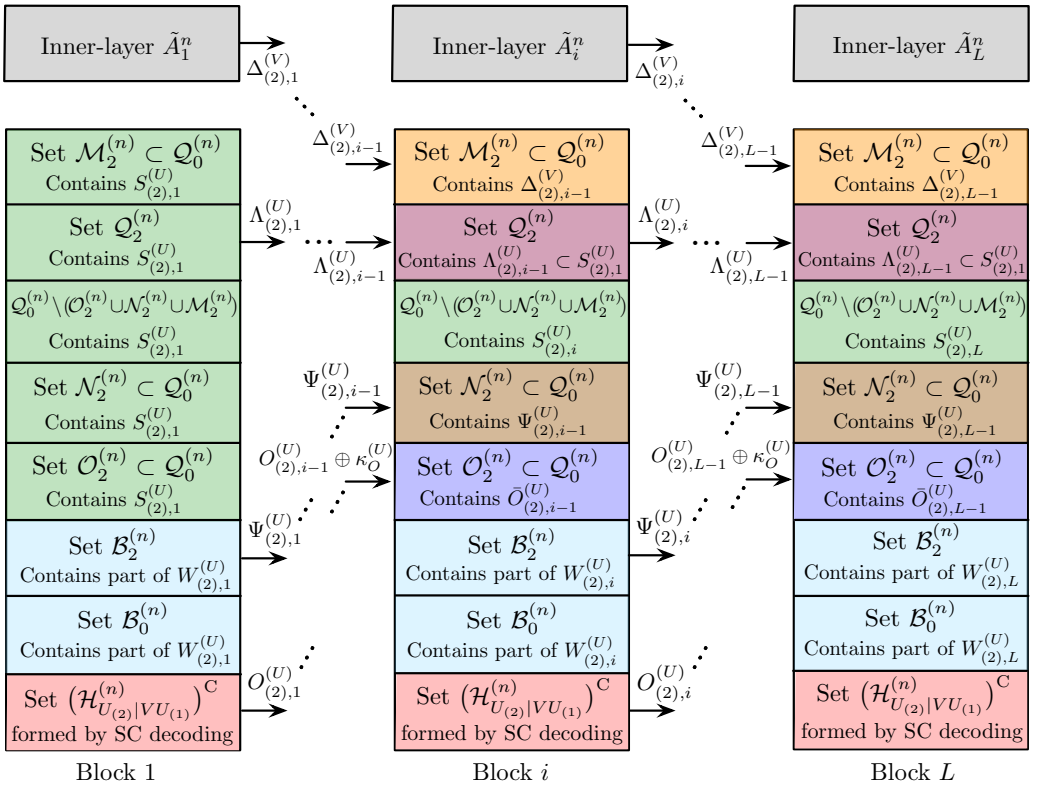

Figure 5.9: Construction of outer-layer $\tilde{T}_{(2),1:L}$ associated to Receiver 2 when the PCS must aproach the corner point $(R_{S_{(1)}}^{\star 1}, R_{S_{(2)}}^{\star 1}, R_{W_{(1)}}^{\star 1}, R_{W_{(2)}}^{\star 1}) \subseteq \mathfrak{R}_{\text{MI-WTBC}}^{(1)}$. For any Block $i \in [1, L]$, blue and green colors are used to represent the elements of $\tilde{T}_{(2),i}^n$ that contain independent private and confidential information, respectively. For $i \in [2, L]$, orange, brown, red-purple and blue-purple colors represent those entries that contain information repeated from Block $i-1$: $\tilde{T}_{(2),i}[\mathcal{M}_2^{(n)}]$ (in orange) repeats information from $\tilde{A}_{i-1}^n$, $\tilde{T}_{(2),i}[\mathcal{N}_2^{(n)}]$ (in brown) repeats $\Psi_{(2),i-1}^{(U)}$, $\tilde{T}_{(2),i}[\mathcal{O}_2^{(n)}]$ (in blue-purple) repeats $\bar{O}_{(2),i-1}^{(U)}$, and $\tilde{T}_{(2),i}[\mathcal{Q}_2^{(n)}]$ (in red-purple) repeats $\Lambda_{(2),i-1}^{(U)}$. Finally, for $i \in [1, L]$, $\tilde{T}_{(2),i}[(\mathcal{H}_{U_{(2)}|VU_{(1)}}^{(n)})^{\mathrm{C}}]$ (in red) is drawn by SC encoding.

those entries of $\tilde{T}_{(2),i}\big[\big(\mathcal{H}_{U_{(2)}|VU_{(1)}}^{(n)}\big)^{\mathrm{C}}\big]$ that are needed by Receiver 2 to reliably estimate $\tilde{T}_{(2),i}^n$, that is, $\big[O_{(2),i}^{(U)}, \Phi_{(2),i}^{(U)}\big] = \tilde{T}_{(2),i}\big[\big(\mathcal{H}_{U_{(2)}|VU_{(1)}}^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{L}_{U_{(2)}|VY_{(2)}}^{(n)}\big]$. Let $\kappa_O^{(U)}$ be a uniformly distributed key with size $\big|\big(\mathcal{H}_{U_{(2)}|VU_{(1)}}^{(n)}\big)^{\mathrm{C}} \cap \mathcal{H}_{U_{(2)}|V}^{(n)} \setminus \mathcal{L}_{U_{(2)}|VY_{(2)}}^{(n)}\big|$ that is privately-shared between transmitter and Receiver 2. For $i \in [1, L]$, we define $\bar{O}_{(2),i}^{(U)} \triangleq O_{(2),i}^{(U)} \oplus \kappa_O^{(U)}$. Since $O_{(2),i}^{(U)}$ is required by Receiver 2 to estimate $\tilde{T}_{(2),i}^n$, for $i \in [2, L]$ the encoder repeats $\bar{O}_{(2),i-1}^{(U)}$ in $\tilde{T}_{(2),i}\big[\mathcal{O}_2^{(n)}\big]$. Notice that $\kappa_O^{(U)}$ is reused in all blocks, so it is clear that its size becomes negligible in terms of rate for L large enough. Furthermore, the encoder obtains $\Upsilon_{(2)}^{(U)} \triangleq \tilde{T}_{(2),L}\big[\mathcal{H}_{U_{(2)}|V}^{(n)} \setminus \mathcal{L}_{U_{(2)}|VY_{(2)}}^{(n)}\big]$ from Block L, and

the transmitter additionally sends $\big(\Upsilon_{(2)}^{(U)}, \Phi_{(2),1:L}^{(U)}\big) \oplus \kappa_{\Upsilon\Phi_{(2)}}^{(U)}$ to Receiver 2, $\kappa_{\Upsilon\Phi_{(2)}}^{(U)}$ being a uniformly distributed key with size $L\big|\big(\mathcal{H}_{U_{(2)}|V}^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{L}_{U_{(2)}|VY_{(2)}}^{(n)}\big| + \big|\mathcal{H}_{U_{(2)}|V}^{(n)} \setminus \mathcal{L}_{U_{(2)}|VY_{(2)}}^{(n)}\big|$ that is privately shared between transmitter and Receiver 2.

Finally, for $i \in [1, L]$, the encoder obtains $\tilde{X}_i^n \triangleq f\big(\tilde{V}_i^n, \tilde{U}_{(1),i}^n, \tilde{U}_{(2),i}^n\big)$, where recall that $f(\cdot)$ may be any deterministic one-to-one function. The transmitter sends $\tilde{X}_i^n$ over the WTBC, which induces the channel outputs $(\tilde{Y}_{(1),i}^n, \tilde{Y}_{(2),i}^n, \tilde{Z}_i^n)$.

Remark 5.7. *For $i \in [2, L]$, notice that $O_{(2),i-1}^{(U)}$, which is not negligible in terms of rate, is almost uniformly distributed and independent of $\tilde{V}_{i-1}^n$, but is dependent on $(\tilde{V}_{i-1}^n, \tilde{T}_{(1),i-1}^n)$. Since $\tilde{T}_{(2),i}\big[\mathcal{O}_2^{(n)}\big] \subset \tilde{T}_{(2),i}\big[\mathcal{Q}_0^{(n)}\big]$ is suitable for storing sequences that are uniform and independent of $(\tilde{V}_i^n, \tilde{T}_{(1),i}^n)$, the secret-key $\kappa_O^{(U)}$ is used to ensure that $\bar{O}_{(2),i-1}^{(U)}$ is totally random (see Section 5.3.2).*

Construction of $\tilde{T}_{(1),1:L}^n$ and $\tilde{T}_{(2),1:L}^n$ for $(R_{S_{(1)}}^{\star 2}, R_{S_{(2)}}^{\star 2}, R_{W_{(1)}}^{\star 2}, R_{W_{(2)}}^{\star 2}) \in \mathfrak{R}_{\text{MI-WTBC}}^{(2)}$

In this case ($k = 2$ and $\bar{k} = 1$), given $\tilde{V}_i^n$, for $i \in [1, L]$ the encoder first constructs $\tilde{T}_{(2),i}^n$ associated to Receiver 2. Then, given $\tilde{V}_i^n$ and $\tilde{T}_{(2),i}^n$, it forms $\tilde{T}_{(1),i}^n$ associated to Receiver 1.

1. Construction of $\tilde{T}_{(2),i}^n$. Associated to $\tilde{T}_{(2),i}^n$, we have defined the sets $\mathcal{F}_0^{(n)}$, $\mathcal{F}_2^{(n)}$, $\mathcal{J}_0^{(n)}$ and $\mathcal{J}_2^{(n)}$ as in (5.40)–(5.43), and $\mathcal{D}_2^{(n)}$ and $\mathcal{L}_2^{(n)}$ as in (5.44) and (5.45) respectively.

   For $i \in [1, L]$, let $W_{(2),i}^{(U)}$ be a uniformly distributed vector of length $\big|\mathcal{J}_0^{(n)} \cup \mathcal{J}_2^{(n)}\big|$ that represents part of the private message intended for Receiver 2. The encoder forms $\tilde{T}_{(2),i}\big[\mathcal{J}_0^{(n)} \cup \mathcal{J}_2^{(n)}\big]$ by simply storing $W_{(2),i}^{(U)}$. Then, now we define $\Psi_{(2),i}^{(U)} \triangleq \tilde{T}_{(2),i}\big[\mathcal{J}_2^{(n)}\big]$, which is required by Receiver 2 to reliably estimate $\tilde{T}_{(2),i}^n$. Thus, for $i \in [2, L]$, $\Psi_{(2),i-1}^{(U)}$ is repeated in $\tilde{T}_{(2),i}\big[\mathcal{D}_2^{(n)}\big] \subseteq \tilde{T}_{(2),i}\big[\mathcal{F}_0^{(n)}\big]$. This sequence is not repeated directly, but the encoder copies instead $\bar{\Psi}_{(2),i-1}^{(U)}$ that is obtained as follows. Let $\kappa_\Psi^{(U)}$ be a uniformly distributed key with length $\big|\mathcal{J}_2^{(n)}\big|$. Then, for $i \in [1, L]$, we obtain $\bar{\Psi}_{(2),i}^{(U)} \triangleq \Psi_{(2),i}^{(U)} \oplus \kappa_\Psi^{(U)}$. Since $\kappa_\Psi^{(U)}$ is reused in all blocks, its size is negligible in terms of rate for L large enough.

   For $i \in [1, L]$, let $S_{(2),i}^{(U)}$ be a uniformly distributed vector that represents the confidential message intended for Receiver 2. At Block 1, $S_{(2),1}^{(U)}$ has size $\big|\mathcal{F}_0^{(n)} \cup \mathcal{F}_2^{(n)}\big|$ and is stored in $\tilde{T}_{(2),1}\big[\mathcal{F}_0^{(n)} \cup \mathcal{F}_2^{(n)}\big]$; and for $i \in [2, L]$, $S_{(2),i}^{(U)}$ has size $\big|\mathcal{F}_0^{(n)} \setminus \big(\mathcal{D}_2 \cup \mathcal{L}_2^{(n)}\big)\big|$ and is stored into $\tilde{T}_{(2),i}\big[\mathcal{F}_0^{(n)} \setminus \big(\mathcal{D}_2 \cup \mathcal{L}_2^{(n)}\big)\big]$. Moreover, for $i \in [1, L]$ we define $\Lambda_{(2),i}^{(U)} \triangleq \tilde{T}_{(2),i}\big[\mathcal{F}_2^{(n)}\big]$. For $i \in [2, L]$, $\Lambda_{(2),i-1}^{(U)}$ is repeated in $\tilde{F}_{(2),i}\big[\mathcal{F}_2^{(n)}\big]$ and, therefore, $\Lambda_{(2),1}^{(U)}$, which contains part of the confidential message $S_{(2),1}^{(U)}$, is replicated in all blocks.

   Furthermore, for $i \in [2, L]$, the encoder repeats $\Delta_{(2),i-1}^{(V)}$, which recall that contains part of $\tilde{A}_{i-1}^n$, in $\tilde{T}_{(2),i}\big[\mathcal{L}_2^{(n)}\big]$. According to the summary of the construction of $\tilde{A}_{1:L}\big[\mathcal{G}^{(n)}\big]$ in the last part of Section 5.2.1, the length of sequence $\Delta_{(2),i-1}^{(V)}$ is $\big|\mathcal{L}_2^{(n)}\big|$.

For $i \in [1, L]$, given $\tilde{T}_{(2),i}\big[\mathcal{H}^{(n)}_{U_{(2)}|V}\big]$ and $\tilde{V}_i^n$ the encoder forms $\tilde{T}_{(2),i}\big[\big(\mathcal{H}^{(n)}_{U_{(2)}|V}\big)^{\mathrm{C}}\big]$ by using SC encoding: deterministic for $\tilde{T}_{(2),i}\big[\mathcal{L}^{(n)}_{U_{(2)}|V}\big]$, and random for $\tilde{T}_{(2),i}\big[\big(\mathcal{H}^{(n)}_{U_{(2)}|V}\big)^{\mathrm{C}} \setminus \mathcal{L}^{(n)}_{U_{(2)}|V}\big]$.

For $i \in [1, L]$, the encoder obtains $\Phi^{(U)}_{(2),i} \triangleq \tilde{T}_{(2),i}\big[\big(\mathcal{H}^{(n)}_{U_{(2)}|V}\big)^{\mathrm{C}} \setminus \mathcal{L}^{(n)}_{U_{(2)}|VY_{(1)}}\big]$. Also, it obtains $\Upsilon^{(U)}_{(2)} \triangleq \tilde{T}_{(2),L}\big[\mathcal{H}^{(n)}_{U_{(2)}|V} \setminus \mathcal{L}^{(n)}_{U_{(2)}|VY_{(2)}}\big]$ from Block L. The transmitter additionally sends $\big(\Upsilon^{(U)}_{(2)}, \Phi^{(U)}_{(2),1:L}\big) \oplus \kappa^{(U)}_{\Upsilon\Phi_{(2)}}$ to Receiver 2, where $\kappa^{(U)}_{\Upsilon\Phi_{(2)}}$ now is a uniformly distributed key with size $L\big|\big(\mathcal{H}^{(n)}_{U_{(2)}|V}\big)^{\mathrm{C}} \setminus \mathcal{L}^{(n)}_{U_{(2)}|VY_{(2)}}\big| + \big|\mathcal{H}^{(n)}_{U_{(2)}|V} \setminus \mathcal{L}^{(n)}_{U_{(2)}|VY_{(2)}}\big|$ that is privately shared between transmitter and Receiver 2.

Figure 5.9 may graphically represent this construction of $\tilde{T}^n_{(2),1:L}$ if we do the following substitutions: $\mathcal{F}^{(n)}_0 \leftarrow \mathcal{Q}^{(n)}_0$, $\mathcal{F}^{(n)}_2 \leftarrow \mathcal{Q}^{(n)}_2$, $\mathcal{J}^{(n)}_0 \leftarrow \mathcal{B}^{(n)}_0$, $\mathcal{J}^{(n)}_2 \leftarrow \mathcal{B}^{(n)}_2$, $\mathcal{D}^{(n)}_2 \leftarrow \mathcal{N}^{(n)}_2$, $\mathcal{L}^{(n)}_2 \leftarrow \mathcal{M}^{(n)}_2$, $\emptyset \leftarrow \mathcal{O}^{(n)}_2$, $\big(\mathcal{H}^{(n)}_{U_{(2)}|V}\big)^{\mathrm{C}} \leftarrow \big(\mathcal{H}^{(n)}_{U_{(2)}|VU_{(1)}}\big)^{\mathrm{C}}$, $O^{(U)}_{(2),1:L} \leftarrow \varnothing$. Moreover, at Block $i \in [2, L]$, the encoder repeats $\Psi^{(U)}_{(2),i-1} \oplus \kappa^{(U)}_{\Psi}$ instead of $\Psi^{(U)}_{(2),i-1}$.

2. Construction of $\tilde{T}^n_{(1),i}$. Associated to $\tilde{T}^n_{(1),i}$, now we have defined $\mathcal{Q}^{(n)}_0$, $\mathcal{Q}^{(n)}_1$, $\mathcal{B}^{(n)}_0$ and $\mathcal{B}^{(n)}_1$ as in (5.48)–(5.51), and $\mathcal{O}^{(n)}_1$, $\mathcal{N}^{(n)}_1$ and $\mathcal{M}^{(n)}_1$ as in (5.52), (5.53) and (5.55) respectively.

   The construction of $\tilde{T}^n_{(2),1:L}$ is graphically summarized in Figure 5.10. For $i \in [1, L]$, let $W^{(U)}_{(1),i}$ be a uniformly distributed vector of length $\big|\mathcal{B}^{(n)}_0 \cup \mathcal{B}^{(n)}_1\big|$ that represents the entire private message intended for legitimate Receiver 1. The encoder forms $\tilde{T}_{(1),i}\big[\mathcal{B}^{(n)}_0 \cup \mathcal{B}^{(n)}_1\big]$ by simply storing $W^{(U)}_{(1),i}$. Then, we define $\Theta^{(U)}_{(1),i} \triangleq \tilde{T}_{(1),i}\big[\mathcal{B}^{(n)}_1\big]$, which is required by Receiver 1 to reliably estimate $\tilde{T}^n_{(1),i}$. Hence, for $i \in [1, L-1]$, sequence $\Theta^{(U)}_{(1),i+1}$ is repeated in $\tilde{T}_{(1),i}\big[\mathcal{N}^{(n)}_1\big] \subseteq \tilde{T}_{(1),i}\big[\mathcal{Q}^{(n)}_0\big]$.

   For $i \in [1, L]$, let $S^{(U)}_{(1),i}$ be a uniform vector that represents the confidential message intended for Receiver 1. At Block 1, $S^{(U)}_{(1),1}$ has size $\big|\big(\mathcal{Q}^{(n)}_0 \cup \mathcal{Q}^{(n)}_1\big) \setminus \big(\mathcal{O}^{(n)}_1 \cup \mathcal{N}^{(n)}_1 \cup \mathcal{M}^{(n)}_1\big)\big|$ and is stored in $\tilde{T}_{(1),1}\big[\big(\mathcal{Q}^{(n)}_0 \cup \mathcal{Q}^{(n)}_1\big) \setminus \big(\mathcal{O}^{(n)}_1 \cup \mathcal{N}^{(n)}_1 \cup \mathcal{M}^{(n)}_1\big)\big]$; for $i \in [2, L-1]$, $S^{(U)}_{(1),i}$ has size $\big|\mathcal{Q}^{(n)}_0 \setminus \big(\mathcal{O}^{(n)}_1 \cup \mathcal{N}^{(n)}_1 \cup \mathcal{M}^{(n)}_1\big)\big|$ and is stored in $\tilde{T}_{(1),i}\big[\mathcal{Q}^{(n)}_0 \setminus \big(\mathcal{O}^{(n)}_1 \cup \mathcal{N}^{(n)}_1 \cup \mathcal{M}^{(n)}_1\big)\big]$; and at Block L, $S^{(U)}_{(1),L}$ has size $\big|\mathcal{Q}^{(n)}_0\big|$ and is stored into $\tilde{T}_{(1),L}\big[\mathcal{Q}^{(n)}_0\big]$. Moreover, for $i \in [1, L]$ we define $\Lambda^{(U)}_{(1),i} \triangleq \tilde{T}_{(1),i}\big[\mathcal{Q}^{(n)}_1\big]$. For $i \in [2, L]$, $\Lambda^{(U)}_{(1),i-1}$ is repeated in $\tilde{T}_{(1),i}\big[\mathcal{Q}^{(n)}_1\big]$. Hence, $\Lambda^{(U)}_{(1),1}$, which contains part of $S^{(U)}_{(1),1}$, is replicated in all blocks.

   Furthermore, for $i \in [1, L-1]$, the encoder repeats $\big[\Pi^{(V)}_{(1),i+1}\Delta^{(V)}_{(1),i+1}\big]$, which contains part of $\tilde{A}^n_{i+1}$, in $\tilde{T}_{(1),i}\big[\mathcal{M}^{(n)}_1\big]$. According to the summary of the construction of $\tilde{A}_{1:L}\big[\mathcal{G}^{(n)}\big]$ in the last part of Section 5.2.1, the overall length of $\big[\Pi^{(V)}_{(1),i+1}, \Delta^{(V)}_{(1),i+1}\big]$ is $\big|\mathcal{M}^{(n)}_1\big|$.

   Then, for $i \in [1, L]$, given $\tilde{T}_{(1),i}\big[\mathcal{H}^{(n)}_{U_{(1)}|VU_{(2)}}\big]$, $\tilde{V}_i^n$ and $\tilde{U}^n_{(2),i}$, the encoder forms the remaining entries of $\tilde{T}^n_{(1),i}$ by using SC encoding. Now, $\tilde{T}_{(1),i}\big[\big(\mathcal{H}^{(n)}_{U_{(1)}|VU_{(2)}}\big)^{\mathrm{C}}\big]$ must depend not only on $\tilde{V}_i^n$, but also on $\tilde{U}^n_{(2),i}$. Moreover, $\tilde{T}_{(1),i}\big[\mathcal{L}^{(n)}_{U_{(1)}|VU_{(2)}}\big]$ is formed by performing deterministic SC encoding, while $\tilde{T}_{(1),i}\big[\big(\mathcal{H}^{(n)}_{U_{(1)}|VU_{(2)}}\big)^{\mathrm{C}} \setminus \mathcal{L}^{(n)}_{U_{(1)}|VU_{(2)}}\big]$ is drawn randomly.

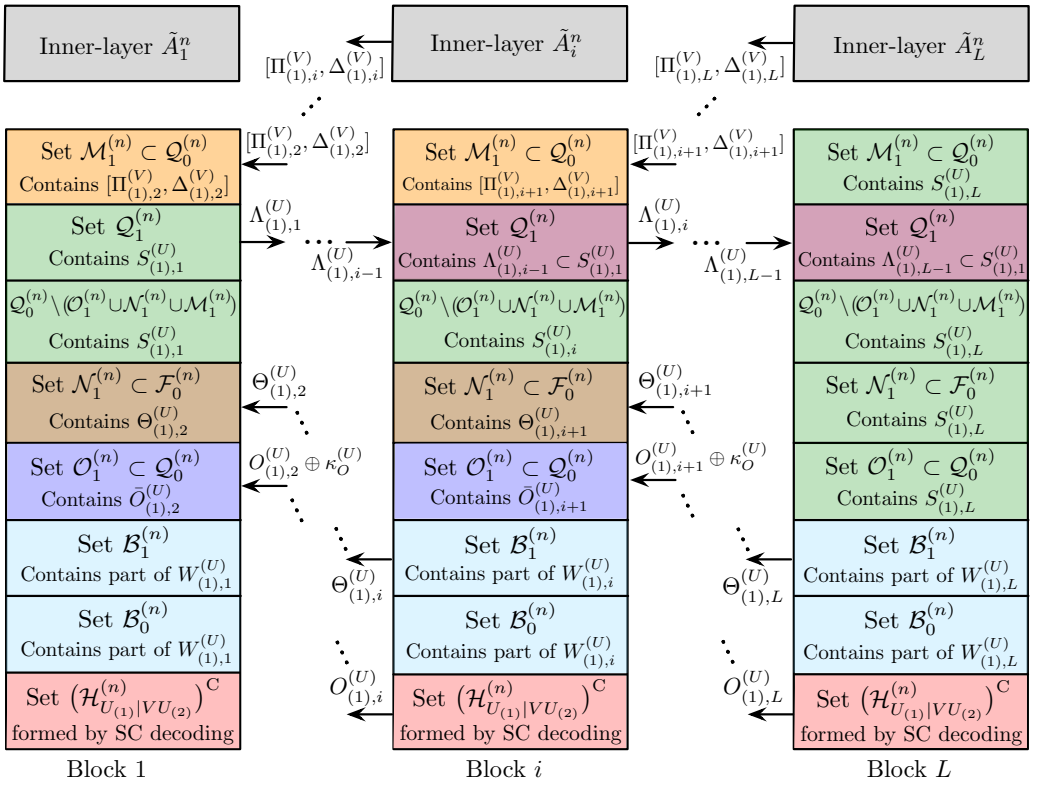

Figure 5.10: Construction of outer-layer $\tilde{T}_{(1),1:L}$ associated to Receiver 1 when the PCS must aproach the corner point $(R_{S_{(1)}}^{\star 2}, R_{S_{(2)}}^{\star 2}, R_{W_{(1)}}^{\star 2}, R_{W_{(2)}}^{\star 2}) \subseteq \mathfrak{R}_{\text{MI-WTBC}}^{(2)}$. For any Block $i \in [1, L]$, blue and green colors are used to represent the elements of $\tilde{T}_{(1),i}^n$ that contain independent private and confidential information, respectively. For $i \in [1, L-1]$, orange, brown and blue-purple colors represent those entries that contain information repeated from Block $i+1$: $\tilde{T}_{(1),i}[\mathcal{M}_1^{(n)}]$ (in orange) repeats information from $\tilde{A}_{i+1}^n$, $\tilde{T}_{(1),i}[\mathcal{N}_1^{(n)}]$ (in brown) repeats $\Theta_{(1),i+1}^{(U)}$, and $\tilde{T}_{(1),i}[\mathcal{O}_1^{(n)}]$ (in blue-purple) repeats $\bar{O}_{(1),i+1}^{(U)}$. Recall that $\Lambda_{(1),1}^{(U)}$, which contain part of the confidential information of Block 1, is replicated in $\tilde{T}_{(1),2:L}[\mathcal{Q}_1^{(n)}]$ (in red-purple). Finally, for $i \in [1, L]$, the elements of $\tilde{T}_{(1),i}[(\mathcal{H}_{U_{(1)}|VU_{(2)}}^{(n)})^{\mathrm{C}}]$ (in red) are drawn by SC encoding.

For $i \in [1, L]$, we define sequences $O_{(1),i}^{(U)} \triangleq \tilde{T}_{(1),i}\big[\big(\mathcal{H}_{U_{(1)}|VU_{(2)}}^{(n)}\big)^{\mathrm{C}} \cap \mathcal{H}_{U_{(1)}|V}^{(n)} \setminus \mathcal{L}_{U_{(1)}|VY_{(1)}}^{(n)}\big]$ and $\Phi_{(1),i}^{(U)} \triangleq \tilde{T}_{(1),i}\big[\big(\mathcal{H}_{U_{(1)}|V}^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{L}_{U_{(1)}|VY_{(1)}}^{(n)}\big]$, where notice that $\big[O_{(1),i}^{(U)}, \Phi_{(1),i}^{(U)}\big]$ contains those entries of $\tilde{T}_{(1),i}\big[\big(\mathcal{H}_{U_{(1)}|VU_{(2)}}^{(n)}\big)^{\mathrm{C}}\big]$ that are needed by Receiver 1 to reliably estimate $\tilde{T}_{(1),i}^n$, that is, $\big[O_{(1),i}^{(U)}, \Phi_{(1),i}^{(U)}\big] = \tilde{T}_{(1),i}\big[\big(\mathcal{H}_{U_{(1)}|VU_{(2)}}^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{L}_{U_{(1)}|VY_{(1)}}^{(n)}\big]$. Let $\kappa_O^{(U)}$ be a uniformly distributed key with size $\big|\big(\mathcal{H}_{U_{(1)}|VU_{(2)}}^{(n)}\big)^{\mathrm{C}} \cap \mathcal{H}_{U_{(1)}|V}^{(n)} \setminus \mathcal{L}_{U_{(1)}|VY_{(1)}}^{(n)}\big|$ that is privately-shared between transmitter and Receiver 1. For $i \in [1, L]$, we define $\bar{O}_{(1),i}^{(U)} \triangleq O_{(1),i}^{(U)} \oplus \kappa_O^{(U)}$. Since $O_{(1),i}^{(U)}$ is required by Receiver 1 to estimate $\tilde{T}_{(1),i}^n$, for $i \in [1, L-1]$ the encoder repeats

$\bar{O}^{(U)}_{(1),i+1}$ in $\tilde{T}_{(1),i}\big[\mathcal{O}^{(n)}_1\big]$. Notice that $\kappa^{(U)}_O$ is reused in all blocks, so it is clear that its size becomes negligible in terms of rate for L large enough. Furthermore, the encoder obtains $\Upsilon^{(U)}_{(1)} \triangleq \tilde{T}_{(1),1}\big[\mathcal{H}^{(n)}_{U_{(1)}|V} \setminus \mathcal{L}^{(n)}_{U_{(1)}|VY_{(1)}}\big]$ from Block 1. The transmitter additionally sends $\big(\Upsilon^{(U)}_{(1)}, \Phi^{(U)}_{(1),1:L}\big) \oplus \kappa^{(U)}_{\Upsilon\Phi_{(1)}}$ to Receiver 1, where $\kappa^{(U)}_{\Upsilon\Phi_{(1)}}$ is a uniformly distributed key with size $L\big|\big(\mathcal{H}^{(n)}_{U_{(1)}|V}\big)^{\mathrm{C}} \setminus \mathcal{L}^{(n)}_{U_{(1)}|VY_{(1)}}\big| + \big|\mathcal{H}^{(n)}_{U_{(1)}|V} \setminus \mathcal{L}^{(n)}_{U_{(1)}|VY_{(1)}}\big|$ that is privately shared between transmitter and Receiver 1.

Finally, for $i \in [1, L]$, the encoder obtains $\tilde{X}^n_i \triangleq f\big(\tilde{V}^n_i, \tilde{U}^n_{(1),i}, \tilde{U}^n_{(2),i}\big)$, where recall that $f(\cdot)$ may be any deterministic one-to-one function. The transmitter sends $\tilde{X}^n_i$ over the WTBC, which induces the channel outputs $(\tilde{Y}^n_{(1),i}, \tilde{Y}^n_{(2),i}, \tilde{Z}^n_i)$.

Remark 5.8. *Consider the construction of $\tilde{T}^n_{(k),1:L}$ for the achievability of the corner point $(R^{\star k}_{S_{(1)}}, R^{\star k}_{S_{(2)}}, R^{\star k}_{W_{(1)}}, R^{\star k}_{W_{(2)}}) \in \mathfrak{R}^{(k)}_{MI\text{-}WTBC}$. If we consider that $I(U_{(k)};Y_{(k)}|V) < I(U_{(k)};Z|V)$, according to (5.46) and (5.47), notice that $\big|\mathcal{F}^{(n)}_0\big| - \big|\mathcal{J}^{(n)}_k\big| < 0$. Consequently, if $k = 1$, for $i \in [1, L-1]$ the encoder cannot repeat entirely the sequence $\bar{\Theta}^{(U)}_{(1),i+1}$ of length $\big|\mathcal{J}^{(n)}_1\big|$ in some elements of $\tilde{T}_{(1),i}\big[\mathcal{F}^{(n)}_0\big]$. Similarly, if $k = 2$, for $i \in [2, L]$ the encoder cannot repeat the sequence $\bar{\Psi}^{(U)}_{(2),i-1}$ of length $\big|\mathcal{J}^{(n)}_2\big|$ in $\tilde{T}_{(2),i}\big[\mathcal{F}^{(n)}_0\big]$.*

Therefore, under this assumption, the encoding strategy will be as follows. If $k = 1$, for $i \in [1, L]$ we will define $\Delta^{(U)}_{(1),i}$ as any part of $\bar{\Theta}^{(U)}_{(1),i}$ with size $\big|\mathcal{J}^{(n)}_1\big| - \big|\mathcal{F}^{(n)}_0\big|$. For $i \in [1, L-1]$, the sequence $\Delta^{(U)}_{(1),i+1}$ will be repeated in some part of the inner-layer $\tilde{A}_i\big[\mathcal{I}^{(n)}\big]$, whereas the remaining elements of $\bar{\Theta}^{(U)}_{(1),i+1}$ will be stored in $\tilde{T}_{(1),i}\big[\mathcal{F}^{(n)}_0\big]$. Similarly, if $k = 2$, for $i \in [1, L]$ we will define $\Delta^{(U)}_{(2),i}$ as any part of $\bar{\Psi}^{(U)}_{(2),i}$ with size $\big|\mathcal{J}^{(n)}_2\big| - \big|\mathcal{F}^{(n)}_0\big|$. For $i \in [2, L]$, the sequence $\Delta^{(U)}_{(2),i-1}$ will be repeated in some part of the inner-layer $\tilde{A}_i\big[\mathcal{I}^{(n)}\big]$, whereas the remaining elements of $\bar{\Psi}^{(U)}_{(2),i-1}$ will be repeated in $\tilde{T}_{(2),i}\big[\mathcal{F}^{(n)}_0\big]$.

Remark 5.9. *If we consider input distributions that imply $(R^{\star k}_{S_{(1)}}, R^{\star k}_{S_{(2)}}, R^{\star k}_{W_{(1)}}, R^{\star k}_{W_{(2)}}) \in \mathbb{R}^4_+$ for some $k \in [1, 2]$, it is clear that if $I(U_{(k)};Y_{(k)}|V) < I(U_{(k)};Z|V)$ then we must only consider those Situations (among 1 to 3) in the inner-layer where $I(V;Y_{(k)}) \geq I(V;Z)$. In this case, part of the elements of the inner-layer that previously carried confidential information could be used now to carry $\Delta^{(U)}_{(1),2:L}$ or $\Delta^{(U)}_{(2),1:L-1}$.*

We will not go into the details of the encoding/decoding when $I(U_{(k)};Y_{(k)}|V) < I(U_{(k)};Z|V)$ because both the construction and the performance analysis will be very similar to those of the the contemplated cases such that the outer-layer must repeat some elements of the inner-layer.

5.2.3 Decoding

By using $\kappa^{(V)}_{\Upsilon\Phi_{(k)}}$ and $\kappa^{(U)}_{\Upsilon\Phi_{(k)}}$, consider that $\big(\Phi^{(V)}_{(k),1:L}, \Upsilon^{(V)}_{(k)}\big)$ and $\big(\Phi^{(U)}_{(k),1:L}, \Upsilon^{(U)}_{(k)}\big)$ have been reliably obtained by Receiver $k \in [1, 2]$ before starting the decoding process.

Decoding at Receiver 1

This receiver forms the estimates $\hat{A}_{1:L}^n$ and $\hat{T}_{(1),1:L}^n$ of $\tilde{A}_{1:L}^n$ and $\tilde{T}_{(1),1:L}^n$ respectively by going forward, i.e., from $(\hat{A}_1^n, \hat{T}_{(1),1}^n)$ to $(\hat{A}_L^n, \hat{T}_{(1),L}^n)$. For $i \in [1, L]$, it forms $\hat{A}_i^n$ first, and then $\hat{T}_{(1),i}^n$.

The decoding process at Receiver 1 when the PCS must achieve the corner point of $\mathfrak{R}_{\text{MI-WTBC}}^{(1)}$ or $\mathfrak{R}_{\text{MI-WTBC}}^{(2)}$ is summarized in Algorithm 5.3. Despite $\tilde{A}_{1:L}^n$ does not carry information intended for Receiver 1 when the PCS operates to achieve the corner point of $\mathfrak{R}_{\text{MI-WTBC}}^{(2)}$, recall that this receiver needs $\tilde{A}_{1:L}^n$ to reliably reconstruct $\tilde{T}_{(1),1:L}^n$.

In both cases, Receiver 1 constructs $\hat{A}_1^n$ and $\hat{T}_{(1),1}^n$ as follows. Given $\big(\Upsilon_{(1)}^{(V)}, \Phi_{(1),1}^{(V)}\big)$ and $\big(\Upsilon_{(1)}^{(U)}, \Phi_{(1),1}^{(U)}\big)$, it knows $\tilde{A}_1\big[\big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}}\big]$ and $\tilde{T}_{(1),1}\big[\big(\mathcal{L}_{U_{(1)}|VY_{(1)}}^{(n)}\big)^{\mathrm{C}}\big]$, respectively. Therefore, from observations $\tilde{Y}_{(1),1}^n$ and $\tilde{A}_1\big[\big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}}\big]$, it entirely constructs $\hat{A}_1^n$ by performing SC decoding. Then, from $\tilde{Y}_{(1),1}^n$, $\tilde{T}_{(1),1}\big[\big(\mathcal{L}_{U_{(1)}|VY_{(1)}}^{(n)}\big)^{\mathrm{C}}\big]$ and $\hat{V}_1^n = \hat{A}_1^n G_n$, this receiver form $\hat{T}_{(1),1}^n$.

Recall that $\Lambda_1^{(V)}$ and $\Lambda_{(1),1}^{(U)}$ have been replicated in all blocks. Thus, Receiver 1 obtains $\hat{\Lambda}_{1:L}^{(V)} = \hat{A}_1\big[\mathcal{R}_\Lambda^{(n)}\big]$, while it obtains $\hat{\Lambda}_{(1),1:L}^{(U)} = \hat{T}_{(1),1}\big[\mathcal{F}_1^{(n)}\big]$ or $\hat{\Lambda}_{(1),1:L}^{(U)} = \hat{T}_{(1),1}\big[\mathcal{Q}_1^{(n)}\big]$ depending on whether the PCS must achieve the corner point of $\mathfrak{R}_{\text{MI-WTBC}}^{(1)}$ or $\mathfrak{R}_{\text{MI-WTBC}}^{(2)}$ respectively.

For $i \in [1, L-1]$, consider that $\hat{A}_{1:i}^n$ and $\hat{T}_{(1),1:i}^n$ have already been constructed. Then, the construction of $\hat{A}_{i+1}^n$ and $\hat{T}_{(1),i+1}^n$ is slightly different depending on whether the PCS must achieve the corner point of $\mathfrak{R}_{\text{MI-WTBC}}^{(1)}$ $(k=1)$ or $\mathfrak{R}_{\text{MI-WTBC}}^{(2)}$ $(k=2)$:

$k=1$) From $\hat{A}_i^n$ and $\hat{T}_{(1),i}^n$, it obtains $\Upsilon_{(1),i+1}^{\prime(V)} \triangleq \big(\hat{\Psi}_{1,i}^{(V)}, \hat{\Gamma}_{2,i}^{(V)}, \hat{\Pi}_{(2),i}^{(V)}, \hat{\Theta}_{i+1}^{(V)}, \hat{\Gamma}_{i+1}^{(V)}, \hat{\Lambda}_{i+1}^{(V)}\big)$. Notice in Algorithm 5.3 that secret-keys $\kappa_\Theta^{(V)}$ and $\kappa_\Gamma^{(V)}$ are needed to obtain $\hat{\Theta}_{i+1}^{(V)}$ and $\hat{\Gamma}_{i+1}^{(V)}$, respectively. Moreover, $\Psi_{i-1}^{(V)}$ and $\Gamma_{i-1}^{(V)}$ may also be necessary for this purpose, and notice that they are available because $\big(\tilde{A}_{i-1}^n, \hat{T}_{(1),i-1}^n\big)$ has already been constructed. Recall that part of $\hat{\Theta}_{i+1}^{(V)}$ and $\hat{\Gamma}_{i+1}^{(V)}$ are obtained from $\hat{T}_{(1),i}^n$. On the other hand, from $\hat{T}_{(1),i}^n$, it obtains $\Upsilon_{(1),i+1}^{\prime(U)} \triangleq \big(\hat{\Theta}_{(1),i+1}^{(U)}, \hat{\Lambda}_{(1),i+1}^{(U)}\big)$, and $\kappa_\Theta^{(U)}$ is needed to get $\hat{\Theta}_{(1),i+1}^{(U)}$.

$k=2$) From $\hat{A}_i^n$ and $\hat{T}_{(1),i}^n$, it obtains $\hat{\Upsilon}_{(1),i+1}^{\prime(V)} \triangleq \big(\hat{\tilde{\Psi}}_{1,i}^{(V)}, \hat{\tilde{\Gamma}}_{2,i}^{(V)}, \hat{\Pi}_{(2),i}^{(V)}, \hat{\Theta}_{i+1}^{(V)}, \hat{\Gamma}_{i+1}^{(V)}, \hat{\Lambda}_{i+1}^{(V)}\big)$ and $\Upsilon_{(1),i+1}^{\prime(U)} \triangleq \big(\hat{\Theta}_{(1),i+1}^{(U)}, \hat{\Lambda}_{(1),i+1}^{(U)}, \hat{O}_{(1),i+1}^{(U)}\big)$. Now, for $i \in [1, L-1]$ the encoder have repeated an *encrypted* version of $\Psi_i^{(V)}$ and $\Gamma_i^{(V)}$ at Block $i+1$, whereas $\Theta_{i+1}^{(V)}$, $\Gamma_{i+1}^{(V)}$ and $\Theta_{(1),i+1}^{(U)}$ have been repeated in Block i directly. Hence, notice in Algorithm 5.3 that secret-keys $\kappa_\Psi^{(V)}$ and $\kappa_\Gamma^{(V)}$ are needed, whereas neither $\kappa_\Theta^{(V)}$ nor $\kappa_\Theta^{(U)}$ are used in this case. Moreover, notice that Receiver 1 now obtains $\hat{O}_{(1),i+1}^{(U)} = \hat{T}_{(1),i}[\mathcal{O}_1^{(n)}] \oplus \kappa_O^{(U)}$, which recall that contains part of the elements of $\hat{T}_{(1),i+1}^n$ that have been drawn by performing SC encoding and are needed by Receiver 1 to reliably reconstruct $\hat{T}_{(1),i+1}^n$.

Finally, given $\big(\Upsilon_{(1),i+1}^{\prime(V)}, \Phi_{(1),i+1}^{(V)}\big) \supseteq \hat{A}_{i+1}\big[\big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}}\big]$ and $\tilde{Y}_{(1),i+1}^n$, it performs SC decoding to construct $\hat{A}_{i+1}^n$. Then, given $\big(\Upsilon_{(1),i+1}^{\prime(U)}, \Phi_{(1),i+1}^{(U)}\big) \supseteq \hat{T}_{(1),i+1}\big[\big(\mathcal{L}_{U_{(1)}|VY_{(1)}}^{(n)}\big)^{\mathrm{C}}\big]$, $\hat{V}_{i+1}^n = \hat{A}_{i+1}^n G_n$ and $\tilde{Y}_{(1),i+1}^n$, it performs SC decoding to construct $\hat{T}_{(1),i+1}^n$.

Algorithm 5.3 Decoding at Receiver 1 when PCS operates to achieve the corner point of $\mathfrak{R}_{\text{MI-WTBC}}^{(k)}$

Require: $\Upsilon_{(1)}^{(V)}$, $\Phi_{(1),1:L}^{(V)}$, $\Upsilon_{(1)}^{(U)}$, $\Phi_{(1),1:L}^{(U)}$, and $\tilde{Y}_{(1),1:L}^{n}$.
Require: **if** $k=1$ **then** $\{\kappa_{\Gamma}^{(V)}, \kappa_{\Theta}^{(V)}, \kappa_{\Theta}^{(U)}\}$ **else** $\{\kappa_{\Gamma}^{(V)}, \kappa_{\Psi}^{(V)}, \kappa_{O}^{(U)}\}$
$\hat{A}_1^n \leftarrow \left(\Upsilon_{(1)}^{(V)}, \Phi_{(1),1}^{(V)}, \tilde{Y}_{(1),1}^{n}\right)$ ▷ by using SC decoding
$\hat{T}_{(1),1}^{n} \leftarrow \left(\Upsilon_{(1)}^{(U)}, \Phi_{(1),1}^{(U)}, \hat{A}_1^n G_n, \tilde{Y}_{(1),1}^{n}\right)$ ▷ by using SC decoding
$\hat{\Lambda}_{2:L}^{(V)} \leftarrow \hat{A}_1\left[\mathcal{R}_{\Lambda}^{(n)}\right]$
if $k=1$ **then** $\hat{\Lambda}_{2:L}^{(U)} \leftarrow \hat{T}_{(1),1}\left[\mathcal{F}_1^{(n)}\right]$ **else** $\hat{\Lambda}_{2:L}^{(U)} \leftarrow \hat{T}_{(1),1}\left[\mathcal{Q}_1^{(n)}\right]$
for $i=1$ to $L-1$ **do**
  $\hat{\Pi}_{(2),i}^{(V)} \leftarrow \hat{A}_i[\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)}]$
  if $k=1$ **then**
    $\hat{\Psi}_i^{(V)} \leftarrow \hat{A}_i[\mathcal{C}_2^{(n)}]$ **and** $\hat{\Gamma}_i^{(V)} \leftarrow \hat{A}_i[\mathcal{C}_{1,2}^{(n)}]$
    $\hat{\tilde{\Theta}}_{1,i+1}^{(V)} \leftarrow \hat{A}_i[\mathcal{R}_1^{(n)}]$ **and** $\hat{\tilde{\Theta}}_{2,i+1}^{(V)} \leftarrow \hat{A}_i[\mathcal{R}_{1,2}'^{(n)}] \oplus \hat{\Psi}_{2,i-1}^{(V)}$
    $\hat{\tilde{\Gamma}}_{1,i+1}^{(V)} \leftarrow \hat{A}_i[\mathcal{R}_{1,2}^{(n)}] \oplus \hat{\Gamma}_{1,i-1}^{(V)}$ **and** $\hat{\tilde{\Gamma}}_{2,i+1}^{(V)} \leftarrow \hat{A}_i[\mathcal{R}_1'^{(n)}]$
    $\Delta_{(1),i+1}^{(U)} \leftarrow \hat{T}_{(1),i}[\mathcal{L}_1^{(n)}]$ ▷ $\Delta_{(1),i+1}^{(U)} = \left[\hat{\tilde{\Theta}}_{3,i+1}^{(V)}, \hat{\tilde{\Gamma}}_{3,i+1}^{(V)}\right]$
    $\hat{\Theta}_{i+1}^{(V)} \leftarrow \left[\hat{\tilde{\Theta}}_{1,i+1}^{(V)}, \hat{\tilde{\Theta}}_{2,i+1}^{(V)}, \hat{\tilde{\Theta}}_{3,i+1}^{(V)}\right] \oplus \kappa_{\Theta}^{(V)}$
    $\hat{\Gamma}_{i+1}^{(V)} \leftarrow \left[\hat{\tilde{\Gamma}}_{1,i+1}^{(V)}, \hat{\tilde{\Gamma}}_{2,i+1}^{(V)}, \hat{\tilde{\Gamma}}_{3,i+1}^{(V)}\right] \oplus \kappa_{\Gamma}^{(V)}$
    $\hat{\Upsilon}'^{(V)}_{(1),i+1} \leftarrow \left(\hat{\Psi}_{1,i}^{(V)}, \hat{\Gamma}_{2,i}^{(V)}, \hat{\Pi}_{(2),i}^{(V)}, \hat{\Theta}_{i+1}^{(V)}, \hat{\Gamma}_{i+1}^{(V)}, \hat{\Lambda}_{i+1}^{(V)}\right)$
    $\hat{\Theta}_{(1),i+1}^{(U)} \leftarrow \hat{T}_{(1),i}[\mathcal{D}_1^{(n)}] \oplus \kappa_{\Theta}^{(U)}$
    $\hat{\Upsilon}'^{(U)}_{(1),i+1} \leftarrow \left(\hat{\Theta}_{(1),i+1}^{(U)}, \hat{\Lambda}_{(1),i+1}^{(U)}\right)$
  else
    $\hat{\Psi}_i^{(V)} \leftarrow \hat{A}_i[\mathcal{C}_2^{(n)}]$ **and** $\hat{\Gamma}_i^{(V)} \leftarrow \hat{A}_i[\mathcal{C}_{1,2}^{(n)}]$
    $\hat{\tilde{\Psi}}_i^{(V)} \leftarrow \hat{\Psi}_i^{(V)} \oplus \kappa_{\Psi}^{(V)}$ **and** $\hat{\tilde{\Gamma}}_i^{(V)} \leftarrow \hat{\Gamma}_i^{(V)} \oplus \kappa_{\Gamma}^{(V)}$
    $\hat{\Theta}_{1,i+1}^{(V)} \leftarrow \hat{A}_i[\mathcal{R}_1^{(n)}]$ **and** $\hat{\Theta}_{2,i+1}^{(V)} \leftarrow \hat{A}_i[\mathcal{R}_{1,2}'^{(n)}] \oplus \hat{\tilde{\Psi}}_{2,i-1}^{(V)}$
    $\hat{\Gamma}_{1,i+1}^{(V)} \leftarrow \hat{A}_i[\mathcal{R}_{1,2}^{(n)}] \oplus \hat{\tilde{\Gamma}}_{1,i-1}^{(V)}$ **and** $\hat{\Gamma}_{2,i+1}^{(V)} \leftarrow \hat{A}_i[\mathcal{R}_1'^{(n)}]$
    $\left(\hat{\Pi}_{(1),i+1}^{(V)}, \Delta_{(1),i+1}^{(U)}\right) \leftarrow \hat{T}_{(1),i}[\mathcal{M}_1^{(n)}]$ ▷ $\Delta_{(1),i+1}^{(U)} = \left[\hat{\Theta}_{3,i+1}^{(V)}, \hat{\Gamma}_{3,i+1}^{(V)}\right]$
    $\hat{\Upsilon}'^{(V)}_{(1),i+1} \leftarrow \left(\hat{\tilde{\Psi}}_{1,i}^{(V)}, \hat{\tilde{\Gamma}}_{2,i}^{(V)}, \hat{\Pi}_{(2),i}^{(V)}, \hat{\Pi}_{(1),i+1}^{(V)}, \hat{\Theta}_{i+1}^{(V)}, \hat{\Gamma}_{i+1}^{(V)}, \hat{\Lambda}_{i+1}^{(V)}\right)$
    $\hat{\Theta}_{(1),i+1}^{(U)} \leftarrow \hat{T}_{(1),i}[\mathcal{N}_1^{(n)}]$
    $\hat{O}_{(1),i+1}^{(U)} \leftarrow \hat{T}_{(1),i}[\mathcal{O}_1^{(n)}] \oplus \kappa_{O}^{(U)}$
    $\hat{\Upsilon}'^{(U)}_{(1),i+1} \leftarrow \left(\hat{\Theta}_{(1),i+1}^{(U)}, \hat{\Lambda}_{(1),i+1}^{(U)}, \hat{O}_{(1),i+1}^{(U)}\right)$
  end if
  $\hat{A}_{i+1}^n \leftarrow \left(\hat{\Upsilon}'^{(V)}_{(1),i+1}, \Phi_{(1),i+1}^{(V)}, \tilde{Y}_{(1),i+1}^{n}\right)$
  $\hat{T}_{(1),i+1}^{n} \leftarrow \left(\hat{\Upsilon}'^{(U)}_{(1),i+1}, \Phi_{(1),i+1}^{(U)}, \hat{A}_{i+1}^n G_n, \tilde{Y}_{(1),i+1}^{n}\right)$
end for
Return $\left(\hat{W}_{(1),1:L}, \hat{S}_{(1),1:L}\right) \leftarrow \left(\hat{A}_{i+1}^n \hat{T}_{(1),i+1}^{n}\right)$

Decoding at Receiver 2

This receiver forms the estimates $\hat{A}_{1:L}^n$ and $\hat{T}_{(2),1:L}^n$ of $\tilde{A}_{1:L}^n$ and $\tilde{T}_{(2),1:L}^n$ respectively by going backward, that is, from $(\hat{A}_L^n, \hat{T}_{(2),L}^n)$ to $(\hat{A}_1^n, \hat{T}_{(2),1}^n)$.

The decoding process at Receiver 2 when the PCS must achieve the corner point of $\mathfrak{R}_{\text{MI-WTBC}}^{(1)}$ or $\mathfrak{R}_{\text{MI-WTBC}}^{(2)}$ is summarized in Algorithm 5.4. Despite $\tilde{A}_{1:L}^n$ does not carry information intended for Receiver 2 when the PCS operates to achieve the corner point of $\mathfrak{R}_{\text{MI-WTBC}}^{(1)}$, recall that this receiver needs $\tilde{A}_{1:L}^n$ to reliably reconstruct $\tilde{T}_{(2),1:L}^n$.

In both cases, Receiver 2 constructs $\hat{A}_L^n$ and $\hat{T}_{(2),L}^n$ as follows. Given $\big(\Upsilon_{(2)}^{(V)}, \Phi_{(2),L}^{(V)}\big)$ and $\big(\Upsilon_{(2)}^{(U)}, \Phi_{(2),L}^{(U)}\big)$, it knows $\tilde{A}_L\big[\big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}}\big]$ and $\tilde{T}_{(2),L}\big[\big(\mathcal{L}_{U_{(2)}|VY_{(2)}}^{(n)}\big)^{\mathrm{C}}\big]$, respectively. Hence, from observations $\tilde{Y}_{(2),L}^n$ and $\tilde{A}_L\big[\big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}}\big]$, it entirely constructs $\hat{A}_L^n$ by performing SC decoding. Then, from $\tilde{Y}_{(2),L}^n$, $\tilde{T}_{(2),L}\big[\big(\mathcal{L}_{U_{(2)}|VY_{(2)}}^{(n)}\big)^{\mathrm{C}}\big]$ and $\hat{V}_L^n = \hat{A}_L^n G_n$, this receiver form $\hat{T}_{(2),L}^n$.

Recall that $\Lambda_1^{(V)}$ and $\Lambda_{(2),1}^{(U)}$ have been replicated in all blocks. Thus, Receiver 2 obtains $\hat{\Lambda}_{1:L}^{(V)} = \hat{A}_L\big[\mathcal{R}_\Lambda^{(n)}\big]$, while it gets $\hat{\Lambda}_{(2),1:L}^{(U)} = \hat{T}_{(2),L}\big[\mathcal{F}_2^{(n)}\big]$ or $\hat{\Lambda}_{(2),1:L}^{(U)} = \hat{T}_{(2),L}\big[\mathcal{Q}_2^{(n)}\big]$ depending on whether the PCS must achieve the corner point of $\mathfrak{R}_{\text{MI-WTBC}}^{(1)}$ or $\mathfrak{R}_{\text{MI-WTBC}}^{(2)}$ respectively.

For $i \in [2, L]$, consider that $\hat{A}_{i:L}^n$ and $\hat{T}_{(2),i:L}^n$ have already been formed. Then, the construction of $\hat{A}_{i-1}^n$ and $\hat{T}_{(2),i-1}^n$ is slightly different depending on whether the PCS must achieve the corner point of $\mathfrak{R}_{\text{MI-WTBC}}^{(1)}$ $(k=1)$ or $\mathfrak{R}_{\text{MI-WTBC}}^{(2)}$ $(k=2)$:

$k=1$) From $\hat{A}_i^n$ and $\hat{T}_{(2),i}^n$, it obtains $\hat{\Upsilon}_{(2),i-1}^{\prime(V)} \triangleq \big(\hat{\tilde{\Theta}}_{1,i}^{(V)}, \hat{\tilde{\Gamma}}_{2,i}^{(V)}, \hat{\Pi}_{(2),i-1}^{(V)}, \hat{\Psi}_{i-1}^{(V)}, \hat{\Gamma}_{i-1}^{(V)}, \hat{\Lambda}_{i-1}^{(V)}\big)$ and $\hat{\Upsilon}_{(2),i-1}^{\prime(U)} \triangleq \big(\hat{\Psi}_{(2),i-1}^{(U)}, \hat{\Lambda}_{(2),i-1}^{(U)}, \hat{O}_{(2),i-1}^{(U)}\big)$. Notice in Algorithm 5.4 that $\kappa_\Theta^{(V)}$ and $\kappa_\Gamma^{(V)}$ are needed because the encoder have repeated an *encrypted* version of $\hat{\Theta}_i^{(V)}$ and $\hat{\Gamma}_i^{(V)}$ at Block $i-1$. In order to obtain $\hat{\Psi}_{i-1}^{(V)}$ and $\hat{\Gamma}_{i-1}^{(V)}$, recall that part of these sequences may have been repeated in $\tilde{T}_{(2),i}^n$. Moreover, notice that part of the encrypted versions of $\hat{\Theta}_{i+1}^{(V)}$ and $\hat{\Gamma}_{i+1}^{(V)}$ may also be needed to obtain $\hat{\Psi}_{i-1}^{(V)}$ and $\hat{\Gamma}_{i-1}^{(V)}$, which are available because $\big(\tilde{A}_{i+1}^n, \hat{T}_{(2),i+1}^n\big)$ has already been constructed. Now Receiver 2 obtains $\Psi_{(2),i-1}^{(U)}$ and $\hat{O}_{(2),i-1}^{(U)} = \hat{T}_{(2),i}[\mathcal{O}_2^{(n)}] \oplus \kappa_O^{(U)}$ from $\tilde{T}_{(2),i}^n$, where recall that $\hat{O}_{(2),i-1}^{(U)}$ contains part of the elements of $\hat{T}_{(2),i-1}^n$ that have been drawn by performing SC encoding.

$k=2$) From $\hat{A}_i^n$ and $\hat{T}_{(2),i}^n$, it obtains $\hat{\Upsilon}_{(2),i-1}^{\prime(V)} \triangleq \big(\hat{\tilde{\Theta}}_{1,i}^{(V)}, \hat{\tilde{\Gamma}}_{2,i}^{(V)}, \hat{\Pi}_{(2),i-1}^{(V)}, \hat{\Psi}_{i-1}^{(V)}, \hat{\Gamma}_{i-1}^{(V)}, \hat{\Lambda}_{i-1}^{(V)}\big)$ and $\hat{\Upsilon}_{(2),i-1}^{\prime(U)} \triangleq \big(\hat{\Psi}_{(2),i-1}^{(U)}, \hat{\Lambda}_{(2),i-1}^{(U)}\big)$. Now, the Receiver 2 uses $\kappa_\Psi^{(V)}$, $\kappa_\Gamma^{(V)}$ and $\kappa_\Psi^{(U)}$ because the encoder have repeated an encrypted version of $\hat{\Psi}_{i-1}^{(V)}$, $\hat{\Gamma}_{i-1}^{(V)}$ and $\hat{\Psi}_{i-1}^{(U)}$ in Block i.

Finally, given $\big(\Upsilon_{(2),i-1}^{\prime(V)}, \Phi_{(2),i-1}^{(V)}\big) \supseteq \hat{A}_{i-1}\big[\big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}}\big]$ and $\tilde{Y}_{(2),i-1}^n$, it performs SC decoding to construct $\hat{A}_{i-1}^n$. Then, given $\big(\Upsilon_{(2),i-1}^{\prime(U)}, \Phi_{(2),i-1}^{(U)}\big) \supseteq \hat{T}_{(2),i-1}\big[\big(\mathcal{L}_{U_{(2)}|VY_{(2)}}^{(n)}\big)^{\mathrm{C}}\big]$, $\hat{V}_{i-1}^n = \hat{A}_{i-1}^n G_n$ and $\tilde{Y}_{(2),i-1}^n$, it performs SC decoding to construct $\hat{T}_{(2),i-1}^n$.

Algorithm 5.4 Decoding at Receiver 2 when PCS operates to achieve the corner point of $\mathfrak{R}_{\text{MI-WTBC}}^{(k)}$

Require: $\Upsilon_{(2)}^{(V)}$, $\Phi_{(2),1:L}^{(V)}$, $\Upsilon_{(2)}^{(U)}$, $\Phi_{(2),1:L}^{(U)}$, and $\tilde{Y}_{(2),1:L}^{n}$.
Require: **if** $k=1$ **then** $\{\kappa_{\Gamma}^{(V)}, \kappa_{\Theta}^{(V)}, \kappa_{O}^{(U)}\}$ **else** $\{\kappa_{\Gamma}^{(V)}, \kappa_{\Psi}^{(V)}, \kappa_{\Psi}^{(U)}\}$
$\hat{A}_L^n \leftarrow \left(\Upsilon_{(2)}^{(V)}, \Phi_{(2),L}^{(V)}, \tilde{Y}_{(2),L}^{n}\right)$ ▷ by using SC decoding
$\hat{T}_{(2),L}^{n} \leftarrow \left(\Upsilon_{(2)}^{(U)}, \Phi_{(2),L}^{(U)}, \hat{A}_L^n G_n, \tilde{Y}_{(2),L}^{n}\right)$ ▷ by using SC decoding
$\hat{\Lambda}_{1:L-1}^{(V)} \leftarrow \hat{A}_L\left[\mathcal{R}_{\Lambda}^{(n)}\right]$
if $k=1$ **then** $\hat{\Lambda}_{1:L-1}^{(U)} \leftarrow \hat{T}_{(2),L}\left[\mathcal{F}_2^{(n)}\right]$ **else** $\hat{\Lambda}_{1:L-1}^{(U)} \leftarrow \hat{T}_{(2),L}\left[\mathcal{Q}_2^{(n)}\right]$
for $i=L$ to 2 **do**
  $\hat{\Pi}_{(2),i-1}^{(V)} \leftarrow \hat{A}_i[\mathcal{R}_{\mathrm{S}}^{(n)}]$
  if $k=1$ **then**
    $\hat{\Theta}_i^{(V)} \leftarrow \hat{A}_i[\mathcal{C}_1^{(n)}]$ **and** $\hat{\Gamma}_i^{(V)} \leftarrow \hat{A}_i[\mathcal{C}_{1,2}^{(n)}]$
    $\hat{\tilde{\Theta}}_i^{(V)} \leftarrow \hat{\Theta}_i^{(V)} \oplus \kappa_{\Theta}^{(V)}$ **and** $\hat{\tilde{\Gamma}}_i^{(V)} \leftarrow \hat{\Gamma}_i^{(V)} \oplus \kappa_{\Gamma}^{(V)}$
    $\hat{\Psi}_{1,i-1}^{(V)} \leftarrow \hat{A}_i[\mathcal{R}_2^{(n)}]$ **and** $\hat{\Psi}_{2,i-1}^{(V)} \leftarrow \hat{A}_i[\mathcal{R}_{1,2}'^{(n)}] \oplus \hat{\tilde{\Theta}}_{2,i+1}^{(V)}$
    $\hat{\Gamma}_{1,i-1}^{(V)} \leftarrow \hat{A}_i[\mathcal{R}_{1,2}^{(n)}] \oplus \hat{\tilde{\Gamma}}_{1,i+1}^{(V)}$ **and** $\hat{\Gamma}_{2,i-1}^{(V)} \leftarrow \hat{A}_i[\mathcal{R}_2'^{(n)}]$
    $\Delta_{(2),i-1}^{(U)} \leftarrow \hat{T}_{(2),i}[\mathcal{M}_2^{(n)}]$ ▷ $\Delta_{(2),i-1}^{(U)} = \left[\hat{\Psi}_{3,i-1}^{(V)}, \hat{\Gamma}_{3,i-1}^{(V)}\right]$
    $\hat{\Upsilon}'^{(V)}_{(1),i-1} \leftarrow \left(\hat{\tilde{\Theta}}_{1,i}^{(V)}, \hat{\tilde{\Gamma}}_{2,i}^{(V)}, \hat{\Pi}_{(2),i-1}^{(V)}, \hat{\Psi}_{i-1}^{(V)}, \hat{\Gamma}_{i-1}^{(V)}, \hat{\Lambda}_{i-1}^{(V)}\right)$
    $\hat{\Psi}_{(2),i-1}^{(U)} \leftarrow \hat{T}_{(2),i}[\mathcal{N}_2^{(n)}]$
    $\hat{O}_{(2),i-1}^{(U)} \leftarrow \hat{T}_{(2),i}[\mathcal{O}_2^{(n)}] \oplus \kappa_{O}^{(U)}$
    $\hat{\Upsilon}'^{(U)}_{(2),i-1} \leftarrow \left(\hat{\Psi}_{(2),i-1}^{(U)}, \hat{\Lambda}_{(2),i-1}^{(U)}, \hat{O}_{(2),i-1}^{(U)}\right)$
  else
    $\hat{\Theta}_i^{(V)} \leftarrow \hat{A}_i[\mathcal{C}_1^{(n)}]$ **and** $\hat{\Gamma}_i^{(V)} \leftarrow \hat{A}_i[\mathcal{C}_{1,2}^{(n)}]$
    $\hat{\tilde{\Psi}}_{1,i-1}^{(V)} \leftarrow \hat{A}_i[\mathcal{R}_2^{(n)}]$ **and** $\hat{\tilde{\Psi}}_{2,i-1}^{(V)} \leftarrow \hat{A}_i[\mathcal{R}_{1,2}'^{(n)}] \oplus \hat{\Theta}_{2,i+1}^{(V)}$
    $\hat{\tilde{\Gamma}}_{1,i-1}^{(V)} \leftarrow \hat{A}_i[\mathcal{R}_{1,2}^{(n)}] \oplus \hat{\Gamma}_{1,i+1}^{(V)}$ **and** $\hat{\tilde{\Gamma}}_{2,i-1}^{(V)} \leftarrow \hat{A}_i[\mathcal{R}_2'^{(n)}]$
    $\Delta_{(2),i-1}^{(U)} \leftarrow \hat{T}_{(2),i}[\mathcal{L}_2^{(n)}]$ ▷ $\Delta_{(2),i-1}^{(U)} = \left[\hat{\tilde{\Psi}}_{3,i-1}^{(V)}, \hat{\tilde{\Gamma}}_{3,i-1}^{(V)}\right]$
    $\hat{\Psi}_{i-1}^{(V)} \leftarrow \left[\hat{\tilde{\Psi}}_{1,i-1}^{(V)}, \hat{\tilde{\Psi}}_{2,i-1}^{(V)}, \hat{\tilde{\Psi}}_{3,i-1}^{(V)}\right] \oplus \kappa_{\Psi}^{(V)}$
    $\hat{\Gamma}_{i-1}^{(V)} \leftarrow \left[\hat{\tilde{\Gamma}}_{1,i-1}^{(V)}, \hat{\tilde{\Gamma}}_{2,i-1}^{(V)}, \hat{\tilde{\Gamma}}_{3,i-1}^{(V)}\right] \oplus \kappa_{\Gamma}^{(V)}$
    $\hat{\Upsilon}'^{(V)}_{(2),i-1} \leftarrow \left(\hat{\Theta}_{1,i}^{(V)}, \hat{\Gamma}_{2,i}^{(V)}, \hat{\Pi}_{(2),i-1}^{(V)}, \hat{\Psi}_{i-1}^{(V)}, \hat{\Gamma}_{i-1}^{(V)}, \hat{\Lambda}_{i-1}^{(V)}\right)$
    $\hat{\Psi}_{(2),i-1}^{(U)} \leftarrow \hat{T}_{(2),i}[\mathcal{D}_2^{(n)}] \oplus \kappa_{\Psi}^{(U)}$
    $\hat{\Upsilon}'^{(U)}_{(2),i-1} \leftarrow \left(\hat{\Psi}_{(2),i-1}^{(U)}, \hat{\Lambda}_{(2),i-1}^{(U)}\right)$
  end if
  $\hat{A}_{i-1}^n \leftarrow \left(\hat{\Upsilon}'^{(V)}_{(2),i-1}, \Phi_{(2),i-1}^{(V)}, \tilde{Y}_{(2),i-1}^{n}\right)$
  $\hat{T}_{(2),i-1}^{n} \leftarrow \left(\hat{\Upsilon}'^{(U)}_{(2),i-1}, \Phi_{(2),i-1}^{(U)}, \hat{A}_{i-1}^n G_n, \tilde{Y}_{(2),i-1}^{n}\right)$
end for
Return $\left(\hat{W}_{(2),1:L}, \hat{S}_{(2),1:L}\right) \leftarrow \left(\hat{A}_{i-1}^n \hat{T}_{(2),i-1}^{n}\right)$

Remark 5.10. *According to the previous decoding algorithms, Receiver $k \in [1,2]$ decodes both $\tilde{A}_i^n$ and $\tilde{T}_{(k),i}^n$ from Block $i \in [1,L]$ before moving to adjacent blocks (polar-based jointly decoding). Indeed, Receiver 1 needs to obtain first $\hat{T}_{(1),i}^n$ before decoding $\tilde{A}_{i+1}^n$ because $\big[\Pi_{(1),i+1}^{(V)}, \Delta_{(1),i+1}^{(V)}\big]$, which is required by this receiver to reliably estimate $\tilde{A}_{i+1}^n$, is repeated in $\tilde{T}_{(1),i}^n$. Similarly, Receiver 2 needs $\Delta_{(2),i-1}^{(V)}$ to reliably decode $\tilde{A}_{i-1}^n$, but it is repeated in $\hat{T}_{(2),i}^n$.*

Consider another decoding strategy for Receiver $k \in [1,2]$ that obtains first $\hat{A}_{1:L}^n$, and then decodes the outer-layer $\tilde{T}_{(k),1:L}^n$. We refer to this decoding strategy as polar-based successive decoding. Clearly, $(R_{S_{(1)}}^{\star 2}, R_{S_{(2)}}^{\star 2}, R_{W_{(1)}}^{\star 2}, R_{W_{(2)}}^{\star 2}) \subset \mathfrak{R}_{MI\text{-}WTBC}^{(2)}$ is not achievable by using successive decoding because, according to the summary of the construction of $\tilde{A}_{1:L}\big[\mathcal{G}^{(n)}\big]$ in the last part of Section 5.2.1, in all cases $\tilde{T}_{(k),i}^n$ contains elements required by Receiver 1 to reliably decode $\tilde{A}_{i+1}^n$. Furthermore, for the same reason, all situations where $I(V;Y_{(k)}) < I(V;Z)$ for some $k \in [1,2]$ are not possible by using this strategy. Consequently, it is clear that joint decoding enlarges the inner-bound on the achievable region for a particular distribution[2].

5.3 Performance of the polar coding scheme

The analysis of the polar coding scheme of Section 5.2 leads to the following theorem.

Theorem 5.1. *Let $(\mathcal{X}, p_{Y_{(1)}Y_{(2)}Z|X}, \mathcal{Y}_{(1)} \times \mathcal{Y}_{(2)} \times \mathcal{Z})$ be an arbitrary WTBC where $\mathcal{X} \in \{0,1\}$. The PCS in Section 5.2 achieves any corner point $(R_{S_{(1)}}^{\star k}, R_{S_{(2)}}^{\star k}, R_{W_{(1)}}^{\star k}, R_{W_{(2)}}^{\star k}) \subset \mathfrak{R}_{MI\text{-}WTBC}^{(k)}$ given in (5.3)–(5.6) for any $k \in [1,2]$.*

Corollary 5.1. *The PCS achieves any rate tuple of $\mathfrak{R}_{MI\text{-}WTBC}^{(k)}$ defined in Proposition 5.2.*

The proof of Theorem 5.1 follows in four steps and is provided in the following subsections. In Section 5.3.1 we show that the PCS approaches $(R_{S_{(1)}}^{\star k}, R_{S_{(2)}}^{\star k}, R_{W_{(1)}}^{\star k}, R_{W_{(2)}}^{\star k}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(k)}$ for any $k \in [1,2]$. In Section 5.3.2 we prove that, for all $i \in [1,L]$, the joint distribution of $(\tilde{V}_i^n, \tilde{U}_{(1),i}^n, \tilde{U}_{(2),i}^n, \tilde{X}_i^n, \tilde{Y}_{(1),i}^n, \tilde{Y}_{(2),i}^n, \tilde{Z}_i^n)$ is asymptotically indistinguishable of the one of the original DMS that is used for the polar code construction. Finally, in Section 5.3.3 and Section 5.3.4 we show that the polar coding scheme satisfies the reliability and the secrecy conditions given in (5.1) and (5.2) respectively.

5.3.1 Transmission rates

We prove that the polar coding scheme described in Section 5.2 approaches the rate tuple $(R_{S_{(1)}}^{\star k}, R_{S_{(2)}}^{\star k}, R_{W_{(1)}}^{\star k}, R_{W_{(2)}}^{\star k}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(k)}$ defined in (5.3)–(5.6) for any $k \in [1,2]$. Also, we

[2] Although for a particular distribution the inner-bound is strictly larger with joint decoding, we cannot affirm that this decoding strategy enlarges $\mathfrak{R}_{\text{MI-WTBC}}$: rate points that are not achievable with successive decoding for this particular distribution may be achievable under another distribution.

show that the overall length of secret keys $\kappa_{\Gamma}^{(V)}$, $\kappa_{\Upsilon\Phi_{(1)}}^{(V)}$, $\kappa_{\Upsilon\Phi_{(2)}}^{(V)}$, $\kappa_{O}^{(U)}$, $\kappa_{\Upsilon\Phi_{(1)}}^{(U)}$, $\kappa_{\Upsilon\Phi_{(2)}}^{(U)}$ is asymptotically negligible in terms of rate, and so is the overall length of $\kappa_{\Theta}^{(V)}$ and $\kappa_{\Theta}^{(U)}$ if the PCS operates to achieve the corner point of $\mathfrak{R}_{\text{MI-WTBC}}^{(1)}$, or that of $\kappa_{\Psi}^{(V)}$ and $\kappa_{\Psi}^{(U)}$ if the PCS operates to achieve the corner point of $\mathfrak{R}_{\text{MI-WTBC}}^{(2)}$. Moreover, we show that so is the amount of randomness required by the encoding (number of entries drawn by random SC encoding).

Private message rate

1. Rate of $W_{(k)}$. For $i \in [1, L]$, we have $W_{(k),i} = \big[W_{(k),i}^{(V)}, W_{(k),i}^{(U)}\big]$, where $W_{(k),i}^{(V)} = \tilde{A}_i\big[\mathcal{C}^{(n)}\big]$ and $W_{(k),i}^{(U)} = \tilde{T}_{(k),i}\big[\mathcal{J}_0^{(n)} \cup \mathcal{J}_k^{(n)}\big]$. Therefore, we obtain

$$\begin{aligned}\frac{1}{nL}\sum_{i=1}^{L}\big(\big|W_{(k),i}^{(V)}\big| + \big|W_{(k),i}^{(U)}\big|\big) &\overset{(a)}{=} \frac{1}{n}\Big(\Big|\mathcal{H}_{V}^{(n)} \setminus \mathcal{H}_{V|Z}^{(n)}\Big| + \Big|\mathcal{H}_{U_{(k)}|V}^{(n)} \setminus \mathcal{H}_{U_{(k)}|VZ}^{(n)}\Big|\Big)\\ &\overset{(b)}{=} \frac{1}{n}\big(\big|\mathcal{H}_{V}^{(n)}\big| - \big|\mathcal{H}_{V|Z}^{(n)}\big| + \big|\mathcal{H}_{U_{(k)}|V}^{(n)}\big| - \big|\mathcal{H}_{U_{(k)}|VZ}^{(n)}\big|\big)\\ &\xrightarrow{n\to\infty} H(V) - H(V|Z) + H(U_{(k)}|V) - H(U_{(k)}|VZ),\end{aligned}$$

   where (a) holds because $\mathcal{C}^{(n)} = \mathcal{H}_{V|Z}^{(n)}$ and by the definition of $\mathcal{J}_0^{(n)}$ and $\mathcal{J}_k^{(n)}$ in (5.42) and (5.43) respectively; (b) follows from the fact that $\mathcal{H}_{V}^{(n)} \supseteq \mathcal{H}_{V|Z}^{(n)}$ and $\mathcal{H}_{U_{(k)}|V}^{(n)} \supseteq \mathcal{H}_{U_{(k)}|VZ}^{(n)}$; and the limit holds by Theorem 2.1.

2. Rate of $W_{(\bar{k})}$. For $i \in [1, L]$, all private information $W_{(\bar{k}),i}$ is carried in layer $\tilde{T}_{(\bar{k}),i}^{n}$. Specifically, we have $W_{(\bar{k}),i}^{(U)} = \tilde{T}_{(\bar{k}),i}\big[\mathcal{B}_0^{(n)} \cup \mathcal{B}_{\bar{k}}^{(n)}\big]$. Hence, we obtain

$$\begin{aligned}\frac{1}{nL}\sum_{i=1}^{L}\big|W_{(\bar{k}),i}^{(U)}\big| &\overset{(a)}{=} \frac{1}{n}\Big|\mathcal{H}_{U_{(\bar{k})}|VU_{(k)}}^{(n)} \setminus \mathcal{H}_{U_{(\bar{k})}|VU_{(k)}Z}^{(n)}\Big|\\ &\overset{(b)}{=} \frac{1}{n}\big|\mathcal{H}_{U_{(\bar{k})}|VU_{(k)}}^{(n)}\big| - \frac{1}{n}\big|\mathcal{H}_{U_{(\bar{k})}|VU_{(k)}Z}^{(n)}\big|\\ &\xrightarrow{n\to\infty} H(U_{(\bar{k})}|VU_{(k)}) - H(U_{(\bar{k})}|VU_{(k)}Z),\end{aligned}$$

   where (a) holds by definition of $\mathcal{B}_0^{(n)}$ and $\mathcal{B}_{\bar{k}}^{(n)}$ in (5.50) and (5.51) respectively; (b) holds because $\mathcal{H}_{U_{(\bar{k})}|VU_{(k)}}^{(n)} \supseteq \mathcal{H}_{U_{(\bar{k})}|VU_{(k)}Z}^{(n)}$; and the limit holds by Theorem 2.1.

Therefore, the PCS attains $R_{W_{(k)}}^{\star k}$ and $R_{W_{(\bar{k})}}^{\star k}$ defined in (5.5) and (5.6) respectively.

Confidential message rate

According to the PCS described in Section 5.2, in order to approach the corner point $(R_{S_{(1)}}^{\star k}, R_{S_{(2)}}^{\star k}, R_{W_{(1)}}^{\star k}, R_{W_{(2)}}^{\star k}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(k)}$, the inner-layer $\tilde{A}_{1:L}^{n}$ and the outer-layer $\tilde{T}_{(k),1:L}^{n}$ carry confidential information $S_{(k)}$ intended for Receiver k, while the outer-layer $\tilde{T}_{(\bar{k}),1:L}^{n}$ carries confidential information $S_{(\bar{k})}$ intended for Receiver $\bar{k}$.

1. Rate of $S_{(k)}$. First, consider the confidential information $S_{(k)}^{(V)}$ that is carried in the inner-layer $\tilde{A}_{1:L}^{n}$. From Section 5.2.1, in all cases we have $S_{(k),1}^{(V)} = \tilde{A}_1\big[\mathcal{I}^{(n)} \cup \mathcal{G}_1^{(n)} \cup \mathcal{G}_{1,2}^{(n)}\big]$; for $i \in [2, L-1]$, we have $S_{(k),i}^{(V)} = \tilde{A}_i\big[\mathcal{I}^{(n)}\big]$; and $S_{(k),L}^{(V)} = \tilde{A}_L\big[\mathcal{I}^{(n)} \cup \mathcal{G}_2^{(n)}\big]$. Recall that the definition of the set $\mathcal{I}^{(n)}$ depends on whether the PCS must achieve the corner point of regions $\mathfrak{R}_{\text{MI-WTBC}}^{(1)}$ or $\mathfrak{R}_{\text{MI-WTBC}}^{(2)}$.

   If the PCS operates to achieve the corner point of $\mathfrak{R}_{\text{MI-WTBC}}^{(1)}$, we have

$$\begin{aligned}
\big|\mathcal{I}^{(n)}\big| &\overset{(a)}{=} \big|\mathcal{G}_0^{(n)}\big| + \big|\mathcal{G}_2^{(n)}\big| - \big|\mathcal{R}_{1,2}^{(n)}\big| - \big|\mathcal{R}_{1,2}^{\prime(n)}\big| - \big|\mathcal{R}_1^{(n)}\big| - \big|\mathcal{R}_1^{\prime(n)}\big| \\
&\overset{(b)}{=} \Big\{\big|\mathcal{G}_0^{(n)}\big| + \big|\mathcal{G}_2^{(n)}\big| - \big|\mathcal{C}_1^{(n)}\big| - \big|\mathcal{C}_{1,2}^{(n)}\big|\Big\}^{+} \\
&\overset{(c)}{=} \Big\{\Big|\mathcal{H}_{V|Z}^{(n)} \cap \mathcal{L}_{V|Y_{(1)}}^{(n)}\Big| - \Big|\big(\mathcal{H}_{V|Z}^{(n)}\big)^{\mathrm{C}} \cap \big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}}\Big|\Big\}^{+} \\
&= \Big\{\big|\mathcal{H}_{V|Z}^{(n)}\big| - \big|\big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}}\big|\Big\}^{+},
\end{aligned} \tag{5.56}$$

   where (a) holds by the definition of $\mathcal{I}^{(n)}$ in (5.31); (b) holds because, in all cases when $I(V;Y_{(1)}) < I(V;Z)$, we have $\big|\mathcal{G}_0^{(n)}\big| + \big|\mathcal{G}_2^{(n)}\big| = \big|\mathcal{R}_{1,2}^{(n)}\big| + \big|\mathcal{R}_{1,2}^{\prime(n)}\big| + \big|\mathcal{R}_1^{(n)}\big| + \big|\mathcal{R}_1^{\prime(n)}\big|$ and $\big|\mathcal{G}_0^{(n)}\big| + \big|\mathcal{G}_2^{(n)}\big| < \big|\mathcal{C}_1^{(n)}\big| - \big|\mathcal{C}_{1,2}^{(n)}\big|$ (see conditions in (5.28) and (5.29)) and, otherwise, we have $\big|\mathcal{R}_{1,2}^{(n)}\big| + \big|\mathcal{R}_1^{\prime(n)}\big| = \big|\mathcal{C}_{1,2}^{(n)}\big|$, $\big|\mathcal{R}_1^{(n)}\big| + \big|\mathcal{R}_{1,2}^{\prime(n)}\big| = \big|\mathcal{C}_1^{(n)}\big|$ and $\big|\mathcal{G}_0^{(n)}\big| + \big|\mathcal{G}_2^{(n)}\big| \geq \big|\mathcal{C}_1^{(n)}\big| - \big|\mathcal{C}_{1,2}^{(n)}\big|$ (see condition in (5.27)); and (c) follows from the partition of $\mathcal{H}_V^{(n)}$ defined in (5.19)–(5.26).

   Similarly, if the PCS operates to achieve the corner point of $\mathfrak{R}_{\text{MI-WTBC}}^{(2)}$, we have

$$\begin{aligned}
\big|\mathcal{I}^{(n)}\big| &\overset{(a)}{=} \big|\mathcal{G}_0^{(n)}\big| + \big|\mathcal{G}_1^{(n)}\big| + \big|\mathcal{G}_2^{(n)}\big| - \big|\mathcal{R}_{1,2}^{(n)}\big| - \big|\mathcal{R}_{1,2}^{\prime(n)}\big| \\
&\quad - \big|\mathcal{R}_1^{(n)}\big| - \big|\mathcal{R}_1^{\prime(n)}\big| - \big|\mathcal{R}_2^{(n)}\big| - \big|\mathcal{R}_2^{\prime(n)}\big| - \big|\mathcal{R}_{\mathrm{S}}^{(n)}\big| \\
&\overset{(b)}{=} \big|\mathcal{G}_0^{(n)}\big| + \big|\mathcal{G}_1^{(n)}\big| - \big|\mathcal{R}_{1,2}^{(n)}\big| - \big|\mathcal{R}_{1,2}^{\prime(n)}\big| - \big|\mathcal{R}_2^{(n)}\big| - \big|\mathcal{R}_2^{\prime(n)}\big| \\
&\overset{(c)}{=} \Big\{\big|\mathcal{G}_0^{(n)}\big| + \big|\mathcal{G}_1^{(n)}\big| - \big|\mathcal{C}_2^{(n)}\big| - \big|\mathcal{C}_{1,2}^{(n)}\big|\Big\}^{+} \\
&\overset{(d)}{=} \Big\{\Big|\mathcal{H}_{V|Z}^{(n)} \cap \mathcal{L}_{V|Y_{(2)}}^{(n)}\Big| - \Big|\big(\mathcal{H}_{V|Z}^{(n)}\big)^{\mathrm{C}} \cap \big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}}\Big|\Big\}^{+} \\
&= \Big\{\big|\mathcal{H}_{V|Z}^{(n)}\big| - \big|\big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}}\big|\Big\}^{+},
\end{aligned} \tag{5.57}$$

   where (a) holds by the definition of $\mathcal{I}^{(n)}$ in (5.33); (b) follows from (5.30) because the set $\mathcal{R}_{\mathrm{S}}^{(n)}$ has size $\big|\mathcal{G}_2^{(n)}\big| - \big|\mathcal{R}_1^{(n)}\big| - \big|\mathcal{R}_1^{\prime(n)}\big|$; (c) holds because, in all cases contemplated in Section 5.2.1 when $I(V;Y_{(2)}) < I(V;Z)$, we have $\big|\mathcal{G}_0^{(n)}\big| + \big|\mathcal{G}_1^{(n)}\big| = \big|\mathcal{R}_{1,2}^{(n)}\big| + \big|\mathcal{R}_{1,2}^{\prime(n)}\big| + \big|\mathcal{R}_2^{(n)}\big| + \big|\mathcal{R}_2^{\prime(n)}\big|$ and $\big|\mathcal{G}_0^{(n)}\big| + \big|\mathcal{G}_1^{(n)}\big| < \big|\mathcal{C}_2^{(n)}\big| - \big|\mathcal{C}_{1,2}^{(n)}\big|$ (see condition in (5.29)) and, otherwise, we have $\big|\mathcal{R}_2^{(n)}\big| + \big|\mathcal{R}_{1,2}^{\prime(n)}\big| = \big|\mathcal{C}_2^{(n)}\big|$ and $\big|\mathcal{R}_{1,2}^{(n)}\big| + \big|\mathcal{R}_2^{\prime(n)}\big| = \big|\mathcal{C}_{1,2}^{(n)}\big|$ (see conditions in (5.27) and (5.28)); and (d) follows from the partition of $\mathcal{H}_V^{(n)}$ defined in (5.19)–(5.26).

Consequently, the rate of $S_{(k)}^{(V)}$, which is carried by the inner-layer $\tilde{A}_{1:L}^n$, is

$$\begin{aligned}
\frac{1}{nL}\sum_{i=1}^{L}\big|S_{(k),i}^{(V)}\big| &= \frac{(L-2)}{nL}\big|\mathcal{I}^{(n)}\big| + \frac{1}{nL}\Big(\big|\mathcal{I}^{(n)}\cup\mathcal{G}_1^{(n)}\cup\mathcal{G}_{1,2}^{(n)}\big| + \big|\mathcal{I}^{(n)}\cup\mathcal{G}_2^{(n)}\big|\Big)\\
&= \frac{1}{n}\big|\mathcal{I}^{(n)}\big| + \frac{1}{nL}\Big(\big|\mathcal{G}_1^{(n)}\big| + \big|\mathcal{G}_2^{(n)}\big| + \big|\mathcal{G}_{1,2}^{(n)}\big|\Big)\\
&\overset{(a)}{=} \frac{1}{n}\big|\mathcal{I}^{(n)}\big| + \frac{1}{nL}\Big|\mathcal{H}_{V|Z}^{(n)}\cap\Big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\cap\mathcal{L}_{V|Y_{(2)}}^{(n)}\Big)^{\mathrm{C}}\Big|\\
&\overset{(b)}{\geq} \frac{1}{n}\big|\mathcal{I}^{(n)}\big| + \frac{1}{nL}\Big(\big|\mathcal{H}_{V|Z}^{(n)}\big| - \Big|\big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}}\Big|\Big)\\
&\overset{(c)}{=} \frac{1}{n}\Big\{\big|\mathcal{H}_{V|Z}^{(n)}\big| - \big|\big(\mathcal{L}_{V|Y_{(k)}}^{(n)}\big)^{\mathrm{C}}\big|\Big\}^{+} + \frac{1}{nL}\Big(\big|\mathcal{H}_{V|Z}^{(n)}\big| - \big|\big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}}\big|\Big)\\
&\xrightarrow{n\to\infty} \big\{H(V|Z) - H(V|Y_{(k)})\big\}^{+} + \frac{1}{L}\big(H(V|Z) - H(V|Y_{(1)})\big)\\
&\xrightarrow{L\to\infty} \big\{H(V|Z) - H(V|Y_{(k)})\big\}^{+},
\end{aligned} \tag{5.58}$$

where (a) holds by the partition of $\mathcal{H}_V^{(n)}$ in (5.19)–(5.26); (b) follows from applying elementary set operations and because $\big|\mathcal{L}_{V|Y_{(1)}}^{(n)}\cap\mathcal{L}_{V|Y_{(2)}}^{(n)}\big| \leq \big|\mathcal{L}_{V|Y_{(\ell)}}^{(n)}\big|$ for any $\ell\in[1,2]$; (c) follows from (5.56) and (5.57); and the limit when n goes to infinity follows from applying Theorem 2.1.

Now, consider the confidential information $S_{(k)}^{(U)}$ that is carried in the outer-layer $\tilde{T}_{(k),1:L}^n$. According to Section 5.2.2, if $i\in[2,L-1]$, we have $S_{(k),i}^{(U)} = \tilde{T}_{(k),i}\big[\mathcal{F}_0^{(n)}\setminus\big(\mathcal{D}_k^{(n)}\cup\mathcal{L}_k^{(n)}\big)\big]$. At Block 1, if $k=1$ then we have $S_{(1),1}^{(U)} = \tilde{T}_{(1),1}\big[\big(\mathcal{F}_0^{(n)}\cup\mathcal{F}_1^{(n)}\big)\setminus\big(\mathcal{D}_1^{(n)}\cup\mathcal{L}_1^{(n)}\big)\big]$ and, otherwise, we have $S_{(2),1}^{(U)} = \tilde{T}_{(2),1}\big[\mathcal{F}_0^{(n)}\cup\mathcal{F}_2^{(n)}\big]$. Finally, at Block L, if $k=1$ then we have $S_{(1),L}^{(U)} = \tilde{T}_{(1),L}\big[\mathcal{F}_0^{(n)}\big]$, while if $k=2$ then $S_{(2),L}^{(U)} = \tilde{T}_{(2),L}\big[\mathcal{F}_0^{(n)}\setminus\big(\mathcal{D}_2^{(n)}\cup\mathcal{L}_2^{(n)}\big)\big]$. Consequently, the rate of $S_{(k)}^{(U)}$, which is carried by the outer-layer $\tilde{T}_{(k),1:L}^n$, is

$$\begin{aligned}
&\frac{1}{nL}\sum_{i=1}^{L}\big|S_{(k),i}^{(U)}\big|\\
&\quad= \frac{1}{n}\big|\mathcal{F}_0^{(n)}\setminus\big(\mathcal{D}_k^{(n)}\cup\mathcal{L}_k^{(n)}\big)\big| + \frac{1}{nL}\big|\mathcal{D}_k^{(n)}\cup\mathcal{L}_k^{(n)}\cup\mathcal{F}_k^{(n)}\big|\\
&\quad\overset{(a)}{\geq} \frac{1}{n}\Big(\big|\mathcal{H}_{U_{(k)}|VZ}^{(n)}\big| - \big|\big(\mathcal{L}_{U_{(k)}|VY_{(k)}}^{(n)}\big)^{\mathrm{C}}\big| - \big\{\big|\mathcal{C}_k^{(n)}\big| + \big|\mathcal{C}_{1,2}^{(n)}\big| - \big|\mathcal{G}_0^{(n)}\big| - \big|\mathcal{G}_{\tilde{k}}^{(n)}\big|\big\}^{+}\Big)\\
&\qquad+ \frac{1}{nL}\Big(\big|\mathcal{H}_{U_{(k)}|VY_{(k)}}^{(n)}\big| + \Big\{\big|\mathcal{C}_k^{(n)}\big| + \big|\mathcal{C}_{1,2}^{(n)}\big| - \big|\mathcal{G}_0^{(n)}\big| - \big|\mathcal{G}_{\tilde{k}}^{(n)}\big|\Big\}^{+}\Big)\\
&\quad\xrightarrow{n\to\infty} H(U_{(k)}|VZ) - H(U_{(k)}|VY_{(k)}) - \big\{H(V|Y_{(k)}) - H(V|Z)\big\}^{+}\\
&\qquad+ \frac{1}{L}\big(H(U_{(k)}|VY_{(k)}) + \big\{H(V|Y_{(k)}) - H(V|Z)\big\}^{+}\big)\\
&\quad\xrightarrow{L\to\infty} H(U_{(k)}|VZ) - H(U_{(k)}|VY_{(k)}) - \big\{H(V|Y_{(k)}) - H(V|Z)\big\}^{+},
\end{aligned} \tag{5.59}$$

where (a) holds by (5.40)–(5.46) and recall that $\big|\mathcal{D}_k^{(n)}\big| + \big|\mathcal{F}_k^{(n)}\big| = \big|\mathcal{H}_{U_{(k)}|V}^{(n)} \setminus \mathcal{L}_{U_{(k)}|VY_{(k)}}^{(n)}\big|$, which is greater or equal to $\big|\mathcal{H}_{U_{(k)}|VY_{(k)}}^{(n)}\big|$; and the limit when n goes to infinity follows from applying Theorem 2.1, where we have used similar reasoning as in (5.56) and (5.57) to obtain $\big\{\big|\mathcal{C}_k^{(n)}\big| + \big|\mathcal{C}_{1,2}^{(n)}\big| - \big|\mathcal{G}_0^{(n)}\big| - \big|\mathcal{G}_{\bar{k}}^{(n)}\big|\big\}^+ \xrightarrow{n\to\infty} \big\{H(V|Y_{(k)}) - H(V|Z)\big\}^+$.

Finally, by combining (5.58) and (5.59), we obtain that the rate of $S_{(k)}$ is

$$\frac{1}{nL}\sum_{i=1}^{L}\big|S_{(k),i}\big| = \frac{1}{nL}\sum_{i=1}^{L}\big(\big|S_{(k),i}^{(V)}\big| + \big|S_{(k),i}^{(U)}\big|\big) \xrightarrow{n\to\infty} H(VU_{(k)}|Z) - H(VU_{(k)}|Y_{(k)}),$$

which is equal to the rate $R_{S_{(k)}}^{\star k}$ defined in (5.3).

2. Rate of $S_{(\bar{k})}$. The confidential message $S_{(\bar{k})}$ is carried entirely in $\tilde{T}_{(\bar{k}),1:L}^n$. According to Section 5.2.2, if $i \in [2, L-1]$, we have $S_{(\bar{k}),i}^{(U)} = \tilde{T}_{(\bar{k}),i}\big[\mathcal{Q}_0^{(n)} \setminus \big(\mathcal{O}_{\bar{k}}^{(n)} \cup \mathcal{N}_{\bar{k}}^{(n)} \cup \mathcal{M}_{\bar{k}}^{(n)}\big)\big]$. At Block 1, if $\bar{k} = 1$ then $S_{(1),1}^{(U)} = \tilde{T}_{(1),1}\big[\big(\mathcal{Q}_0^{(n)} \cup \mathcal{Q}_1^{(n)}\big) \setminus \big(\mathcal{O}_1^{(n)} \cup \mathcal{N}_1^{(n)} \cup \mathcal{M}_1^{(n)}\big)\big]$ and, otherwise, $S_{(2),1}^{(U)} = \tilde{T}_{(2),1}\big[\mathcal{Q}_0^{(n)} \cup \mathcal{Q}_2^{(n)}\big]$. At Block L, if $\bar{k} = 1$ then we have $S_{(1),L}^{(U)} = \tilde{T}_{(1),L}\big[\mathcal{Q}_0^{(n)}\big]$, while if $\bar{k} = 2$ then $S_{(2),L}^{(U)} = \tilde{T}_{(2),L}\big[\mathcal{Q}_0^{(n)} \setminus \big(\mathcal{O}_2^{(n)} \cup \mathcal{N}_2^{(n)} \cup \mathcal{M}_2^{(n)}\big)\big]$. Consequently, we obtain

$$\begin{aligned}
&\frac{1}{nL}\sum_{i=1}^{L}\big|S_{(\bar{k}),i}^{(U)}\big| \\
&\quad= \frac{1}{n}\big|\mathcal{Q}_0^{(n)} \setminus \big(\mathcal{O}_{\bar{k}}^{(n)} \cup \mathcal{N}_{\bar{k}}^{(n)} \cup \mathcal{M}_{\bar{k}}^{(n)}\big)\big| + \frac{1}{nL}\big|\mathcal{O}_{\bar{k}}^{(n)} \cup \mathcal{N}_{\bar{k}}^{(n)} \cup \mathcal{M}_{\bar{k}}^{(n)} \cup \mathcal{Q}_{\bar{k}}^{(n)}\big| \\
&\quad\overset{(a)}{=} \frac{1}{n}\Big(\Big|\mathcal{H}_{U_{(\bar{k})}|VU_{(k)}Z}^{(n)} \cap \mathcal{L}_{U_{(\bar{k})}|VY_{(\bar{k})}}^{(n)}\Big| - \Big|\big(\mathcal{H}_{U_{(\bar{k})}|VU_{(k)}}^{(n)}\big)^{\mathrm{C}} \cap \mathcal{H}_{U_{(\bar{k})}|V}^{(n)} \setminus \mathcal{L}_{U_{(\bar{k})}|VY_{(\bar{k})}}^{(n)}\Big| \\
&\qquad - \Big|\mathcal{H}_{U_{(\bar{k})}|VU_{(k)}}^{(n)} \cap \big(\mathcal{H}_{U_{(\bar{k})}|VU_{(k)}Z}^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{L}_{U_{(\bar{k})}|VY_{(\bar{k})}}^{(n)}\Big| - \big|\mathcal{M}_{\bar{k}}^{(n)}\big|\Big) \\
&\qquad + \frac{1}{nL}\big|\mathcal{O}_{\bar{k}}^{(n)} \cup \mathcal{N}_{\bar{k}}^{(n)} \cup \mathcal{M}_{\bar{k}}^{(n)} \cup \mathcal{Q}_{\bar{k}}^{(n)}\big| \\
&\quad\overset{(b)}{\geq} \frac{1}{n}\Big(\Big|\mathcal{H}_{U_{(\bar{k})}|VU_{(k)}Z}^{(n)} \cap \mathcal{L}_{U_{(\bar{k})}|VY_{(\bar{k})}}^{(n)}\Big| - \Big|\big(\mathcal{H}_{U_{(\bar{k})}|VU_{(k)}Z}^{(n)}\big)^{\mathrm{C}} \setminus \mathcal{L}_{U_{(\bar{k})}|VY_{(\bar{k})}}^{(n)}\Big| - \big|\mathcal{M}_{\bar{k}}^{(n)}\big|\Big) \\
&\qquad + \frac{1}{nL}\Big(\Big|\mathcal{H}_{U_{(\bar{k})}|VY_{(\bar{k})}}^{(n)}\Big| + \big|\mathcal{M}_{\bar{k}}^{(n)}\big|\Big) \\
&\quad= \frac{1}{n}\Big(\Big|\mathcal{H}_{U_{(\bar{k})}|VU_{(k)}Z}^{(n)}\Big| - \Big|\big(\mathcal{L}_{U_{(\bar{k})}|VY_{(\bar{k})}}^{(n)}\big)^{\mathrm{C}}\Big| - \big|\mathcal{M}_{\bar{k}}^{(n)}\big|\Big) + \frac{1}{nL}\Big(\Big|\mathcal{H}_{U_{(\bar{k})}|VY_{(\bar{k})}}^{(n)}\Big| + \big|\mathcal{M}_{\bar{k}}^{(n)}\big|\Big) \\
&\xrightarrow{n\to\infty} H(U_{(\bar{k})}|VU_{(k)}Z) - H(U_{(\bar{k})}|VY_{(\bar{k})}) - \big(H(V|Y_{(\bar{k})}) - \min\{H(V|Y_{(2)}), H(V|Z)\}\big) \\
&\qquad\qquad + \frac{1}{L}\big(H(U_{(\bar{k})}|VY_{(\bar{k})}) - (H(V|Y_{(\bar{k})}) - \min\{H(V|Y_{(2)}), H(V|Z)\})\big) \\
&\xrightarrow{L\to\infty} H(U_{(\bar{k})}|VU_{(k)}Z) - H(U_{(\bar{k})}|VY_{(\bar{k})}) - \big(H(V|Y_{(\bar{k})}) - \min\{H(V|Y_{(2)}), H(V|Z)\}\big),
\end{aligned}$$

where (a) holds by the definition of sets in (5.48)–(5.53); (b) follows from the fact that sets $\big(\mathcal{H}_{U_{(\bar{k})}|VU_{(k)}}^{(n)}\big)^{\mathrm{C}} \cap \mathcal{H}_{U_{(\bar{k})}|V}^{(n)}$ and $\mathcal{H}_{U_{(\bar{k})}|VU_{(k)}}^{(n)} \cap \big(\mathcal{H}_{U_{(\bar{k})}|VU_{(k)}Z}^{(n)}\big)^{\mathrm{C}}$ are disjoint and

subsets of $\big(\mathcal{H}^{(n)}_{U_{(\bar{k})}|VU_{(k)}Z}\big)^{\mathrm{C}}$, and because $\big|\mathcal{O}^{(n)}_{\bar{k}}\big|+\big|\mathcal{N}^{(n)}_{\bar{k}}\big|+\big|\mathcal{Q}^{(n)}_{\bar{k}}\big| = \big|\mathcal{H}^{(n)}_{U_{(\bar{k})}|V}\setminus\mathcal{L}^{(n)}_{U_{(\bar{k})}|VY_{(\bar{k})}}\big|$, which is greater or equal to $\big|\mathcal{H}^{(n)}_{U_{(\bar{k})}|VY_{(\bar{k})}}\big|$; and the limit when n goes to infinity follows from applying Theorem 2.1 and the definition of $\mathcal{M}^{(n)}_{\bar{k}}$. If $\bar{k}=1$, according to (5.55) we have $\big|\mathcal{M}^{(n)}_1\big| = \big|\mathcal{G}^{(n)}_1\big| + \big|\mathcal{C}^{(n)}_1\big| - \big|\mathcal{G}^{(n)}_2\big| - \big|\mathcal{C}^{(n)}_2\big|$ if $I(V;Z)\leq I(V;Y_{(2)})$, whereas $\big|\mathcal{M}^{(n)}_1\big| = \big|\mathcal{C}^{(n)}_1\big| + \big|\mathcal{C}^{(n)}_{1,2}\big| - \big|\mathcal{G}^{(n)}_0\big| - \big|\mathcal{G}^{(n)}_2\big|$ if $I(V;Z)>I(V;Y_{(2)})$, and we have

$$\big|\mathcal{C}^{(n)}_1\big| + \big|\mathcal{C}^{(n)}_{1,2}\big| - \big|\mathcal{G}^{(n)}_0\big| - \big|\mathcal{G}^{(n)}_2\big| \xrightarrow{n\to\infty} H(V|Y_{(1)}) - H(V|Z)),$$

which follows from (5.56), while from the partition of $\mathcal{H}^{(n)}_V$ in (5.19)–(5.26) we obtain

$$\begin{aligned}\big|\mathcal{G}^{(n)}_1\big| + \big|\mathcal{C}^{(n)}_1\big| - \big|\mathcal{G}^{(n)}_2\big| - \big|\mathcal{C}^{(n)}_2\big| &= \big|\big(\mathcal{L}^{(n)}_{V|Y_{(1)}}\big)^{\mathrm{C}}\cap\mathcal{L}^{(n)}_{V|Y_{(2)}}\big| - \big|\big(\mathcal{L}^{(n)}_{V|Y_{(2)}}\big)^{\mathrm{C}}\cap\mathcal{L}^{(n)}_{V|Y_{(1)}}\big| \\ &= \big|\big(\mathcal{L}^{(n)}_{V|Y_{(1)}}\big)^{\mathrm{C}}\big| - \big|\big(\mathcal{L}^{(n)}_{V|Y_{(2)}}\big)^{\mathrm{C}}\big|, \\ &\xrightarrow{n\to\infty} H(V|Y_{(1)}) - H(V|Y_{(2)}).\end{aligned}$$

Otherwise, if $\bar{k}=2$, from (5.54) we have $\big|\mathcal{M}^{(n)}_2\big| = \big\{\big|\mathcal{C}^{(n)}_2\big| + \big|\mathcal{C}^{(n)}_{1,2}\big| - \big|\mathcal{G}^{(n)}_0\big| - \big|\mathcal{G}^{(n)}_1\big|\big\}^+$ and

$$\begin{aligned}\big\{\big|\mathcal{C}^{(n)}_2\big| + \big|\mathcal{C}^{(n)}_{1,2}\big| - \big|\mathcal{G}^{(n)}_0\big| - \big|\mathcal{G}^{(n)}_1\big|\big\}^+ &\xrightarrow{n\to\infty} \big\{H(V|Y_{(2)}) - H(V|Z)\big\}^+ \\ &= H(V|Y_{(2)}) - \min\{H(V|Y_{(2)}), H(V|Z)\}.\end{aligned}$$

Therefore, the PCS attains $R^{\star k}_{S_{(\bar{k})}}$ defined in (5.4).

Private-shared sequence rate

First, recall that in Chapter 4 (Section 4.3.1) we have proved that

$$\frac{1}{nL}\Big(\big|\kappa^{(V)}_{\Theta}\big| + \big|\kappa^{(V)}_{\Gamma}\big| + \sum_{k=1}^{2}\big|\kappa^{(V)}_{\Upsilon\Phi_{(k)}}\big|\Big) \xrightarrow{n,L\to\infty} 0.$$

If we substitute $\big|\kappa^{(V)}_{\Theta}\big|$ by $\big|\kappa^{(V)}_{\Psi}\big|$, it is very easy to prove, by applying similar reasoning, that the overall length is negligible in terms of rate as well.

If $k=1$, we have $\big|\kappa^{(U)}_{\Theta}\big| = \big|\mathcal{J}^{(n)}_1\big|$ and $\big|\kappa^{(U)}_{\Psi}\big| = 0$, whereas $\big|\kappa^{(U)}_{\Theta}\big| = 0$ and $\big|\kappa^{(U)}_{\Psi}\big| = \big|\mathcal{B}^{(n)}_2\big|$ if $k=2$. From the definition of $\mathcal{J}^{(n)}_1$ and $\mathcal{B}^{(n)}_2$ in (5.43) and (5.51) respectively, we obtain

$$\begin{aligned}\frac{1}{nL}\big|\kappa^{(U)}_{\Theta}\big| \leq \big|\big(\mathcal{L}^{(n)}_{U_{(1)}|VY_{(1)}}\big)^{\mathrm{C}}\big| &\xrightarrow{n\to\infty} \frac{1}{L}H(U_{(1)}|VY_{(1)}) \xrightarrow{L\to\infty} 0, \\ \frac{1}{nL}\big|\kappa^{(U)}_{\Psi}\big| \leq \big|\big(\mathcal{L}^{(n)}_{U_{(2)}|VY_{(2)}}\big)^{\mathrm{C}}\big| &\xrightarrow{n\to\infty} \frac{1}{L}H(U_{(2)}|VY_{(2)}) \xrightarrow{L\to\infty} 0.\end{aligned}$$

where the limit when n goes to infinity follows from applying Theorem 2.1.

Finally, we have

$$\begin{aligned}
&\frac{1}{nL}\sum_{\ell=1}^{2}\big|\kappa^{(U)}_{\Upsilon\Phi_{(\ell)}}\big|+\frac{1}{nL}\big|\kappa^{(U)}_{O}\big| \\
&\quad=\frac{1}{nL}\Big(L\big|\big(\mathcal{H}^{(n)}_{U_{(k)}|V}\big)^{\mathrm{C}}\setminus\mathcal{L}^{(n)}_{U_{(k)}|VY_{(k)}}\big|+\big|\mathcal{H}^{(n)}_{U_{(k)}|V}\setminus\mathcal{L}^{(n)}_{U_{(k)}|VY_{(k)}}\big|\Big) \\
&\qquad+\frac{1}{nL}\Big(L\big|\big(\mathcal{H}^{(n)}_{U_{(\bar{k})}|V}\big)^{\mathrm{C}}\setminus\mathcal{L}^{(n)}_{U_{(\bar{k})}|VY_{(\bar{k})}}\big|+\big|\mathcal{H}^{(n)}_{U_{(\bar{k})}|V}\setminus\mathcal{L}^{(n)}_{U_{(\bar{k})}|VY_{(\bar{k})}}\big|\Big) \\
&\qquad+\frac{1}{nL}\Big(\big|\big(\mathcal{H}^{(n)}_{U_{(\bar{k})}|VU_{(k)}}\big)^{\mathrm{C}}\cap\mathcal{H}^{(n)}_{U_{(\bar{k})}|V}\setminus\mathcal{L}^{(n)}_{U_{(\bar{k})}|VY_{(\bar{k})}}\big|\Big) \\
&\quad\le\frac{1}{n}\sum_{\ell=1}^{2}\big|\big(\mathcal{H}^{(n)}_{U_{(\ell)}|V}\big)^{\mathrm{C}}\setminus\mathcal{L}^{(n)}_{U_{(\ell)}|VY_{(\ell)}}\big|+\frac{1}{nL}\big|\big(\mathcal{L}^{(n)}_{U_{(k)}|VY_{(k)}}\big)^{\mathrm{C}}\big|+\frac{2}{nL}\big|\big(\mathcal{L}^{(n)}_{U_{(\bar{k})}|VY_{(\bar{k})}}\big)^{\mathrm{C}}\big| \\
&\quad\overset{(a)}{\le}\frac{1}{n}\sum_{\ell=1}^{2}\big|\big(\mathcal{H}^{(n)}_{U_{(\ell)}|VY_{(\ell)}}\big)^{\mathrm{C}}\setminus\mathcal{L}^{(n)}_{U_{(\ell)}|VY_{(\ell)}}\big|+\frac{1}{nL}\big|\big(\mathcal{L}^{(n)}_{U_{(k)}|VY_{(k)}}\big)^{\mathrm{C}}\big|+\frac{2}{nL}\big|\big(\mathcal{L}^{(n)}_{U_{(\bar{k})}|VY_{(\bar{k})}}\big)^{\mathrm{C}}\big| \\
&\quad\xrightarrow{n\to\infty}\frac{1}{L}\big(H(U_{(k)}|VY_{(k)})+2H(U_{(\bar{k})}|VY_{(\bar{k})})\big)\xrightarrow{L\to\infty}0,
\end{aligned}$$

where (a) holds because $\mathcal{H}^{(n)}_{U_{(\ell)}|VY_{(\ell)}}\subseteq\mathcal{H}^{(n)}_{U_{(\ell)}|V}$ for any $\ell\in[1,2]$; and the limit when n goes to infinity follows from applying Theorem 2.1.

Therefore, the amount of private-shared information between transmitter and legitimate receivers is negligible in terms of rate, and so is the rate of the additional transmissions.

Rate of the additional randomness

For $i\in[1,L]$, the encoder randomly draws (by SC encoding) the elements $\tilde{A}_i\big[\big(\mathcal{H}^{(n)}_{V}\big)^{\mathrm{C}}\setminus\mathcal{L}^{(n)}_{V}\big]$, $\tilde{T}_{(k),i}\big[\big(\mathcal{H}^{(n)}_{U_{(k)}|V}\big)^{\mathrm{C}}\setminus\mathcal{L}^{(n)}_{U_{(k)}|V}\big]$ and $\tilde{T}_{(\bar{k}),i}\big[\big(\mathcal{H}^{(n)}_{U_{(\bar{k})}|VU_{(k)}}\big)^{\mathrm{C}}\setminus\mathcal{L}^{(n)}_{U_{(\bar{k})}|VU_{(k)}}\big]$. Nevertheless, we have

$$\frac{1}{n}\Big(\big|\big(\mathcal{H}^{(n)}_{V}\big)^{\mathrm{C}}\setminus\mathcal{L}^{(n)}_{V}\big|+\Big|\big(\mathcal{H}^{(n)}_{U_{(k)}|V}\big)^{\mathrm{C}}\setminus\mathcal{L}^{(n)}_{U_{(k)}|V}\Big|+\Big|\big(\mathcal{H}^{(n)}_{U_{(\bar{k})}|VU_{(k)}}\big)^{\mathrm{C}}\setminus\mathcal{L}^{(n)}_{U_{(\bar{k})}|VU_{(k)}}\Big|\Big)\xrightarrow{n\to\infty}0,$$

where the limit as n approaches infinity follows from applying Theorem 2.1.

5.3.2 Distribution of the DMS after the polar encoding

For $i\in[1,L]$, let $\tilde{q}_{A_i^nT^n_{(1),i}T^n_{(2),i}}$ denote the distribution of $(\tilde{A}_i^n,\tilde{T}^n_{(1),i},\tilde{T}^n_{(2),i})$ after the encoding. The following lemma proves that $\tilde{q}_{A_i^nT^n_{(1),i}T^n_{(2),i}}$ and the marginal distribution $p_{A^nT^n_{(1)}T^n_{(2)}}$ of the original DMS are nearly statistically indistinguishable for sufficiently large n and, consequently, so are $\tilde{q}_{V_i^nT^n_{(1),i}T^n_{(2),i}X_i^nY^n_{(1),i}Y^n_{(2),i}Z_i^n}$ and $p_{V^nT^n_{(1)}T^n_{(2)}X^nY^n_{(1)}Y^n_{(2)}Z^n}$. This result is crucial for the reliability and secrecy performance of the polar coding scheme.

Lemma 5.1. *For any $i \in [1, L]$, we obtain*

$$\mathbb{V}(\tilde{q}_{A_i^n T_{(1),i}^n T_{(2),i}^n}, p_{A^n T_{(1)}^n T_{(2)}^n}) \leq \delta_n^{(*)},$$
$$\mathbb{V}(\tilde{q}_{V_i^n T_{(1),i}^n T_{(2),i}^n X_i^n Y_{(1),i}^n Y_{(2),i}^n Z_i^n}, p_{V^n T_{(1)}^n T_{(2)}^n X^n Y_{(1)}^n Y_{(2)}^n Z^n}) \leq \delta_n^{(*)},$$

where $\delta_n^{(*)} \triangleq n \sum_{\ell=1}^{3} \sqrt{2\sqrt{\ell n \delta_n 2 \ln 2}\big(\ell n - \log \sqrt{\ell n \delta_n 2 \ln 2}\big) + \delta_n} + \sqrt{3}\sqrt{n \delta_n 2 \ln 2}$.

Proof. For the first claim, see Lemma 2.3 taking $T_{\mathrm{V}} \triangleq 3$. The second holds by Corollary 2.2 because, for all $i \in [1, L]$, sequence $\tilde{X}_i^n$ and X_i^n are deterministic functions of $(\tilde{A}_i^n, \tilde{T}_{(1),i}^n, \tilde{T}_{(2),i}^n)$ and $(A^n, T_{(1)}^n, T_{(2)}^n)$ respectively, and $\tilde{q}_{V_i^n T_{(1),i}^n T_{(2),i}^n X_i^n Y_{(1),i}^n Y_{(2),i}^n Z_i^n} \equiv \tilde{q}_{X_i^n} p_{Y_{(1)}^n Y_{(2)}^n Z^n | X^n}$. □

Remark 5.11. *Consider the PCS operating to achieve the corner point of $\mathfrak{R}_{\text{MI-WTBC}}^{(k)}$ for some $k \in [1, 2]$. In this case, $O_{(\bar{k}),i}^{(U)} \subset \tilde{T}_{(\bar{k}),i}\big[\big(\mathcal{H}_{U_{(\bar{k})}|VU_{(k)}}^{(n)}\big)^{\mathrm{C}} \cap \mathcal{H}_{U_{(\bar{k})}|V}^{(n)}\big]$ is repeated, for $i \in [2, L]$, in $\tilde{T}_{(\bar{k}),i-1}^n$ (if $\bar{k} = 1$) or, for $i \in [1, L-1]$, in $\tilde{T}_{(\bar{k}),i+1}^n$ (if $\bar{k} = 2$). In both situations, $O_{(\bar{k}),i}^{(U)}$ is drawn by performing SC encoding and is repeated in some of the elements of the corresponding adjacent block whose indices correspond to $\mathcal{H}_{U_{(\bar{k})}|VU_{(k)}Z}^{(n)}$. Nevertheless, $O_{(\bar{k}),i}^{(U)}$ is not repeated directly, but the encoder copies $\bar{O}_{(\bar{k}),i}^{(U)} = O_{(\bar{k}),i}^{(U)} \oplus \kappa_O^{(U)}$ (see Figure 5.9 and Figure 5.10). Hence, notice that $\kappa_O^{(U)}$ ensures that $\bar{O}_{(\bar{k}),i}^{(U)}$ is uniformly distributed and, consequently, we can consider that $\tilde{q}_{A_i^n T_{(1),i}^n T_{(2),i}^n}$ is equivalent to (2.16) and apply Lemma 2.3 in the previous proof.*

5.3.3 Reliability analysis

Consider that the PCS must achieve $(R_{S_{(1)}}^{\star k}, R_{S_{(2)}}^{\star k}, R_{W_{(1)}}^{\star k}, R_{W_{(2)}}^{\star k}) \subset \mathfrak{R}_{\text{MI-WTBC}}^{(k)}$. In this section we prove that Receiver k is able to reconstruct $(W_{(k)}, S_{(k)})$ with arbitrary small error probability, while Receiver $\bar{k}$ is able to reconstruct $(W_{(\bar{k})}, S_{(\bar{k})})$. Recall that the inner-layer $\tilde{A}_{1:L}^n$ and the outer-layer $\tilde{T}_{(k),1:L}^n$ carry $(W_{(k)}, S_{(k)})$, and the outer-layer $\tilde{T}_{(\bar{k}),1:L}^n$ carries $(W_{(\bar{k})}, S_{(\bar{k})})$. Although $\tilde{A}_{1:L}^n$ only contains information intended for Receiver k, the other receiver must reliably reconstruct them in order to be able to decode $\tilde{T}_{(\bar{k}),1:L}^n$.

Consider the probability of incorrectly decoding $\big(\tilde{A}_{1:L}^n, \tilde{T}_{(1),1:L}^n\big)$ at Receiver $\ell \in [1, 2]$. For $i \in [1, L]$, let $\tilde{q}_{V_i^n T_{(\ell),i}^n Y_{(\ell),i}^n}$ and $p_{V^n T_{(\ell)}^n Y_{(\ell)}^n}$ be marginals of $\tilde{q}_{V_i^n T_{(1),i}^n T_{(2),i}^n X_i^n Y_{(1),i}^n Y_{(2),i}^n Z_i^n}$ and $p_{V^n T_{(1)}^n T_{(2)}^n X^n Y_{(1)}^n Y_{(2)}^n Z^n}$ respectively, and define an optimal coupling [LPW09] (Proposition 4.7) between $\tilde{q}_{V_i^n T_{(\ell),i}^n Y_{(\ell),i}^n}$ and $p_{V^n T_{(\ell)}^n Y_{(\ell)}^n}$ such that $\mathbb{P}\big[\mathcal{E}_{V_i^n T_{(\ell),i}^n Y_{(\ell),i}^n}\big] = \mathbb{V}\big(\tilde{q}_{V_i^n T_{(\ell),i}^n Y_{(\ell),i}^n}, p_{V^n T_{(\ell)}^n Y_{(\ell)}^n}\big)$, where $\mathcal{E}_{V_i^n T_{(\ell),i}^n Y_{(\ell),i}^n} \triangleq \big\{\big(\tilde{V}_i^n, T_{(\ell)}^n, \tilde{Y}_{(\ell),i}^n\big) \neq \big(V^n, T_{(\ell)}^n, Y_{(\ell)}^n\big)\big\}$. Additionally, define

$$\mathcal{E}_{(\ell),i} \triangleq \Big\{\Big(\hat{A}_{(\ell),i}\big[\big(\mathcal{L}_{V|Y_{(\ell)}}^{(n)}\big)^{\mathrm{C}}\big], \hat{T}_{(\ell),i}\big[\big(\mathcal{L}_{U_{(\ell)}|VY_{(\ell)}}^{(n)}\big)^{\mathrm{C}}\big]\Big) \neq \Big(\tilde{A}_i\big[\big(\mathcal{L}_{V|Y_{(\ell)}}^{(n)}\big)^{\mathrm{C}}\big], \tilde{T}_{(\ell),i}\big[\big(\mathcal{L}_{U_{(\ell)}|VY_{(\ell)}}^{(n)}\big)^{\mathrm{C}}\big]\Big)\Big\}.$$

Recall that $(\Upsilon_{(\ell)}^{(V)}, \Phi_{(\ell),1:L}^{(V)})$ and $(\Upsilon_{(\ell)}^{(U)}, \Phi_{(\ell),1:L}^{(U)})$ is available to legitimate Receiver ℓ. Thus, $\mathbb{P}[\mathcal{E}_{(1),1}] = \mathbb{P}[\mathcal{E}_{(2),L}] = 0$ because given $(\Upsilon_{(1)}^{(V)}, \Phi_{(1),1:L}^{(V)})$ and $(\Upsilon_{(1)}^{(U)}, \Phi_{(1),1:L}^{(U)})$ Receiver 1 knows $\tilde{A}_1\big[\big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}}\big]$ and $\tilde{T}_{(1),1}\big[\big(\mathcal{L}_{U_{(1)}|VY_{(1)}}^{(n)}\big)^{\mathrm{C}}\big]$, while given $(\Upsilon_{(2)}^{(V)}, \Phi_{(2),1:L}^{(V)})$ and $(\Upsilon_{(2)}^{(U)}, \Phi_{(2),1:L}^{(U)})$ legitimate Receiver 2 knows $\tilde{A}_L\big[\big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}}\big]$ and $\tilde{T}_{(2),L}\big[\big(\mathcal{L}_{U_{(2)}|VY_{(2)}}^{(n)}\big)^{\mathrm{C}}\big]$. Furthermore, due to the chaining structure, recall that $\big(\tilde{A}_i\big[\big(\mathcal{L}_{V|Y_{(1)}}^{(n)}\big)^{\mathrm{C}}\big], \tilde{T}_{(1),i}\big[\big(\mathcal{L}_{U_{(1)}|VY_{(1)}}^{(n)}\big)^{\mathrm{C}}\big]\big)$ can be constructed from $\big(\tilde{A}_{i-1}^n, \tilde{T}_{(1),i-1}^n\big)$ for $i \in [2, L]$. Therefore, at legitimate Receiver 1, for $i \in [2, L]$ we have

$$\mathbb{P}[\mathcal{E}_{(1),i}] \leq \mathbb{P}\big[\big(\hat{A}_{i-1}^n, \hat{T}_{(1),i-1}^n\big) \neq \big(\tilde{A}_{i-1}^n, \tilde{T}_{(1),i-1}^n\big)\big]. \tag{5.60}$$

Similarly, we have seen that $\big(\tilde{A}_i\big[\big(\mathcal{L}_{V|Y_{(2)}}^{(n)}\big)^{\mathrm{C}}\big], \tilde{T}_{(2),i}\big[\big(\mathcal{L}_{U_{(2)}|VY_{(2)}}^{(n)}\big)^{\mathrm{C}}\big]\big)$ is repeated, for $i \in [1, L-1]$, in $\big(\tilde{A}_{i+1}^n, \tilde{T}_{(2),i+1}^n\big)$. Thus, at legitimate Receiver 2, for $i \in [1, L-1]$ we obtain

$$\mathbb{P}[\mathcal{E}_{(2),i}] \leq \mathbb{P}\big[\big(\hat{A}_{i+1}^n, \hat{T}_{(2),i+1}^n\big) \neq \big(\tilde{A}_{i+1}^n, \tilde{T}_{(2),i+1}^n\big)\big]. \tag{5.61}$$

Hence, the probability of incorrectly decoding $\big(\tilde{A}_i^n, \tilde{T}_{(\ell),i}^n\big)$ at the Receiver $\ell \in [1, 2]$ is

$$\begin{aligned}
&\mathbb{P}\big[\big(\hat{A}_{(\ell),i}^n, \hat{T}_{(\ell),i}^n\big) \neq \big(\tilde{A}_i^n, \tilde{T}_{(\ell),i}^n\big)\big] \\
&\quad= \mathbb{P}\Big[\big(\hat{A}_{(\ell),i}^n, \hat{T}_{(\ell),i}^n\big) \neq \big(\tilde{A}_i^n, \tilde{T}_{(\ell),i}^n\big) \big| \mathcal{E}_{V_i^n U_{(\ell)} Y_{(\ell),i}^n}^{\mathrm{C}} \cap \mathcal{E}_{(\ell),i}^{\mathrm{C}}\Big] \mathbb{P}\Big[\mathcal{E}_{V_i^n U_{(\ell)} Y_{(\ell),i}^n}^{\mathrm{C}} \cap \mathcal{E}_{(\ell),i}^{\mathrm{C}}\Big] \\
&\qquad+ \mathbb{P}\Big[\big(\hat{A}_{(\ell),i}^n, \hat{T}_{(\ell),i}^n\big) \neq \big(\tilde{A}_i^n, \tilde{T}_{(\ell),i}^n\big) \big| \mathcal{E}_{V_i^n U_{(\ell)} Y_{(\ell),i}^n} \cup \mathcal{E}_{(\ell),i}\Big] \mathbb{P}\Big[\mathcal{E}_{V_i^n U_{(\ell)} Y_{(\ell),i}^n} \cup \mathcal{E}_{(\ell),i}\Big] \\
&\quad\leq \mathbb{P}\Big[\big(\hat{A}_{(\ell),i}^n, \hat{T}_{(\ell),i}^n\big) \neq \big(\tilde{A}_i^n, \tilde{T}_{(\ell),i}^n\big) \big| \mathcal{E}_{V_i^n U_{(\ell)} Y_{(\ell),i}^n}^{\mathrm{C}} \cap \mathcal{E}_{(\ell),i}^{\mathrm{C}}\Big] + \mathbb{P}\Big[\mathcal{E}_{V_i^n U_{(\ell)} Y_{(\ell),i}^n}\Big] + \mathbb{P}\Big[\mathcal{E}_{(\ell),i}\Big] \\
&\quad\overset{(a)}{\leq} 2\delta_n + \mathbb{P}\big[\mathcal{E}_{V_i^n U_{(\ell)} Y_{(\ell),i}^n}\big] + \mathbb{P}\big[\mathcal{E}_{(\ell),i}\big] \\
&\quad\overset{(b)}{\leq} 2\delta_n + \delta_n^{(*)} + \mathbb{P}\big[\mathcal{E}_{(\ell),i}\big] \\
&\quad\overset{(c)}{\leq} i\big(2\delta_n + \delta_n^{(*)}\big)
\end{aligned}$$

where (a) holds by Theorem 2.1; (b) follows from the optimal coupling and Lemma 5.1; and (c) holds by induction and (5.60)–(5.61). Therefore, by the union bound, we obtain

$$\begin{aligned}
\mathbb{P}\big[(W_{(\ell),1:L}, S_{(\ell),1:L}) \neq (\hat{W}_{(\ell),1:L}, \hat{S}_{(\ell),1:L})\big] &\leq \sum_{i=1}^{L} \mathbb{P}\big[\big(\hat{A}_{(\ell),i}^n, \hat{T}_{(\ell),i}^n\big) \neq \big(\tilde{A}_i^n, \tilde{T}_{(\ell),i}^n\big)\big] \\
&\leq \frac{L(L+1)}{2}\big(2n\delta_n + \delta_n^{(*)}\big),
\end{aligned}$$

and, consequently, for sufficiently large n the PCS satisfies the reliability condition in (5.1).

5.3.4 Secrecy analysis

Since the encoding of Section 5.2 takes place over L blocks of size n, we need to prove that

$$\lim_{n\to\infty} I\left(S_{(1),1:L}S_{(2),1:L};\tilde{Z}^n_{1:L}\right)=0.$$

Consider that the PCS operates to achieve $(R^{\star k}_{S_{(1)}},R^{\star k}_{S_{(2)}},R^{\star k}_{W_{(1)}},R^{\star k}_{W_{(2)}})\subset\mathfrak{R}^{(k)}_{\text{MI-WTBC}}$, where $k\in[1,2]$. For any $i\in[1,L]$, the confidential message $S_{(k),i}$ is stored in $\tilde{A}_i\big[\mathcal{H}^{(n)}_{V|Z}\big]$ and $\tilde{T}_{(k),i}\big[\mathcal{H}^{(n)}_{U_{(k)}|VZ}\big]$, and $S_{(\bar{k}),i}$ is stored in $\tilde{T}_{(\bar{k}),i}\big[\mathcal{H}^{(n)}_{U_{(\bar{k})}|VU_{(\bar{k})}Z}\big]$. Hence, the following lemma shows that strong secrecy holds for any Block $i\in[1,L]$.

Lemma 5.2. *For any $i\in[1,L]$ and sufficiently large n, we have*

$$I\big(\tilde{A}_i\big[\mathcal{H}^{(n)}_{V|Z}\big]\tilde{T}_{(k),i}\big[\mathcal{H}^{(n)}_{U_{(k)}|VZ}\big]\tilde{T}_{(\bar{k}),i}\big[\mathcal{H}^{(n)}_{U_{(\bar{k})}|VU_{(k)}Z}\big];\tilde{Z}^n_i\big)\leq\delta^{(\mathrm{S})}_n,$$

where $\delta^{(\mathrm{S})}_n\triangleq 3n\delta_n+2\delta^{(*)}_n\big(3n-\log\delta^{(*)}_n\big)$ and $\delta^{(*)}_n$ is defined as in Lemma 5.1.

Proof. See Appendix 5.A. □

The following step is to prove asymptotically statistically independence between eavesdropper's observations from Blocks 1 to L. We address this part slightly differently depending on whether the PCS must achieve the corner point of $\mathfrak{R}^{(1)}_{\text{MI-WTBC}}$ or $\mathfrak{R}^{(2)}_{\text{MI-WTBC}}$.

Secrecy analysis when polar code operates to achieve the corner point of $\mathfrak{R}^{(1)}_{\text{MI-WTBC}}$

For convenience and with slight abuse of notation, for $i\in[1,L]$ let $\tilde{R}^n_{(1),i}\triangleq\big(\tilde{A}^n_i,\tilde{T}^n_{(1),i}\big)$, which carries $W_{(1),i}\triangleq\big[W^{(V)}_{(1),i},W^{(U)}_{(1),i}\big]$ and $S_{(1),i}\triangleq\big[S^{(V)}_{(1),i},S^{(U)}_{(1),i}\big]$. According to the previous encoding, we have $W^{(V)}_{(1),i}=\tilde{A}_i\big[\mathcal{C}^{(n)}\big]$ and $W^{(U)}_{(1),i}=\tilde{T}_{(1),i}\big[\mathcal{J}^{(n)}_0\cup\mathcal{J}^{(n)}_1\big]$. Therefore, we define $W_{(1),i}\triangleq\big[W'_{(1),i},W''_{(1),i}\big]$, where $W'_{(1),i}\triangleq\big[W'^{(V)}_{(1),i},W'^{(U)}_{(1),i}\big]$, being $W'^{(V)}_{(1),i}=\tilde{A}_i\big[\mathcal{C}^{(n)}_1\cup\mathcal{C}^{(n)}_{1,2}\big]$ and $W'^{(U)}_{(1),i}=\tilde{T}_{(1),i}\big[\mathcal{J}^{(n)}_1\big]$. Then, $W''_{(1),i}\triangleq\big[W''^{(V)}_{(1),i},W''^{(U)}_{(1),i}\big]$, being $W''^{(V)}_{(1),i}=\tilde{A}_i\big[\mathcal{C}^{(n)}_0\cup\mathcal{C}^{(n)}_2\big]$ and $W''^{(U)}_{(1),i}=\tilde{T}_{(1),i}\big[\mathcal{J}^{(n)}_0\big]$. Recall that, for $i\in[1,L-1]$, an *encrypted* version of $W'_{(1),i+1}$, namely $\bar{\Omega}_{(1),i+1}\triangleq\big[\bar{\Theta}^{(V)}_{i+1},\bar{\Gamma}^{(V)}_{i+1},\bar{\Theta}^{(U)}_{(1),i+1}\big]$, is repeated in $\tilde{R}^n_{(1),i}$. In fact, from $\tilde{A}^n_{i+1}$, recall that sequence $\Delta^{(V)}_{(1),i+1}=\big[\bar{\Theta}^{(V)}_{3,i+1},\bar{\Gamma}^{(V)}_{3,i+1}\big]\subseteq\bar{\Omega}_{(1),i+1}$ is repeated in $\tilde{T}^n_{(1),i}$ but now this dependency appears implicitly. Furthermore, for $i\in[1,L]$ define $\Xi_{(1),i}\triangleq\big[\Psi^{(V)}_i,\Gamma^{(V)}_i,\Pi^{(V)}_{(2),i},\Lambda^{(V)}_i,\Lambda^{(U)}_{(1),i}\big]$, which denotes the entire sequence depending on $\tilde{R}^n_{(1),i}$ that is repeated in $\tilde{R}^n_{(1),i+1}$ if $i\in[1,L-1]$.

Finally, for $i\in[1,L]$ we have $\tilde{T}^n_{(2),i}$ that carries $W_{(2),i}$ and $S_{(2),i}$. For convenience, define $\Xi_{(2),i}\triangleq\big[\Psi^{(U)}_{(2),i},\Lambda^{(U)}_{(2),i}\big]$, which, together with $\bar{O}^{(U)}_{(2),i}$, will be repeated in $\tilde{T}^n_{(2),i+1}$ if $i\in[1,L-1]$.

According to these previous definitions and setting $\kappa_\Omega\triangleq[\kappa^{(V)}_\Theta,\kappa^{(V)}_\Gamma,\kappa^{(U)}_\Theta]$, notice that Figure 5.11 represents a Bayesian graph that describes the dependencies between the variables involved in the PCS of Section 5.2 when it operates to achieve the corner point of $\mathfrak{R}^{(1)}_{\text{MI-WTBC}}$.

Although we have seen that the PCS introduces bidirectional dependencies, we have reformulated the encoding to obtain that they take place forward only. To do so, additionally we regard $\bar{\Omega}_{(1),i}$ as an independent random sequence generated at Block $i-1$ and properly stored in $\tilde{R}^n_{i-1}$. Then, by using κ_Ω, the encoder obtains $W'_{(1),i}$ that is repeated in Block i.

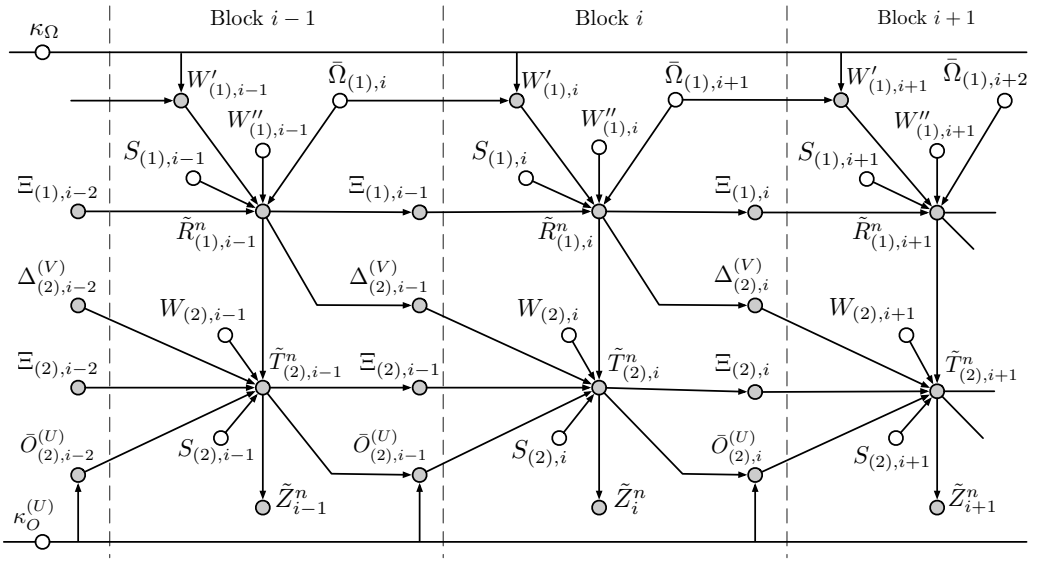

Figure 5.11: Graphical representation (Bayesian graph) of the dependencies between random variables involved in the PCS when it operates to achieve the corner point of $\mathfrak{R}^{(1)}_{\text{MI-WTBC}}$. Independent random variables are indicated by white nodes, whereas those that are dependent are indicated by gray nodes.

The following lemma shows that eavesdropper observations $\tilde{Z}^n_i$ are asymptotically statistically independent of observations $\tilde{Z}^n_{1:i-1}$ from previous blocks.

Lemma 5.3. *For any $i \in [2, L]$ and sufficiently large n, we have*

$$I\big(S_{(1),1:L}S_{(2),1:L}\tilde{Z}^n_{1:i-1}; \tilde{Z}^n_i\big) \leq \delta^{(\mathrm{S})}_n,$$

where $\delta^{(\mathrm{S})}_n$ is defined as in Lemma 5.2.

Proof. See Appendix 5.B. □

Therefore, we obtain

$$\begin{aligned} I\big(S_{(1),1:L}S_{(2),1:L}; \tilde{Z}^n_{1:L}\big) &= I\big(S_{(1),1:L}S_{(2),1:L}; \tilde{Z}^n_1\big) + \sum_{i=2}^{L} I\big(S_{(1),1:L}S_{(2),1:L}; \tilde{Z}^n_i \big| \tilde{Z}^n_{1:i-1}\big) \\ &\overset{(a)}{\leq} I\big(S_{(1),1:L}S_{(2),1:L}; \tilde{Z}^n_1\big) + (L-1)\delta^{(\mathrm{S})}_n \\ &\overset{(b)}{\leq} L\delta^{(\mathrm{S})}_n, \end{aligned}$$

where (a) holds by Lemma 5.3; and (b) holds by independence between $(S_{(1),2:L}S_{(2),2:L})$ and any random variable from Block 1, and from applying Lemma 5.2 to bound $I(S_{(1),1}S_{(2),1};\tilde{Z}_1^n)$.

Thus, for sufficiently large n, the PCS satisfies the strong secrecy condition in (5.2).

Secrecy analysis when polar code operates to achieve the corner point of $\mathfrak{R}^{(2)}_{\text{MI-WTBC}}$

Now, for convenience and with slight abuse of notation, for $i \in [1,L]$ let $\tilde{R}^n_{(2),i} \triangleq \big(\tilde{A}_i^n, \tilde{T}^n_{(2),i}\big)$, which carries $W_{(2),i} \triangleq \big[W^{(V)}_{(2),i}, W^{(U)}_{(2),i}\big]$ and $S_{(2),i} \triangleq \big[S^{(V)}_{(2),i}, S^{(U)}_{(2),i}\big]$. According to the previous encoding, we have $W^{(V)}_{(2),i} = \tilde{A}_i\big[\mathcal{C}^{(n)}\big]$ and $W^{(U)}_{(2),i} = \tilde{T}_{(2),i}\big[\mathcal{J}_0^{(n)} \cup \mathcal{J}_2^{(n)}\big]$. Therefore, we define $W_{(2),i} \triangleq \big[W'_{(2),i}, W''_{(2),i}\big]$, where $W'_{(2),i} \triangleq \big[W'^{(V)}_{(2),i}, W'^{(U)}_{(2),i}\big]$, being $W'^{(V)}_{(2),i} = \tilde{A}_i\big[\mathcal{C}_2^{(n)} \cup \mathcal{C}_{1,2}^{(n)}\big]$ and $W'^{(U)}_{(2),i} = \tilde{T}_{(2),i}\big[\mathcal{J}_2^{(n)}\big]$. Then, $W''_{(2),i} \triangleq \big[W''^{(V)}_{(2),i}, W''^{(U)}_{(2),i}\big]$, being $W''^{(V)}_{(2),i} = \tilde{A}_i\big[\mathcal{C}_0^{(n)} \cup \mathcal{C}_1^{(n)}\big]$ and $W''^{(U)}_{(2),i} = \tilde{T}_{(2),i}\big[\mathcal{J}_0^{(n)}\big]$. Recall that, for $i \in [2,L]$, now an *encrypted* version of $W'_{(2),i-1}$, namely $\bar{\Omega}_{(2),i-1} \triangleq \big[\bar{\Psi}^{(V)}_{i-1}, \bar{\Gamma}^{(V)}_{i-1}, \bar{\Psi}^{(U)}_{(2),i-1}\big]$, is repeated in $\tilde{R}^n_{(2),i}$. Indeed, $\Delta^{(V)}_{(2),i-1} = \big[\bar{\Psi}^{(V)}_{3,i-1}, \bar{\Gamma}^{(V)}_{3,i-1}\big] \subseteq \bar{\Omega}_{(2),i-1}$ is repeated in $\tilde{T}^n_{(2),i}$, and now this dependency appears implicitly.

Recall that, for $i \in [1,L-1]$, $\Pi^{(V)}_{(2),i} = \tilde{A}_i\big[\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)}\big]$, which contains part of $S^{(V)}_{(2),i}$, is repeated in $\tilde{A}_{i+1}\big[\mathcal{R}_{\text{S}}^{(n)}\big]$, while $\Lambda_1^{(V)} = \tilde{A}_1\big[\mathcal{R}_{\Lambda}^{(n)}\big]$, which contains part of $S^{(V)}_{(2),1}$, is replicated in $\tilde{A}_{2:L}\big[\mathcal{R}_{\Lambda}^{(n)}\big]$. For convenience, now we would like to have backward dependencies only. Therefore, we can consider that $S'^{(V)}_{(2),1} = \tilde{A}_1\big[\big(\mathcal{I}^{(n)} \cup \mathcal{G}_1^{(n)}\big) \setminus \big(\mathcal{R}_{\Lambda}^{(n)} \cup \mathcal{R}_{\text{S}}^{(n)}\big)\big]$, for $i \in [2,L-1]$ then $S'^{(V)}_{(2),i} = \tilde{A}_i\big[\big(\mathcal{I}^{(n)} \setminus \mathcal{G}_2^{(n)}\big) \cup \mathcal{R}_{\text{S}}^{(n)}\big]$, and $S'^{(V)}_{(2),L} = \tilde{A}_i\big[\mathcal{I}^{(n)} \cup \mathcal{R}_{\text{S}}^{(n)} \cup \mathcal{R}_{\Lambda}^{(n)}\big]$. Then, for $i \in [2,L]$, we have that $\Pi'^{(V)}_{(2),i} = \tilde{A}_i\big[\mathcal{I}^{(n)} \cap \mathcal{R}_{\text{S}}^{(n)}\big]$ and $\Lambda_i'^{(V)} = \tilde{A}_i\big[\mathcal{R}_{\Lambda}^{(n)}\big]$ are repeated in $\tilde{A}_{i-1}\big[\big(\mathcal{I}^{(n)} \cap \mathcal{G}_2^{(n)}\big) \cup \mathcal{R}_{\Lambda}^{(n)}\big]$. Similarly, we can regard $S'^{(U)}_{(2),1} = \tilde{T}_{(2),1}\big[\mathcal{F}_0^{(n)}\big]$, for $i \in [2,L-1]$ then $S'^{(U)}_{(2),i} = S^{(U)}_{(2),i} = \tilde{T}_{(2),i}\big[\mathcal{F}_0^{(n)} \setminus \big(\mathcal{D}_2^{(n)} \cup \mathcal{L}_2^{(n)} \cup \mathcal{O}_2^{(n)}\big)\big]$, and $S'^{(U)}_{(2),L} = \tilde{T}_{(2),L}\big[\mathcal{F}_0^{(n)} \cup \mathcal{F}_2^{(n)}\big]$. Then, for $i \in [2,L]$, we can consider that $\Lambda'^{(U)}_{(2),i} = \tilde{T}_{(2),i}\big[\mathcal{F}_2^{(n)}\big]$ is repeated in $\tilde{T}_{(2),i-1}\big[\mathcal{F}_2^{(n)}\big]$. Therefore, for $i \in [1,L-1]$ we define $\Xi_{(2),i+1} \triangleq \big[\Theta^{(V)}_{i+1}, \Gamma^{(V)}_{i+1}, \Pi'^{(V)}_{(2),i+1}, \Lambda'^{(V)}_{i+1}, \Lambda'^{(U)}_{(2),i+1}\big]$, which denotes the entire sequence depending on $\tilde{R}^n_{(2),i+1}$ that is repeated in $\tilde{R}^n_{(2),i}$.

Finally, we have $\tilde{T}^n_{(1),i}$ that carries $W_{(1),i}$ and $S_{(1),i}$. Now, for $i \in [1,L-1]$, we regard $S'^{(U)}_{(1),i} = \tilde{T}_{(1),i}\big[\mathcal{Q}_0^{(n)} \setminus \big(\mathcal{N}_1^{(n)} \cup \mathcal{M}_1^{(n)} \cup \mathcal{O}_1^{(n)}\big)\big]$, and $S'^{(U)}_{(1),L} = \tilde{T}_{(1),L}\big[\mathcal{Q}_0^{(n)} \cup \mathcal{Q}_1^{(n)}\big]$. Then, for $i \in [2,L]$ we consider that $\Lambda_i'^{(U)} = \tilde{T}_{(1),i}\big[\mathcal{Q}_1^{(n)}\big]$ is repeated in $\tilde{T}_{(1),i-1}\big[\mathcal{Q}_1^{(n)}\big]$. Thus, we define $\Xi_{(1),i} \triangleq \big[\Theta^{(U)}_{(1),i}, \Lambda'^{(U)}_{(1),i}\big]$, which, together with $\bar{O}^{(U)}_{(1),i}$, will be repeated in $\tilde{T}^n_{(1),i-1}$ if $i \in [2,L]$. Also, define $\ominus^{(V)}_{(1),i} \triangleq \big[\Delta^{(V)}_{(1),i}, \Pi^{(V)}_{(1),i}\big]$, which denotes the part of $\tilde{A}_i^n$ that is repeated in $\tilde{T}^n_{(1),i-1}$.

According to these previous definitions and setting $\kappa_\Omega \triangleq [\kappa^{(V)}_\Psi, \kappa^{(V)}_\Gamma, \kappa^{(U)}_\Psi]$, notice that Figure 5.12 represents a Bayesian graph that describes the dependencies between the variables involved in the PCS of Section 5.2 when it operate to achieve the corner point of $\mathfrak{R}^{(2)}_{\text{MI-WTBC}}$.

In order to obtain that dependencies take place backward only, we regard $\bar{\Omega}_{(2),i}$, for $i \in [2,L]$, as an independent random sequence that is generated at Block $i+1$ and is properly stored in $\tilde{R}^n_{(2),i+1}$. Then, by using κ_Ω, the encoder obtains $W'_{(2),i}$ that is repeated in Block i.

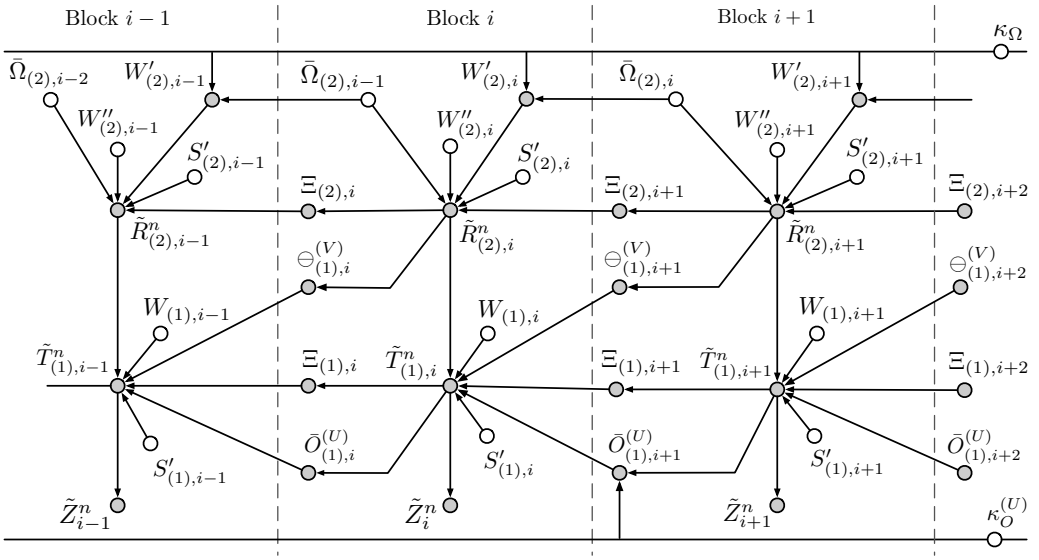

Figure 5.12: Graphical representation (Bayesian graph) of the dependencies between random variables involved in the PCS when it operates to achieve the corner point of $\mathfrak{R}^{(2)}_{\text{MI-WTBC}}$. Independent random variables are indicated by white nodes, whereas those that are dependent are indicated by gray nodes.

The following lemma shows that eavesdropper observations $\tilde{Z}^n_i$ are asymptotically statistically independent of observations $\tilde{Z}^n_{i+1:L}$.

Lemma 5.4. *For any $i \in [1, L-1]$ and sufficiently large n, we have*

$$I\big(S_{(1),1:L}S_{(2),1:L}\tilde{Z}^n_{i+1:L}; \tilde{Z}^n_i\big) \leq \delta^{(\mathrm{S})}_n,$$

where $\delta^{(\mathrm{S})}_n$ is defined as in Lemma 5.2.

Proof. See Appendix 5.C. □

Therefore, we obtain

$$\begin{aligned}
&I\big(S_{(1),1:L}S_{(2),1:L}; \tilde{Z}^n_{1:L}\big) \\
&= I\big(S_{(1),1:L}S_{(2),1:L}; \tilde{Z}^n_L\big) + \sum_{i'=1}^{L-1} I\big(S_{(1),1:L}S_{(2),1:L}; \tilde{Z}^n_{L-i'}\big|\tilde{Z}^n_{L-i'+1:L}\big) \\
&\overset{(a)}{\leq} I\big(S_{(1),1:L}S_{(2),1:L}; \tilde{Z}^n_L\big) + (L-1)\delta^{(\mathrm{S})}_n \\
&\overset{(b)}{\leq} L\delta^{(\mathrm{S})}_n
\end{aligned}$$

where (a) holds by Lemma 5.4; and (b) holds by independence between $(S_{(1),1:L-1}, S_{(2),1:L-1})$ and variables from Block L, and from applying Lemma 5.2 to bound $I(S_{(1),L}S_{(2),L}; \tilde{Z}^n_L)$.

Thus, for sufficiently large n, the PCS satisfies the strong secrecy condition in (5.2).

Remark 5.12. *For $i \in [1, L]$, recall that $O_{(1),i}^{(U)}$ is not generated independently, but drawn by using SC encoding. Hence, if the PCS operates to achieve the corner point of $\mathfrak{R}_{MI\text{-}WTBC}^{(2)}$, we only can obtain a causal Bayesian graph by reformulating the encoding so that dependencies between blocks take place backward only.*

Remark 5.13. *We conjecture that only the secret-key $\kappa_O^{(U)}$ is needed for the PCS to satisfy the strong secrecy condition when operates to achieve any of the corner points. However, the others are required to prove this condition by means of analyzing a causal Bayesian graph.*

5.4 Concluding remarks

A strongly secure PCS has been proposed for the WTBC with two legitimate receivers and one eavesdropper. We have compared two inner-bounds on the achievable region of the MI-WTBC model, where a transmitter wants to send different information (private and confidential) intended for each receiver. Then, we have provided a polar code that achieves the inner-bound that is strictly larger for a particular input distribution. The only difference between the random coding techniques used to characterize the two bounds is the decoding strategy: *joint decoding* in the stronger inner-bound, and *successive decoding* in the other.

Our scheme uses polar-based Marton's coding, which requires three encoding layers: one inner-layer that must be reliably decoded by both receivers, and two outer-layers associated to each legitimate receiver. Due to the non-degradedness assumption of the channel, the encoder builds a chaining construction that induces bidirectional dependencies between adjacent blocks, which need to be taken carefully into account in the secrecy analysis.

In order to achieve the larger inner-bound for a particular distribution, the chaining construction must repeat some elements from the inner-layer to the outer-layers of adjacent blocks, and turns out that this cross-dependency between encoding layers makes the use of *polar-based joint decoding* crucial. As in Chapter 4, the use of a negligible secret-key is required to prove that eavesdropper's observations for different blocks are statistically independent of one another, which is necessary to show that the polar code satisfies the strong secrecy condition. Furthermore, now the PCS needs to use another secret-key that also becomes negligible in terms of rate as the number of blocks grows indefinitely. This key is required to randomize a non-negligible set of elements of one outer-layer that are drawn by means of SC encoding and are needed by the corresponding receiver. In this way, the chaining construction can repeat these elements in adjacent blocks without causing a significant distortion on the input distribution.

Appendix

5.A Proof of Lemma 5.2

For n sufficiently large, we have

$$
\begin{aligned}
&I\big(\tilde{A}_i\big[\mathcal{H}^{(n)}_{V|Z}\big]\tilde{T}_{(k),i}\big[\mathcal{H}^{(n)}_{U_{(k)}|VZ}\big]\tilde{T}_{(\bar{k}),i}\big[\mathcal{H}^{(n)}_{U_{(\bar{k})}|VU_{(k)}Z}\big];\tilde{Z}_i^n\big)\\
&\quad\le \big|\mathcal{H}^{(n)}_{V|Z}\big|+\big|\mathcal{H}^{(n)}_{U_{(k)}|VZ}\big|+\big|\mathcal{H}^{(n)}_{U_{(\bar{k})}|VU_{(k)}Z}\big|\\
&\qquad - H\big(\tilde{A}_i\big[\mathcal{H}^{(n)}_{V|Z}\big]\tilde{T}_{(k),i}\big[\mathcal{H}^{(n)}_{U_{(k)}|VZ}\big]\tilde{T}_{(\bar{k}),i}\big[\mathcal{H}^{(n)}_{U_{(\bar{k})}|VU_{(k)}Z}\big]\big|\tilde{Z}_i^n\big)\\
&\quad\overset{(a)}{\le} \big|\mathcal{H}^{(n)}_{V|Z}\big|+\big|\mathcal{H}^{(n)}_{U_{(k)}|VZ}\big|+\big|\mathcal{H}^{(n)}_{U_{(\bar{k})}|VU_{(k)}Z}\big|\\
&\qquad - H\big(A\big[\mathcal{H}^{(n)}_{V|Z}\big]T_{(k)}\big[\mathcal{H}^{(n)}_{U_{(k)}|VZ}\big]T_{(\bar{k})}\big[\mathcal{H}^{(n)}_{U_{(\bar{k})}|VU_{(k)}Z}\big]\big|Z^n\big)+6n\delta_n^{(*)}-2\delta_n^{(*)}\log\delta_n^{(*)}\\
&\quad\overset{(b)}{\le} 3n\delta_n+6n\delta_n^{(*)}-2\delta_n^{(*)}\log\delta_n^{(*)}
\end{aligned}
$$

where (a) holds by Lemma 2.4 (where $T_{\mathrm{V}}\triangleq 3$ and $T_{\mathrm{O}}\triangleq 1$) and Lemma 5.1; and (b) because

$$
\begin{aligned}
&H\big(A\big[\mathcal{H}^{(n)}_{V|Z}\big]T_{(k)}\big[\mathcal{H}^{(n)}_{U_{(k)}|VZ}\big]T_{(\bar{k})}\big[\mathcal{H}^{(n)}_{U_{(\bar{k})}|VU_{(k)}Z}\big]\big|Z^n\big)\\
&\quad\ge H\big(A\big[\mathcal{H}^{(n)}_{V|Z}\big]\big|Z^n\big)+H\big(T_{(k)}\big[\mathcal{H}^{(n)}_{U_{(k)}|VZ}\big]\big|V^nZ^n\big)+H\big(T_{(\bar{k})}\big[\mathcal{H}^{(n)}_{U_{(\bar{k})}|VU_{(k)}Z}\big]\big|V^nU^n_{(k)}Z^n\big)\\
&\quad\ge \sum_{j\in\mathcal{H}^{(n)}_{V|Z}} H\big(A(j)\big|A^{1:j-1}Z^n\big)+\sum_{j\in\mathcal{H}^{(n)}_{U_{(k)}|VZ}} H\big(T_{(k)}(j)\big|T^{1:j-1}_{(k)}V^nZ^n\big)\\
&\qquad+\sum_{j\in\mathcal{H}^{(n)}_{U_{(\bar{k})}|VU_{(k)}Z}} H\big(T_{(\bar{k})}(j)\big|T^{1:j-1}_{(\bar{k})}V^nT^n_{(k)}Z^n\big)\\
&\quad\ge \big|\mathcal{H}^{(n)}_{V|Z}\big|(1-\delta_n)+\big|\mathcal{H}^{(n)}_{U_{(k)}|VZ}\big|(1-\delta_n)+\big|\mathcal{H}^{(n)}_{U_{(\bar{k})}|VU_{(\bar{k})}Z}\big|(1-\delta_n)
\end{aligned}
$$

where we have used the fact that conditioning does not increase entropy, the invertibility of G_n, and the definition of $\mathcal{H}^{(n)}_{V|Z}$, $\mathcal{H}^{(n)}_{U_{(k)}|VZ}$ and $\mathcal{H}^{(n)}_{U_{(\bar{k})}|VU_{(\bar{k})}Z}$ in (5.9), (5.13) and (5.17) respectively.

5.B Proof of Lemma 5.3

For any $i \in [2, L]$ and sufficiently large n, we have

$$
\begin{aligned}
&I\big(S_{(1),1:L}S_{(2),1:L}\tilde{Z}^n_{1:i-1};\tilde{Z}^n_i\big)\\
&\quad= I\big(S_{(1),1:i}S_{(2),1:i}\tilde{Z}^n_{1:i-1};\tilde{Z}^n_i\big) + I\big(S_{(1),i+1:L}S_{(2),i+i:L};\tilde{Z}^n_i\big|S_{(1),1:i}S_{(2),1:i}\tilde{Z}^n_{1:i-1}\big)\\
&\quad\overset{(a)}{=} I\big(S_{(1),1:i}S_{(2),1:i}\tilde{Z}^n_{1:i-1};\tilde{Z}^n_i\big)\\
&\quad\le I\big(S_{(1),1:i}S_{(2),1:i}\tilde{Z}^n_{1:i-1}\Xi_{(1),i-1}\Delta^{(V)}_{(2),i-1}\Xi_{(2),i-1}\bar{O}^{(U)}_{(2),i-1};\tilde{Z}^n_i\big)\\
&\quad= I\big(S_{(1),i}S_{(2),i}\Xi_{(1),i-1}\Delta^{(V)}_{(2),i-1}\Xi_{(2),i-1}\bar{O}^{(U)}_{(2),i-1};\tilde{Z}^n_i\big)\\
&\qquad+ I\big(S_{(1),1:i-1}S_{(2),1:i-1}\tilde{Z}^n_{1:i-1};\tilde{Z}^n_i\big|S_{(1),i}S_{(2),i}\Xi_{(1),i-1}\Delta^{(V)}_{(2),i-1}\Xi_{(2),i-1}\bar{O}^{(U)}_{(2),i-1}\big)\\
&\quad\overset{(b)}{\le} \delta^{(\mathrm{S})}_n + I\big(S_{(1),1:i-1}S_{(2),1:i-1}\tilde{Z}^n_{1:i-1};\tilde{Z}^n_i\big|S_{(1),i}S_{(2),i}\Xi_{(1),i-1}\Delta^{(V)}_{(2),i-1}\Xi_{(2),i-1}\bar{O}^{(U)}_{(2),i-1}\big)\\
&\quad\overset{(c)}{=} \delta^{(\mathrm{S})}_n + I\big(S_{(1),1:i-1}S_{(2),1:i-1}\tilde{Z}^n_{1:i-1};\tilde{Z}^n_i\big|\mathsf{B}_{i-1}\big)\\
&\quad\le \delta^{(\mathrm{S})}_n + I\big(S_{(1),1:i-1}S_{(2),1:i-1}\tilde{Z}^n_{1:i-1};\tilde{Z}^n_iW'_{(1),i}\big|\mathsf{B}_{i-1}\big)\\
&\quad= \delta^{(\mathrm{S})}_n + I\big(S_{(1),1:i-1}S_{(2),1:i-1}\tilde{Z}^n_{1:i-1};W'_{(1),i}\big|\mathsf{B}_{i-1}\big)\\
&\qquad+ I\big(S_{(1),1:i-1}S_{(2),1:i-1}\tilde{Z}^n_{1:i-1};\tilde{Z}^n_i\big|\mathsf{B}_{i-1}W'_{(1),i}\big)\\
&\quad\overset{(d)}{=} \delta^{(\mathrm{S})}_n + I\big(S_{(1),1:i-1}S_{(2),1:i-1}\tilde{Z}^n_{1:i-1};W'_{(1),i}\big|\mathsf{B}_{i-1}\big)\\
&\quad\le \delta^{(\mathrm{S})}_n + I\big(\tilde{R}_{(1),1:i-1}S_{(2),1:i-1};\tilde{Z}^n_{1:i-1}W'_{(1),i}\big|\mathsf{B}_{i-1}\big)\\
&\quad= \delta^{(\mathrm{S})}_n + I\big(\tilde{R}_{(1),1:i-1}S_{(2),1:i-1};W'_{(1),i}\big|\mathsf{B}_{i-1}\big) + I\big(\tilde{Z}^n_{1:i-1};W'_{(1),i}\big|\mathsf{B}_{i-1}\tilde{R}_{(1),1:i-1}S_{(2),1:i-1}\big)\\
&\quad\overset{(e)}{=} \delta^{(\mathrm{S})}_n + I\big(\tilde{R}_{(1),1:i-1}S_{(2),1:i-1};W'_{(1),i}\big|\mathsf{B}_{i-1}\big)\\
&\quad= \delta^{(\mathrm{S})}_n + I\big(\tilde{R}_{(1),1:i-1}S_{(2),1:i-1};\bar{\Omega}_{(1),i}\oplus\kappa^{(V)}_{\Omega}\big|\mathsf{B}_{i-1}\big)\\
&\quad\overset{(f)}{=} \delta^{(\mathrm{S})}_n
\end{aligned}
$$

where (a) holds by independence between $(S_{(1),i+1:L}, S_{(2),i+1:L})$ and any random variable from Blocks 1 to i; (b) holds by Lemma 5.2 because, according to Section 5.2, we have

$$
\begin{aligned}
&\big[S_{(1),i}S_{(2),i}\Xi_{(1),i-1}\Delta^{(V)}_{(2),i-1}\Xi_{(2),i-1}\bar{O}^{(U)}_{(2),i-1}\big]\\
&\qquad= \big[\tilde{A}_i\big[\mathcal{H}^{(n)}_{V|Z}\big]\tilde{T}_{(1),i}\big[\mathcal{H}^{(n)}_{U_{(1)}|VZ}\big]\tilde{T}_{(2),i}\big[\mathcal{H}^{(n)}_{U_{(2)}|VU_{(1)}Z}\big]\big];
\end{aligned}
$$

in (c) we have defined $\mathsf{B}_{i-1} \triangleq \big[S_{(1),i}S_{(2),i}\Xi_{(1),i-1}\Delta^{(V)}_{(2),i-1}\Xi_{(2),i-1}\bar{O}^{(U)}_{(2),i-1}\big]$; (d) follows from applying d-separation [Pea09] over the Bayesian graph in Figure 5.11 to obtain that $\tilde{Z}^n_i$ and $(S_{(1),1:i-1}S_{(2),1:i-1}\tilde{Z}^n_{1:i-1})$ are conditionally independent given $\big(\mathsf{B}_{i-1}, W'_{(1),i}\big)$; (e) also follows from applying *d-separation* to obtain that $W'_{(1),i}$ and $\tilde{Z}^n_{1:i-1}$ are conditionally independent given $(\mathsf{B}_{i-1}, \tilde{R}_{(1),1:i-1}, S_{(2),1:i-1})$; and (f) holds because $\bar{\Omega}^{(V)}_{(1),i}$ is independent of B_{i-1}, $S_{(2),1:i-1}$ and any random variable from Block 1 to $(i-2)$, and because from applying crypto-lemma [G.D03] we obtain that $\bar{\Omega}^{(V)}_{(1),i} \oplus \kappa^{(V)}_{\Omega}$ is independent of $\tilde{R}^n_{(1),i-1}$.

5.C Proof of Lemma 5.4

For any $i \in [2, L]$ and sufficiently large n, we have

$$
\begin{aligned}
&I\big(S_{(1),1:L}S_{(2),1:L}\tilde{Z}^n_{i+1:L};\tilde{Z}^n_i\big)\\
&\quad= I\big(S'_{(1),1:L}S'_{(2),1:L}\tilde{Z}^n_{i+1:L};\tilde{Z}^n_i\big)\\
&\quad= I\big(S'_{(1),i:L}S'_{(2),i:L}\tilde{Z}^n_{i+1:L};\tilde{Z}^n_i\big) + I\big(S'_{(1),1:i-1}S'_{(2),1:i-1};\tilde{Z}^n_i\big|S'_{(1),i:L}S'_{(2),i:L}\tilde{Z}^n_{i+1:L}\big)\\
&\quad\overset{(a)}{=} I\big(S'_{(1),i:L}S'_{(2),i:L}\tilde{Z}^n_{i+1:L};\tilde{Z}^n_i\big)\\
&\quad\le I\big(S'_{(1),i:L}S'_{(2),i:L}\tilde{Z}^n_{i+1:L}\Xi_{(2),i+1}\ominus^{(V)}_{(1),i+1}\Xi_{(1),i+1}\bar{O}^{(U)}_{(1),i+1};\tilde{Z}^n_i\big)\\
&\quad= I\big(S'_{(1),i}S'_{(2),i}\Xi_{(2),i+1}\ominus^{(V)}_{(1),i+1}\Xi_{(1),i+1}\bar{O}^{(U)}_{(1),i+1};\tilde{Z}^n_i\big)\\
&\qquad+ I\big(S'_{(1),i+1:L}S'_{(2),i+1:L}\tilde{Z}^n_{i+1:L};\tilde{Z}^n_i\big|S'_{(1),i}S'_{(2),i}\Xi_{(2),i+1}\ominus^{(V)}_{(1),i+1}\Xi_{(1),i+1}\bar{O}^{(U)}_{(1),i+1}\big)\\
&\quad\overset{(b)}{\le} \delta^{(\mathrm{S})}_n + I\big(S'_{(1),i+1:L}S'_{(2),i+1:L}\tilde{Z}^n_{i+1:L};\tilde{Z}^n_i\big|S'_{(1),i}S'_{(2),i}\Xi_{(2),i+1}\ominus^{(V)}_{(1),i+1}\Xi_{(1),i+1}\bar{O}^{(U)}_{(1),i+1}\big)\\
&\quad\overset{(c)}{=} \delta^{(\mathrm{S})}_n + I\big(S'_{(1),i+1:L}S'_{(2),i+1:L}\tilde{Z}^n_{i+1:L};\tilde{Z}^n_i\big|\mathsf{B}_{i+1}\big)\\
&\quad\le \delta^{(\mathrm{S})}_n + I\big(S'_{(1),i+1:L}S'_{(2),i+1:L}\tilde{Z}^n_{i+1:L};\tilde{Z}^n_iW'_{(2),i}\big|\mathsf{B}_{i+1}\big)\\
&\quad= \delta^{(\mathrm{S})}_n + I\big(S'_{(1),i+1:L}S'_{(2),i+1:L}\tilde{Z}^n_{i+1:L};W'_{(2),i}\big|\mathsf{B}_{i+1}\big)\\
&\qquad+ I\big(S'_{(1),i+1:L}S'_{(2),i+1:L}\tilde{Z}^n_{i+1:L};\tilde{Z}^n_i\big|\mathsf{B}_{i+1}W'_{(2),i}\big)\\
&\quad\overset{(d)}{=} \delta^{(\mathrm{S})}_n + I\big(S'_{(1),i+1:L}S'_{(2),i+1:L}\tilde{Z}^n_{i+1:L};W'_{(2),i}\big|\mathsf{B}_{i+1}\big)\\
&\quad\le \delta^{(\mathrm{S})}_n + I\big(\tilde{R}_{(2),i+1:L}S'_{(1),i+1:L}\tilde{Z}^n_{i+1:L};W'_{(2),i}\big|\mathsf{B}_{i+1}\big)\\
&\quad= \delta^{(\mathrm{S})}_n + I\big(\tilde{R}_{(2),i+1:L}S'_{(1),i+1:L};W'_{(2),i}\big|\mathsf{B}_{i+1}\big) + I\big(\tilde{Z}^n_{i+1:L};W'_{(2),i}\big|\mathsf{B}_{i+1}\tilde{R}_{(2),i+1:L}S'_{(1),i+1:L}\big)\\
&\quad\overset{(e)}{=} \delta^{(\mathrm{S})}_n + I\big(\tilde{R}_{(2),i+1:L}S'_{(1),i+1:L};W'_{(2),i}\big|\mathsf{B}_{i+1}\big)\\
&\quad= \delta^{(\mathrm{S})}_n + I\big(\tilde{R}_{(2),i+1:L}S'_{(1),i+1:L};\bar{\Omega}_{(2),i}\oplus\kappa_{\Omega}\big|\mathsf{B}_{i+1}\big)\\
&\quad\overset{(f)}{=} \delta^{(\mathrm{S})}_n
\end{aligned}
$$

where (a) holds by independence between $(S'_{(1),1:i-1}, S'_{(2),1:i-1})$ and any random variable from Blocks i to L; (b) holds by Lemma 5.2 because

$$\begin{aligned}&\big[S'_{(1),i}S'_{(2),i}\Xi_{(2),i+1}\ominus^{(V)}_{(1),i+1}, \Xi_{(1),i+1}\bar{O}^{(U)}_{(1),i+1}\big]\\ &\quad= \big[\tilde{A}_i\big[\mathcal{H}^{(n)}_{V|Z}\big]\tilde{T}_{(2),i}\big[\mathcal{H}^{(n)}_{U_{(2)}|VZ}\big]\tilde{T}_{(1),i}\big[\mathcal{H}^{(n)}_{U_{(1)}|VU_{(2)}Z}\big]\big];\end{aligned}$$

in (c) we have defined $\mathsf{B}_{i+1} \triangleq \big[S'_{(1),i}S'_{(2),i}\Xi_{(2),i+1}\ominus^{(V)}_{(1),i+1}, \Xi_{(1),i+1}\bar{O}^{(U)}_{(1),i+1}\big]$; (d) follows from applying d-separation [Pea09] over the Bayesian graph in Figure 5.12 to obtain that $\tilde{Z}^n_i$ and $(S'_{(1),i+1:L}S'_{(2),i+1:L}\tilde{Z}^n_{i+1:L})$ are conditionally independent given $\big(\mathsf{B}_{i+1}, W'_{(2),i}\big)$; (e) also follows from applying *d-separation* to obtain that $W'_{(2),i}$ and $\tilde{Z}^n_{i+1:L}$ are conditionally independent given $(\mathsf{B}_{i+1}, \tilde{R}_{(2),i+1:L}, S'_{(1),i+1:L})$; and (f) holds because $\bar{\Omega}^{(V)}_{(2),i}$ is independent of B_{i+1}, $S_{(1),1:i-1}$ and any random variable from Block $i+2$ to L, and because from applying crypto-lemma [G.D03] we obtain that $\bar{\Omega}^{(V)}_{(2),i} \oplus \kappa^{(V)}_{\Omega}$ is independent of $\tilde{R}^n_{(2),i+1}$.

6

Conclusion and final remarks

In this thesis we have presented and analyzed polar coding schemes for different channel models over the wiretap broadcast channel. This channel is characterized by one transmitter that wishes to send confidential (and non-confidential) information to different legitimate receivers in the presence of eavesdroppers. Besides reliability, all the channel models considered in this dissertation impose the polar coding scheme to satisfy the strong secrecy condition, which is an information-theoretic security condition that requires asymptotically independence between the confidential information transmitted over the channel and the eavesdropper's observations. In the following, we summarize the main contributions of this thesis and propose possible directions for future work.

In Chapter 2, we have revisited the fundamental theorems of polar codes and their application for different channel models from the viewpoint of source polarization. Specifically, we have seen the source polarization theorem, which states that the elements of a random vector can be divided into two disjoint sets after applying the polar transform: one which contains practically all the randomness, and another one that is almost deterministic. However, there is a negligible (in terms of rate) set of elements that have not polarized, that is, neither are practically random nor deterministic. This theorem is crucial for source coding because, given the *random elements*, one can reliably reconstruct the entire vector by performing successive cancellation decoding. Furthermore, for those models where the broadcast channel is degraded, we have seen that the subset property of the polarized elements is important. Otherwise, if the broadcast channel is non-degraded, the subset property does not hold and, therefore, we must consider that transmission takes place over several blocks and a chaining

construction that allows different receivers to decode their corresponding messages reliably and confidentially. In channel coding, the polar-based encoder must construct codewords whose joint distribution matches with the one used for the polar code construction. In this sense, in the last part of this chapter we provided a generic polar-based encoding for multi-user settings that satisfies the previous requirement making use of a randomness which is asymptotically negligible in terms of rate.

In Chapter 3, we described two different polar coding schemes for two different settings over the degraded wiretap broadcast channel, where a transmitter wishes to send confidential information to an arbitrary number of receivers with the presence of an arbitrary number of eavesdroppers. In these models, a layered decoding structure requires receivers with better channel quality to reliably decode more messages, and a layered secrecy structure requires eavesdroppers with worse channel quality to be kept ignorant of more messages. The degradedness condition of the broadcast channel allows to avoid any chaining construction, and the polar coding scheme is able to satisfy the reliability and secrecy condition in one single block. Furthermore, in this chapter we proposed practical methods for the construction of polar codes under reliability and secrecy constraints. Although we focused in particular settings, our methods can be extended to any channel model with secrecy constraints. Indeed, as far as we know, this is the first time that the secrecy performance of a polar coding scheme has been evaluated in terms of an information-theoretic security measure.

In Chapter 4, we described a polar coding scheme for a model over the general wiretap broadcast channel, were the transmitter wishes to send confidential (and non-confidential) information to two legitimate receivers in the presence of one eavesdropper. We do not make any assumption regarding the degraded nature of the broadcast channel, which implies building a chaining construction to achieve the best-known inner bound on the achievable region of this model. This chaining construction in the encoding introduces bidirectional dependencies between blocks. Consequently, a secret key with negligible size in terms of rate is necessary to represent all these dependencies by means of a causal Bayesian graph that allows us proving that the polar code satisfies the strong secrecy condition.

Finally, in Chapter 5 we extended the results of the previous chapter by considering a model over the wiretap broadcast channel in which the transmitter sends different confidential (and non-confidential) information to each legitimate receiver in the presence of one eavesdropper. We proposed a polar coding scheme that achieves the best-known inner-bound on the achievable region of this model. In the proposed scheme, the encoding uses polar-based Marton's coding where one inner-layer must be reliably decoded by both legitimate receivers, and each receiver must decode its own corresponding outer-layer. Due to the non-degradedness condition of the broadcast channel, the encoder builds a chaining construction

that induces bidirectional dependencies between adjacent blocks. Indeed, we showed that these dependencies can occur between different encoding layers of different blocks. As in Chapter 4, the use of a negligible secret-key (in terms of rate) is required to prove that the polar code satisfies the strong secrecy condition. Moreover, now we need another secret-key that incurs a negligible rate penalty to ensure that the joint distribution induced by the encoder is close to the one used for the code construction, which is crucial for the reliability and secrecy performance of the coding scheme.

Despite polar codes look promising for forthcoming communication scenarios requiring information-theoretic security, some questions remain open and need to be addressed in the future:

1. In Chapter 2 we provided a generic polar-based encoder that minimizes the amount of randomness required at the transmitter. Nevertheless, how to completely remove all the random decisions is a problem that remains open. Specifically, this random decisions are needed for the elements that have not polarized. Unfortunately, the behavior of these elements after applying the polar transform is still not properly understood.

2. The need for additional secret transmissions. The polar coding scheme of Chapter 3 must separately send those elements that are not uniformly distributed and are required by the corresponding receivers to reliably decode the information. Despite the size of this additional transmission becomes negligible in terms of rate when the blocklength grows to infinity, it may be a drawback in practical scenarios. Again, notice that it is the set of elements that have not polarized the one that is problematic.

   On the other hand, the polar coding schemes described in Chapter 4 and Chapter 5 must separately send those non-uniformly distributed elements that are required by the corresponding receivers of each encoding block. Moreover, in these coding schemes the chaining construction requires an additional transmission of a non-negligible set of elements (with respect to the blocklength) that are needed to initialize the decoding algorithms. Indeed, when we consider the transmission taking place over several blocks, it may be possible to convey those non-uniformly distributed elements by means of the chaining construction as long as we use an additional secret-key that randomizes them. Hence, part of the elements that previously contained confidential information could be used to convey the randomized version of these problematic elements without causing significant distortion. Since they are negligible in terms of rate with respect to the blocklength, the polar coding schemes will still approach the capacity asymptotically. However, notice that this means having to use another secret-key.

3. The need for secret-keys. Despite the length of the secret-keys required by the polar coding schemes described in this dissertation are asymptotically negligible in terms of rate, their use may seem contradictory in the context of keyless secret communication. We must distinguish three different uses of these secret-keys. First, they may be required to send the previous additional transmissions confidentially to the corresponding receivers (one-time pad encryption). Second, in Chapter 4 and Chapter 5 we have described polar coding schemes that induce bidirectional dependencies between blocks, and secret-keys are required to prove statistical independence between eavesdropper's observations of each block and, hence, to prove that the polar coding scheme satisfy the corresponding strong secrecy condition. Third, due to the polar-based Marton's coding, the polar coding scheme of Chapter 5 needs to repeat some elements that are drawn by means of successive cancellation decoding. However, in order to introduce insignificant distortion, only a randomized version of these elements can be repeated.

   Regarding the use of secret-keys to prove statistical independence between eavesdropper's observations, we have conjectured indeed that they may not be necessary for this purpose. Nevertheless, without using these secret-keys, probably one should evaluate the information leakage differently. The following example may help to understand why we use them and why we conjecture that they may not be necessary.

   Consider the Bayesian network of Figure 6.1. Clearly, random variables W_1 and W_2 make Z_1 and Z_2 dependent. Moreover, we assume that $I(W_1;Z_2) \leq \epsilon_n$ and $I(W_2;Z_1) \leq \epsilon_n$, where $\epsilon_n \xrightarrow{n\to\infty} 0$. Notice that this Bayesian graph may be an oversimplification of the bidirectional dependencies induced by the polar coding schemes of Chapter 4 and Chapter 5, where W_1 and W_2 may denote private messages that are stored in *non-confidential* elements corresponding to Block 1 and Block 2 respectively, and part of these elements are properly repeated in *confidential* positions of the other block. We would like to show that Z_1 and Z_2 are asymptotically independent, and we obtain

$$\begin{aligned} I(Z_1;Z_2) &\leq I(Z_1W_1;Z_2) \\ &\leq \epsilon_n + I(Z_1;Z_2|W_1) \\ &\leq \epsilon_n + I(Z_1;W_2Z_2|W_1) \\ &\leq \epsilon_n + I(W_2;Z_1|W_1). \end{aligned}$$

   where the last inequality holds because $I(Z_1;Z_2|W_1W_2) = 0$ by applying *d-separation*. Although $I(W_2;Z_1) \leq \epsilon_n$, we are not able to upper-bound $I(W_2;Z_1|W_1)$ and, consequently, we are not able to prove asymptotic independence between Z_1 and Z_2.

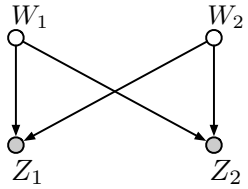

Figure 6.1: Bayesian graph that represents an oversimplification of the dependencies between random variables involved in the polar coding schemes of Chapter 4 and Chapter 5.

In fact, if only W_1 is repeated in *confidential* positions of Block 2, or only W_2 is repeated in *confidential* positions of Block 1, we would have $I(Z_1; Z_2|W_1) = 0$ or $I(Z_1; Z_2|W_2) = 0$, respectively. Hence, despite it seems reasonable to expect that Z_1 and Z_2 are independent, we are not able to found an upper-bound on $I(Z_1; Z_2)$.

4. Practical aspects of the coding schemes. Despite in Chapter 3 we proposed practical methods for constructing polar coding schemes for models with secrecy constraints, further work still remains to be done in this direction. For instance, it seems important to find tighter bounds on the information-theoretic measures that we have used to construct *good* polar codes. Moreover, notice that the chaining construction of the polar coding schemes described in Chapter 4 and Chapter 5 implies a large memory capacity requirement at either the transmitter or one of the receivers side. For instance, consider that the encoder sends the codeword corresponding to each block as soon as it is constructed. Then, in the proposed coding schemes, Receiver 1 can start the decoding after receiving the corresponding observations of each block but Receiver 2 must await the observations of the last block.

Bibliography

[Ari09] Erdal Arikan. Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. *IEEE Transactions on Information Theory*, 55(7):3051–3073, 2009.

[Ari10] Erdal Arikan. Source polarization. In *IEEE International Symposium on Information Theory (ISIT)*, pages 899–903, 2010.

[BB11] Matthieu Bloch and Joao Barros. *Physical-layer security: from information theory to security engineering*. Cambridge University Press, 2011.

[BP15] M. Benammar and P. Piantanida. Secrecy capacity region of some classes of wiretap broadcast channels. *IEEE Transactions on Information Theory*, 61(10):5564–5582, Oct 2015.

[CB15] R. A. Chou and M. R. Bloch. Using deterministic decisions for low-entropy bits in the encoding and decoding of polar codes. In *2015 53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 1380–1385, Sept 2015.

[CB16] R. A. Chou and M. R. Bloch. Polar coding for the broadcast channel with confidential messages: A random binning analogy. *IEEE Transactions on Information Theory*, 62(5):2410–2429, May 2016.

[CEG12] Yeow-Khiang Chia and Abbas El Gamal. Three-receiver broadcast channels with common and confidential messages. *IEEE Transactions on Information Theory*, 58(5):2748–2765, 2012.

[CK78] I. Csiszár and J. Körner. Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 24(3):339–348, May 1978.

[CK11] Imre Csiszar and János Körner. *Information theory: coding theorems for discrete memoryless systems*. Cambridge University Press, 2011.

[CT12] Thomas M Cover and Joy A Thomas. *Elements of information theory*. John Wiley & Sons, 2012.

[CY18] R. A. Chou and A. Yener. Polar coding for the multiple access wiretap channel via rate-splitting and cooperative jamming. *IEEE Transactions on Information Theory*, 64(12):7903–7921, Dec 2018.

[EU09] Ersen Ekrem and Sennur Ulukus. Secrecy capacity of a class of broadcast channels with an eavesdropper. *EURASIP Journal on Wireless Communications and Networking*, pages 1:1–1:29, March 2009.

[EU13] E. Ekrem and S. Ulukus. Multi-receiver wiretap channel with public and confidential messages. *IEEE Transactions on Information Theory*, 59(4):2165–2177, April 2013.

[GAG15] N. Goela, E. Abbe, and M. Gastpar. Polar codes for broadcast channels. *IEEE Transactions on Information Theory*, 61(2):758–782, Feb 2015.

[GB17] T. C. Gulcu and A. Barg. Achieving secrecy capacity of the wiretap channel and broadcast channel with a confidential component. *IEEE Transactions on Information Theory*, 63(2):1311–1324, Feb 2017.

[G.D03] Jr. G.D.Forney. On the role of mmse estimation in approaching the information-theoretic limits of linear gaussian channels: Shannon meets wiener. In *41st Annual Allerton Conference on Communication, Control, and Computing*, Oct 2003.

[HU14] S.H. Hassani and R. Urbanke. Universal polar codes. In *2014 IEEE International Symposium on Information Theory (ISIT)*, pages 1451–1455, June 2014.

[HY13] J. Honda and H. Yamamoto. Polar coding without alphabet extension for asymmetric models. *IEEE Transactions on Information Theory*, 59(12):7829–7838, Dec 2013.

[KT10] M. Karzand and E. Telatar. Polar codes for q-ary source coding. In *2010 IEEE International Symposium on Information Theory*, pages 909–912, June 2010.

[KU10] Satish Babu Korada and Rüdiger L Urbanke. Polar codes are optimal for lossy source coding. *IEEE Transactions on Information Theory*, 56(4):1751–1768, 2010.

[LLPS14] Y. Liang, L. Lai, H. V. Poor, and S. Shamai. A broadcast approach for fading wiretap channels. *IEEE Transactions on Information Theory*, 60(2):842–858, Feb 2014.

[LPW09] David Asher Levin, Yuval Peres, and Elizabeth Lee Wilmer. *Markov chains and mixing times*. American Mathematical Soc., 2009.

[Mar79] K. Marton. A coding theorem for the discrete memoryless broadcast channel. *IEEE Transactions on Information Theory*, 25(3):306–311, May 1979.

[MHSU15] M. Mondelli, S.H. Hassani, I. Sason, and R.L. Urbanke. Achieving Marton's region for broadcast channels using polar codes. *IEEE Transactions on Information Theory*, 61(2):783–800, Feb 2015.

[MUH14] Marco Mondelli, Rüdiger Urbanke, and S Hamed Hassani. How to achieve the capacity of asymmetric channels. In *2014 52nd Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 789–796. IEEE, 2014.

[MV11] H. Mahdavifar and A. Vardy. Achieving the secrecy capacity of wiretap channels using polar codes. *IEEE Transactions on Information Theory*, 57(10):6428–6443, Oct 2011.

[MW00] Ueli Maurer and Stefan Wolf. Information-theoretic key agreement: From weak to strong secrecy for free. In *Advances in Cryptology—EUROCRYPT 2000*, pages 351–368. Springer, 2000.

[Pea09] Judea Pearl. *Causality*. Cambridge university press, 2009.

[RRS13] Joseph M Renes, Renato Renner, and David Sutter. Efficient one-way secret-key agreement and private channel coding via polarization. In *Advances in Cryptology-ASIACRYPT*, pages 194–213. Springer, 2013.

[ŞTA09] Eren Şasoğlu, Emre Telatar, and Erdal Arikan. Polarization for arbitrary discrete memoryless channels. In *IEEE Information Theory Workshop.*, pages 144–148, 2009.

[SV13] E. Sasoglu and A. Vardy. A new polar coding scheme for strong security on wiretap channels. In *IEEE International Symposium on Information Theory Proceedings (ISIT)*, pages 1117–1121, July 2013.

[TV13] Ido Tal and Alexander Vardy. How to construct polar codes. *IEEE Transactions on Information Theory*, 59(10):6562–6582, 2013.

[VVH15] Harish Vangala, Emanuele Viterbo, and Yi Hong. A comparative study of polar code constructions for the AWGN channel. *arXiv preprint arXiv:1501.02473*, 2015.

[WO15] Shun Watanabe and Yasutada Oohama. The optimal use of rate-limited randomness in broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 61(2):983–995, 2015.

[WU16] Y. Wei and S. Ulukus. Polar coding for the general wiretap channel with extensions to multiuser scenarios. *IEEE Journal on Selected Areas in Communications*, 34(2):278–291, Feb 2016.

[Wyn75] A.D. Wyner. The wire-tap channel. *The Bell System Technical Journal*, 54(8):1355–1387, Oct 1975.

[XC08] Jin Xu and Biao Chen. Broadcast confidential and public messages. In *2008 42nd Annual Conference on Information Sciences and Systems*, pages 630–635. IEEE, 2008.

[ZLL+15] Shaofeng Zou, Yingbin Liang, Lifeng Lai, H.V. Poor, and S. Shamai. Broadcast networks with layered decoding and layered secrecy: Theory and applications. *Proceedings of the IEEE*, 103(10):1841–1856, Oct 2015.