Institut
de Ciències
Fotòniques

Entanglement and Quantum Cryptography

Joonwoo Bae

Barcelona, January, 2007

Universitat de Barcelona

Departament d'Estructura i Constituents de la Matèria

UNIVERSITAT DE BARCELONA

Tesis presentada para optar al grado de doctor, January 2007.

Programa de doctorado: **Física Avanzada.** *Bienio:* **2003-2005.**

Thesis advisor: **Dr. Antonio Acín Dal Maschio**(Assistant Professor in ICFO and ICREA Junior)

Dear friend,
I pray that you may enjoy good health
And that all may go well with you,
Even as your soul is getting along well.

Acknowledgement

I am grateful to all the people who helped me throughout my education. My advisor, Antonio Acín, has patiently guided me with his creative insights. In particular, many thanks for his kind care and ceaseless encouragement. He allowed me to have the journey in quantum information when I was just a beginner, and I am grateful for his clear, ideaful, and well-motivated explanations. I thank Ignacio Cirac who allowed me to join Barcelona quantum information. Also, thanks for the opportunity to visit MPQ. I thank José Ignacio Latorre for his kind support as my university tutor.

I would also like to thank collaborators, Maciej Lewenstein, Anna Sanpera, Emili Bagan, Ramon Muñoz-Tapia, Maria Baig, Lluis Masanes, Ujjwal Sen, Aditi Sen De, and Sofyan Iblisdir. I have enjoyed attending discussions; these helped me improve immensely. Many thanks go to Nicolas Gisin, Sofyan Iblisdir, Renato Renner, Andreas Buchleitner, Anna Sanpera, Maciej Lewenstein, and Ramon Muñoz-Tapia, for being on the thesis committee.

I am very grateful for the people who assisted me while I was traveling as well. Many thanks go to Andreas Buchleitner and Florian Mintert duing my visit to the MPI-PKS; especially for their discussions and hospitality. Leong Chuan Kwek kindly invited me to Singapore and gave me opportunities to interact with people there. Many thanks to Leong Chuan Kwek, and the members of the group for discussions and hospitality: Dagomir Kaszlikowski, Berthold-Georg Englert, Artur Ekert, Tzu-Chieh Wei, Thomas Durt, Wee Kang Chua, Darwin Gosal. In 2006, many thanks to Sangchul Oh because he recommended me to pass a conference in my home country. Also, thanks to Jaewan Kim for inviting me, and also to Hyunchul Nha and Jaewon Lee for their hospitality and discussions. Many thanks go to Yoonho Kim for inviting me to his group and for all his hospitality.

Muchas gracias a mi grupo: Miguel Navascués, Artur Garcia, Mafalda Almeida, Daniel Cavalcanti, y también Alessandro Ferraro y Stefano Pironio. I am very grateful to have the opportunity to interact with them, and appreciate all their kind help.

I would like to thank some people for the discussions: Toby Cubitt, Norbert Lutkenhaus, Barbara Kraus, and Joseph Renes. I would like to thank Giacomo Mauro D'Ariano for selecting my proposed open problem in the arrangement at MPI-PKS, and many thanks go to Reinhard Werner for sug-

감사의 글

Please, neither Chinese nor Japanese, this is Korean(Coreà, Coreano, Coréen, Koreanisch,...), meaning **acknowledgement**. Thanks!

gesting it be included in the open problem list on his website. Thanks to Marco Piani, Rafal Demkowicz-Dobrzanski, Leandro Aolita, Giulio Chiribella, and Oriol Romero-Isart for the discussions as well.

I would like to thank the former and the present Icfonians: Lluis Torner, who founded the institute; the secretaries, who kindly take care of my things; and my Ph.D friends.

In particular I would like to express a deep gratitude to Yuan Liang Lim, friend in faith, for sharing his soul, and also for kindly explaining his work. I would like to thank Younghun Kwon for his kind advice and support each time I returned to Korea. I would like to thank people in my church: pastors (the Jang and the Yun families), the Ko family, the Jeon family, and the Cho family, for their loving care and help during my stay in Barcelona. Thanks to Charis and Ashley for correcting my English.

Last but not least, my deep gratitude goes to Seeun Kim and my family for their heartful support, encouragement, and love; nothing can even compare to it. And to God, who loves me and so kindly guides me; he is always my strength and my foundation. *I can do everything through him, who gives me strength. (NIV)*

Abstract

Quantum cryptography is one of the most important quantum information applications. The present thesis covers several topics on quantum cryptography, such as the security analysis of quantum channels for key distribution protocols and the study of quantum cloning.

First, we introduce a general formalism to characterize the cryptographic properties of quantum channels in the realistic scenario where the two honest parties employ prepare and measure protocols and the known two-way communication reconciliation techniques. We derive a necessary and sufficient condition to distill a secret key using this type of schemes for arbitrary bipartite quantum systems of finite dimension. The obtained results suggest that there may exist weakly entangling channels useless for key distribution using prepare and measure schemes.

Next, we consider Gaussian states and Gaussian operations for cryptographic tasks and derive a new security condition. As it happens for quantum systems of finite dimension, our results suggest that there may also exist weakly entangled Gaussian states useless for key distribution, using Gaussian operations.

Finally, we study the connection between cloning and state estimation. It was a long-standing problem to show whether state estimation becomes equivalent to quantum cloning in the asymptotic limit of an infinite number of clones. The equivalence is proven here using two known results in quantum information theory, the monogamy of quantum states and the properties of entanglement-breaking channels.

Thesis Publications

The thesis is based on the following publications:

- J. Bae and A. Acín, *Key distillation from quantum channels using two-way communication protocols*, Physical Review A **75** 012334 (2007)
- J. Bae and A. Acín, *Asymptotic quantum cloning is state estimation*, Physical Review Letters **97** 030402 (2006)
- A. Acín, J. Bae, E. Bagan, M. Baig, Ll. Masanes and R. Muñoz-Tapia, *Secrecy properties of quantum channels*, Physical Review A **73** 012327 (2006)
- M. Navascués, J. Bae, J. I. Cirac, M. Lewestein, A. Sanpera and A. Acín, *Key distillation from Gaussian states by Gaussian operations*, Physical Review Letters **94** 010502 (2005)

Resumen

La teoría cuántica describe la física de sistemas microscópicos. Describiendo la física de la pequeña escala, explota un formalismo diferente al utilizado por la física clásica, ya que las cantidades observables en teoría cuántica no conmutan. Esto conduce a que la realidad física es no determinista, y deriva en resultados antiintuitivos. Una de las características peculiares de la teoría cuántica es la correlación presente en sistemas cuánticos, el *entanglement*.

Desde hace una década, la teoría de la información cuántica ha empezado a reconocer la importancia de considerar el punto de vista informático-teórico en la teoría cuántica. El mejor ejemplo que ilustra la teoría de la información cuántica puede ser la teleportación cuántica, un protocolo para transmitir un estado cuántico a una distancia arbitraria, y el algoritmo de factorización cuántico, que soluciona el problema de la factorización [1] en tiempo polinómico. De hecho, resulta que el *entanglement* permite a la teoría de la información cuántica superar al correspondiente clásico. Muchas investigaciones importantes en teoría de la información cuántica se realizan teórica y experimentalmente, y afectan hoy en día otras áreas de investigación en física.

Uno de los principales usos, asi como logros, de la teoría de la información cuántica es la criptografía cuántica, *i.e.* la distribución cuántica de claves, que distribuye una clave secreta mediante estados cuánticos y procesado clásico, ambas tecnologías actualmente factibles. Recientemente, ésta tecnología ha abierto un nuevo mercado en la criptografía. La actual tesis sigue la línea del desarrollo reciente en teoría de la información cuántica, estudiando el papel del *entanglement* en escenarios criptográficos cuánticos: nuevo análisis de seguridad de los canales cuánticos para los escenarios criptográficos, posibilidad de aplicar estados gausianos en los escenarios de distribucion de claves, y la prueba de equivalencia entre la *clonación* asintótica cuántica y la *estimación* del estado.

[1] Clásicamente el problema se considera muy duro, en el sentido que puede no ser generalmente soluble en tiempo polinómico.

0.1 Introducción

Esta tesis cubre diversos aspectos de la criptografía cuántica, principalmente nuevas condiciones de seguridad y el estudio de la *clonacion* cuántica. La tesis demuestra condiciones de seguridad que indican si una clave secreta se puede destilar de un canal cuántico dado, que puede ser un canal de un *qubit*, un canal de un *qudit*, o un canal gausiano. Esta condición prueba la seguridad de protocolos ya conocidos tales como el protocolo BB84 [8]. La estimación y la clonación de estados cuánticos aparece naturalmente en el contexto de un escenario criptográfico con presencia de un espía, y se ha conjeturado la equivalencia entre la clonación asintótica cuántica y la estimación. La tesis prueba esta conjetura realizada hace muchos años, demostrando que son de hecho equivalentes.

0.2 Motivación

0.2.1 *Key distillation* de canales cuánticos

Los métodos criptográficos existentes que utilizan recursos clásicos basan su seguridad en asunciones técnicas relativas al espia, llamado a menudo Eve, capacidades tales como potencia de cálculo finita o memoria limitada [70]. Contrariamente a todos estos esquemas, las pruebas de la seguridad de protocolos de distribucion cuántica (QKD[2]), e.g. el protocolo BB84 [8], no se apoyan en ninguna asunción sobre las capacidades de Eve: se basan simplemente en el hecho de que Eve, asi como los dispositivos de los participantes, son governados por las leyes cuánticas [43]. Las características cuánticas, tales como la *monogamia* de las correlaciones cuánticas (*entanglement*) o la imposibilidad de la clonación perfecta del estado [91], hacen QKD seguro. Controlando el canal, Eve introduciría errores y modificaría las correlaciones cuánticas previstas entre los participantes, Alice y Bob. La cantidad de estos errores se puede estimar usando la discusión pública, así que los participantes honestos pueden juzgar si su canal cuántico se puede utilizar para QKD seguro, o abortan una transmisión probada insegura.

El problema estándar en pruebas de seguridad es determinar el *critical quantum bit error rate* (QBER) en el canal tal que la destilación de claves es posible con técnicas uni o bidireccionales de destilación usando el protocolo BB84. Sin embargo, parece significativo identificar y cuantificar las características criptográficas de un canal cuántico por sí mismo, independientemente de cualquier protocolo QKD predeterminado. De hecho, esto está más cercano a lo que sucede en realidad, donde está fijado el canal que conecta a Alice y Bob. Por lo tanto, después de estimar características de

[2] La terminologiá QKD viene de su expresión inglesa, Quantum Key Distribution, que significa distribución de una clave secreta usando los protocolos que aplican estados cuánticos.

un canal cuántico dado, los dos participantes deben diseñar el protocolo que se adapta mejor a los parámetros estimados del canal. En este sentido, es bien sabido que ningn QKD seguro puede ser establecido usando canales *entanglement-breaking* [42, 28], mientras que la detección del *entanglement* garantiza ya la presencia de una cierta forma de correlación [3]. Más allá de estos dos resultados, poco se sabe sobre que características del canal són necesarias y/o suficientes para QKD seguro.

0.2.2 *Key distillation* en un escenario gausiano

Desde que la teleportación cuántica fue implementada en experimentos con dos estados *squeezed*, se ha dedicado una cantidad significativa de trabajo a desarrollar la teoría de la información cuántica para variables continuas. Recientemente, muchos conceptos introducidos en sistemas de variables discretas se traducen a los sistemas de variables continuas. En estos sistemas, los estados gausianos y las operaciones gausianas desempeñan el papel dominante. Aparecen naturalmente en experimentos y pueden ser manipulados con la tecnología actual de óptica cuántica.

Un resultado negativo importante en el contexto de las variables continuas es que los estados gausianos no se pueden destilar mediante operaciones gausianas [38, 33]. Aunque se sabe que todos los estados gausianos con transposición parcial no positiva son destilables [37], cualquier protocolo de destilación debe incluir una operación no gausiana que resulta ser muy compleja desde el punto de vista experimental. Esto puede ser reformulado como *todos los estados mezcla* entangled *están* bound-entangled *en un escenario gausiano*. Sin embargo, estos estados pueden todavía ser útiles en el régimen gausiano, puesto que los *bits secretos* pueden ser extraídos de ellos usando operaciones locales gausianas y comunicación clásica.

0.2.3 Estimación y clonación asintótica de estados

Es sabido que la clonación cuántica perfecta y la estimación perfecta de un estado cuántico son operaciones imposibles. Son también los ingredientes que hacen QKD seguro. La imposibilidad de la estimación perfecta de un estado cuántico es una consecuencia importante de la no ortogonalidad de los estados cuánticos: *el estado del un solo sistema cuántico no se puede medir perfectamente*. Así, cualquier medida en el nivel de una única copia proporciona solamente información parcial. El teorema de la no clonación, una de las piedras angulares de la teoría de la información cuántica, representa otra de las consecuencias de la no ortogonalidad de los estados cuánticos. Prueba que dado un sistema cuántico en un estado desconocido, es imposible diseñar un dispositivo produciendo dos copias idénticas.

De hecho, estos dos conceptos estan muy relacionados. Por un lado, si la valoración perfecta del estado fuera posible, uno podría utilizarla para preparar cualquier número de copias de un estado dado, únicamente realizando la medida y la preparación. Por otra parte, si la clonación perfecta fuera posible, uno podría estimar perfectamente el estado desconocido de un sistema cuántico preparándose infinitas copias de él y midiéndolas. Más allá de estas discusiones cualitativas, la conexión entre la estimación del estado y la clonación fueron consolidadas por su equivalencia en el límite asintótico, es decir el proceso óptimo de clonación cuando $N \to \infty$ [39, 15]: la clonación asintótica es equivalente a la estimación del estado. Realmente, esto se prueba para dos casos, clonación universal [3] [15] y clonación *phase-covariant* [4] [17]. La validez de la equivalencia de la clonación asintótica y la estimación del estado ha sido identificada como uno de los problemas abiertos de la teoría de la información cuántica [5].

0.3 Protocolos realistas de *Key Distillation*

Existen gran cantidad de protocolos QKD en la literatura. Aquí, restringimos nuestras consideraciones a lo que llamamos los protocolos realistas, conocidos como protocolos de *preparacion y medida*, donde Alice prepara y envía estados de una base elegida a Bob, que mide en otra (posiblemente diferente) base. Esto establece algunas correlaciones clásicas entre los dos participantes. Por supuesto este proceso por si solo es claramente inseguro, ya que Eve podría aplicar una estrategia de intercepción y reenvio en la misma base que la preparación del estado de Alice, adquiriendo completa información sin ser detectado. Por lo tanto, cada cierto tiempo, Alice y Bob deben cambiar su preparación y medidas del estado para supervisar el canal y poder excluir esta posibilidad. Alice y Bob anuncian estos símbolos para extraer la información sobre su canal, así que estos casos no contribuyen a la tasa de transmisión final. Estos símbolos son de hecho consumidos en el proceso tomográfico mencionado previamente. Sin embargo, en el límite de secuencias grandes, la fracción de los casos donde Alice y Bob supervisan el canal se puede hacer insignificante en comparación con la longitud de la clave, pero aún así suficiente para tener una descripción fiel de algunos parámetros del canal, tales como el QBER. Los estados enviados por Alice serán transformados en un estado mezcla debido a la interacción de Eve. Esta decoherencia producirá errores en los valores de la medida obtenidos por Bob. El análisis de seguridad tiene como objetivo determinar si la decoherencia observada en el canal es bastante pequeña para permitir a Alice y a Bob que destilen una clave secreta. Llamamos a estos protocolos realistas en el sentido que no implican operaciones cuánticas experimentalmente difíciles, tales como medidas coherentes, memorias cuánticas o la generación

[3] El estado inicial consiste en estados puros aleatoriamente elegidos.

[4] El estado inicial yace en el ecuador de la esfera de Bloch.

[5] Ver el problema 22 de la lista del problemas abiertos en [57].

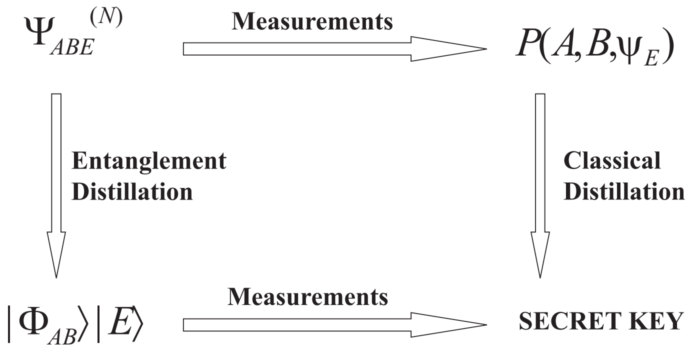

Figure 1: Una llave secreta se puede destilar bien por la destilación del *entanglement* más una medida (un proceso costoso), o por la medida más el procesado clásico, que es actualmente factible.

de partículas *entangled*. El establecimiento de correlaciones es realizado generando estados de un qubit y midiéndolos en dos o más bases. Además, uno podría pensar en incluir una medida de filtración de una sola copia en el lado de Bob. Esta operación es más dificil que una medida proyectiva estándar, pero aún factible con la tecnologia actual [58].

Esquema basado en el *entanglement*

El panorama antes descrito se puede explicar en un escenario equivalente basado en el *entanglement* [9], que resulta ser mucho más conveniente para el análisis teórico. En el esquema basado en el *entanglement*, la codificación de la información de Alice es substituida generando y midiendo la mitad de un estado máximamente *entangled*. Es decir, Alice primero genera localmente un estado máximamente *entangled* de dos qubits y envía la mitad de éste a Bob a travs del canal. Un estado mezcla ρ_{ab} es entonces compartido por los dos participantes, debido a la interacción con el ambiente controlado por Eve. Ahora, Alice y Bob miden en dos bases para mapear sus correlaciones cuánticas en correlaciones clásicas. Por ejemplo, si Alice y Bob miden en las bases computacionales, el QBER resulta simplemente

$$\epsilon_{AB} = \langle 01|\rho_{AB}|01\rangle + \langle 10|\rho_{AB}|10\rangle.$$

Puede ser impuesto que el estado local de Alice no pueda ser modificado por Eve, puesto que la partícula correspondiente nunca sale del laboratorio de Alice, que se asume seguro. Denotamos aquí estas *single-copy measurement plus classical processing* como SIMCAP [2]. Debe quedar claro que las técnicas de [9] implican la equivalencia entre los protocolos de SIMCAP

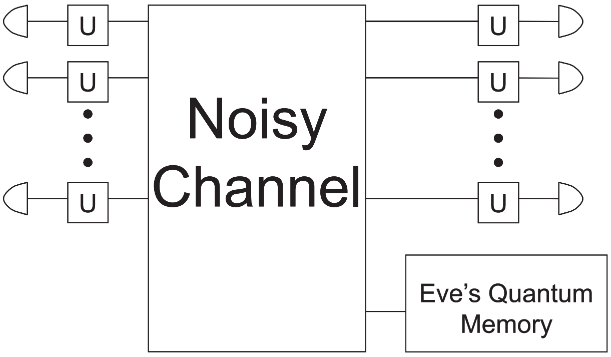

Figure 2: Un estado puro tripartito es preparado por Eve, que envía dos de las partículas a Alice y Bob y conserva una. Del punto de vista de Alice y de Bob la situación se asemeja a un canal estándar con ruido. Los participantes realizan medidas al nivel de una sola copia, posiblemente con un cierto proceso de filtración preliminar. Eve guarda sus estados cuánticos y puede retrasar arbitrariamente su medida colectiva.

en estados *entangled* y esquemas de preparacion-medida de QKD: la distribución de las correlaciones es, desde el punto de vista de la seguridad, idéntico. Se pierde esta equivalencia, por ejemplo, si uno considera los protocolos de destilación del *entanglement* para QKD, donde las partículas son medidas por los participantes después de aplicar operaciones cuánticas coherentes.

0.3.1 *Key Distillation* clásica

Después de la distribución de las correlaciones, bien usando protocolos de preparacion-medida o protocolos SIMCAP, Alice y Bob comparten correlaciones parcialmente secretas que se destilarán en la clave perfecta. El problema de destilar correlaciones con ruido y parcialmente secretas en una clave secreta no se ha resuelto totalmente. Recientemente, límites inferiores generales a la *secret-key rate* que usa comunicación unidireccional se han obtenido en [31]. En el caso de que las correlaciones sean demasiado ruidosas para el uso directo de las técnicas unidireccionales de destilación, Alice y Bob pueden aplicar antes un protocolo usando comunicación bidireccional. Las correlaciones obtenidas después de este proceso bidireccional pueden convertirse en destilables utilizando protocolos unidireccionales. Mucho menos se sabe sobre la destilación de claves usando comunicación bidireccional. Aquí aplicamos principalmente el protocolo de comunicación bidireccional estándar introducido por Maurer en [69], también conocido como *classical advantage distillation* (CAD). De hecho, analizamos los siguientes dos protocolos CAD ligeramente distintos:

- *CAD1.* Alice y Bob comparten una lista de bits correlacionados. Alice selecciona N de sus bits que tengan el mismo valor y anuncia públicamente la posición de estos símbolos. Bob comprueba si sus símbolos correspondientes son también iguales. Si éste es el caso, Bob anuncia a Alice que él acepta, así que utilizan los valores de la medida (son todos iguales) de un bit para la nueva lista. Si no, rechazan los N valores y comienzan otra vez el proceso con otro bloque.

- *CAD2.* Alice localmente genera un bit aleatorio s. Toma un bloque de N de sus bits, A, y computa el vector
$$X = (X_1, \cdots, X_N) \tag{1}$$
tal que $A_i + X_i = s$. Introduce entonces el nuevo bloque X a través del canal público y clásicamente autentificado. Después de recibir X, Bob lo aade a su correspondiente bloque, $B + X$, y acepta cualquier valor que resulte ser igual. Si no, los símbolos son descartados y el proceso se inicia de nuevo, como antes.

Estos protocolos son equivalentes en criptografía clásica y en el escenario general totalmente cuántico.

0.3.2 Estrategias de Espionaje

Una vez descritas las operaciones que efectúan Alice y Bob, consideraremos los ataques de Eve. Supondremos que Eve tiene la capacidad de controlar todo el entorno, esto es, que toda la información que se pierde a lo largo del canal que une a Alice y a Bob va a parar a Eve. Dicho de otro modo, toda la decoherencia que observan Alice y Bob procede de la interacción de Eve con el canal cuántico. De acuerdo con [4], las estrategias de espionaje se pueden clasificar en tres tipos: (i) individual, (ii) collectiva y (iii) coherente. De nuevo, a pesar de que la mayor parte de la discusión que sigue se presenta en el enfoque basado en el entanglement, las conclusiones también son aplicables al enfoque basado en preparar y medir.

Ataques individuales

En un ataque individual, se asume que Eve aplica la misma interacción a cada estado, sin introducir correlaciones entre las copias, y mide su estado justo después de esta interacción. En este tipo de ataques, las tres partes miden inmediatamente sus estados, ya que se supone que ninguno de ellos tiene la habidad de almacenar estados cuánticos. Por ello, acaban compartiendo correlaciones del tipo clásico-clásico-clásico[6], descritos por una distribución

[6] A lo largo del capítulo, denotaremos las variables clásicas y cuánticas por C y Q, respectivamente. Al escribir las correlaciones entre las tres partes, el order es Alice-Bob-Eve. Por ejmeplo, CCQ significa que Alice y Bob tienen valores clásicos correlacionados (tras unas medidas), mientras que Eve tiene un estado cuántico.

de probabilidad $P(A, B, E)$. En este caso, los resultados estándar de Teoría de la INformación Clásica no se pueden aplicar directamente. Por ejemplo, es sabido que la tasa de generación de claves secretas usando comunicación unidireccional, $K_{\rightarrow}$, está acotada por la llamada cota de Csiszár-Körner [27],

$$K_{\rightarrow} \geq I(A : B) - I(A : E). \tag{2}$$

Aquí $I(A : B)$ es la información mutua entre los resultados de las medidas de A y B. En este tipo de ataques, la interacción de Eve se puede ver como un tipo de clonación asimétrica [20] que produce dos copias aproximadas diferentes, una para Bob y otra para ella. Esta transformación tiene la forma $U_{BE} : |\Phi^+\rangle_{AB}|E\rangle \rightarrow |\Psi\rangle_{ABE}$, donde $\rho_{AB} = \mathrm{tr}_E|\Psi\rangle\langle\Psi|_{ABE}$. Se ha demostrado que, en el caso de dos qubits, dos partes honestas son capaces de destilar una clave secreta segura frente a todo tipo de ataque individual siempre que el estado cuántico ρ_{AB} esté entangled [2].

Está claro que una prueba de seguridad frente ataques individuales no es satisfactoria desde el punto de vista teórico. Sin embargo, creemos que dicha prueba es relevante cuando consideramos espías realistas. Supongamos que la memoria cuántica de Eve presenta una tasa de decoherencia distinta de core y que las dos partes honestas son capaces de estimarla. Entonces podrían introducir un retraso entre la distribución de estados y el proceso de destilación suficientemente largo como para evitar que Eve conservara sin errores sus estados almacenados. Eve se vería, pues, forzada a medir sus estados antes de la reconciliación, al igual que en los ataques individuales.

Ataques colectivos

Los ataques colectivos representan, en principio, un paso intermedio entre los individuales y el ataque más general. De nuevo, asumimos que Eve aplica la misma interacción a cada estado cuántico, pero esta vez tiene memoria cuántica. En otras palabras, puede esperar hasta el final del proceso de reconciliación y adaptar su medida de acuerdo con la información pública intercambiada por Alice y Bob. Después de un ataque colectivo, las dos partes honestas comparten N copias independientes del mismo estado, $\rho_{AB}^{\otimes N}$, y no hay correlación entre copia y copia. Si pérdida de generalidad, el estado completo de las tres partes se puede tomar como $|\psi\rangle_{ABE}^{\otimes N}$, donde

$$|\psi\rangle_{ABE} = (I_A \otimes U_{BE})|\Phi^+\rangle_{AB}|E\rangle. \tag{3}$$

Tras un ataque colectivo y las medidas de Alice y Bob, las tres partes comparten correlaciones de tipo clásico-clásico-cuántico, descritas por un estado

$$\sum_{a,b} |a\rangle\langle a| \otimes |b\rangle\langle b| \otimes |e_{ab}\rangle\langle_{ab}|, \tag{4}$$

donde a y b denotan los resultados de las medidas de Alice y Bob asociados a los proyectores $|a\rangle\langle a|$ y $|b\rangle\langle b|$. Nótese que $|e_{ab}\rangle$ no está normalizado, pues $|e_{ab}\rangle = \langle ab|\psi\rangle_{ABE}$ y $p\,(a, b) = \mathrm{tr}[|e_{ab}\rangle\langle e_{ab}|]$.

El siguiente resultado, obtenido en [31, 63], es ampliamente usado en escenaros realistas de distribución de claves. Tras un ataque colectivo descrito por un estado (4), la tasa de destilación de clave secreta alcanzable a través de protoclos de comunicación unidireccionales satisface

$$K_{\rightarrow} \geq I(A : B) - I(A : E). \tag{5}$$

Aquí, las correlaciones entre las variables clásicas de Alice y Bob se hallan de nuevo cuantificadas por la información mutua $I(A : B)$. Las correlacioens entre las variabels clásicas de Alice y las cuánticas de Eve, A y E, están cuantificadas por la cota de Holevo,

$$I(A : E) = S(E) - S(E|A), \tag{6}$$

donde S denota la entropía de von Neumann, por lo que $S(E) = S(\rho_E)$ y $S(E|A) = \sum_a p\,(a) S(\rho_E|A = a)$. De hecho, la "misma" ecuación (5) se aplica cuando Bib es también capaz de almacenar estados cuánticos y las tres partes comparten correlacioens de tipo clasico-cuántico-cuántico (CQQ). En este caso, las dos medidas de la información que comparten la variable clásica de Alice A y cada uno de los estados cuánticos de Bob e Eve, que se denotan B y E, deberían ser cuantificadas a través de las correspondientes cotas de Holevo [31]. Obsérvense las similaridades entre (2) y (5). De hecho, las cotas que se obtienen son una generalización natural del la cota de C-K en los escenarios CCQ y CQQ.

Ataques generales y el teorema de de Finetti

Aquí Uno debe considerar el ataque más general cuando Eve lleva a cabo cualquier tipo de interacción. En este caso, Alice y bob no pueden asumir que comparten N copias del mismo estado cuántico. Al contrario que en los ataques previos, hasta hace bien poco no existían buenas cotas para la tasa de generación de clave secreta que fueran válidas ante ataques genéricos. Sin embargo, recientemente se obtuvo una dramática simplificación del análisis de seguridad de los protocolos de QKD bajo ataques generales gracias al llamado teorema de de Finetti [78]. De hecho, Renner ha demostrado que los ataques generales no pueden ser más poderosos que los ataques colectivos en ningún protocolo que sea simétrico en el el uso del canal cuántico. Esto permite simplificar enormemente las pruebas de seguridad, puesto que gracias a argumentos de tipo de Finetti (ver [78] para más detalles), Alice y Bob pueden asumir con seguridad que comparten N copias de un estado cuántico consistente con su proceso tomográfico, y después aplicar las cotas existentes para este escenario. Nótese que el teorema de de Finetti podría ser empleado también si uno quiere aplicar destilación cuántica de entanglement como técnica para obtener una clave secreta. En lo que sigue, por tanto, podemos restringir nuestro análisis al caso de ataques colectivos sin subestimar las habilidades de Eve.

0.4 Condiciones para la destilación cuántica en canales cuánticos de variables discretas

Analizamos las propiedades criptográficas de los canales cuánticos cuando Alice y Bob emplean estrategias de QKD donde (i) la distribución de correlaciones se lleva a cabo usando estrategias de preparación y medida (ii) el proceso de destilación de claves usa los protocolos clásicos estándar de comuinicación unidireccinal y bidireccional. De hecho, éstas son las técnicas actualmente empleadas en cualquier implementación realista de QKD. También supondremos que previamente las dos partes honestas llevarán a cabo operaciones de filtrado, que transformarán el estado que comparten en un estado diagonal en la base de Bell,

$$\rho_{AB} = \lambda_1|\Phi_1\rangle\langle\Phi_1| + \lambda_2|\Phi_2\rangle\langle\Phi_2| + \lambda_3|\Phi_3\rangle\langle\Phi_3| + \lambda_4|\Phi_4\rangle\langle\Phi_4|, \tag{7}$$

donde $\sum_j \lambda_j = 1$, $\lambda_j > 0$, y

$$\begin{aligned}
|\Phi_1\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
|\Phi_2\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\
|\Phi_3\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\
|\Phi_4\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)
\end{aligned} \tag{8}$$

Primeramente derivamos la condición de seguridad para estos canales de qubits, mejorando el análisis de seguridad estándar. Dado que los ataques colectivos son tan poderosos como los ataques generales [78], consideramos ataques colectivos y obtenemos la siguiente condición de seguridad general

$$|\langle e_{0,0}|e_{1,1}\rangle|^2 > \frac{\epsilon_{AB}}{1-\epsilon_{AB}}. \tag{9}$$

O lo que es más preciso: si esta consición se satisface, Alice y Bob siempre pueden generar una clave secreta de una longitud N larga, pero finita. La eq. (9) se puede reescribir como

$$(\lambda_1 + \lambda_2)(\lambda_3 + \lambda_4) < (\lambda_1 - \lambda_2)^2. \tag{10}$$

Esta condición es, de hecho, necesaria y suficiente para garantizar privacidad. Por lo que sabemos, ésta es la primera condición estricta para la seguridad del protocolo. Aplicamos esta condición a los protocolos estándar BB84 y six-state protocol, y determinamos los valores críticos de QBER 20% y 27.6%, respectivamente.

A continuación, exploramos varias posibilidades para mejorar las cotas de seguridad obtenidas, i) preprocesamiento de la información por una de las partes, ii) preprocesamiento de la información por las dos aprtes, iii) operaciones cuánticas coherentes por una de las partes. Curiosamente, todas estas alternativas fracasan lo cual sugiere la existencia de estados entangled que no permiten destilar una clave secreta en protocolos generales realistas.

A continuación consideramos escenarios de destilación de claves realistas en sistemas cuánticos de mayor dimensión, llamados *qudits*, y extendemos los resultados a canales de qudits diagonalizables en la base de estados de Bell generalizados. En este escenario multidimensional, Alice prepara el estado de Bell generalizado

$$|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |k\rangle|k\rangle, \tag{11}$$

y la generalización de los operadores de error viene dada por los operadores unitarios $U_{m,n} = \sum_{k=0}^{d-1} \exp(\frac{2\pi i}{d} kn)|k+m\rangle\langle k|$. Por tanto, un sistema cuántico en un estado ρ propagándose a través de un canal de Pauli generalizado se ve afectado por la acción de $U_{m,n}$ con probabilidad $p_{m,n}$. Esto implica que el estado resultante es diagonal en la base de los estados de Bell,

$$(\mathbb{1} \otimes D)(\Phi) = \sum_{m=0}^{d-1} \sum_{n=0}^{d-1} p_{m,n} |B_{m,n}\rangle\langle B_{m,n}|, \tag{12}$$

donde los estados $|B_{m,n}\rangle$ definen la base de Bell generalizada $|B_{m,n}\rangle = (\mathbb{1} \otimes U_{m,n})|\Phi\rangle$. En este escenario, tenemos que

$$F \quad = \quad \sum_{k=0}^{d-1} \langle kk|\rho_{AB}|kk\rangle = \sum_{n} p_{0,n}.$$

De manera similar al caso de los qubits, introducimos una medida de distorsión para los $d-1$ errores posibles. Denotemos el resultado de la medida de Alice por α. Entonces, Bob obtiene $\alpha + j$, con probabilidad

$$D_j = \sum_{\alpha=0}^{d-1} P(A = \alpha, B = \alpha + j) = \sum_{n=0}^{d-1} p_{j,n}.$$

La distorsión total se define como $D = \sum_{j \neq 0} D_j$. Por supuesto, $D_0 = F$. Obsérvese que todos los D_j se pueden tomar más pequeños que F, sin pérdida de generalidad. De hecho, si éste no fuera el caso, las dos partes honestas podrían aplicar operacioens locales $U_{m,n}$ para hacer la fidelidad F mayor que cualquier otro D_j. Nótese también que los errores presentan diferentes probabilidades D_j.

Seguidamente obtenemos la condición de seguridad total para QKD en canales de qudits

$$\max_{k\neq k'} |\langle e_{k,k}|e_{k',k'}\rangle|^2 > \max_j \frac{D_j}{F}, \tag{13}$$

donde

$$\begin{aligned} |e_{\alpha,\alpha}\rangle &= \frac{1}{\sqrt{F}} \sum_{n=0}^{d-1} c_{0,n} e^{\frac{2\pi i}{d}\alpha n} |0, n\rangle \\ |e_{\alpha,\beta}\rangle &= \frac{1}{\sqrt{D_{\beta-\alpha}}} \sum_{n=0}^{d-1} c_{\beta-\alpha,n} e^{\frac{2\pi i}{d}\alpha n} |\beta - \alpha, n\rangle \end{aligned} \tag{14}$$

donde el álgebra es módulo d y $\beta \neq \alpha$. La condición de seguridad obtenida resulta ser óptima para los llamados protocolos de $d+1$ bases y dos bases que aparecen en la referencia [21].

0.5 Destilación de claves a partir de estados gausianos mediante operaciones gausianas

A continuación consideramos el escenario criptográfico anteriormente definido cuando los estados cuánticos son estados gausianos y restringimos a Alice y a Bob a aplicar operaciones gausianas y analizamos las propiedades de privacidad del canal cuántico. Dado que todos los estados gausianos de tipo NPPT pueden ser transformados en estados simétricos entangled de dos modos mediante operacioens locales gausianas y comunicación clásica (GLOCC), restringimos nuestro análisis a este tipo de estados. Equivalentemente, uno puede pensar que el primer paso en el protocolo de destilación es la transformación de tipo GLOCC de [37] que transforma cualquier estado NPPT en un estado gausiano NPPT de dos modos [37], cuya matriz de covarianza tiene la forma

$$\gamma_A = \gamma_B = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \qquad C = \begin{pmatrix} c_x & 0 \\ 0 & -c_p \end{pmatrix} \tag{15}$$

donde $\lambda \geq 0$ y $c_x \geq c_p \geq 0$. La condición para que este estado sea físico, i.e., $\rho \geq 0$ es que $\lambda^2 - c_x c_p - 1 \geq \lambda(c_x - c_p)$, mientras que la condición de entanglement (que en este caso es equivalente a la condición NPPT) es

$$\lambda^2 + c_x c_p - 1 < \lambda(c_x + c_p). \tag{16}$$

Seguidamente, ambas partes miden la cuadratura X, donde X_A y X_B denotan los operadores medidos; y x_A y x_B, los resultados de cada medida. Alice y Bob somunican públicamente los valores $|x_A|, |x_A|$, y sólo dan por válidos aquellos casos en que $|x_A| = |x_B| = x_0$. Cada parte asocia el valor lógico 0 (1) a un resultado positivo (negativo). Este proceso transforma el estado cuántico en una lista de parejas de bits clásicos correlacionados (i, j). La probabilidad de error de Alice y Bob, esto es, la probabilidad de que sus símbolos no coincidan, viene dada por

$$\epsilon_{AB} = \frac{\sum_{i \neq j} p\,(i, j)}{\sum_{i,j} p\,(i, j)} = \frac{1}{1 + \exp\left(\frac{4c_x x_0^2}{\lambda^2 - c_x^2}\right)}. \tag{17}$$

Entonces Alice y Bob ejecutan CAD para establecer una clave secreta.

Seguimos los mismos pasos que antes. Primero estudiamos la seguridad de nuestro protocolo cuando Eve aplica un ataque individual, lo cual muestra que todos los estados gausianos que pierden su positividad tras la transposición parcial (NPPT) son seguros. Tal como se muestra en [2], el error de Eve en la estimación de bit final b está acotado por abajo por un término proporcional a $|\langle e_{++}|e_{--}\rangle|^N$, que, en este escenario gausiano viene dado por

$$|\langle e_{++}|e_{--}\rangle|^2 = \exp\left(-\frac{4(\lambda^2 + \lambda(c_x - c_p) - c_x c_p - 1)x_0^2}{\lambda + c_x}\right). \tag{18}$$

De este modo, Alice y Bob establecerán una clave secreta si

$$\frac{\epsilon_{AB}}{1 - \epsilon_{AB}} < |\langle e_{++}|e_{--}\rangle|. \tag{19}$$

Más exactamente, si esta condición se cumple, existe un N finito tal que se puede destilar una clave secreta a partir de la nueva lista de símbolos usando protocolos de comunicación unidireccionales [27]. Esto se indica en la figura (3).

Ahora consideramos ataques generales y calculamos (9), como se ve en la figura (3). Los resultados muestran que nuestra prueba de seguridad deja de funcionar para algunos estados NPPT. Esto sugiere la existencia de estados gaussianos poco entangled de los cuales no se puede extraer un clave secreta mediande operaciones gausianas.

0.6 Equivalencia entre clonación asintótica y estimación de estados

Mostramos la equivalencia entre la clonación asintótica y la estimación de estados para cualquier distribución inicial de estados puros, demostrando

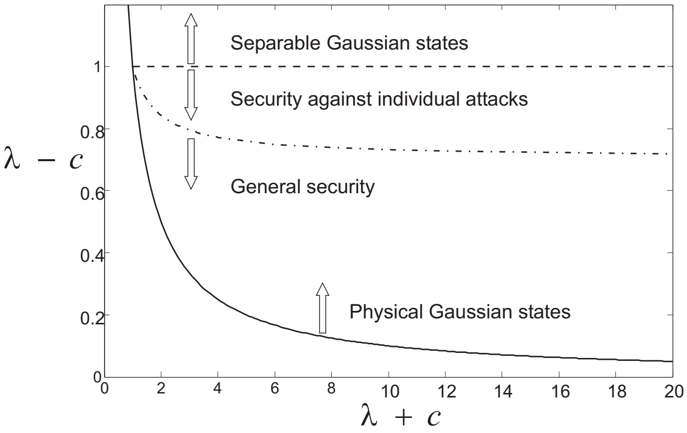

Figure 3: Análisis de seguridad de estados gausianos simétricos de 1 × 1 modos cuando $c_x = c_p = c$. Todos los estados físicos están sobre la línea de abajo. La línea de más arriba define el límite del entanglement, que coincide con la cota de seguridad frente a ataques individuales. Los estados por debajo de la línea del medio son seguros frente a cualquier ataque. Esta condición de seguridad general es más fuerte que el límite del entanglement, lo cual puede implicar la existencia de estados gausianos levemente entangled inútiles para la destilación de claves.

que *la clonación asintótica realmente se corresponde con la estimación de estados*. Clonar M estados entrantes a N salientes se denota como $M \to N$. Cuando $N \to \infty$, lo llamamos clonación asintótica.

La prueba se basa en dos resultados conocidos de la teoría de la información cuántica: la monogamia de las correlaciones cuánticas y las propiedades de los canales destructores de entanglement. El entanglement es, de hecho, un recurso de naturaleza monógama, en el sentido en que no puede ser arbitrariamente compartido. Uno de los resultados más fuertes en esta dirección fue obtenido por Werner en 1989 [89]. Éste mostró que los únicos estados que pueden ser arbitrariamente compartidos son los estados separables. Recuérdese que un estado cuántico bipartito ρ_{AC} en $\mathbb{C}^d \otimes \mathbb{C}^d$ se dice N-compartible cuando es posible entontrar un estado cuántico $\rho_{AC_1 \ldots C_N}$ en $\mathbb{C}^d \otimes (\mathbb{C}^d)^{\otimes N}$ tal que $\rho_{AC_k} = \mathrm{tr}_{\bar{k}} \rho_{AC_1 \ldots C_N} = \rho_{AC}$, $\forall k$. Se dice, pues que el estado $\rho_{AC_1 \ldots C_N}$ es una N-extensión de ρ_{AC}. Las correlaciones iniciales entre los subsistemas A y C son ahora compartidas entre A y cada uno de los N subistemas C_i, ver figura 4.. Es inmediato ver que

$$\rho_{AC_1 \ldots C_N} = \sum_i q_i |\alpha_i\rangle\langle\alpha_i| \otimes |\gamma_i\rangle\langle\gamma_i|^{\otimes N} \tag{20}$$

proporciona una N-extensión válida de un estado separable $\rho^s_{AC} = \sum_i q_i |\alpha_i\rangle\langle\alpha_i| \otimes |\gamma_i\rangle\langle\gamma_i|$ para todo N. Tal como Werner demostró, si un estado ρ_{AC} es en-

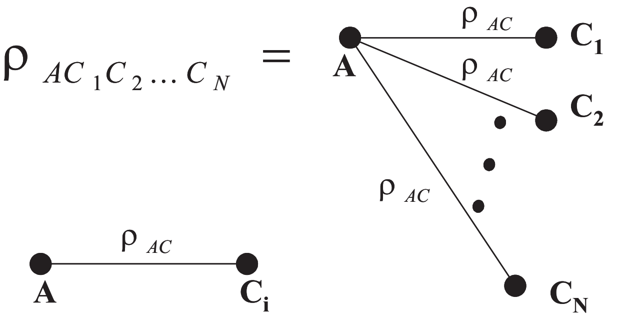

Figure 4: The state ρ_{AC} is said to be N-shareable when there exists a global state $\rho_{AC_1\ldots C_N}$ such that the local state shared between A and C_i is equal to ρ_{AC}, for all i.

tangled, entonces existe un número finito $N(\rho_{AC})$ tal que la correspondiente N-extensión del estado no puede ser hallada.

El segundo ingrediente que necesitamos son las propiedades de los canales destructores de entanglement (EBC). Un canal Υ se dice destructor de entanglement cuando no puede ser usado para distribuir entanglement. La referencia [55] contiene la prueba de que las siguientes tres afirmaciones son equivalentes: (1) Υ es destructor de entanglement, (2) Υ se puede escribir en la forma

$$\Upsilon(\rho) = \sum_j \mathrm{tr}(M_j \rho)\rho_j, \tag{21}$$

donde ρ_j son estados cuánticos y $\{M_j\}$ define una medida y (3) $(\mathbb{1}\otimes\Upsilon)|\Phi\rangle$ es un estado separable, donde $|\Phi\rangle$ aparece en (11). La equivalencia entre (1) y (2) simplemente significa que cualquier EBC se puede entender como una medida del estado inicial, ρ, seguida por la preparación de un nuevo estado ρ_j dependiendo del resultado de la medida. La equivalencia entre (1) y (3) refleja que la estrategia intuitiva para la distribución de entanglement en la que la mitad de un estado máximamente entangled es enviado a través del canal basta para detectar si Υ es un EBC.

Basándonos en estos dos hechos, demostramos que en el límite asintótico, la clonación de estados locales converge hacia un EBC debido a la monogamia del entanglement. Desde un punto de vista cuantitativo, nuestro resultado se puede expresar a través del siguiente teorema (ver el capítulo 6 para más detalles):

Theorem 1 *La clonación asintótica se corresponde con la estimación de estados. Por tanto, $F_M = F_C$ para cualquier distribución de estados.*

Esto resuelve la vieja conjetura sobre la equivalencia de la clonación asintótica y la estimación de estados.

Contents

Chapter 1

Introduction

Quantum theory describes the physics of microscopic systems. Its mathematical structure is based on linear algebra and is briefly described in Appendix A. The formalism and spirit of quantum theory is radically different from classical physics, often leading to counter-intuitive results. Perhaps, one of the most peculiar features in quantum theory is the correlation present in composite quantum systems, named as entanglement, that does not have any counter-part in a classical theory.

About two decades ago, several researchers realized that the quantum formalism could be a useful tool for designing new information applications, putting the ground basis for quantum information theory. New and remarkable information results appeared using the quantum formalism, such as quantum teleportation [10], a protocol to transmit a quantum state to arbitrarily long distance, and the quantum factorization algorithm [81], that solves the factorization problem[1] using polynomial resources. Indeed, it turns out that entanglement enables quantum information theory to outperform its classical counter-part. Nowadays a strong theoretical and experimental effort is devoted to quantum information theory, and concepts from this discipline are also used in other research areas of Science.

One of the most remarkable applications of quantum information theory is quantum cryptography [43], and, more precisely, quantum key distribution (denoted by QKD in what follows), where a secret key is distributed by means of quantum states and measurements. One of the reasons of the impact of QKD is that it is feasible using current technology. The present thesis studies the role played by entanglement, or quantum correlations, in quantum cryptographic scenarios: we present a new security analysis of quantum channels for cryptographic scenarios, study the use of Gaussian states in key distillation scenarios, and give the proof of equivalence between asymptotic quantum cloning and state estimation.

[1] Classically the problem is considered to be very hard, in the sense that it may not be generally solvable using polynomial resources.

1.1 Motivation

The main topic of the thesis is the relation between entanglement and the security of QKD. The thesis gives several security conditions that detect if a secret key can be distilled from a given quantum channel, which can be finite-dimensional or Gaussian. The obtained condition can be applied to prove the security of standard protocols, such as the BB84 protocol [8]. The thesis also studies the relation between quantum cloning and state estimation, fundamental concepts that naturally appear in the context of QKD. It is well known that perfect cloning and state estimation are impossible due to the non-orthogonality of quantum states. Actually, it has been conjectured that quantum cloning becomes equivalent to state estimation in the limit of a large number of clones. The present thesis proves this long-standing open problem.

Key distillation from quantum channels

The existing cryptographic methods using classical resources base their security on technical assumptions on the eavesdropper, often called Eve, capabilities, such as finite computational power or bounded memory [70]. Contrary to all these schemes, the security proofs of QKD protocols, e.g. the BB84 protocol [8], do not rely on any assumption on Eve's power: they are simply based on the fact that Eve's, as well as the honest parties' devices are governed by quantum theory [43]. Well-established quantum features, such as the monogamy of entanglement or the impossibility of perfect cloning [91], make QKD secure. Controlling the legitimate channel, Eve would introduce errors and modify the expected quantum correlations between the honest parties, Alice and Bob. The amount of these errors can be estimated using public discussion, so the honest parties can judge whether their quantum channel can be used for secure QKD, or abort the insecure transmission otherwise.

Then a natural problem in QKD is to determine whether a given channel is useful for QKD. A standard question in this context is to find the critical quantum bit error rate (QBER) in the channel such that key distillation is possible using the BB84 protocol. However, it appears meaningful to identify and quantify the cryptographic properties of a quantum channel by itself, independently of any pre-determined QKD protocol. Indeed, this is closer to what happens in reality, where the channel connecting Alice and Bob is fixed. Therefore, after estimating properties of a given quantum channel, the two honest parties should design the protocol which is better tailored to the estimated channel parameters. In this sense, it is well known that no secure QKD can be established using entanglement-breaking channel [42, 28], while the detection of entanglement already guarantees the presence of some form of secrecy [3]. Beyond these two results, little is known about which channel properties are necessary and/or sufficient for secure QKD.

Key distillation in the Gaussian scenario

Since quantum teleportation was experimentally implemented using a two-mode squeeze state, a significant amount of work has been devoted to develop quantum information theory using continuous variables systems (i.e. systems of infinite dimension). Many concepts introduced in discrete variables systems are being translated to continuous variable systems. In these systems, Gaussian states and Gaussian operations play a key role. They naturally appear in experiments and can be handled with current quantum optics technology.

An important negative result in the context of continuous variable quantum information theory is that it is impossible to distill pure-state entanglement from Gaussian states using Gaussian operations [38, 33]. Although it is known that all Gaussian states with non-positive partial transposition are distillable [37], any distillation protocol must include non-Gaussian operations, which are quite challenging from an experimental point of view. This can be rephrased saying that *all entangled mixed states are bound entangled in a Gaussian scenario*. However, these states may still be useful for cryptographic applications, since *secret bits* may be extracted from them using Gaussian Local Operations and Classical Communication.

State estimation and asymptotic cloning

Perfect quantum cloning and perfect state estimation are well-known impossible quantum operations. They are also ingredients that make QKD secure. The impossibility of perfect state estimation is a major consequence of the nonorthogonality of quantum states: *the state of a single quantum system cannot be perfectly measured.* Thus, any measurement at the single-copy level only provides partial information. The no-cloning theorem, one of the cornerstones of quantum information theory, represents another consequences of the nonorthogonality of quantum states. It proves that given a quantum system in an unknown state, it is impossible to design a device producing two identical copies.

In fact, these two results are closely related. On the one hand, if perfect state estimation was possible, one could use it to prepare any number of clones of a given state, just by measurement and preparation. On the other hand, if perfect cloning was possible, one could perfectly estimate the unknown state of a quantum system by preparing infinite clones of it and then measuring them. Beyond these qualitative arguments, the connection between state estimation and cloning was strengthened in [39, 15], where it was conjectured that quantum cloning is equivalent to state estimation in the asymptotic limit of an infinite number of clones. Actually, this conjecture was later proven for two cases, namely universal cloning[2] [15] and phase-covariant cloning[3] [17]. However the complete equivalence of state estimation and asymptotic cloning remained open and had been identified as one of the open problems in quantum information theory[4].

1.2 Contributions

We analyze the cryptographic properties of quantum channels when Alice and Bob employ QKD schemes where (i) the correlation distribution is done using prepare and measure techniques and (ii) the key distillation process uses the standard one-way and two-way classical protocols. Throughout the thesis, we call these protocols 'realistic', since these are the techniques presently used in any realistic QKD implementation. We first derive a security condition for qubit channels in the case of the so-called collective attacks. Since collective attacks have been proven to be as powerful as general attacks [78], our condition actually applies to any attack. We apply this condition to the standard BB84 and six-state protocols. Next, we explore several possibilities to improve the obtained security bounds. Remarkably, all these alternatives fail, which suggests the existence of non-distillable entangled states under general realistic protocols. We then generalize this security condition to higher dimensional systems, called *qudits*, and extend the results to generalized Bell diagonal qudit channels. The obtained security condition turns out to be tight for the so-called $(d+1)$- and 2-bases protocol of Ref. [21].

We employ Gaussian states and operations to the same cryptographic scenario, and analyze the secrecy properties of Gaussian channels. First, we study the security of our protocol when Eve applies an individual attack, and show that all Gaussian states that remain Non-Positive under Partial Transposition (NPPT) turn out to be secure. Then, we consider general attacks and show that our security proof ceases to work for some NPPT states. The result suggests that there may exist weakly entangling channels of Gaussian states that are useless for key distribution using Gaussian operations.

Finally, we show the equivalence between optimal asymptotic cloning and state estimation for any initial ensemble of pure states. Actually, we prove that *asymptotic cloning does effectively correspond to state estimation.* The proof is based on two known results of quantum information theory: the monogamy of quantum correlations and the properties of entanglement-breaking channels.

[2] The initial ensemble consists of a randomly chosen pure states.

[3] The initial ensemble corresponds to a state lying on equators of the Bloch sphere.

[4] See problem 22 in the open problem list [57].

1.3 Thesis Overview

The thesis is structured as follows. After this introductory chapter, Chapter 2 presents several basic notions of quantum information theory, mainly about entanglement and quantum cryptography, that are used in what follows. Entanglement in discrete and continuous variable systems is summarized. Then, quantum cryptography is introduced, with a general discussion on protocols, security and cloning. Readers with some expertise in quantum information theory may skip this part.

In Chapter 3 we define the ingredients used in the so-called realistic protocol that are feasible using present technology. The security of these realistic protocols is then considered in the following chapters. The following three chapters contain the original results of this Thesis.

In Chapter 4 we study the secrecy properties of quantum channels under realistic protocols. For qubit or qudit channels, a simple security condition is obtained. Furthermore, the specific attacks that break the protocol whenever a channel does not satisfy the obtained security condition is presented, proving that this condition is tight. For any finite dimension, we show the existence of a gap between the entanglement condition and our security condition. Several possibilities to improve this condition and fill the gap are explored, such as pre-processing and the use of coherent quantum operations by one of the honest parties. Interestingly, the gap remains unchanged.

In Chapter 5 we adapt the realistic protocols to the Gaussian regime, Gaussian states and Gaussian operations. We show that a secret key can be distilled from sufficiently entangled Gaussian states by Gaussian operations, and provide security bounds against individual and general attacks. The security bounds also have a gap with the entanglement condition.

In Chapter 6 we prove the equivalence between asymptotic quantum cloning and state estimation. In fact, it is shown that quantum cloning asymptotically corresponds to state estimation. The proof follows from the combination of two known results in quantum information theory, the properties of entanglement-breaking channels and the monogamy of entangled states.

Finally, Chapter 7 contains a summary of the results and discusses some related problems.

Several appendices are included for the sake of completeness. In Appendix A, we provide a short introduction to the mathematical formalism of quantum theory. Appendices B, C, D, and E contain technical calculations that are needed in the derivation of the results of Chapter 4.

Chapter 2

Entanglement, QKD, ...

This Chapter collects some known results on quantum information theory that are later important in the derivation of our results. We first review several concepts and results related to the characterization of entangled states. Then, we move to QKD protocols and the problem of cloning in quantum theory.

2.1 Entanglement

Quantum states in composite systems are ubiquitous in quantum information theory. A standard scenario consists of several distant parties sharing a quantum state. The goal is to exploit the quantum correlations that can be obtained after measuring this state to accomplish a given information task. A state is potentially useful in this general scenario whenever it is entangled, i.e. it contains quantum correlations. In what follows, we present some of the main results on the characterization of entangled states.

2.1.1 Entangled State

Two parties, traditionally called as Alice and Bob, share a bipartite state belonging to a composite space, $\mathcal{H}_A \otimes \mathcal{H}_B$. If it is pure, the state can be written as

$$|\psi\rangle_{AB} = \sum_{i,j} c_{i,j} |a_i\rangle |b_j\rangle$$

where i and j run over $\dim(\mathcal{H}_A)$ and $\dim(\mathcal{H}_B)$. A state is product whenever it can be written as

$$|\psi\rangle_{AB} = (\sum_i \alpha_i |a_i\rangle)(\sum_j \beta_j |b_j\rangle).$$

These states contain no correlations between the two parties. A state is called *entangled* if it is not product. Entangled states, then, contain quantum correlations. A well-known example of entangled state is given by

$$|\phi_d\rangle \;=\; \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|ii\rangle. \tag{2.1}$$

Actually, these states are the maximally entangled state of a composite $(d \times d)$-dimensional Hilbert space. Entangled states do not have a classical counter-part and have been recognized as the resource behind the new applications of quantum information theory, such as computational speedup and quantum teleportation. Therefore, given a quantum state, it is important to detect whether it is entangled. In the case of pure states, the detection of entanglement turns out to be rather simple.

Proposition 1 *A pure bipartite state $|\psi\rangle_{AB}$ is entangled if and only if $\rho_A = \mathrm{tr}_B|\psi\rangle\langle\psi|_{AB}$, or equivalently $\rho_B = \mathrm{tr}_A|\psi\rangle\langle\psi|_{AB}$, is a mixed state.*

The definition of entangled mixed states was first given in Ref. [88]. A mixed state is said to be separable when it can be written as a mixture of product states,

$$\rho_{AB} = \sum_i p_i \rho_A^i \otimes \rho_B^i, \tag{2.2}$$

Alice and Bob can prepare any of these states by Local Operations and Classical Communication (LOCC). These states do not contain any quantum correlations, since its preparation is possible using only classical correlations. A mixed state is entangled when it cannot be written as in (2.2). That is, its preparation using only product states and classical correlations is impossible.

For mixed states, it turns out that distinguishing entangled from separable states is one of the most challenging problems in quantum information theory [49]. However, a remarkable development was carried out by Peres, based on the intuition that time-reversal is a non-physical operation [77]. Mathematically this is expressed by the transposition operation T, $T(|i\rangle\langle j|) = |j\rangle\langle i|$. Transposition is the simplest example of a positive but not completely positive map. A map Λ is positive but not completely positive when $\Lambda(\rho)$ is positive for all positive ρ but $\mathbb{1} \otimes \Upsilon$ is non-positive. Then the partial transposition with respect to B, $\mathbb{1} \otimes T_B$, transforms a bipartite state $\rho_{AB} = \sum_{ij,kl} \lambda_{ij,kl}|i\rangle_A\langle j| \otimes |k\rangle_B\langle l|$ into

$$(\mathbb{1}_A \otimes T_B)\rho_{AB} = \sum_{ij,kl} \lambda_{ij,kl}|i\rangle_A\langle j| \otimes |l\rangle_B\langle k|.$$

Note that all entangled pure states are non-positive under partial transposition, i.e. for all entangled state $|\psi\rangle$, $(\mathbb{1} \otimes T_B)(|\psi\rangle\langle\psi|) \ngeq 0$, while

$(\mathbb{1} \otimes T_B)(|\psi\rangle\langle\psi|)$ is positive for all product states [77]. Since transposition is linear, whenever the partial transposition of a mixed state state is non-positive, the state cannot be written as (2.2), so it is entangled. The partial transposition criterion, then, is a necessary condition for separability.

Theorem 2 (Peres-Horodecki) *A state ρ over $\mathcal{H}_A \otimes \mathcal{H}_B$ where $\dim(\mathcal{H}_A) = 2$ and $\dim(\mathcal{H}_B) = 2$, or 3, remains positive after partial transposition, i.e. $(\mathbb{1}_A \otimes T_B)\rho_{AB} \geq 0$, if and only if it is separable.*

It was then thought that for arbitrary $d_A \times d_B$ systems the partial transposition criterion could also be sufficient for separability. However, Horodecki *et al.* provided counter-examples to this conjecture in [53]. They showed entangled states that remain positive after partial transposition, and such states are called positive-partial-transpose (PPT) entangled states.

The Horodecki also realized that a more complete approach to the separability problem follows from general positive but not completely positive maps Λ. It is clear that a separable state remains positive after application of any positive map. Interestingly, it is also known that for any entangled state $|\psi\rangle$ there is a positive map such that $(\mathbb{1} \otimes \Lambda)(|\psi\rangle\langle\psi|)$ is non-positive. This property can also be rephrased in terms of operators, by means of the so-called entanglement witnesses.

Definition 1 (Entanglement Witness) *A Hermitian operator W is called an entangled witness if it satisfies $\mathrm{tr}[\rho_{ent} W] < 0$ for some entangled states ρ_{ent} and $\mathrm{tr}[\rho_{sep} W] \geq 0$ for all separable states ρ_{sep}.*

For any entangled state, there exists an entanglement witness operator that detects it. This follows from two facts, i) separable states form a convex set and ii) quantum states reside in a Hilbert space where they can be topologically distinguished by a Hermitian operator, which is the entanglement witness W that distinguishes entangled states from separable states. Indeed one can relate positive maps and entanglement witnesses through the isomorphism

$$W = (\mathbb{1} \otimes \Lambda)(|\phi_d\rangle\langle\phi_d|). \tag{2.3}$$

If one was able to construct all possible entanglement witness operators, or equivalently all positive maps, one would solve the separability problem. However very little is known on the characterization of positive maps. From an experimental point of view, entanglement witnesses are also useful. Since any operator can be decomposed in terms of local operators, entanglement witnesses can be estimated by means of local measurement and classical communication [47].

2.1.2 Entanglement Measure

Entanglement has been recognized as a useful resource that enables quantum information processing to outperform classical processing. It is then natural to wonder how entanglement should be quantified, i.e. given a state, how much entanglement it contains?

For pure states, the amount of entanglement is uniquely determined by the *entropy of entanglement*. This is the von Neumann entropy of the reduced state [11].

Definition 2 (Entropy of entanglement) *For a bipartite pure state $|\psi\rangle_{AB}$, the entropy of entanglement is the von Neumann entropy of the reduced state,*

$$E(\rho_A) = -\mathrm{tr}[\rho_A \log \rho_A].$$

As expected, this quantity attains its maximal value, $\log d$, for the state $|\phi_d\rangle$ in (2.1), while it is zero for all product states.

The direct generalization of the entropy of entanglement to mixed states is not possible, since it does not distinguish classical from intrinsically quantum correlations. Moreover, in the case of mixed states one is faced to the problem that mixed states do not have a unique decomposition in terms of pure states. In order to illustrate this problem we can consider the mixture of two maximally entangled states, $|\phi^{\pm}\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}$,

$$\rho_{AB} = \frac{1}{2}|\phi^{+}\rangle\langle\phi^{+}| + \frac{1}{2}|\phi^{-}\rangle\langle\phi^{-}| = \frac{1}{2}|00\rangle\langle 00| + \frac{1}{2}|11\rangle\langle 11|.$$

Note that $\rho_A = \mathbb{1}_A/2$ so $E(\rho_A) = 1$, while this state is in fact separable. Actually, the separability of the state is clear only after the second decomposition is considered. Therefore, most of the entanglement measures for mixed states are defined as an optimization over all possible decompositions of the state, which is in fact a highly nontrivial task. Following this intuition, the *Entanglement of formation* generalizes the entropy of entanglement to mixed states [11].

Definition 3 (Entanglement of formation) *For a bipartite state ρ_{AB}, the entanglement of formation is the least expected entanglement over all ensemble decomposition of ρ_{AB},*

$$E_f(\rho_{AB}) = \min_{\{p_i,\psi_i\}} \sum_i p_i E(\psi_i),$$

where the minimization is done over all ensembles $\{p_i, \psi_i\}$ such that $\rho_{AB} = \sum_i p_i |\psi_i\rangle\langle\psi_i|$.

This minimization is very hard in general. However, in the case of two qubits, Wootters was able to derive the exact expression for the entanglement of formation [93].

Theorem 3 (Entanglement of formation for two qubits) *Entanglement of formation for a two-qubit state ρ is*

$$E_f(\rho) = h[\frac{1}{2}(1+\sqrt{1-C(\rho)^2})]$$

where h is the binary entropy, $h(x) = -x\ln x - (1-x)\ln(1-x)$ and $C(\rho)$ is the so-called concurrence

$$C(\rho) = \max(0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4),$$

where λ_i, $i = 1,2,3,4$, are the eigenvalues of $(\rho^{1/2}\tilde{\rho}\rho^{1/2})^{1/2}$ and $\tilde{\rho} = (\sigma_y \otimes \sigma_y)\rho^*(\sigma_y \otimes \sigma_y)$.

Finally, let us state another result for two-qubit states that will be used in chapter 4. Given a state ρ_{AB}, we would like to determine the local operations such that the resulting state ρ'_{AB},

$$\rho_{AB} \longrightarrow \rho'_{AB} = \frac{(A\otimes B)\rho_{AB}(A\otimes B)^\dagger}{\mathrm{tr}[(A\otimes B)\rho_{AB}(A\otimes B)^\dagger]}$$

that happens with some non-zero probability $\mathrm{tr}[(A\otimes B)\rho_{AB}(A\otimes B)^\dagger]$, has maximal entanglement.

Theorem 4 *For a given two-qubit state ρ_{AB}, the entanglement of formation, or equivalently the concurrence, is maximized, after local operations and classical communication at the single-copy level, by a Bell-diagonal state,*

$$\rho'_{AB} = \lambda_1|\phi^+\rangle\langle\phi^+| + \lambda_2|\phi^-\rangle\langle\phi^-| + \lambda_3|\psi^+\rangle\langle\psi^+| + \lambda_4|\psi^-\rangle\langle\psi^-|.$$

If the state is Bell diagonal, it remains unchanged. This result was proven in Ref. [87], where more details on the measurements and the resulting states can be found.

Before concluding this brief review on entanglement, we introduce two other entanglement measures [11], based on the fact that the maximally entangled state $|\phi_2\rangle$ represents the unit of pure-state entanglement, also called *ebit*.

Definition 4 (Entanglement of distillation) *Given a state ρ, the entanglement of distillation, E_D, quantifies the number N of copies of the state $|\phi_2\rangle$ that can be distilled out of $\rho^{\otimes M}$ by LOCC in the limit of a large number of copies, i.e. $E_D = \lim_{M\to\infty} N/M$.*

Definition 5 (Entanglement cost) *Given a state ρ, the entanglement cost, E_C, quantifies the number N of copies of the state $|\phi_2\rangle$ needed to prepare M copies of ρ in the limit of a large number of copies, i.e. $E_C = \lim_{M\to\infty} N/M$.*

For pure states, the entanglement cost asymptotically coincides with the distillable entanglement. For mixed states, the entanglement cost is in general larger than the entanglement of distillation, $E_c(\rho) \geq E_d(\rho)$. A state ρ with distillable entanglement strictly larger than zero is called *distillable*. An entangled state ρ is called *bound entangled* if no pure-state entanglement can be distilled out of it, $E_d(\rho) = 0$ but $E_c(\rho) > 0$. Entangled states with positive partial transposition are not distillable. This follows from the facts that i) the final state $|\phi_d\rangle$ of the distillation processing is an entangled pure state, so it is NPPT and ii) a PPT state cannot turn into NPPT by LOCC.

2.1.3 Gaussian Regime

All the previous results were originally considered for finite dimensional systems. Recently, many of these concepts have been translated to the infinite dimensional case [13]. In these systems, the set of Gaussian states and Gaussian operations plays a key role, since they naturally appear in experiments. They can be prepared by means of simple optical elements, such as beam splitter and squeezers, while non-Gaussian operations turn out to be very challenging from an experimental point of view. Moreover, the theoretical analysis of Gaussian states and operations can be simplified due to the fact that all their properties can be expressed in terms of finite-dimensional matrices and vectors.

Gaussian states

Continuous variable systems are often termed as modes. We consider quantum systems of n modes, $\mathcal{H} = \mathrm{L}^2(\Re^n)$. The commutation relations for the canonical coordinates $R = (X_1, P_1, \ldots, X_n, P_n) = (R_1 \ldots, R_{2n})$ read $[R_a, R_b] = i(J_n)_{ab}$, where $a, b = 1, \ldots, 2n$ and

$$J_n = \oplus_{i=1}^n J \qquad J \equiv \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \tag{2.4}$$

where J is known as the symplectic matrix. Quantum states are normalized positive operators, $\mathrm{tr}[\rho] = 1$. For a given state, it is often convenient to consider its characteristic function, defined as $\chi_\rho(x) = \mathrm{tr}(\rho W(x))$, where $W(x)$ are the so-called Weyl opertors,

$$W(x) = \exp(-ix^T R),$$

where $x \in \Re^{2n}$. Weyl operators satisfy the Weyl commutation relations,

$$W(x)W(y) = \exp(-i\sigma(x,y))W(y)W(x),$$

where $\sigma(x,y) = x^T J_n y$. On the other hand, any state of n modes can be written as

$$\rho = \frac{1}{(2\pi)^n} \int_{\Re^{2n}} \chi_\rho(x) W(-x) d^{2n}x.$$

Gaussian states are those states such that χ_ρ is a Gaussian function,

$$\chi_\rho(x) = \exp(ix^T d - \frac{1}{4}x^T \gamma x). \tag{2.5}$$

where d is a $2n$ real vector, called displacement vector (DV), and γ is a $2n \times 2n$ symmetric real matrix, known as covariance matrix (CM).

Theorem 5 *A gaussian characteristic function described by its covariance matrix γ corresponds to a physical state if γ has the Symplectic diagonal form,*

$$\gamma = S(D \oplus D)S^T,$$

where $D \geq \mathbb{1}$ is diagonal and S is a symplectic map satisfying $SJS^T = J$. This condition is also equivalent to $\gamma + iJ \geq 0$, or $J\gamma J^T \geq \gamma^{-1}$.

All the information about d and γ is contained in the first and second moments of the state, $\mathrm{tr}(\rho R_i)$ and $\mathrm{tr}(\rho R_i R_j)$. The displacement vector can always be modified by local operations, while the covariance matrix includes the correlations between modes.

Entanglement of Gaussian states

We now consider two parties, Alice(A) and Bob(B), that share a state ρ in a composite systems of $n + m$ modes. The global CM is

$$\gamma_{AB} = \begin{pmatrix} \gamma_A & C \\ C^T & \gamma_B \end{pmatrix} \geq iJ_{n+m}, \tag{2.6}$$

where γ_A (γ_B) is the CM for the n-mode (m-mode) Gaussian state of system A (B). As said, the entanglement properties of ρ are completely specified by its CM.

The effect of partial transposition at the level of CMs can be understood from the fact that this map is equivalent to time-reversal. After partial transposition on, say, A, the sign of Alice's momenta is changed while the rest of canonical coordinates is kept unchanged. Denote by θ the matrix equal to the identity for the position coordinates and minus the identity for the momenta. Partial transposition means that $\gamma_{AB} \to \gamma'_{AB} = \theta_A \gamma_{AB} \theta_A$. Therefore, the state ρ is PPT when γ'_{AB} defines a positive operator, that is $\gamma'_{AB} \geq iJ_{n+m}$. The PPT criterion provides a necessary and sufficient condition for separability for 1×1 [32] and $1 \times N$ Gaussian states [90], while it is only a necessary condition for the rest of systems [90]. The non-positivity of the partial transposition is a necessary and sufficient condition for distillability [37].

Given an n-mode mixed Gaussian state ρ_1 with CM γ_1, it can always be purified by constructing a $2n$ mode pure Gaussian state $|\Psi_{12}\rangle$ such that

$\mathrm{tr}_2(|\Psi_{12}\rangle\langle\Psi_{12}|) = \rho_1$ [52]. The global CM γ_{12}, see Eq. (2.6), has $\gamma_A = \gamma_1$ and

$$\begin{aligned} \gamma_B &= \theta\gamma_1\theta \\ C &= J_n S \left(\oplus_{i=1}^{n} \sqrt{\lambda_k^2 - 1} \mathbb{1}_2 \right) S^{-1}\theta, \end{aligned} \tag{2.7}$$

where $\{\lambda_k\}$ defines the symplectic spectrum of γ_1 and S is the symplectic matrix such that $S^T\gamma_1 S$ is diagonal.

As we have previously discussed(2.1.2), given a noisy entangled state, it is relevant to know when pure-state entanglement can be distilled out of it. An important negative result in this direction was obtained in Refs. [38], (see also [33]):

Theorem 6 *Gaussian states cannot be distilled by Gaussian operation. However, distillation of NPPT Gaussian state is always possible if non-Gaussian operations are applied.*

This can be rephrased saying that *all entangled mixed states are bound entangled in the Gaussian scenario.*

2.2 Quantum Key Distribution

Cryptography looks for methods for information exchange between distant parties in a completely secure way. Here being completely secure means no party, but the legitimate ones, obtains any information about the sent message. In the simpler cryptographic scenario, there are two honest parties, Alice and Bob, and the eavesdropper called Eve. Alice and Bob's goal is to transmit a message M in a completely secure way.

Currently known cryptosystems are classified into asymmetric and symmetric, depending on whether they use a public or a private key. Asymmetric cryptosystems are based on the existence of one-way functions, which are functions that can be easily computed in one direction but not in the other. A good example of these functions is factorization: while it is easy to compute the product of two large prime numbers, to find the prime factors of the result is much harder. Actually RSA, one of the most known encryption methods, is based on the computational difficulty of the factorization problem. Then, these methods base their security on the difficulty of some computational problems, so they are said to provide *computational security.* The advent of quantum computation sheds some doubts on the long-term applicability of these methods, since an adversary equipped with a quantum computer could run Shor's factorization algorithm, which is efficient, and read the encrypted message.

The symmetric cryptosystem is based on a pre-shared *a secret key K* that only the two honest parties know. Using the key, the two honest parties encrypt a message M, for instance by means of one-time pad[1]. Since the eavesrdropper does not know the key, it can be proven that she cannot obtain any information from the encrypted message. The method is then completely secure. However, it appears the almost identical problem of how to distribute the key K in a secure way.

2.2.1 Quantum Protocols

Quantum cryptography provides a way of distributing a key between two honest parties in provable secure way. The security relies on the fundamental assumption that Alice, Bob and Eve's devices cannot contradict quantum theory [43]. From a very qualitative point of view, the security of QKD comes from the fact that

> One cannot make a measurement of the state of a quantum system without perturbing it.

This is just a consequence of the non-orthogonality of quantum states. Indeed, it is impossible to perfectly discriminate two non-orthogonal quantum states. This is the central idea behind any protocol of QKD: by encoding the information in non-orthogonal states, any intervention by the eavesdropper perturbs the transmission and is detected by the two honest parties, who stop the insecure transmission.

The BB84 and the six-state protocols

The first QKD protocol was proposed by Charles Bennett and Gilles Brassard in 1984, so named BB84 [8]. This protocol employs four states, $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$, where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. Alice encodes classical values, 0 in the quantum states $|0\rangle$ or $|+\rangle$ randomly and 1 into $|1\rangle$ or $|-\rangle$ randomly, and sends the quantum state to Bob. Bob measures the received state in the $z-$basis $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ or the the $x-$basis $\{|+\rangle\langle +|, |-\rangle\langle -|\}$. After public communication, the honest parties keep the symbols where they used the same basis for encoding and measurement. This is called the *sifting* process. In the ideal noise-free situation, the obtained classical symbols are perfectly correlated and can be used as secret key.

If Alice and Bob include a third basis in the $y-$direction, $|\pm i\rangle = (|0\rangle \pm i|1\rangle)/\sqrt{2}$, the protocol is called the six-state protocol, where $|+i\rangle$ is for encoding 0 and $|-i\rangle$ for encoding 1 [16].

Quantum Bit Error Rate

After the sifting processing, the two honest parties share correlated values. In any realistic situation, these values are noisy, so Alice and Bob have to

[1] The key and the message to be sent are summed modulo 2

apply classical protocols to distill them into a perfect secret key. If the errors in the channel are moderate, a secret key can be extracted from the noisy data. In the qubit case, the errors are often quantified by the quantum-bit-error rate (QBER) defined by

$$Q = p_{AB}(0,1) + p_{AB}(1,0).$$

A standard question in the study of qubit protocols is to determine the maximum QBER such that key distillation is possible.

Indeed, the value of QBER quantifies not only the mutual information between the honest parties but also the information gained by the eavesdropper. This is because, as said, any intervention by the eavesdropper introduces errors in the channel: the larger the observed errors, the more the information Eve is gaining.

2.2.2 Information Theory

In this subsection, we introduce information-theoretic notions needed for security issues in key distribution, and will be used in the security proofs in chapters 4 and 5. Probability distribution of Alice, Bob, and Eve will be denoted by $P(A, B, E)$, throughout the thesis.

The first quantity is *entropy* proposed by Shannon, that quantifies a given probability distribution in terms of randomness.

Definition 6 *The Shannon entropy $H(A)$ of a variable A whose probability distribution is given by $P(A)$ is defined*

$$H(A) = -\sum_{a \in A} P(a) \log P(a). \tag{2.8}$$

The Shannon entropy satisfies $1 \leq H(A) \leq \log(|A|)$, where $|A|$ is the cardinality of the set X. As more random a probability distribution is, entropy provides strictly a larger value. It was derived by considering noiseless coding, in which the motivated problem is the following: when n-bit strings are given with a given probability distribution, how many bits are required to optimally encode them? The answer he found is approximately $|A|^{nH(A)}$ bits. This is resulted from the law of large numbers[2] [80].

Based on the Shannon entropy, other quantities can be derived more. Condition entropy $H(B|A)$ which quantifies knowledge of B when A is given, is

$$H(B|A) = H(AB) - H(A).$$

[2] The average of a large number of independent measurements of a random quantity tends toward the theoretical average of that quantity.

And the mutual information $I(A:B)$ which quantifies knowledge common to A and B, is

$$I(A:B) = H(A) + H(B) - H(AB).$$

The Shannon entropy, based on probability distributions, can be translated to the von Neumann entropy that is with quantum states.

Definition 7 (von Neumann Entropy) *The von Neumann entropy of quantum states ρ is:*

$$S(\rho) = -\mathrm{tr}\rho \log(\rho).$$

When a bipartite quantum state is in a product form $\rho_A \otimes \rho_B$, the entropy is additive, $S(\rho_A \otimes \rho_B) = S(\rho_A) + S(\rho_B)$.

Quantum conditional and mutual entropies are also as follow,

$$\begin{aligned} H(A|B) &= S(AB) - S(B) \\ I(A:B) &= S(A) + B(B) - S(AB). \end{aligned}$$

Since quantum states are not orthogonal each other, if two classical random values 0 and 1 are encoded into non-orthogonal states ρ_0 and ρ_1, this imposes the uncertainty in discrimination. The question cast is then: how much classical information can be used from quantum states? Holevo discovered the connection between quantum states and classical information quantity.

Theorem 7 (Holevo bound) *Suppose Alice prepares ρ_a with probability p_a and sends it to Bob. Then, the Bob's state is*

$$\rho_B = \sum_a p_a \rho_a.$$

Bob then applies a POVM $\{E_b\}$ to know about ρ_B, and gets probability distribution $p_b = \mathrm{tr}[E_b \rho_B]$. The maximum classical information that Bob can get from his quantum states is the mutual information between the quantum state ρ_B and the probability distribution p_b and is bounded by

$$I(X:Y) \leq S(\rho_B) - \sum_a p_a S(\rho_a).$$

2.2.3 Quantum Cloning

Cloning a quantum state is a well-known impossible quantum processing, and termed as the *no-cloning theorem.* This is one of well-known no-go theorems in quantum theory, and closely concerned with other quantum information processing such as state estimation and quantum cloning. There have been extensive studies from various viewpoints, and a good review can be found in Ref. [79].

The no-cloning theorem was first shown by Wootters and Zurek in [92]. It was a simple proof compared to its physical importance, and nowadays can be found in many books of quantum information theory. In the proof, unitarity was employed to show the impossibility of copying quantum states. Yuen showed that linearity, a more relaxed constraint, also implies the no-cloning theorem [94]. Recently it was shown that, as one particular consequence of no-signalling constraint, the no-cloning phenomena exist in all no-signalling theories [67] [40].

The problem of approximating quantum cloning was addressed in [19]. The first quantum cloning machine transforms arbitrary single qubit into two approximate clones that are identical. A reasonable figure of merit in qualifying cloning operations can be the fidelity of one clone with the original. In detail about the first cloning machine, assumed that $|\psi\rangle \in \mathcal{H}_2$ is to be cloned, the cloning operation is a unitary operation U over $\mathcal{H}_2 \otimes \mathcal{H}_2$ performing $U|\psi\rangle|0\rangle$ such that $\rho_1 = \rho_2$, where

$$\rho_i = \mathrm{tr}_{\bar{i}} U|\psi\rangle|0\rangle\langle 0|\langle\psi|U^\dagger$$

with the constraint that the fidelity $F(|\psi\rangle, \rho_i)$ is maximized. Here $\bar{k}$ denotes the complement of k, so $\mathrm{tr}_{\bar{k}}$ is the trace with respect to all the systems but k. Then, the optimal cloning machine carries out the fidelity $F = 5/6$ and the output state of the following form

$$\rho_i = F|\psi\rangle\langle\psi| + (1-F)|\psi^\perp\rangle\langle\psi^\perp|$$

Cloning Machines

Since the first quantum cloning machine was provided, there have been extensive studies on quantum cloning [79]. Then, quantum cloning machines are in general classified by two standards, the inputs and the outputs. When *a priori* information about input states is given so that input quantum states can be particularly characterized, we call *state-dependent* quantum cloning. Otherwise, that is, when no constraint to the input state is provided, we call *universal.* For instance, universal cloning machine for qubits considers cloning of the whole Bloch sphere. By outputs, there are *symmetric* and *asymmetric* cloning machines. In symmetric cloning of M copies of initial states to N clones, all outputs are identical one another and it is denoted by $M \rightarrow N$ cloning. If some clones provide different from one another, i.e. their fidelities are larger or smaller than the others, it is said asymmetric cloning. Among N clones, if N_j clones provide fidelity F_j, it is denoted by $M \rightarrow N_1 + N_2 + \cdots$ cloning, where $\sum_j N_j = N$. Symmetric cloning is related more with estimation of quantum states in the sense of making use of symmetric subspace, and asymmetric cloning has direct application to eavesdropping strategies in QKD.

Connection to state estimation

One may easily realize that the no-cloning theorem and the impossibility of perfect state estimation are closely related. On the one hand, if perfect state estimation was possible, one could use it to prepare any number of clones of a given state, just by measurement and preparation. On the other hand, if perfect cloning was possible, one could perfectly estimate the unknown state of a quantum system by preparing infinite clones of it and then measuring them.

Beyond these qualitative arguments, state estimation can be one possible and trivial cloning, i.e. to estimate given quantum states and to prepare guessed states according to the estimation result. This can be thought of as a classical processing in that quantum operation is not applied. As shown in [26], optimal state estimation of $\rho^{\otimes M}$ is done in the symmetric subspace $\mathcal{H}_{+}^{(M)} \in \mathcal{H}^{\otimes M}$. Remarkably, universal quantum cloning when $N \rightarrow \infty$ is proven equivalent to optimal state estimation, in the sense that, for any ensemble of states, the fidelity F_C obtained by cloning and the fidelity F_M by state estimation are equal[3]:

$$F_C = F_C(N \rightarrow \infty) = F_M. \tag{2.9}$$

This equality was proven in [15], under the assumption that the output of the cloning machine is supported on the symmetric subspace. Later, it was shown in [62] that this assumption does not imply any loss of optimality, so the equality of the two fidelitites for universal cloning and state estimation followed. This equivalence has also been proven for phase-covariant qubit cloning [17], where the initial ensemble corresponds to a state in $\mathbb{C}^2$ lying on one of the equators of the Bloch sphere. Since then, the validity of this equality for any ensemble has been conjectured and, indeed, has been identified as one of the open problems in quantum information theory[4].

Connection to QKD scenarios

Quantum cloning is very relevant to QKD scenarios as applications. It describes interaction of an eavesdropper, Eve, with a quantum channel con-

[3] The universal cloning $M \rightarrow N$ is obtained in [39]and the fidelity is

$$F_{M\rightarrow N} = \frac{NM + N + M}{N(M+2)}.$$

The asymptotic cloning operation shows, by taking $N \rightarrow \infty$, that the fidelity converges to $(M+1)/(M+2)$ which is the fidelity of optimal state estimation processing.

[4] See problem 22 in the open problem list [57].

necting two honest parties. There, $1 \to 1+1$ cloning is the main consideration. Suppose Alice encodes a value a to a quantum state $|a\rangle$ and sends a prepared quantum state. Eve then interacts with the state

$$U_{BE}|a\rangle|E\rangle = |\varphi\rangle_{BE},$$

in such a way that her state $\rho_E = \mathrm{tr}_B[|\varphi\rangle\langle\varphi|_{BE}]$ allows her to make best guess to the encoded value a. In the entanglement-based picture of QKD, Alice prepares

$$|\Phi_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

and measure the first qubit and send the other. The qubit sent by Alice then experiences interaction with Eve, and the interaction can be detected to Bob, as bit-flip or phase errors[5]. Then, the shared state after interaction with environment is a Bell-diagonal state.

In the BB84 protocol, phase-covariant cloning naturally appears, in which Eve considers cloning only the following states

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\varphi}|1\rangle).$$

These states are lying on the equator of the Bloch sphere. The cloning operation was analyzed in [17], and remarkably, just by considering the $1 \to 2$ cloning, the critical QBER of the protocol is derived. Eve in the six-state protocol considers universal cloning, see also Appendix B.

[5] Of course, one can consider a more general interaction. However, by the filtering operations and symmetrization processing, two honest parties can reduce to the two errors. See the chapter 4 for the detail.

Chapter 3

Key Distillation

There can be plenty of QKD protocols in the literature. However, whatever they form, the relevance of a proposed QKD protocol depends highly on its connection to technological feasibility. Then, the significant step in designing a QKD protocol follows from how realistic it is.

In this Chapter, we define the realistic scenario that is later considered in the following chapters, 4 and 5. We introduce the analyzed QKD protocols, discuss several key-distillation techniques and review the known security bounds for the BB84 and six-state protocol.

3.1 Realistic Protocol

Now our consideration is restricted to what we call realistic protocols, that apply measurements at the single-copy level of quantum states and classical key-distillation techniques. In what follows, we denote these *single-copy measurement plus classical processing* as SIMCAP [2]. As shown in Ref [9], for the secret distribution entanglement is actually not necessary at all. First the so-called *prepare and measure* type protocols are introduced, which are then translated to the equivalent, so-called SIMCAP protocols in general, in the entanglement-based picture.

Prepare & Measure protocols

In *prepare and measure* type protocols, Alice prepares and sends states from a chosen basis to Bob, who then measures in another (possibly different) basis. This establishes some classical correlations between the two honest parties. Of course this process alone is clearly insecure, since Eve could apply an intercept resend strategy in the same basis as Alice's state preparation, acquiring the whole information without being detected. Therefore, from time to time, Alice and Bob should change their state preparation and measurements to monitor the channel and exclude this possibility. Alice and

Bob announce these symbols to extract information about their channel, so these instances do not contribute to the final key rate. Indeed these symbols are waisted in the tomographic process previously mentioned. However, in the limit of large sequences, the fraction of cases where Alice and Bob monitor the channel can be made negligible in comparison with the key length, but still sufficient to have a faithful description of some channel parameters, such as the QBER[1]. The states sent by Alice will be transformed into a mixed state because of Eve's interaction. This decoherence will produce errors in the measurement values obtained by Bob. The security analysis aims at answering whether the observed decoherence in the channel is small enough to allow Alice and Bob distilling a secret key. We call these protocols realistic in the sense that they do not involve experimentally difficult quantum operations, such as coherent measurements, quantum memories or the generation of entangled particles. The establishment of correlations is done by just generating one-qubit states and measuring them in two or more bases. Additionally, one could think of including a filtering single-copy measurement on Bob's side. This operation is harder than a standard projective measurement, but still feasible with present-day technology [58].

Entanglement-based scheme

Actually, it is well known that the honest parties do not have to use entanglement at all for the correlation distribution [9]. Only for the convenience for the theoretical analysis, the scenario above can be explained in the completely equivalent entanglement-based scenario.

In the entanglement-based scheme, the information encoding by Alice is replaced by generating and measuring half of a maximally entangled state. That is, Alice first locally generates a maximally entangled two-qubit state and sends half of it to Bob through the channel. A mixed state ρ_{AB} is then shared by the two honest parties, due to the interaction with the environment controlled by Eve. Now, Alice and Bob measure in two bases to map their quantum correlations into classical correlations. For instance, if Alice and Bob measure in the computational bases, the QBER simply reads

$$\epsilon_{AB} = \langle 01|\rho_{AB}|01\rangle + \langle 10|\rho_{AB}|10\rangle.$$

It can be imposed that Alice's local state cannot be modified by Eve, since the corresponding particle never leaves Alice's lab, which is assumed to be

[1] For instance, it is sometimes said that in the BB84 protocol half of the symbols in the raw key are rejected after the sifting process. Although this is correct if one considers the original proposal, it is clear that Alice and Bob can employ just one of the basis for information encoding, and use it almost all the time, and occasionally change to the second basis to monitor the channel. Then, the sifted key length can, asymptotically, be as close as desired to the raw key, without compromising the security. See H.-K. Lo, H. F. Chau and M. Ardehali, quant-ph/0011056.

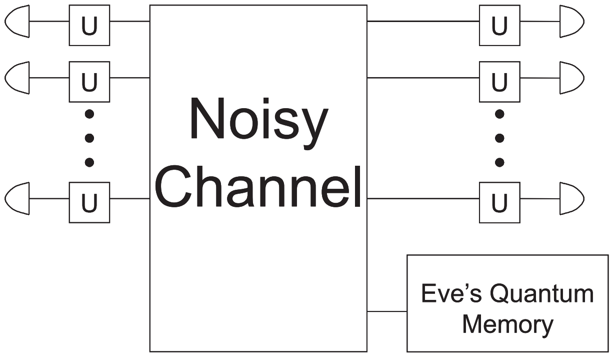

Figure 3.1: A tripartite pure state is prepared by Eve, who send two of the particles to Alice and Bob and keeps one. From Alice and Bob viewpoint the situation resembles a standard noisy channel. The honest parties perform measurements at the single copy level, possibly with some preliminary filtering step. Eve keeps her quantum states and can arbitrarily delay her collective measurement.

secure. It has to be clear that the techniques of [9] imply the equivalence between SIMCAP protocols on entangled states and prepare and measure QKD schemes: the correlation distribution is, from the secrecy point of view, identical. This equivalence, for instance, is lost if one considers entanglement distillation protocols for QKD, where the particles are measured by the honest parties after applying coherent quantum operations.

3.1.1 Classical Key Distillation

After the correlation distribution, either using prepare and measure or SIMCAP protocols, Alice and Bob share partially secret correlations to be distilled into the perfect key. The problem of distilling noisy and partially secret correlations into a secret key has not been completely solved. Recently, general lower bounds to the distillable secret-key rate by means of error correction and privacy amplification using one-way communication have been obtained in [31]. In case the correlations are too noisy for the direct use of one-way distillation techniques, Alice and Bob can before apply a protocol using two-way communication. The obtained correlations after this two-way process may become distillable using one-way protocols. Much less is known about key distillation using two-way communication. Here we mostly apply the standard two-way communication protocol introduced by Maurer in [69], also known as classical advantage distillation (CAD). Actually, we analyze the following two slightly different CAD protocols:

- *CAD1.* Alice and Bob share a list of correlated bits. Alice selects N of

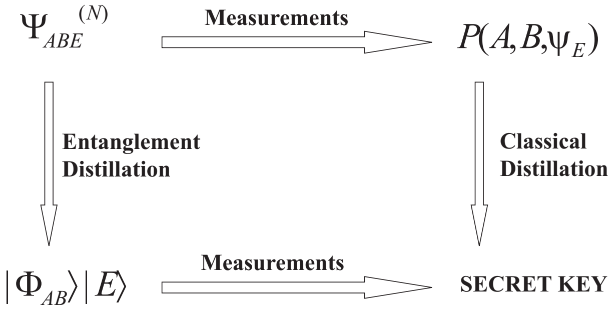

Figure 3.2: A secret key can be distilled either, by entanglement distillation plus measurement, which is a challenging technique, or by measurement plus classical processing, which is currently feasible.

her bits that have the same value and publicly announces the position of these symbols. Bob checks whether his corresponding symbols are also equal. If this is the case, Bob announces to Alice that he accepts, so they use the measurement values (they are all the same) as a bit for the new list. Otherwise, they reject the N values and start again the process with another block.

- *CAD2.* Alice locally generates a random bit s. She takes a block of N of her bits, A, and computes the vector

$$X = (X_1, \cdots, X_N) \tag{3.1}$$

such that $A_i + X_i = s$. She then announces the new block X through the public and authenticated classical channel. After receiving X, Bob adds it to his corresponding block, $B + X$, and accepts whenever all the resulting values are the same. If not, the symbols are discarded and the process is started again, as above.

These protocols are equivalent in classical cryptography and in the completely general quantum scenario. Nevertheless, it is shown in section 4.1.3 that they are different in the less general, but still relevant, scenario of individual attacks. In what follows, we restrict the analysis to key distillation protocols consisting of CAD followed by standard one-way error correction and privacy amplification. Thus, it is important to keep in mind that any security claim is referred to this type of key-distillation protocols. Although these are the protocols commonly used when considering two-way reconciliation techniques, their optimality, at least in terms of robustness, has not been proven.

3.2 Eavesdropping Strategies

After describing Alice and Bob's operations, it is now time to consider Eve's attacks. With full generality, we suppose that Eve has the power to control all the environment. That is, all the information that leaks out through the channel connecting Alice and Bob goes to Eve, so all the decoherence seen by Alice and Bob is introduced by her interaction. Following Ref. [4], eavesdropping strategies can be classified into three types: (i) individual, (ii) collective and (iii) coherent. Once more, although most of the following discussion is presented in the entanglement picture, the same conclusions apply to the corresponding prepare and measure scheme.

3.2.1 Individual Attacks

In an individual attack Eve is assumed to apply the same interaction to each state, without introducing correlations among copies, and measure her state right after this interaction. In this type of attacks, all three parties immediately measure their states, since no one is supposed to have the ability to store quantum states. Therefore, they end up sharing classical-classical-classical (CCC) correlated measurement outcomes[2], described by a probability distribution $P(A, B, E)$. In this case, standard results from Classical Information Theory can be directly applied. For instance, it is well known that the secret-key rate using one-way communication, $K_{\rightarrow}$, is bounded by so-called Csiszár-Körner bound [27],

$$K_{\rightarrow} \geq I(A:B) - I(A:E). \tag{3.2}$$

Here $I(A:B)$ is the mutual information between the measurement outcomes A and B. In this type of attacks, Eve's interaction can be seen as a sort of asymmetric cloning [20] producing two different approximate copies, one for Bob and one for her. This cloning transformation reads $U_{BE} : |\Phi^+\rangle_{AB}|E\rangle \rightarrow |\Psi\rangle_{ABE}$ where $\rho_{AB} = \mathrm{tr}_E|\Psi\rangle\langle\Psi|_{ABE}$. It has been shown that in the case of two qubits, two honest parties can distill a secret key secure against any individual attacks whenever their quantum state ρ_{AB} is entangled [2].

It is clear that to prove security against individual attacks is not satisfactory from a purely theoretical point of view. However, we believe it is a relevant issue when dealing with realistic eavesdroppers. Assume Eve's quantum memory decoherence rate is nonzero and the honest parties are able to estimate it. Then, they can introduce a delay between the state distribution and the distillation process long enough to prevent Eve keeping

[2] Throughout the chapter, we denote classical and quantum variables by C and Q, respectively. When writing correlations among the three parties, the order is Alice-Bob-Eve. For instance, CCQ means that Alice and Bob have correlated classical values (for instance, after some measurements), while Eve has a quantum state.

her states without errors. Eve is then forced to measure her states before the reconciliation, as for an individual attack.

3.2.2 Collective Attacks

Collective attacks represent, in principle, an intermediate step between individual and the most general attack. Eve is again assumed to apply the same interaction to each quantum state, but she has a quantum memory. In other words, she is not forced to measure her state after the interaction and can arbitrarily delay her measurement. In particular, she can wait until the end of the reconciliation process and adapt her measurement to the public information exchanged by Alice and Bob. After a collective attack, the two honest parties share N independent copies of the same state, $\rho_{AB}^{\otimes N}$, where no correlation exists from copy to copy. Without losing generality, the full state of the three parties can be taken equal to $|\psi\rangle_{ABE}^{\otimes N}$, where

$$|\psi\rangle_{ABE} = (I_A \otimes U_{BE})|\Phi^+\rangle_{AB}|E\rangle. \tag{3.3}$$

After a collective attack, and the measurements by Alice and Bob, the three parties share classical-classical-quantum (CCQ) correlations, described by a state

$$\sum_{a,b} |a\rangle\langle a| \otimes |b\rangle\langle b| \otimes |e_{ab}\rangle\langle_{ab}|, \tag{3.4}$$

where a and b denote Alice and Bob's measurement outcomes associated to the measurement projectors $|a\rangle\langle a|$ and $|b\rangle\langle b|$. Note that $|e_{ab}\rangle$ is not normalized, since $|e_{ab}\rangle = \langle ab|\psi\rangle_{ABE}$ and $p\,(a,b) = \mathrm{tr}[|e_{ab}\rangle\langle e_{ab}|]$.

The following result, obtained in [31, 63], is largely used in the next chapters 4 and 5. After a collective attack described by a state like (3.4), Alice and Bob's one-way distillable key rate satisfies

$$K_{\rightarrow} \geq I(A:B) - I(A:E). \tag{3.5}$$

Here, the correlations between Alice and Bob's classical variables are again quantified by the standard mutual information, $I(A:B)$. The correlations between Alice's classical and Eve's quantum variables, A and E, are quantified by the Holevo quantity,

$$I(A:E) = S(E) - S(E|A), \tag{3.6}$$

where S denotes the Shannon entropy, so $S(E) = S(\rho_E)$ and $S(E|A) = \sum_a p\,(a) S(\rho_E|A = a)$. Actually the "same" equation (3.5) applies when Bob is also able to store quantum states and the three parties share classical-quantum-quantum (CQQ) correlations. In this case, both mutual information quantities between Alice's classical variable, A, and Bob's and Eve's quantum states, denoted by B and E, should be understood as Holevo quantities [31]. Notice the similarities between (3.2) and (3.5). Indeed, the obtained bounds represent a natural generalization of the CK-bound to the CCQ and CQQ correlations scenarios.

3.2.3 General Attacks and the de Finetti Theorem

One has to consider the most general attack where Eve can perform any kind of interaction. In this case, Alice and Bob cannot assume to share N copies of the same quantum state. Compared to the previous attacks, there did not exist nice bounds for the extractable key-rate under general attacks. However, very recently a dramatic simplification on the security analysis of QKD protocols under general attacks has been achieved by means of the so-called de Finetti theorem [78]. Indeed, Renner has proven that general attacks cannot be more powerful than collective attacks in any protocol that is symmetric in the use of the quantum channel. This provides a huge simplification in security proofs, since by means of the de Finetti arguments (see [78] for more details), Alice and Bob can safely assume to share N copies of a quantum state consistent with their tomographic process, and then apply the existing bounds for this scenario. Note that the de Finetti theorem should also be employed if one wants to use entanglement distillation as a key distillation technique. In what follows, then, we can restrict our analysis to collective attacks, without underestimating Eve's capabilities.

3.3 Review of the existing Security Bounds

Finally, we would like to summarize the existing security bounds for the two most known QKD protocols, BB84 and six-state. These bounds are usually stated in terms of the critical QBER such that key distillation is possible. Of course, these bounds depend on the type of key distillation techniques employed by the honest parties. Since the first general security proof of BB84 by Mayers [71], security bounds have been constantly improved. Using a quantum error-correction (of bit-flip and phase-inversion) description of classical one-way error-correction and privacy amplification, Shor and Preskill showed the general security of BB84 whenever QBER$<$ 11% [82]. Later, Lo adapted their proof to 6-state protocol obtaining a critical QBER of 12.7% [66]. More recently, Kraus, Renner, and Gisin have improved these values by introducing some classical pre-processing by the two honest parties, obtaining critical QBER's of 12.4% for the BB84 and 14.1% for the six-state protocol [63]. More recently, the bound for BB84 has been improved up to 12.9% in Ref. [83]. On the other hand, the known upper bounds on the critical QBER are slightly higher than these lower bounds, so the exact value for the critical QBER remains as an open question.

The honest parties however can apply CAD to their outcomes before using one-way key distillation techniques and improve these bounds. The whole process can now be mapped into a two-way entanglement distillation protocol. Based on this analogy, Gottesman and Lo have obtained that secure QKD is possible whenever the QBER is smaller than 18.9% and 26.4% for the BB84 and six-state protocol, respectively [45]. Chau has improved

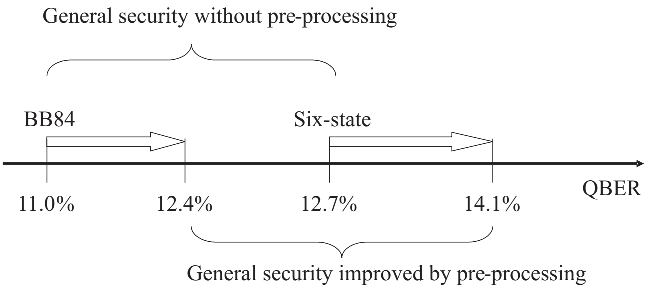
General security without pre-processing
BB84
Six-state
QBER
11.0%
12.4%
12.7%
14.1%
General security improved by pre-processing

Figure 3.3: Security bounds for QKD protocols using key distillation techniques with one-way communication: based on the analogy between these techniques and quantum error correction, the security bounds for the BB84 and the six-state protocols are 11% and 12.7% respectively. These bounds have later been improved by information-theoretic considerations up to 12.4% and 14.1%. The improvement is achieved using some classical preprocessing by one of the parties.

these bounds up to 20.0% and 27.6% respectively [22]. The generalization of the formalism [63] to two-way communication has also been done by Kraus, Branciard and Renner [64].

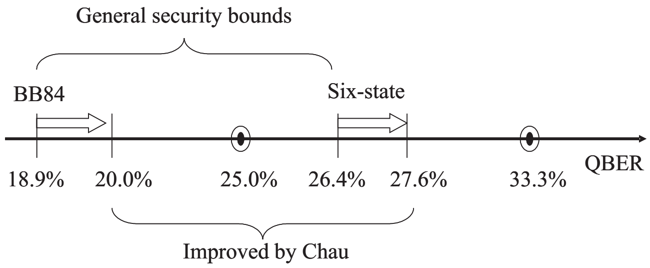

Figure 3.4: Security bounds for QKD protocols using two-way followed by one-way communication techniques: based on the analogy between the two-way plus one-way communication and two-way entanglement distillation protocol, general security bounds of the BB84 and the six-state protocols are given by 18.9% and 26.4% respectively [45]. Later, Chau improved the error correction method and the bounds are moved to 20.0% and 27.6% [22]. In Chapter 4, we show that those bounds are tight. Note that the key distillability condition is stronger than the entanglement condition, which is 25.0% and 33.3% for the BB84 and the six-state protocols.

Chapter 4

Key Distillation in Finite-Dimensional Systems

In this Chapter[1], we analyze the cryptographic properties of quantum channels when Alice and Bob employ the QKD schemes described in the previous chapter. Recall that in these schemes, (i) the correlation distribution is done using prepare and measure techniques and (ii) the key distillation process uses the standard one-way and two-way classical protocols. As said, none of these protocols requires the use of entangled particles. However, for the sake of simplicity, we perform our analysis in the completely equivalent entanglement picture. The problem then consists of identifying those quantum states that can be distilled into secret bits by SIMCAP protocols restricted to the known distillation techniques.

We first study qubit channels and provide a simple security condition, that turns out to be tight, under the considered distillation techniques. Since this condition is stronger than the entanglement condition, we explore several possibilities to improve the bound. We extend our analysis to higher dimensional systems. Finally, we apply the obtained conditions to specific QKD protocols, such as BB84, six-state and their generalizations to higher dimension.

4.1 Secrecy Properties of Qubit Channels

We here consider the situation where Alice and Bob are connected by a qubit channel. Alice locally prepares a maximally entangled state of two qubits and sends half of it through the channel. Then, both parties measure the state. By repetition of this process, they can obtain a complete, or partial, characterization of their channel, up to some precision. Indeed, there exists

[1] The results of this Chapter are based on two publications [4, 6].

a correspondence between a channel, Υ, and the state

$$(\mathbb{1} \otimes \Upsilon)|\Phi^+\rangle = \rho_{AB}. \tag{4.1}$$

Now, the parties agree on a pair of bases, that will later be used for the raw key distribution. They repeat the same process but now measure almost always in these bases. However, with small probability, they have to change their measurement to the previous tomographic process in order to check the channel. After public communication, they discard the asymptotically negligible fraction of symbols where any of them did not use the right basis and proceed with the key distillation. In what follows, we provide a security analysis of this type of schemes. Two important points should be mentioned again: (i) as said, these schemes can be easily transformed into a prepare and measure protocol, without entanglement and (ii) using de Finetti theorem, Alice and Bob can restrict Eve to collective attacks. In other words, they can assume to share N independent copies of the same state, $\rho_{AB}^{\otimes N}$, that is, the channel does not introduce correlation between the states. The goal, then, consists of finding the optimal SIMCAP protocol for the state ρ_{AB}, or equivalently, the best prepare and measure scheme for the channel Υ.

Generically, ρ_{AB} can be any two-qubit state. However, no key distillation is possible from separable states, so Alice and Bob abort their protocol if their measured data are consistent with a separable state [3]. We can assume, if the state preparation is done by Alice, that her local state, ρ_A, cannot be modified by Eve. In our type of schemes, this state is equal to the identity. Although our techniques can be used in the general situation, we mostly restrict our analysis to the case where Bob's state is also equal to the identity. This is likely to be the case in any realistic situation, where the channel affects with some symmetry the flying qubits. This symmetry is reflected by the local state on reception, i.e. $\rho_B = \mathbb{1}$. In the qubit case, the fact that the two local states are completely random simply means that the global state ρ_{AB} is Bell diagonal,

$$\rho_{AB} = \lambda_1|\Phi_1\rangle\langle\Phi_1| + \lambda_2|\Phi_2\rangle\langle\Phi_2| + \lambda_3|\Phi_3\rangle\langle\Phi_3| + \lambda_4|\Phi_4\rangle\langle\Phi_4|, \tag{4.2}$$

where $\sum_j \lambda_j = 1$, $\lambda_j > 0$, and

$$\begin{aligned}
|\Phi_1\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
|\Phi_2\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\
|\Phi_3\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\
|\Phi_4\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)
\end{aligned} \tag{4.3}$$

define the so-called Bell basis. Or in other words, Υ is a Pauli channel. Pauli channels are very useful, as it will become clearer below, in the analysis of the BB84 and six-state protocols.

It is also worth mentioning here that Alice and Bob can always transform their generic state ρ_{AB} into a Bell diagonal state by single-copy filtering operations. Actually, this operation is optimal in terms of entanglement concentration. Indeed, it maximizes the entanglement of formation of any state $\rho'_{AB} \propto (F_A \otimes F_B)\rho(F_A^\dagger \otimes F_B^\dagger)$ obtained after LOCC operations of a single copy of ρ_{AB} [87]. This filtering operation succeeds with probability $\mathrm{tr}(F_A \otimes F_B)\rho(F_A^\dagger \otimes F_B^\dagger)$. If ρ_{AB} is already in a Bell-diagonal form, it remains invariant under the filtering operation. Alternatively, Alice and Bob can also map their state into a Bell diagonal state by a depolarization protocol, where they apply randomly correlated change of basis, but some entanglement may be lost in this process. In view of all these facts, in what follows we mainly consider Bell diagonal states.

It is possible to identify a canonical form for these states. This follows from the fact that Alice and Bob can apply local unitary transformation such that

$$\lambda_1 = \max_i \lambda_i, \qquad \lambda_2 = \min_i \lambda_i \ . \tag{4.4}$$

Indeed, they can permute the Bell basis elements by performing the following operations

$$\begin{aligned} T(|\Phi_1\rangle \leftrightarrow |\Phi_2\rangle) &= 2^{-1} i(\mathbb{1} - i\sigma_z) \otimes (\mathbb{1} - i\sigma_z), \\ T(|\Phi_2\rangle \leftrightarrow |\Phi_3\rangle) &= 2^{-1}(\sigma_x + \sigma_z) \otimes (\sigma_x + \sigma_z), \\ T(|\Phi_3\rangle \leftrightarrow |\Phi_4\rangle) &= 2^{-1}(\mathbb{1} + i\sigma_z) \otimes (\mathbb{1} - i\sigma_z). \end{aligned} \tag{4.5}$$

Once the state has been casted in this canonical form, Alice and Bob measure it in the computational basis. The choice of the computational bases by Alice and Bob will be justified by our analysis. Indeed, once a Bell-diagonal state has been written in the previous canonical form, the choice of the computational bases seems to maximize the secret correlations between Alice and Bob, although, in general, they may not maximize the total correlations.

Before Alice and Bob' measurements, the global state including Eve is a pure state that purifies Alice and Bob's Bell diagonal state, that is,

$$|\Psi\rangle_{ABE} = \sum_{j=1}^{4} \sqrt{\lambda_j} |\Phi_j\rangle |j\rangle_E \tag{4.6}$$

where $|j\rangle_E$ define an orthonormal basis on Eve's space. All the purifications of Alice-Bob state are equivalent from Eve's point of view, since they only differ from a unitary operation in her space. After the measurements, Alice, Bob and Eve share CCQ correlations. In the next sections we study when these correlations can be distilled into a secure key using the standard CAD followed by one-way distillation protocols. We first obtain a sufficient condition for securtiy, using the lower bounds on the secret-key rate given above, c.f. (3.5). Then, we compute a necessary condition that follows from a specific eavesdropping attack. It is then shown that the two conditions coincide, so the resulting security condition is necessary and sufficient, under the mentioned distillation techniques. Next, we apply this condition to two known examples, the BB84 and the six-state protocols. We finally discuss several ways of improving the derived condition, by changing the distillation techniques, including classical pre-processing by the parties or one-party's coherent quantum operations.

4.1.1 Sufficient Condition

In this section we will derive the announced sufficient condition for security using the lower bound on the secret-key rate of Eq. (3.5). Just before the measurements, the honest parties share a Bell diagonal state (4.2). This state is entangled if and only if $\sum_{j=2}^{4}\lambda_j < \lambda_1$, which follows from the fact that the positivity of the partial transposition is a necessary and sufficient condition for separability in 2×2 systems [77]. When Alice and Bob measure in their computational bases, they are left with classical data $|i\rangle_A\langle i|\otimes|j\rangle_B\langle j|$ $(i,j\in\{0,1\})$ whereas Eve still holds a quantum correlated system $|e_{i,j}\rangle_E$. The CCQ correlations they share are described by the state (up to normalization)

$$\rho_{ABE} \propto \sum_{i,j} |i\rangle_A\langle i| \otimes |j\rangle_B\langle j| \otimes |\widetilde{e_{i,j}}\rangle\langle\widetilde{e_{i,j}}|, \tag{4.7}$$

where Eve's states are

$$\begin{aligned}
|\widetilde{e_{0,0}}\rangle &= \sqrt{\lambda_1}|1\rangle + \sqrt{\lambda_2}|2\rangle \\
|\widetilde{e_{0,1}}\rangle &= \sqrt{\lambda_3}|3\rangle + \sqrt{\lambda_4}|4\rangle \\
|\widetilde{e_{1,0}}\rangle &= \sqrt{\lambda_3}|3\rangle - \sqrt{\lambda_4}|4\rangle \\
|\widetilde{e_{1,1}}\rangle &= \sqrt{\lambda_1}|1\rangle - \sqrt{\lambda_2}|2\rangle,
\end{aligned} \tag{4.8}$$

and the corresponding states without tilde denote the normalized vectors. So, after the measurements, Alice and Bob map $\rho_{AB}^{\otimes N}$, into a list of measurement outcomes, whose correlations are given by $P_{AB}(i,j)$, where

$$P_{AB}(i,j) = \langle ij|\rho_{AB}|ij\rangle. \tag{4.9}$$

This probability distribution reads as follows:

A \ B	0	1
0	$(1-\epsilon_{AB})/2$	$\epsilon_{AB}/2$
1	$\epsilon_{AB}/2$	$(1-\epsilon_{AB})/2$

Here, ϵ_{AB} denotes the QBER, that is,

$$\epsilon_{AB} = \langle 01|\rho_{AB}|01\rangle + \langle 10|\rho_{AB}|10\rangle = \lambda_3 + \lambda_4. \qquad (4.10)$$

Alice and Bob now apply CAD to a block of N symbols. Eve listens to the public communication that the two honest parties exchange. In particular, she has the position of the N symbols used by Alice in (3.1), in case the honest parties use $CAD1$ or the N-bit string X for $CAD2$. In the second case, Eve applies to each of her symbols the unitary transformation

$$U_i = |1\rangle\langle 1| + (-1)^{X_i}|2\rangle\langle 2| + |3\rangle\langle 3| + (-1)^{X_i}|4\rangle\langle 4|. \qquad (4.11)$$

This unitary operation transforms $|e_{i,j}\rangle_E$ into $|e_{s,j}\rangle_E$ where s is the secret bit generated by Alice. If Alice and Bob apply CAD1, Eve does nothing. In both cases, the resulting state is

$$\begin{aligned}\rho^N_{ABE} &= \frac{(1-\epsilon_N)}{2}\sum_{s=0,1}|ss\rangle_{AB}\langle ss|\otimes|e_{s,s}\rangle\langle e_{s,s}|^{\otimes N} \\ &+ \frac{\epsilon_N}{2}\sum_{s=0,1}|s\bar{s}\rangle_{AB}\langle s\bar{s}|\otimes|e_{s,\bar{s}}\rangle\langle e_{s,\bar{s}}|^{\otimes N}, \end{aligned} \qquad (4.12)$$

where $\bar{s} = s+1$ and ϵ_N is Alice-Bob error probability after CAD,

$$\epsilon_N = \frac{\epsilon^N_{AB}}{\epsilon^N_{AB} + (1-\epsilon_{AB})^N} \leq \left(\frac{\epsilon_{AB}}{1-\epsilon_{AB}}\right)^N, \qquad (4.13)$$

and the last inequality tends to an equality when $N \to \infty$. That is, whatever the advantage distillation protocol is, i.e. either CAD1 or CAD2, all the correlations among the three parties before the one-way key extraction step are described by the state (4.12).

We can now apply Eq. (3.5) to this CQQ state. The probability distribution between Alice and Bob has changed to

A \ B	0	1
0	$(1-\epsilon_N)/2$	$\epsilon_N/2$
1	$\epsilon_N/2$	$(1-\epsilon_N)/2$

where it can be seen that Alice and Bob have improved their correlation. The CAD protocol has changed the initial probability distribution $P(A,B)$, with error rate ϵ_{AB}, into $P^{'}(A,B)$, with error rate ϵ_N. The mutual information between Alice and Bob $I(A:B)$ is easily computed from the above table. $I(A:E)$ can be derived from (4.12), so, after some algebra, the following equality is obtained

$$\begin{aligned} & I(A:B) - I(A:E) = 1 - h(\epsilon_N) \\ & -(1-\epsilon_N)\,h\left(\frac{1-\Lambda^M_{\text{eq}}}{2}\right) - \epsilon_N\,h\left(\frac{1-\Lambda^M_{\text{dif}}}{2}\right), \end{aligned} \qquad (4.14)$$

where

$$\begin{aligned}\Lambda_{\rm eq} &= \frac{\lambda_1-\lambda_2}{\lambda_1+\lambda_2}=|\langle e_{0,0}|e_{1,1}\rangle| \\ \Lambda_{\rm dif} &= \frac{|\lambda_3-\lambda_4|}{\lambda_3+\lambda_4}=|\langle e_{1,0}|e_{0,1}\rangle|,\end{aligned} \tag{4.15}$$

$h(x)=-x\log_2 x-(1-x)\log_2(1-x)$ is the binary entropy, and the subscript 'eq' ('dif') refers to the resulting value of Alice being equal to (different from) that of Bob.

Let's compute this quantity in the limit of a large number of copies, $N \gg 1$, where $\epsilon_N, \Lambda_{\rm eq}, \Lambda_{\rm dif} \ll 1$. It can be seen that in this limit

$$\begin{aligned} I(A:B) &\approx 1+\epsilon_N\log\epsilon_N \\ I(A:E) &\approx 1-\frac{1}{\ln 4}\Lambda_{\rm eq}^{2N}. \end{aligned} \tag{4.16}$$

The security condition follows from having positive value of the Eq. (4.14), which holds if

$$|\langle e_{0,0}|e_{1,1}\rangle|^2 > \frac{\epsilon_{AB}}{1-\epsilon_{AB}}. \tag{4.17}$$

More precisely, if this condition is satisfied, Alice and Bob can always establish a large but finite N such that Eq. (4.14) becomes positive. Eq. (4.17) can be rewritten as

$$(\lambda_1+\lambda_2)(\lambda_3+\lambda_4) < (\lambda_1-\lambda_2)^2. \tag{4.18}$$

Therefore, whenever the state of Alice and Bob satisfies the security condition (4.17) above, they can extract from ρ_{AB} a secret key with our SIMCAP protocol. This gives the searched sufficient condition for security for two two-qubit Bell diagonal states or, equivalently, Pauli channels. Later, it is proven that whenever condition (4.17) does not hold, there exists an attack by Eve such that no standard key-distillation protocol works.

Condition (4.17) has a clear physical meaning. The r.h.s of (4.17) quantifies how fast Alice and Bob's error probability goes to zero when N increases. In the same limit, and since there are almost no errors in the symbols filtered by the CAD process, Eve has to distinguish between N copies of $|e_{0,0}\rangle$ and $|e_{1,1}\rangle$. The trace distance between these two states provides a measure of this distinguishability. It is easy to see that for large N

$$\begin{aligned} & {\rm tr}||e_{0,0}\rangle\langle e_{0,0}|^{\otimes N}-|e_{1,1}\rangle\langle e_{1,1}|^{\otimes N}| \\ = \;& 2\sqrt{1-|\langle e_{0,0}|e_{1,1}\rangle|^{2N}} \approx 2-|\langle e_{0,0}|e_{1,1}\rangle|^{2N}. \end{aligned}$$

Thus, the l.h.s. of (4.17) quantifies how the distinguishability of the two quantum states on Eve's side after CAD increases with N. This intuitive idea is indeed behind the attack described in the next section.

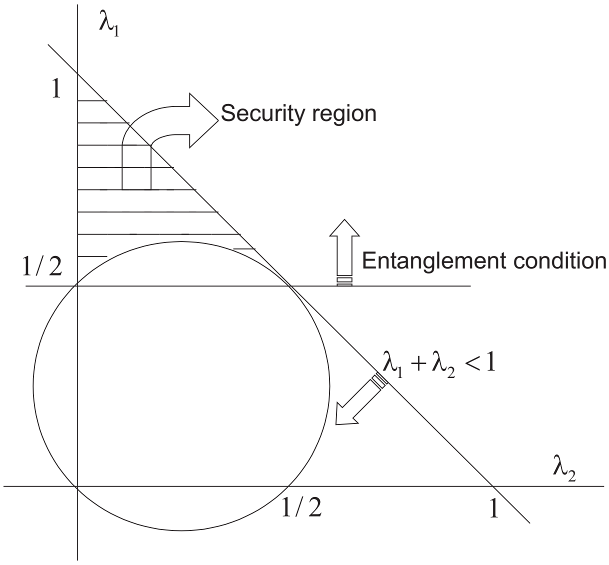

Figure 4.1: Graphical depiction of the security condition (4.18): the security region is defined by the intersection of the entanglement condition $\lambda_1 > 1/2$, the normalization condition $\lambda_1 + \lambda_2 < 1$, and the security condition (4.18).

Once this sufficient condition has been obtained, we can justify the choice of the computational bases for the measurements by Alice and Bob when sharing a state (4.2). Note that the same reasoning as above can be applied to any choice of bases. The derived security condition simply quantifies how Alice-Bob error probability goes to zero with N compared to Eve's distinguishability of the N copies of the states $|e_{0,0}\rangle$ and $|e_{1,1}\rangle$, corresponding to the cases $a = b = 0$ and $a = b = 1$. The obtained conditions are not as simple as for measurements in the computational bases, but they can be easily computed using numerical means. One can, then, perform a numerical optimization over all choice of bases by Alice and Bob. An exhaustive search shows that computational bases are optimal for this type of security condition. It is interesting to mention that the bases that maximize the classical correlations, or minimize the error probability, between Alice and Bob do not correspond to the computational bases for all Bell diagonal states (4.2). Thus, these bases optimize the *secret correlations* between the two honest parties, according to our security condition, although they may be not optimal for classical correlations.

4.1.2 Necessary Condition

After presenting the security condition (4.17), we now give an eavesdropping attack that breaks our SIMCAP protocol whenever this condition does not hold. This attack is very similar to that in Ref. [61].

Without loss of generality, we assume that all the communication in the one-way reconciliation part of the protocol goes from Alice to Bob. In this attack, Eve delays her measurement until Alice and Bob complete the CAD part of the distillation protocol. Then, she applies on each of her systems the two-outcome measurement defined by the projectors

$$F_{\text{eq}} = |1\rangle_E\langle 1| + |2\rangle_E\langle 2|, \quad F_{\text{dif}} = |3\rangle_E\langle 3| + |4\rangle_E\langle 4|. \tag{4.19}$$

According to (4.12), all N measurements give the same outcome. If Eve obtains the outcome corresponding to F_{eq}, the tripartite state is (up to normalization)

$$\begin{aligned} & |00\rangle_{AB}\langle 00| \otimes |e_{0,0}\rangle_E\langle e_{0,0}|^{\otimes N} \\ + \quad & |11\rangle_{AB}\langle 11| \otimes |e_{1,1}\rangle_E\langle e_{1,1}|^{\otimes N}. \end{aligned} \tag{4.20}$$

In order to learn s_A, Alice's bit, she has to discriminate between the two pure states $|e_{0,0}\rangle^{\otimes N}$ and $|e_{1,1}\rangle^{\otimes N}$. The minimum error probability in such discrimination is [51]

$$\epsilon_{\text{eq}} = \frac{1}{2} - \frac{1}{2}\sqrt{1 - |\langle e_{0,0}|e_{1,1}\rangle|^{2N}}, \tag{4.21}$$

Her guess for Alice's symbol is denoted by s_E. On the other hand, if Eve obtains the outcome corresponding to F_{dif}, the state of the three parties is

$$\begin{aligned} & |01\rangle_{AB}\langle 01| \otimes |e_{0,1}\rangle_E\langle e_{0,1}|^{\otimes N} \\ + \quad & |10\rangle_{AB}\langle 10| \otimes |e_{1,0}\rangle_E\langle e_{1,0}|^{\otimes N}. \end{aligned} \tag{4.22}$$

The corresponding error probability ϵ_{dif} is the same as in Eq. (4.21), with the replacement $|\langle e_{0,0}|e_{1,1}\rangle| \to |\langle e_{0,1}|e_{1,0}\rangle|$. Note that $|\langle e_{0,0}|e_{1,1}\rangle| \geq |\langle e_{0,1}|e_{1,0}\rangle|$. Eve's information now consists of s_E, as well as the outcome of the measurement (4.19), $r_E = \{\text{eq}, \text{dif}\}$. It is shown in what follows that the corresponding probability distribution $P(s_A, s_B, (s_E, r_E))$ cannot be distilled using one-way communication. In order to do that, we show that Eve can always map P into a new probability distribution, Q, which is not one-way distillable. Therefore, the non-distillability of P is implied.

Eve's mapping from P to Q works as follows: she increases her error until $\epsilon_{\text{dif}} = \epsilon_{\text{eq}}$. She achieves this by changing with some probability the value of s_E when $r_E = \text{dif}$. After this, Eve forgets r_E. The resulting tripartite probability distribution Q satisfies $Q(s_B, s_E|s_A) = Q(s_B|s_A)\, Q(s_E|s_A)$. Additionally, we know that $Q(s_B|s_A)$ and $Q(s_E|s_A)$ are binary symmetric channels with error probability $\epsilon_B (= \epsilon_N$ in (4.13)) and ϵ_{eq} in (4.21), respectively. It is proven in [69] that in such situation the one-way key rate is

$$K_{\rightarrow} = h(\epsilon_{\text{eq}}) - h(\epsilon_B), \tag{4.23}$$

which is non-positive if

$$\epsilon_{\text{eq}} \leq \epsilon_B \ . \tag{4.24}$$

Let us finally show that this inequality is satisfied for all values of N whenever the condition (4.17) does not hold. Writing $z = \lambda_1 + \lambda_2$, we have $1/2 \leq z \leq 1$, since the state of Alice and Bob is assumed entangled. Using the following inequality

$$\frac{1}{2} - \frac{1}{2}\sqrt{1 - \left(\frac{1-z}{z}\right)^N} \leq \frac{(1-z)^N}{z^N + (1-z)^N}, \tag{4.25}$$

which holds for any positive N, the right-hand side of (4.25) is equal to ϵ_B, whereas the left-hand side is an upper bound for ϵ_{eq}. This bound follows from the inequality $(\lambda_1 - \lambda_2)^2/z^2 \leq (1-z)/z$, which is the negation of (4.17). That is, if condition (4.17) is violated, no secret key can be distilled with our SIMCAP protocol. More precisely, there exists no N such that CAD followed by one-way distillation allows to establish a secret key. Since (4.17) is sufficient for security, the attack we have considered is in some sense optimal and the security bound (4.17) is tight for our SIMCAP protocol.

It is worth analyzing the resources that this optimal eavesdropping attack requires. First of all, note that Eve does not need to perform any coherent quantum operation, but she only requires single-copy level (individual) measurements. This is because when discriminating N copies of two states, there exists an adaptative sequence of individual measurements which achieves the optimal error probability (4.21) [14]. However, what Eve really needs is the ability to store her quantum states after listening to the (public) communication exchanged by Alice and Bob during the CAD part of the protocol.

4.1.3 Inequivalence of CAD1 and CAD2 for Individual Attacks

As we have seen, the two CAD protocols lead to the same security condition. This follows from the fact that Eve is not assumed to measure her state before the CAD takes place. Then, she can effectively map one CAD protocol into the other by means of the reversible operation U_E. This is no longer true in the case of individual attacks. Interestingly, in this scenario, the two two-way distillation methods do not give the same security condition. As mentioned, although the study of individual attacks gives a weaker security, it is relevant in the case of realistic eavesdroppers. Moreover, we believe the present example has some interest as a kind of toy model illustrating the importance of the reconciliation part for security. Recall that in the case of individual attacks, where Eve can neither perform coherent operations nor have a quantum memory, the security condition using $CAD2$ is the entanglement condition $\lambda_1 > 1/2$ [2]. However, when the honest parties apply $CAD1$ plus one-way communication, the security condition is (4.17). This holds true for two-qubit protocols, and remains open for the two-qudit protocols studied in the next sections[2].

Let us suppose that Alice and Bob apply $CAD1$ and consider the following individual attack. Eve knows that for all the instances passing the CAD protocol, Alice and Bob's symbols are equal with very high probability. Moreover, she knows that in all the position announced by Alice, Alice's symbol is the same. Therefore, from her point of view, the problem reduces to the discrimination of N copies of the two states $|e_{i,i}\rangle$. Thus, she has to apply the measurement that optimally discriminates between these two states. As mentioned, the optimal two-state discrimination [14] can be achieved by an adaptive individual measurement strategy. Therefore, Eve can apply this adaptive strategy to her states right after her individual interaction. Her error probability is again given by (4.21). That is, although the attack is individual, the corresponding security condition is the same as for collective attacks.

This N-copy situation on Eve's space does not happen when Alice and Bob apply $CAD2$. Indeed, Eve maps $CAD2$ into $CAD1$ by applying the correcting unitary operation U_i after knowing the vector X used in $CAD2$. This is the key point that allowed her to map one situation into the other above. This is however not possible in the case of individual attacks, where Eve is assumed to measure before the reconciliation part takes place. Under individual attacks, the security condition for $CAD2$ is equivalent to the entanglement condition for Bell diagonal states, as shown in [2]. Therefore, the two CAD protocols, which have proven to be equivalent in terms of robustness against general quantum attacks, become inequivalent in the restricted case of individual attacks.

4.1.4 Examples: BB84 and Six-state Protocols

The goal of the previous study has been to provide a general formalism for determining the security of qubit channels under a class of realistic QKD protocols. Relevant *prepare and measure* schemes, such as the BB84 and six-state protocol, constitute a particular case of our analysis. Indeed, the process of correlation distribution and channel tomography in these protocols is done by Alice preparing states from and Bob measuring in two (BB84) or three (six-state) bases. In this section, we apply the derived security condition to these protocols and compare the obtained results with previous security bounds. As explained in 3.3, a standard figure of merit in the security analysis of a given QKD protocol is given by the maximum error rate such that key distillation is still possible. For instance, in the case of one-way communication, the values of the critical error rates keep

[2] This is closely related to the 31st problem in http://www.imaph.tu-bs.de/qi/problems/.

improving (see [83] for the latest result in this sense) since the first general security proof by Mayers [71]. In the case of reconciliation using two-way communication, the best known results were obtained by Chau in [22]. It is then important to know whether these bound can be further improved. In what follows, it is shown that our necessary condition for security implies that Chau's bounds cannot be improved. In order to do that, then, one has to employ other reconciliation techniques, different from advantage distillation plus one-way standard techniques. Some of these possibilities are discussed in the next sections.

BB84 protocol

One can easily see that in the entanglement-based scheme, a family of attacks by Eve producing a QBER Q is given by the Bell-diagonal states (see also [78])

$$\begin{aligned}\rho_{AB} &= (1-2Q+x)|\Phi_1\rangle\langle\Phi_1| + (Q-x)|\Phi_2\rangle\langle\Phi_2| \\ &\quad +(Q-x)|\Phi_3\rangle\langle\Phi_3| + x|\Phi_4\rangle\langle\Phi_4|, \end{aligned} \tag{4.26}$$

since the QBER is

$$\begin{aligned} Q &= \langle 01|\rho_{AB}|01\rangle + \langle 10|\rho_{AB}|10\rangle \\ &= \langle +-|\rho_{AB}|+-\rangle + \langle -+|\rho_{AB}|-+\rangle \end{aligned} \tag{4.27}$$

and $0 \leq x \leq Q$. When Alice and Bob apply one-way communication distillation, the attack that minimizes (3.5) is $x = Q^2$, and leads to the well-known value of $QBER = 11\%$, first obtained by Shor and Preskill in [82]. The corresponding unitary interaction by Eve is equal to the phase-covariant cloning machine, that optimally clones qubits in an equator (in this case, in the xz plane).

When one considers the two-way distillation techniques studied in this protocol, condition (4.17), or (4.18), applies. Then, one can see that the optimal attack, for fixed QBER, consists of taking $x = 0$. Therefore, Eve's attack is, not surprisingly, strongly dependent on the type of reconciliation employed. In the case of two-way communication, Eve's optimal interaction can also be seen as a generalized phase-covariant cloning transformation, which is shown in the Appendix I. Using this attack, the derived necessary condition for security is violated when $QBER = 20\%$. This is precisely the same value obtained by Chau in his general security proof of BB84 [22]. So, the considered collective attack turns out to be tight, in terms of robustness. Recall that the security bound against individual attacks is at the entanglement limit, in this case giving $QBER = 25.0\%$ [2, 77]. The full comparison is depicted in the Fig. (3.4).

Note also that the state (4.26) with $x = 0$, associated to the optimal attack, does not fit into our canonical form for Bell diagonal states, since λ_2

is not the minimal Bell coefficient. This simply means that key distillation from this state using a SIMCAP protocol is still possible. Alice and Bob only have to measure in a different basis, namely in the y basis. That is, if Alice and Bob knew to share this state, or channel, and could prepare and measure states in the y basis, not used in the considered version of BB84, they would be able to establish a secure key. This channel is still useful for QKD using a prepare and measure scheme, although not using the considered version of BB84. In our opinion, this illustrates why the present approach, that aims at identifying secrecy properties of channels without referring to a given protocol, is more general.

Six-state protocol

It is easy to see that, in the entanglement-based scheme, an attack by Eve producing a QBER equal to Q is given by the Bell diagonal state

$$\begin{aligned}\rho_{AB} &= (1-\frac{3}{2}Q)|\Phi_1\rangle\langle\Phi_1| + \frac{Q}{2}|\Phi_2\rangle\langle\Phi_2| \\ &+\frac{Q}{2}|\Phi_3\rangle\langle\Phi_3| + \frac{Q}{2}|\Phi_4\rangle\langle\Phi_4|. \end{aligned} \tag{4.28}$$

This attack actually corresponds to Eve applying the universal cloning transformation. Contrary to what happened for BB84, this attack is optimal for both types of reconciliation protocols, using one- or two-way communication.

Applying the security condition (4.17), the security bound gives a critical QBER of $Q = 27.6\%$. This value again coincides with the one obtained by Chau in his general security proof of [22] for the six-state protocol. The present attack, then, is again tight. In the case of indidual attacks, the security bound [2] is the entanglement limit $Q = 33.3\%$.

4.2 Can These Bounds Be Improved?

The previous section has applied the obtained security condition to two well-known QKD protocols. In the corresponding attack, Eve is forced to interact individually and in the same way with the sent qubits. As discussed, the de Finetti results by Renner imply that this does not pose any restriction on Eve's attack. However, Eve is also assumed to measure her states right after CAD, while she could have delayed her measurement, for instance until the end of the entire reconciliation. In spite of this apparent limitation, the condition is shown to be tight, under the considered distillation techniques, for the two protocols. As it has been mentioned, the obtained bounds do not coincide with the entanglement limit. This raises the question whether prepare and measure schemes, in general, do attain this limit. Or in other words, it suggests the existence of channels that, although can be used to distribute distillable entanglement, are useless for QKD using prepare and

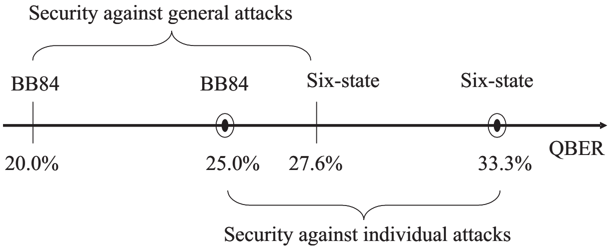
Security against general attacks
BB84
BB84
Six-state
Six-state
QBER
20.0%
25.0%
27.6%
33.3%
Security against individual attacks

Figure 4.2: Security bounds of the BB84 and the six-state protocols against individual and collective attacks: When Eve is supposed to apply individual attacks, all entangled states are distillable to a secret key. Assuming general attacks, security bounds are 20.0% and 27.6%, respectively, for the BB84 and the six-state protocols. This means that non-distillable secret correlations may exist.

measure techniques. Recall that a channel that allows to establish distillable entanglement is secure: this just follows from combining the de Finetti argument with standard entanglement distillation. So, in this sense the channel indeed contains distillable secrecy. However, our results suggest that this secrecy is non-distillable, or bound, using single-copy measurements. That is, this secrecy is distillable only if both parties are able to perform coherent quantum operations. Perhaps, the simplest example of this channel is given by (4.28) with $Q > 27.6\%$, i.e. by a weakly entangling depolarizing channel.

The aim of this section is to explore two possibilities to improve the previous security bounds. We first consider the classical pre-processing introduced in Ref. [63], in which previous security bounds using one-way communication protocols for BB84 and six-state protocols have been improved by allowing one of the honest parties to introduce some local noise. This noise worsens the correlations between Alice and Bob, but it deteriorates in a stronger way the correlations between Alice and Eve. Here, we study whether a similar effect can be obtained in the case of the considered two-way communication protocols. In a similar way as in Ref. [63], we allow one of the two parties to introduce some noise, given by a binary symmetric channel (BSC). In our case, however, this form of pre-processing does not give any improvement on the security bounds. Later, we study whether the use of coherent quantum operations by one of the parties helps. We analyze a protocol that can be understood as a hybrid between classical and entanglement distillation protocol. Remarkably, this protocol does not provide any improvement either. In our opinion, these results strengthen the conjectured bound secrecy of these weakly entangled states when using SIMCAP protocols[3].

[3] It is worth mentioning here that some of the techniques studied in this section may

4.2.1 Pre-processing by One Party

Recently, it has been observed that local classical pre-processing by the honest parties of their measurement outcomes can improve the security bounds of some QKD protocols [63]. For instance, Alice can map her measurement values X into another random variable U, and this transforms the mutual information from $I(X:B)$ into $I(U:B)$. At the same time, $I(X:E)$ changes to $I(U:E)$. In general, this mapping makes the mutual information of Alice and Bob decrease, but bounds on the secret key rate may improve, e.g. $I(U:B)-I(U:E)>I(X:B)-I(X:E)$. Actually, by applying a simple BSC of probability q, where the input value is kept unchanged with probability $1-q$ or flipped with probability q, Alice may be able to improve the one-way secret-key rate [63]. Using this technique, the security bounds have been moved from 11% to 12.4% for the BB84 protocol and from 12.7% to 14.1% in the six-state protocol [63]. Here, we analyze whether a similar effect happens in the case of protocols consisting of two-way communication. Note that pre-processing is useless if applied after CAD. Indeed, recall that the situation after CAD for the attack of Section 4.1.2 is simply given by two independent BSC channels between Alice and Bob and Alice and Eve, where pre-processing is known to be useless. The only possibility left is that Alice and/or Bob apply this pre-processing before the whole reconciliation protocol takes place.

As mentioned, Alice's pre-processing consists of a BSC channel, where her measurement value j is mapped into j and $j+1$ with probabilities $1-q$ and q, respectively. After this classical pre-processing, the state of the three parties is

$$\sigma_{ABE} \propto \sum_{i,j} |i,j\rangle_{AB}\langle i,j| \otimes \widetilde{\rho_{i,j}}$$

where

$$\begin{aligned}
\widetilde{\rho_{0,0}} &= (1-q)(1-\epsilon_{AB})|e_{0,0}\rangle\langle e_{0,0}| + q\epsilon_{AB}|e_{1,0}\rangle\langle e_{1,0}| \\
\widetilde{\rho_{0,1}} &= (1-q)\epsilon_{AB}|e_{0,1}\rangle\langle e_{0,1}| + q(1-\epsilon_{AB})|e_{1,1}\rangle\langle e_{1,1}| \\
\widetilde{\rho_{1,0}} &= q(1-\epsilon_{AB})|e_{0,0}\rangle\langle e_{0,0}| + (1-q)\epsilon_{AB}|e_{1,0}\rangle\langle e_{1,0}| \\
\widetilde{\rho_{1,1}} &= q\epsilon_{AB}|e_{0,1}\rangle\langle e_{0,1}| + (1-q)(1-\epsilon_{AB})|e_{1,1}\rangle\langle e_{1,1}|
\end{aligned} \tag{4.29}$$

and ϵ_{AB} denotes the QBER of the original measurement data, i.e. the error rate before applying pre-processing. The states with tilde are not

improve the key rate for some values of the error rate. However, we prove here that they do not improve the critical tolerable error rate.

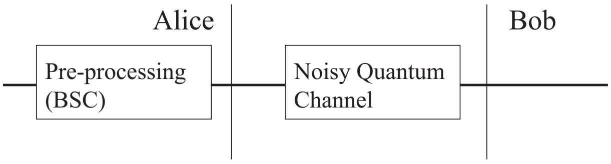

Figure 4.3: Considered classical pre-processing: Alice introduces some extra noise by permuting her classical variable with probability q.

normalized, so

$$\begin{aligned}\widetilde{\rho_{i,i}} &= \left((1-q)(\frac{1-\epsilon_{AB}}{2}) + q\frac{\epsilon_{AB}}{2}\right)\rho_{i,i}\\ \widetilde{\rho_{i,i+1}} &= \left((1-q)\frac{\epsilon_{AB}}{2} + q(\frac{1-\epsilon_{AB}}{2})\right)\rho_{i,i+1}.\end{aligned}$$

Next, Alice and Bob apply two-way CAD to $\sigma_{ABE}^{\otimes N}$. A new error rate is obtained after CAD. The rest of the distillation part, then, follows the same steps as in section V-A.

We now compute the mutual information between the honest parties after CAD. The new error rate of Alice and Bob is introduced by the BSC above, and is expressed as $\omega = tr_{ABE}[\sigma_{ABE}(|01\rangle_{AB}\langle 01| + |10\rangle_{AB}\langle 10|)] = (1-q)\epsilon_{AB} + q(1-\epsilon_{AB})$. For large N, the mutual information of Alice and Bob tends to, c.f. (4.16),

$$I^P(A:B) \approx 1 + (\frac{\omega}{1-\omega})^N \log(\frac{\omega}{1-\omega})^N.$$

In the same limit, Eve's state can be very well approximated by

$$\sigma_E \approx \frac{1}{2}(\rho_{00}^{\otimes N} + \rho_{11}^{\otimes N}),$$

since $||\widetilde{\rho_{i,i}}|| > ||\widetilde{\rho_{i,j}}||$. After some patient algebra, one can see that the Holevo information of Alice and Eve channel is (see also Appendix II):

$$I^P(A:E) \approx 1 - \frac{1}{\ln 4}(u|\langle e_{0,0}|e_{1,1}\rangle|^2 + v|\langle e_{0,1}|e_{1,0}\rangle|^2)^N$$

where

$$u = \frac{(1-q)(1-\epsilon_{AB})}{q\epsilon_{AB} + (1-q)(1-\epsilon_{AB})},$$

and $u + v = 1$. The case of $q = 0$ (or equivalently, $u = 1$) recovers the initial mutual information $I(A:E)$. Therefore, the security condition of this protocol is

$$u|\langle e_{0,0}|e_{1,1}\rangle|^2 + v|\langle e_{0,1}|e_{1,0}\rangle|^2 > \frac{\omega}{1-\omega}. \tag{4.30}$$

More precisely, whenever this condition is satisfied, there exists a finite N such that $I^P(A:B) - I^P(A:E) > 0$.

The derived bound looks again intuitive. The r.h.s quantifies how Alice and Bob's error probability for the accepted symbols converges to zero when N is large. If one computes the trace distance between $\rho_{0,0}$ and $\rho_{1,1}$, as defined in Eq. (4.29), one can see that

$$\begin{aligned} & \mathrm{tr}|\rho_{0,0} - \rho_{1,1}| \\ \approx\ & 2 - (u|\langle e_{0,0}|e_{1,1}\rangle|^2 + v|\langle e_{0,1}|e_{1,0}\rangle|^2)^N, \end{aligned} \tag{4.31}$$

which gives the l.h.s. of (4.30). This result suggests that the derived condition may again be tight. That is, it is likely there exists an attack by Eve breaking the security of the protocol whenever (4.30) is not satisfied. This attack would basically be the same as above, where Eve simply has to measure after the CAD part of the protocol.

Our goal is to see whether there exist situations where pre-processing is useful. Assume this is the case, that is, there exists a state for which (4.30) holds, for some value of q, while (4.17) does not. Then,

$$\frac{\epsilon_{AB}}{1-\epsilon_{AB}} \geq |\langle e_{00}|e_{11}\rangle|^2 > \frac{1}{u}\left(\frac{\omega}{1-\omega} - v|\langle e_{01}|e_{10}\rangle|^2\right). \tag{4.32}$$

After some simple algebra, one gets the inequality:

$$\frac{1}{\epsilon_{AB}} < 1 + |\langle e_{01}|e_{10}\rangle|^2.$$

The r.h.s. of this equation is smaller than 2, and this implies that $\epsilon_{AB} > 1/2$. Since this contradicts to that $0 \leq \epsilon_{AB} < 1/2$, we conclude that one-party pre-processing does not improve the obtained security bound.

Notice that since the reconciliation part uses communication in both directions, it seems natural to consider pre-processing by the two honest parties, where Alice and Bob introduce some noise, described by the probabilities q_A and q_B. In this case, however, the analytical derivation is much more involved, even in the case of symmetric pre-processing. Our preliminary numerical calculations suggest that two-parties pre-processing may be useless as well. However, these calculations should be interpreted in a very careful way. Indeed, they become too demanding already for a moderate N, since one has to compute the von Neumann entropies for states in a large Hilbert space, namely $\rho_{0,0}^{\otimes N}$ and $\rho_{1,1}^{\otimes N}$. Therefore, the detailed analysis of pre-processing by the two honest parties remains to be done.

Before concluding, we would like to mention that pre-processing, before or after CAD, may help in improving the distillable secret-key rate if the initial rate without pre-processing is already positive (see for instance [78]). However, this improvement vanishes for large blocks and the obtained security bounds do not change.

4.2.2 Bob's Coherent Operations Do Not Improve the Security Bound

In order to improve the security bound, we also consider the scenario where Bob performs some coherent quantum operations before his measurement. Thus, he is assumed to be able to store quantum states and manipulate them in a coherent way, see Fig. 8. This is very unrealistic, but it gives the ultimate limit for positive key-rate using the corresponding prepare and measure protocol. We do not solve the problem in full generality. Here we consider the rather natural protocol where Bob applies the recurrence protocol used in entanglement distillation. That is, he applies CNOT operations to N of his qubits and measures all but one. He accepts only when the results of these $N-1$ measurements are zero and keeps the remaining qubit. Later Bob applies a collective measurement on all the accepted qubits. Alice's part of the protocol remains unchanged.

After Alice has measured her states and announced the position of N symbols having the same value, Alice-Bob-Eve state reads

$$\rho_{ABE} = \sum_{k=0,1} |k\rangle_A\langle k| \otimes |\widetilde{be_k}\rangle_{BE}\langle\widetilde{be_k}|^{\otimes N}, \tag{4.33}$$

where $|\widetilde{be_k}\rangle = \langle k|\psi\rangle_{ABE}$. Note that Alice, Bob and Eve now share CQQ correlations. Bob applies his part of the protocol and accepts. The resulting state turns out to be equal to, up to normalization,

$$\begin{aligned} \rho^N_{ABE} \;\; & \propto |0\rangle_A\langle 0| \otimes |\mu_0^N\rangle_{BE}\langle\mu_0^N| + \\ & \quad |1\rangle_B\langle 1| \otimes |\mu_1^N\rangle_{BE}\langle\mu_1^N|, \end{aligned} \tag{4.34}$$

where

$$\begin{aligned} |\mu_0^N\rangle_{BE} &= |0\rangle|\widetilde{e_{0,0}}\rangle^{\otimes N} + |1\rangle|\widetilde{e_{0,1}}\rangle^{\otimes N}, \\ |\mu_1^N\rangle_{BE} &= |0\rangle|\widetilde{e_{1,0}}\rangle^{\otimes N} + |1\rangle|\widetilde{e_{1,1}}\rangle^{\otimes N}. \end{aligned} \tag{4.35}$$

Since Bob is allowed to apply any coherent operation, the extractable key rate satisfies (3.5), where now both information quantities, $I(A:B)$ and $I(A:E)$, are equal to the corresponding Holevo bound. Of course $I(A:E)$ has not changed. It is straightforward to see that one obtains the same bound for the key rate as for the state (4.7). This follows from the fact that

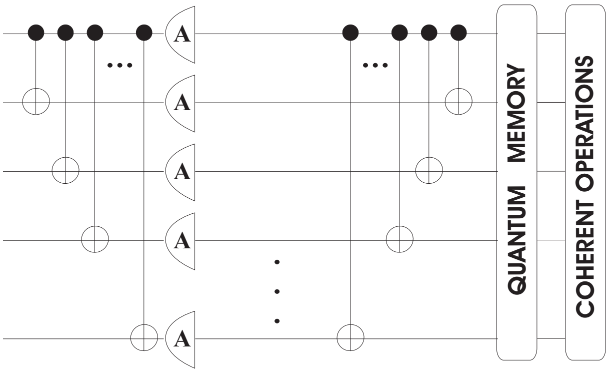

Figure 4.4: Quantum advantage distillation protocol: Alice performs single-copy measurement and processes the obtained classical outcomes. Bob keeps his quantum states on a quantum memory and performs coherent quantum operations.

$\langle e_{i,i}|e_{i,j}\rangle = 0$, where $i \neq j$. Then, this hybrid protocol does not provide any advantage with respect to SIMCAP protocols.

Recall that if the two parties apply coherent quantum operations, they can run entanglement distillation and distill from any entangled two-qubit state. Actually a slightly different protocol where (i) both parties perform the coherent recurrence protocol previously applied only by Bob, (ii) measure in the computational bases and (iii) apply standard one-way reconciliation techniques is secure for any entangled state. As shown, if one of the parties applies the "incoherent" version of this distillation protocol, consisting of first measurement and later CAD, followed by classical one-way distillation, the critical QBER decreases.

4.3 Generalization to Arbitrary Dimension

In the previous sections we have provided a general formalism for the study of key distribution through quantum channels using prepare and measure schemes and two-way key distillation. In the important case of Pauli channels, we have derived a simple necessary and sufficient condition for security, for the considered protocols. In the next sections, we move to higher dimension, where the two honest parties employ $d-$dimensional quantum systems, or qudits. The generalization of the previous qubit scenario to arbitrary dimension is straightforward. Alice locally generates a $d-$dimensional maximally entangled state,

$$|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |k\rangle|k\rangle \tag{4.36}$$

measures the first particle of the pair, and sends the other one to Bob. Since the channel between Alice and Bob is noisy, the shared state will change into a mixed state ρ_{AB}. As usual, all the noise in the channel is due to Eve's interaction.

In what follows, we consider generalized Pauli channels. For these channels, Eve introduces flip and phase errors, generalizing the standard bit-flip σ_x and phase-flip σ_z operators of qubits. This generalization is given by the unitary operators

$$U_{m,n} = \sum_{k=0}^{d-1} \exp(\frac{2\pi i}{d} kn)|k+m\rangle\langle k|.$$

Thus, a quantum system in state ρ propagating through a generalized Pauli channel is affected by a $U_{m,n}$ flip with probability $p_{m,n}$, that is

$$D(\rho) = \sum_{m,n} p_{m,n} U_{m,n} \rho U_{m,n}^{\dagger}.$$

When applied to half of a maximally entangled state $|\Phi\rangle$, the resulting state is Bell-diagonal,

$$(\mathbb{1} \otimes D)(\Phi) = \sum_{m=0}^{d-1}\sum_{n=0}^{d-1} p_{m,n}|B_{m,n}\rangle\langle B_{m,n}|, \tag{4.37}$$

where the states $|B_{m,n}\rangle$ define the generalized Bell basis

$$|B_{m,n}\rangle = (\mathbb{1} \otimes U_{m,n})|\Phi\rangle = \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1} e^{\frac{2\pi i}{d}kn}|k\rangle|k+m\rangle. \tag{4.38}$$

The global state including Eve reads

$$|\psi_{ABE}\rangle = \sum_{m=0}^{d-1}\sum_{n=0}^{d-1} c_{m,n}|B_{m,n}\rangle_{AB}|m,n\rangle_E, \tag{4.39}$$

where $c_{m,n}^2 = p_{m,n}$ and $\{|m,n\rangle\}$ defines a basis.

In the next lines, we derive a security conditions for these channels when the two honest parties measure in the computational bases. We restrict to the computational bases for the sake of simplicity, although the main ideas of the formalism can be applied to any bases, and then numerically optimized. We then generalize the previous eavesdropping attack. Contrary to what happened in the qubit case, we are unable to prove the tightness of our condition in full generality using this attack.

We then apply the derived security condition to the known protocols in d-dimensional systems, such as the 2- and $(d+1)$-bases protocols. These protocols can be seen as the natural generalization of the BB84 and the six-state protocols to higher dimension [21]. Exploiting the symmetries of these schemes, we can prove the tightness of our security condition for these protocols. In the case of the $(d+1)$-bases protocol, some security bounds using two-way communication have been obtained by Chau in [23]. Here, we obtain the same values, therefore proving that they cannot be improved unless another reconciliation protocol is employed. Moreover, in the case of 2-bases protocol, we derive the same security bound as in [74]. Thus, again, another reconciliation protocol is necessary if the bound is to be improved.

4.3.1 Sufficient Condition

After sending half of a maximally entangled state through the Pauli channel, Alice and Bob share the state

$$\rho_{AB} = \sum_{m,n} p_{m,n} |B_{m,n}\rangle\langle B_{m,n}|,$$

where the probabilities $p_{m,n}$ characterize the generalized Pauli channel. After measuring in the computational bases, the two honest parties obtain correlated results. We denote by F, fidelity, the probability that Alice and Bob get the same measurement outcome. It reads

$$F \;=\; \sum_{k=0}^{d-1} \langle kk|\rho_{AB}|kk\rangle = \sum_{n} p_{0,n}.$$

In a similar way as for the qubit case, we introduce a measure of disturbance for the $d-1$ possible errors. Denote Alice's measurement result by α. Then, Bob obtains $\alpha + j$, with probability

$$D_j = \sum_{\alpha=0}^{d-1} P(A=\alpha, B=\alpha+j) = \sum_{n=0}^{d-1} p_{j,n}.$$

The total disturbance is defined as

$$D = \sum_{j\neq 0} D_j. \tag{4.40}$$

Of course, $D_0 = F$. Notice that all the D_j can be taken smaller than F, without loss of generality. Indeed, if this was not the case, the two honest parties could apply local operations $U_{m,n}$ to make the fidelity F larger than any other D_j. Note also that the errors have different probabilities D_j.

We now include Eve in the picture, the resulting global state being (4.39). As for the qubit case, Eve's interaction by means of the Pauli operators can be formulated as an asymmetric $1 \rightarrow 1+1$ cloning transformation [20]. In what follows, and again invoking the de Finetti argument, it is assumed that Alice, Bob and Eve share many copies of the state (4.39). After the measurements by Alice and Bob, the quantum state describing the CCQ correlations between the three parties is

$$\rho_{ABE} \propto \sum_{\alpha=0}^{d-1}\sum_{\beta=0}^{d-1} |\alpha\rangle_A\langle\alpha| \otimes |\beta\rangle_B\langle\beta| \otimes |\widetilde{e_{\alpha,\beta}}\rangle_E\langle\widetilde{e_{\alpha,\beta}}|. \tag{4.41}$$

Eve's states are

$$\begin{aligned} |e_{\alpha,\alpha}\rangle &= \frac{1}{\sqrt{F}}\sum_{n=0}^{d-1} c_{0,n} e^{\frac{2\pi i}{d}\alpha n}|0,n\rangle \\ |e_{\alpha,\beta}\rangle &= \frac{1}{\sqrt{D_{\beta-\alpha}}}\sum_{n=0}^{d-1} c_{\beta-\alpha,n} e^{\frac{2\pi i}{d}\alpha n}|\beta-\alpha,n\rangle \end{aligned} \tag{4.42}$$

where the algebra is modulo d and $\beta \neq \alpha$. As above, the states with tilde are not normalized,

$$\begin{aligned} |\widetilde{e_{\alpha,\alpha}}\rangle &= \sqrt{F}|e_{\alpha,\alpha}\rangle \\ |\widetilde{e_{\alpha,\beta}}\rangle &= \sqrt{D_{\beta-\alpha}}|e_{\alpha,\beta}\rangle. \end{aligned}$$

Note that $\langle e_{\alpha,\beta}|e_{x,y}\rangle = 0$ whenever $\beta - \alpha \neq y - x$, so Eve can know in a deterministic way which error (if any) occurred between Alice and Bob.

After the measurements, Alice and Bob have a list of correlated measurement outcomes. They now apply CAD. First, Alice locally generates a random variable, s_A, that can take any value between 0 and $d-1$ with uniform probability. She then takes N of her symbols $(\alpha_1, \cdots, \alpha_N)$ and announces the vector $\vec{X} = (X_1, \cdots, X_N)$ such that $X_j = s - \alpha_j$. Bob sums this vectors to his corresponding symbols $(\beta_1, \cdots, \beta_N)$. If the N results are equal, and we denote by s_B the corresponding result, he accepts s_B. It is simple to see that Bob accepts a symbol with probability $p_{ok} = F^N + \sum_{j=1}^{d-1} D_j^N$. After listening to the public communication used in CAD, Eve knows $(X_1, \cdots, X_N)$. As in the previous qubit case, she applies the unitary operation:

$$\mathcal{U}_E = \sum_{m=0}^{d-1}\sum_{l=0}^{d-1} e^{\frac{2\pi i}{d}X_j m}|l\rangle\langle l| \otimes |-m\rangle\langle -m| \tag{4.43}$$

This unitary operation transforms Eve's states as follows,

$$\mathcal{U}_E^{\otimes N} : \bigotimes_{j=0}^{N} |e_{\alpha_j,\beta_j}\rangle \longrightarrow \bigotimes_{j=0}^{N} |e_{s,s-(\alpha_j-\beta_j)}\rangle.$$

As above, this operation makes Alice, Bob and Eve's state independent of the specific vector used for CAD. The resulting state reads

$$\sum_{s_A,s_B=0}^{d-1} |s_A\rangle_A\langle s_A| \otimes |s_B\rangle_B\langle s_B| \otimes |e_{s_A,s_B}\rangle_E\langle e_{s_A,s_B}|^{\otimes N}, \tag{4.44}$$

up to normalization. As above, the goal is to see when it is possible to find a finite N such that the CCQ correlations of state (4.44) provide a positive key-rate, according to the bound of Eq. (3.5).

The new disturbances D'_j, $j = 1, \dots, d-1$, after the CAD protocol are equal to

$$D'_j = \frac{D_j^N}{\sum_{k=0}^{d-1} D_k^N} \leq \left(\frac{D_j}{F}\right)^N, \tag{4.45}$$

where, again, the last inequality tends to an equality sign for large N. The mutual information between Alice and Bob is

$$I(A:B) = \log d + \frac{F^N}{p_{ok}} \log \frac{F^N}{p_{ok}} + \sum_{j=1}^{d-1} D'_j \log D'_j. \tag{4.46}$$

For large N, this quantity tends to

$$I(A:B) \;\; = \;\; \log d - N\left(\frac{D_m}{F}\right)^N \log\frac{F}{D_m} + O((\frac{D_m}{F})^N)$$

where $D_m = \max_j D_j$ for $j \in \{1, \cdots, d-1\}$.

Let us now compute Eve's information. Again, since Alice and Eve share a CQ channel, Eve's information is measured by the Holevo bound. For very large N, as in the case of qubits, we can restrict the computation of $\chi(A:E)$ to the cases where there are no errors between Alice and Bob after CAD. So, Eve has to distinguish between N copies of states $|e_{k,k}\rangle$. Thus, in this limit, $\chi(A:E) \approx S(\rho_E)$, where

$$\rho_E = \frac{1}{d}\sum_k |e_{k,k}\rangle\langle e_{k,k}|^{\otimes N}. \tag{4.47}$$

Denote by A_η, with $\eta = 0, \dots, d-1$, the eigenvalues of ρ_E. As shown in Appendix III, one has

$$A_\eta = \frac{1}{d^2}\sum_{k=0}^{d-1}\sum_{k'=0}^{d-1} e^{\frac{2\pi i}{d}\eta(k-k')}\langle e_k|e_{k'}\rangle^N.$$

Decomposing the eigenvalue A_η into the term with $k = k'$ and with $k \neq k'$, we can write $A_\eta = (1 + X_\eta^{(N)}/d)/d$, where

$$X_\eta^{(N)} = \sum_{k\neq k'} e^{\frac{2\pi i}{d}\eta(k-k')}\langle e_{k,k}|e_{k',k'}\rangle^N. \tag{4.48}$$

Note that $X_\eta^{(N)}$ is real since $X_\eta^{(N)} = d^2 A_\eta - d$ and A_η is real, and $\sum_{\eta=0}^{d-1} X_\eta^{(N)} = 0$ because of normalization. Moreover, $X_\eta^{(N)}$ goes to zero when N increases. Using the approximation $\log(1+x) \approx x/\ln 2$ valid when $x \ll 1$, we have

$$\begin{aligned}
\chi(A:E) &\approx -\sum_\eta A_\eta \log A_\eta \\
&\approx \log d - \frac{1}{d^3 \ln 2} \sum_{\eta=0}^{d-1} X_\eta^{(N)} X_\eta^{(N)} \\
&= \log d - \frac{d-1}{d \ln 2} \sum_{k \neq k'} |\langle e_{k,k} | e_{k',k'} \rangle|^{2N}.
\end{aligned}$$

As above, the security condition follows from the comparison of the exponential terms in the asymptotic expressions $I(A:B)$ and $\chi(A:E)$, having

$$\max_{k \neq k'} |\langle e_{k,k} | e_{k',k'} \rangle|^2 > \max_j \frac{D_j}{F}. \tag{4.49}$$

This formula constitutes the searched security condition for generalized Bell diagonal states. Whenever (4.49) is satisfied, there exists a finite N such that the secret-key rate is positive. In the next section, we analyze the generalization of the previous attack for qubits to arbitrary dimension.

4.3.2 Eavesdropping Attack

We consider here the generalization of the previous qubit attack to arbitrary dimension. Unfortunately, we are unable to use this attack to prove the tightness of the previously derived condition, namely Eq. (4.49), in full generality. However, the techniques developed in this section can be applied to standard protocols, such as the 2- and $d+1$-bases protocol. There, thanks to the symmetries of the problem, we can prove the tightness of the security condition.

The idea of the attack is the same as for the case of qubits. As above, Eve measures after the CAD part of the protocol. She first performs the d-outcome measurement defined by the projectors

$$\begin{aligned}
M_{\text{eq}} &= \sum_n |0\rangle\langle 0| \otimes |n\rangle\langle n|, \\
M_j &= \sum_n |j\rangle\langle j| \otimes |n\rangle\langle n|,
\end{aligned} \tag{4.50}$$

where $j \neq 0$. The outcomes of these measurement are denoted by r_E. Using this measurement Eve can know in a deterministic way the difference between Alice and Bob's measurement outcomes, s_A and s_B. If Eve obtains the outcome corresponding to $M_{\rm eq}$, she knows the tripartite state is (up to normalization)

$$\sum_{x=0}^{d-1} |x\rangle_A\langle x| \otimes |x\rangle_B\langle x| \otimes |e_{xx}\rangle_E\langle e_{xx}|^{\otimes N}. \tag{4.51}$$

Now, in order to learn s_A, she must discriminate between the d pure states $|e_{xx}\rangle^{\otimes N}$. Due to the symmetry of these states, the so-called square-root measurement(SRM) [50, 35] is optimal, in the sense that it minimizes the error probability (see Appendix IV for more details). She then guesses the right value of s_A with probability

$$\begin{aligned} P_{\rm eq}^{success} &= \frac{1}{d^2}\left|\sum_\eta \sqrt{\sum_m e^{2\pi i(\eta m/d)}\langle e_{m,m}|e_{0,0}\rangle^N}\right|^2 \\ &= \frac{1}{d^2}\left|\sum_{\eta=0}^{d-1}\sqrt{1+Y_\eta^{(N)}}\right|^2, \end{aligned} \tag{4.52}$$

where

$$Y_\eta^{(N)} = \sum_{m=1}^{d-1} e^{\frac{2\pi i}{d}\eta m}\langle e_{m,m}|e_{0,0}\rangle^N, \tag{4.53}$$

$Y_\eta^{(N)}$ being real. Note that $Y_\eta^{(N)}$ tends to zero for large N. The error probability reads $\epsilon_{\rm eq} = 1 - P_{\rm eq}^{success}$.

If Eve obtains the outcome corresponding to M_j after the first measurement, she knows that the three parties are in the state (up to normalization)

$$\sum_{x=0}^{d-1} |x\rangle_A\langle x| \otimes |x+j\rangle_B\langle x+j| \otimes |e_{x,x+j}\rangle_E\langle e_{x,x+j}|^{\otimes N}. \tag{4.54}$$

Eve again applies the SRM strategy, obtaining

$$P_j^{success} = \frac{1}{d^2}\left|\sum_{\eta=0}^{d-1}\sqrt{1+Y_\eta^{(j,N)}}\right|^2, \tag{4.55}$$

where

$$Y_\eta^{(j,N)} = \sum_{m=1}^{d-1} e^{\frac{2\pi i}{d}\eta m}\langle e_{m,m+j}|e_{0,j}\rangle^N, \tag{4.56}$$

the associated error probability being $\epsilon_j = 1 - P_j^{success}$.

As a result of this measurement, Alice, Bob and Eve share the tripartite probability distribution $P(s_A, s_B, (s_E, r_E))$, where (s_E, r_E) represents Eve's random variables, r_E (s_E) being the result of the first (second) measurement. For each value of r_E, Eve knows the difference between Alice and Bob's symbol and the error in her guess for Alice's symbol. It would be nice to relate the distillation properties of this tripartite probability distribution to the derived security condition (4.49), as we did in the qubit case. Unfortunately, we are at present unable to establish this connection in full generality. Actually, we cannot exclude that there exists a gap for some Bell diagonal states. However, as shown in the next section, the considered attack turns out to be tight when applied to standard protocols, such as the 2- and $d+1$-bases protocols.

Let us conclude with a remark on the resources Eve needs for this attack. After applying the same unitary operation on each qudit, Eve stores her quantum states in a quantum memory. After CAD, she measures her corresponding block of N quantum states. Recall that in the qubit case, Eve does not need any collective measurement, since an adaptative individual measurement strategy achieves the fidelity of the optimal collective measurement [14]. In the case of arbitrary dimension, it is unknown whether there exists an adaptative measurement strategy achieving the optimal error probability, at least asymptotically, when N copies of d symmetrically distributed states are given [4].

4.4 Examples : 2- and $(d+1)$-bases Protocols in Higher Dimensions

We now apply the previous security condition to specific protocols with qudits, namely the so-called 2- and $(d+1)$-bases protocols [21], which are the generalization of the BB84 and the six-state protocols to higher dimension. In the first case, Alice and Bob measure in two mutually unbiased bases, say computational and Fourier transform, while in the second, the honest parties measure in the $d+1$ mutually unbiased bases[5].

The optimal cloning attack for these protocols gives a Bell diagonal state (4.37). However, due to the symmetries of the protocols, the coefficients $c_{m,n}$, or $p_{m,n}$, are such that

$$c = \begin{pmatrix} v & x & \dots & x \\ x & y & \dots & y \\ \vdots & \vdots & \ddots & \vdots \\ x & y & \dots & y \end{pmatrix} \tag{4.57}$$

[4] This is closely related to the 31st problem in the open problem list [57]

[5] The existence of the $d+1$ mutually unbiased bases in nay dimension is a well-known open problem. This existence has only been proven in the case where the dimension is a power of a prime number. Recall that two bases, $\{|u_i\rangle\}$ and $\{|v_i\rangle\}$ with $i = 1, \dots, d$, are said mutually unbiased whenever $|\langle u_i|v_j\rangle|^2 = 1/d$.

where the normalization condition implies $v^2 + 2(d-1)x^2 + (d-1)^2y^2 = 1$. For the $d+1$-bases protocol, which is more symmetric, one also has $x = y$.

The fidelity, that is, the probability that Alice and Bob obtain the same outcome, is

$$F = \sum_{k=0}^{d-1} \langle kk|\rho_{AB}|kk\rangle = v^2 + (d-1)x^2,$$

for all the bases used in the protocol. The errors distribute in a symmetric way, $D_j = (1-F)/(d-1)$ for all $j \neq 0$. For the $d+1$-bases protocol, and since we have the extra constraint $x = y$, the coefficients $c_{m,n}$ read

$$\begin{aligned} c_{0,0} &= \sqrt{\frac{(d+1)F-1}{d}} \\ c_{m,n} &= \sqrt{\frac{1-F}{d(d-1)}} \quad \text{for } m,n \neq 0. \end{aligned} \tag{4.58}$$

In the 2-bases protocol, y is a free parameter that can be optimized for each value of the error rate, D, and depending on the reconciliation protocol. For instance, if Eve's goal is to optimize her classical mutual information, the optimal interaction ($1 \rightarrow 1+1$ cloning machine) gives (see [21] for more details)

$$\begin{aligned} c_{0,0} &= F \\ c_{m,0} &= c_{0,n} = \sqrt{\frac{F(1-F)}{d-1}} \quad \text{for } m(n) \neq 0 \\ c_{m,n} &= \frac{1-F}{d-1} \quad \text{for } m,n \neq 0. \end{aligned} \tag{4.59}$$

In a similar way as in the qubit case, this choice of coefficients is not optimal when considering two-way reconciliation protocols, as shown in the next lines.

4.4.1 Security Bounds

Having introduced the details of the protocols for arbitrary d, we only have to substitute the expression of the coefficients into the derived security condition. Because of the symmetries of the problem, all disturbances D_j and overlaps $\langle e_{m,m}|e_{0,0}\rangle$ are equal, which means that the security condition simply reads

$$|\langle e_{m,m}|e_{0,0}\rangle|^2 > \frac{D}{(d-1)F}. \tag{4.60}$$

After patient algebra, one obtains the following security bounds:

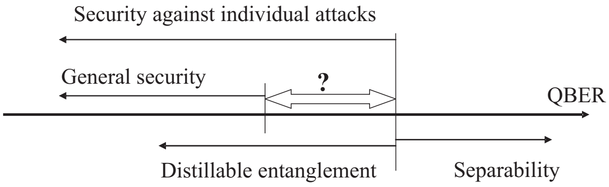

Figure 4.5: Comparison of the security bounds and the entanglement condition. The security condition against collective attacks requires stronger correlation than the entanglement limit. Again, there may exist some entangled states that are useless for key distillation with the considered techniques.

1. For $(d+1)$-bases protocol, positive key rate is possible if

$$D < \frac{(d-1)(2d+1-\sqrt{5})}{2(d^2+d-1)} \tag{4.61}$$

   The critical QBER for the 6-state protocol, 27.6%, is easily recovered by taking $d=2$. Recently, Chau has derived a general security proof for the same protocols in Ref. [23]. Our critical values are the same as in his work.

2. For the 2-bases protocol, the critical disturbances D are

$$D < \frac{(d-1)(4d-1-\sqrt{4d+1})}{2d(4d-3)} \tag{4.62}$$

   The optimal attack, in the sense of minimizing the critical error rate, is always obtained for $y=0$, see (4.57). The critical QBER for the BB84 protocol is recovered when $d=2$. These values coincide with those obtained in [74] for 2-bases protocols.

Once again, there exists a gap between this security condition and the entanglement limit. For instance, in the case of $d+1$-bases protocols, the entanglement limit coincides with the security condition against individual attacks [1]

$$|\langle e_{k,k}|e_{l,l}\rangle| > \frac{D}{(d-1)F},$$

which looks very similar to (4.60). Thus, there exists again weakly entangling channel where we are unable to establish a secure key using a prepare and measure scheme.

4.4.2 Proof of Tightness

Finally, for these protocols, and because of the symmetries, we are able to prove the tightness of the derived security condition, under the considered reconciliation techniques. The goal is to show that the probability distribution $P(s_A, s_B, (s_A, s_E))$, resulting from the attack described in section 4.3.2, cannot be distilled using one-way communication from Alice to Bob (the same can be proven if the communication goes from Bob to Alice by reversing the role of these parties).

In order to do that, we proceed as in the case of qubits. Alice-Bob's probability distribution is very simple: with probability F their symbols agree, with probability $D_j = D/(d-1)$ they differ by j. After CAD on blocks of N symbols, the new fidelity between Alice and Bob is

$$F_N = \frac{F^N}{F^N + (d-1)\left(\frac{D}{d-1}\right)^N}. \qquad (4.63)$$

One can see that, again, Eve's error probability in guessing Alice's symbol is larger when there are no errors between the honest parties. As in the qubit case, Eve worsens her guesses by adding randomness in all these cases and forgets r_E. After this process, she guesses correctly Alice's symbol with probability, see Eq. (4.52),

$$\begin{aligned} P_{\text{eq}}^{success}(N) &= \frac{1}{d^2}\left(\sqrt{1+(d-1)\left(\frac{v-x}{F}\right)^N}\right. \\ &+ \left.(d-1)\sqrt{1+\left(\frac{v-x}{F}\right)^N}\right)^2, \end{aligned} \qquad (4.64)$$

independently of Bob's symbols. Here we used the fact that $\langle e_{m,m}|e_{0,0}\rangle = (v-x)/F$ when $m \neq 0$ for the analyzed protocols.

After Eve's transformation, the one-way distillability properties of the final tripartite probability distribution are simply governed by the errors, as in the qubit case. Thus, we want to prove that at the point where the security condition is no longer satisfied, i.e. when $((v-x)/F)^2 = D/((d-1)F)$, one has

$$P_{\text{eq}}^{success}(N) > F_N, \qquad (4.65)$$

for any block size N. Define $t^2 = D/((d-1)F)$, where $0 \leq t \leq 1$ because $F > 1/D$. What we want to prove can also be written as, see Eqs. (4.63) and (4.64),

$$\left(\frac{\sqrt{1+(d-1)t^N} + (d-1)\sqrt{1+t^N}}{d}\right)^2 > \frac{1}{1+(d-1)t^{2N}}, \qquad (4.66)$$

for all N and all d, where $0 \leq t \leq 1$. Actually, using that $0 \leq t \leq 1$, it suffices to prove the case $N = 1$, since all the remaining cases will follow by replacing $t^N \rightarrow t$ and using the condition for $N = 1$. After patient algebra, one can show that (4.66) is satisfied for $N = 1$, which finishes the proof. Therefore, for the considered protocols, the attack introduced above breaks the security whenever our security condition does not hold. Therefore, this condition is tight for the considered reconciliation techniques.

4.5 Conclusion

In this Chapter, we provide a general formalism for the security analysis of prepare and measure schemes, using standard advantage distillation followed by one-way communication techniques. The main tools used in this formalism are the de Finetti argument introduced by Renner and known bounds on the key rate. We derive a simple sufficient condition for general security in the important case of qubit Pauli channels. By providing a specific attack, we prove that the derived condition is tight. When applied to standard protocols, such as BB84 and six-state, our condition gives the critical error rates previously obtained by Chau. Since our condition is tight, these critical error rates cannot be improved unless another reconciliation technique is employed. Here, most of our analysis focus on conditions for security. However, the same techniques can be used to compute key rates. Actually, our results imply that the critical error rates of 20% ad 27.6% for the BB84 and six-state protocols can be reached without any pre-processing by Alice, contrary to previous derivations by Chau [22] or Renner [78]. The rates we obtain, then, are significantly larger. We then extend the analysis to arbitrary dimension and generalized Bell diagonal states. The corresponding security condition can be applied to obtain critical error rates for the 2- and $d+1$-bases protocols. For these protocols, we can also prove the tightness of the condition.

We explore several possibilities to improve the obtained security bounds. As shown here, pre-processing by Alice or a coherent version of distillation by Bob do not provide any improvement. This is of course far from being an exhaustive analysis of all possibilities, but it suggests that it may be hard, if not impossible, to get the entanglement limit by a prepare and measure scheme. In our opinion, this is the main open question that naturally follows from our analysis. The easiest way of illustrating this problem is by considering the simple qubit depolarizing channel of depolarizing probability $1-p$. This is a channel where the input state is unchanged with probability p and map into completely depolarized noise with probability $1-p$. The corresponding state is a two-qubit Werner state. When $p = 1/3$, the channel is entanglement breaking, that is, it does not allow to distribute entanglement, so it is useless for any form of QKD. As shown here, the same channel can be used to QKD using a prepare and measure scheme when $p > 1/\sqrt{5}$. Trivially, the entanglement limit can be reached if one allows coherent protocols by the two parties, such as entanglement distillation. However, is there a prepare and measure scheme with positive key rate for $1/3 \leq p < 1/\sqrt{5}$?

Chapter 5

Key Distillation with Continuous Variable States

Since quantum teleportation was experimentally implemented using a twomode squeezed state, a significant amount of work has been devoted to develop a quantum information theory of continuous variable systems [36]. Quantum cryptography has also been successfully translated into the Gaussian regime. Gottesman and Preskill proposed to use squeezed states and homodyne measurements in a *prepare & measure* scheme [44]. Actually, no squeezing is required, since coherent states are already sufficient for a secure key distribution with Gaussian operations [46, 59]. The experimental implementation of a coherent-state protocol has been recently realized in [48]. In these systems, Gaussian states and Gaussian operations play the key role, since they naturally appear in experiments. Moreover, their theoretical analysis can be simplified due to the fact that only two quantities, displacement vectors and covariance matrices, can express all properties of Gaussian states.

We denote here these Gaussian Local Operations and Classical Communication as GLOCC. A negative result in GLOCC scenarios is, differently from finite dimensional quantum systems, that Gaussian states cannot be distilled by Gaussian operations. This can be a significant drawback in GLOCC scenarios, contrast to its remarkable experimental feasibility. However, these states may still be useful for cryptographic applications, as a secret key being extracted.

In this Chapter[1], we analyze the secrecy properties of Gaussian states under Gaussian operations[2]. We adapt the SIMCAP protocol to the realistic Gaussian scenario, in which Alice and Bob measure their shared entangled Gaussian state by Gaussian operations at the single-copy level and process

[1] The result of this Chapter is based on the publication [72]

[2] A similar scenario has been considered by J. Eisert and M. Plenio (unpublished).

the obtained classical results[3]. This type of protocols can easily be translated to prepare & measure schemes. As is done in cases of discrete variables, we here obtain security bounds for key distillation from Gaussian states by Gaussian operations. First, we study the security of our protocol against individual attacks, in which all NPPT Gaussian states are shown to be useful in key distillation. Then, we consider the the general security condition, which implies that, as is the case of discrete variables, the protocol ceases to work for some NPPT states.

5.1 Adaptation to the Realistic Protocol

Here we describe how Alice and Bob can distill a secret key from an $n \times m$ Gaussian state by Gaussian operations, adapting the SIMCAP protocols in Chapter 4 to the Gaussian scenario. Any NPPT Gaussian state of $n+m$ modes can be mapped by GLOCC into an NPPT 1×1 Gaussian and symmetric state [37], whose CM, see Eq. (2.6), is

$$\gamma_A = \gamma_B = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \qquad C = \begin{pmatrix} c_x & 0 \\ 0 & -c_p \end{pmatrix} \tag{5.1}$$

where $\lambda \geq 0$ and $c_x \geq c_p \geq 0$. The condition that this is physical, i.e. $\rho > 0$, reads $\lambda^2 - c_x c_p - 1 \geq \lambda(c_x - c_p)$ while the entanglement (NPPT) condition gives

$$\lambda^2 + c_x c_p - 1 < \lambda(c_x + c_p). \tag{5.2}$$

Since all the NPPT Gaussian states can be mapped into symmetric and entangled states of two modes by GLOCC, we restrict our analysis to this type of states. In equivalent terms, one can think that the first step in the key distillation protocol is the GLOCC transformation of [37] that transforms any NPPT state into an entangled state of this family. Then, both parties measure the X quadrature, where X_A and X_B denote the measured operator and x_A and x_B the obtained outcome. After communication, they only accept those cases where $|x_A| = |x_B| = x_0$. Each party associates the logical bit 0 (1) to a positive (negative) result with the probability $p\,(i,j)$, with $i,j = 0,1$. This process transforms the quantum state into a list of correlated classical bits between Alice and Bob. Their error probability, that is the probability that their symbols do not coincide, is given by

$$\epsilon_{AB} = \frac{\sum_{i \neq j} p\,(i,j)}{\sum_{i,j} p\,(i,j)} = \frac{1}{1 + \exp\left(\frac{4 c_x x_0^2}{\lambda^2 - c_x^2}\right)}. \tag{5.3}$$

Then Alice and Bob proceed the CAD to establish a secret key.

[3] As for the entanglement distillability scenario, we assume that Alice and Bob share a known Gaussian state.

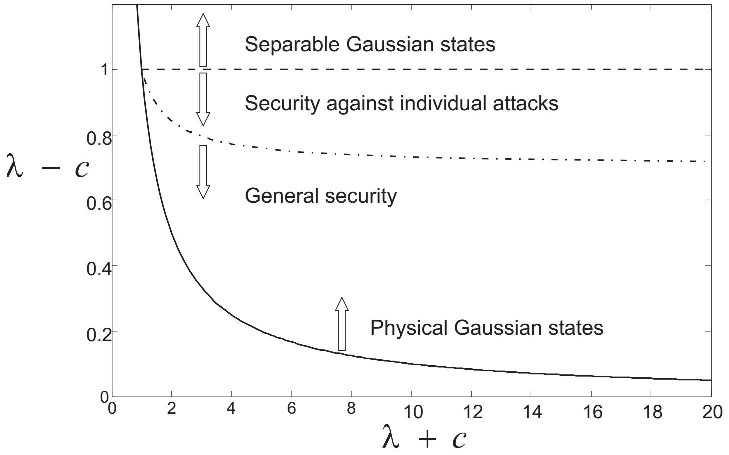

Figure 5.1: Security analysis of symmetric 1 × 1 Gaussian states when $c_x = c_p = c$. All physical states are above the lowest line. The highest line defines the entanglement limit, that coincides with the security bound against individual attacks. States below the line in the middle are secure against any attack. This general security condition is stronger than entanglement limit, which may imply the existence of entangled Gaussian states from which no secret key can be distilled.

5.2 Security Bounds

The information that Eve can obtain during the protocol is computed from her purifying the state shared by Alice and Bob. In the Gaussian regime, as we is done in the previous chapter, all the environment, all the degrees of freedom outside Alice and Bob's systems are assumed to be accessible to Eve. Then the global state including Eve is pure $|\Psi_{ABE}\rangle$ such that $\text{tr}_E(|\Psi_{ABE}\rangle\langle\Psi_{ABE}|) = \rho_{AB}$. Note that the global state is specified by the local state ρ_{AB}, up to a unitary operation on Eves system. Thus, from Eves point of view, all the purifications are equivalent. Denote by $|e_{\pm\pm}\rangle$ Eve's states when Alice and Bob have projected onto $|\pm x_0\rangle$.

Individial attacks

As discussed in Chapter 3, individual attacks are most relevant with realistic eavesdroppers. For the case of individual attacks, it was shown in [2] that Eve's error in the estimation of the final bit b is bounded from below by a term proportional to $|\langle e_{++}|e_{--}\rangle|^N$. Therefore, Alice and Bob can establish a key if

$$\frac{\epsilon_{AB}}{1-\epsilon_{AB}} < |\langle e_{++}|e_{--}\rangle|. \tag{5.4}$$

More precisely, if this condition is fulfilled, there is always a finite N such that the new list of symbols can be distilled into a secret key using one-way protocols [27].

From Eq. (2.7), one can compute the global pure state including Eve. Note that taking the Gaussian purification does not imply any loss of generality on Eve's individual attack, since all the purifications are equivalent up to a unitary operation on Eve's space. After projecting on $|\pm x_0\rangle$, Eve has a Gaussian state of two modes, with the CM and DV for the states $|e_{\pm\pm}\rangle$ given by

$$\begin{aligned} d_{++} &= -\frac{\sqrt{\lambda^2+\lambda(c_x-c_p)-c_xc_p-1}}{\lambda+c_x}(0,0,x_0,x_0) \\ \gamma_{++} &= \begin{pmatrix} \gamma_x & 0 \\ 0 & \gamma_x^{-1} \end{pmatrix} \qquad \gamma_x = \begin{pmatrix} \lambda & c_x \\ c_x & \lambda \end{pmatrix}, \end{aligned} \tag{5.5}$$

while $\gamma_{--} = \gamma_{++}$ and $d_{--} = -d_{++}$. Now, the overlap between these two states is given by

$$|\langle e_{++}|e_{--}\rangle|^2 = \exp\left(-\frac{4(\lambda^2+\lambda(c_x-c_p)-c_xc_p-1)x_0^2}{\lambda+c_x}\right). \tag{5.6}$$

Substituting Eqs. (5.3) and (5.6) in (5.4) one can check, after some algebra, that this condition is equivalent to the entanglement condition of (5.2). That is, all the distillable (NPPT) Gaussian states allow a secure key distribution under individual attacks using Gaussian operations. Moreover, the limits for NPPT entanglement and key distillation also coincide if Eve measures in a coherent way a finite number $N_E \ll N$ of states *before* the reconciliation process[4]. Interestingly, these limits hold for any x_0, and measurements of arbitrary resolution [5].

General security

A more powerful Eve is no longer restricted to individual attacks. Indeed, the most powerful Eve could wait until the end of the advantage distillation protocol and measure in a coherent way all her N symbols. One can see that the corresponding security condition is similar to Eq. (5.4), but replacing Eve's states overlap by its square, as is shown in (4.17) of Chapter 4. This new inequality is violated by some NPPT states (see figure 5.1). Note that this only implies that the analyzed protocol is not good for these states in this more general scenario. That is, these states may be useful for cryptographic purposes using another protocol.

[4] Similarly as in Ref. [2], one can prove that Eq. (5.4) again defines the security condition for finite size attacks.

[5] Although this only happens with zero probability, one can include finite widths $dx_A = dx_B = dx$ for Alice and Bobs outcomes. For small widths, all our conclusions hold by continuity and the modified protocol has finite key rate.

5.3 Discussion

One can envisage different ways of improving the previous security analysis, e.g. finding better measurements for Alice and Bob or new ways of processing their measurement outcomes. A more interesting possibility consists of allowing the honest parties to manipulate in a coherent way several copies of their local states. Actually, the full general study of distilling a secret key from Gaussian states by Gaussian operations should deal with joint (although local and Gaussian) operations by Alice and Bob. This defines a new type of *Gaussian quantum privacy amplification* protocols [30] different from entanglement distillability where Alice and Bob's goal is simply to factor Eve out [38].

A related open question that deserves further investigation is whether secret bits can be extracted from PPT Gaussian states, i.e. strict bound entangled states (cf. [56]). Our scheme does not work for all PPT Gaussian states, which was shown in Ref [73].

5.4 Conclusion

Quantum and classical distillation protocols are two techniques that allow to extract secret bits from entangled states. A schematic comparison between them is shown in figure 3.2. In finite systems, there are examples of non-distillable quantum states for which the classical distillation is possible [56]. Moving to continuous variables systems and the Gaussian scenario, distillation techniques with Gaussian operations are useless for key-agreement [38, 33]. Our analysis proves that distilling a secret key is still useful for (i) all NPPT states under individual attacks and (ii) sufficiently entangled NPPT states under general attacks.

Chapter 6

Equivalence Between Asymptotic Quantum Cloning and State Estimation

In this Chapter[1], we prove the conjectured equivalence between asymptotic quantum cloning and state estimation. We show that the fidelities of optimal asymptotic cloning and of state estimation are equal for any initial ensemble of pure states [5]. Actually, we prove the stronger result that *asymptotic cloning does effectively correspond to state estimation*, from which the equality of the two fidelities automatically follows. The proof of this equivalence is based on two known results of quantum information theory: the monogamy of quantum correlations and the properties of the so-called entanglement breaking channels (EBC).

6.1 State Estimation and Quantum Cloning

The fact that state estimation is in general imperfect leads in a natural way to the problem of building *optimal measurements*. Being a perfect reconstruction impossible, it is relevant to find the measurement strategy that maximizes the gain of information about the unknown state. A standard approach to this problem in quantum information theory is to quantify the quality of a measurement by means of the so-called *fidelity* [68]. This quantity is defined as follows. Consider the situation in which a quantum state $|\psi\rangle$ is chosen from the ensemble $\{p_i, |\psi_i\rangle\}$, i.e. $|\psi\rangle$ can be equal to $|\psi_i\rangle$ with probability p_i. A measurement, defined by N_M positive operators, $M_j \geq 0$, summing up to the identity, $\sum_j M_j = \mathbb{1}$, is applied on this unknown state.

[1] The result of this Chapter is based on the publication [5]

For each obtained outcome j, a guess $|\phi_j\rangle$ for the input state is made. The overlap between the guessed state and the input state, $|\langle\psi_i|\phi_j\rangle|^2$, quantifies the quality of the estimation process. The averaged fidelity of the measurement then reads

$$\bar{F}_M = \sum_{i,j} p_i \, \mathrm{tr}(M_j|\psi_i\rangle\langle\psi_i|) \, |\langle\psi_i|\phi_j\rangle|^2. \tag{6.1}$$

A measurement is optimal according to the fidelity criterion when it provides the largest possible value of $\bar{F}_M$, denoted in what follows by F_M.

The No-cloning theorem [92], one of the cornerstones of quantum information theory [79], represents another known consequence of the nonorthogonality of quantum states. It proves that *given a quantum system in an unknown state $|\psi\rangle$, it is impossible to design a device producing two identical copies, $|\psi\rangle|\psi\rangle$*. Indeed, two nonorthogonal quantum states suffice to prove the no-cloning theorem.

As it happens for state estimation, the impossibility of perfect cloning leads to the characterization of *optimal cloning machines* [19]. In this case, one looks for the quantum map $\mathbb{L}$ that, given a state $|\psi\rangle$ chosen from an ensemble $\{p_i, |\psi_i\rangle\}$ in $\mathbb{C}^d$, produces a state $\mathbb{L}(\psi) = \rho_{C_1 \ldots C_N}$ in $(\mathbb{C}^d)^{\otimes N}$, such that each individual clone $\rho_{C_k} = \mathrm{tr}_{\bar{k}}(\rho_{C_1 \ldots C_N})$ resembles as much as possible the input state. Here $\bar{k}$ denotes the complement of k, so $\mathrm{tr}_{\bar{k}}$ is the trace with respect to all the systems C_i but C_k. The average fidelity of the cloning process is then

$$\bar{F}_C(N) = \sum_{i,k} p_i \, \frac{1}{N} \langle\psi_i|\mathrm{tr}_{\bar{k}}\mathbb{L}(\psi_i)|\psi_i\rangle. \tag{6.2}$$

The goal of the optimal machine is to maximize this quantity, this optimal value being denoted by $F_C(N)$.

As we have discussed in Chapter 2, the no-cloning theorem and the impossibility of perfect state estimation are closely related. The connection between state estimation and cloning was strengthened from the results in Ref. [39, 15] that asymptotic cloning, i.e. the optimal cloning process when $N \to \infty$, is equivalent to state estimation, in the sense that, for any ensemble of states,

$$F_C = F_C(N \to \infty) = F_M. \tag{6.3}$$

Actually, this equality was proven for the case of universal cloning [15], and for phase covariant qubit cloning [17]. Since then, the validity of this equality for any ensemble has been identified as one of the open problems in quantum information theory [57].

6.2 The importance of Correlations

In the conjecture, the trivial part is that $F_M \leq F_C$. Indeed, given the initial state $|\psi\rangle$, a possible asymptotic cloning map, not necessarily optimal, consists of first applying state estimation and then preparing infinite copies of the guessed state. It is sometimes said that the opposite has to be true since "asymptotic cloning cannot represent a way of circumventing optimal state estimation". As already mentioned in [57], this reasoning is too naive, since it neglects the role correlations play in state estimation. For instance, take the simplest case of universal cloning of a qubit, i.e. a state in $\mathbb{C}^2$ isotropically distributed over the Bloch sphere. The optimal cloning machines produces N approximate clones pointing in the same direction in the Bloch sphere as the input state, but with a shrunk Bloch vector [62]. If the output of the asymptotic cloning machine was in a product form, it would be possible to perfectly estimate the direction of the local Bloch vector, whatever the shrinking was. Then, a perfect estimation of the initial state would be possible. And of course, after the perfect estimation one could prepare an infinite number of perfect clones. This simple reasoning shows that the correlations between the clones play an important role in the discussion. Actually, it has recently been shown that the correlations present in the output of the universal cloning machine are the worst for the estimation of the reduced density matrix [29].

6.3 Monogamy of Entanglement and Entanglement-breaking Channels

As announced, the proof of the conjecture is based on two known results of quantum information theory: the monogamy of entanglement and the properties of EBC. For the sake of completeness, we state here these results, without proof.

Quantum correlations, or entanglement, represent a monogamous resource, in the sense that they cannot be arbitrarily shared. One of the strongest results in this direction was obtained by Werner in 1989 [89]. There, it was shown that the only states that can be arbitrarily shared are the separable ones. Recall that a bipartite quantum state ρ_{AC} in $\mathbb{C}^d \otimes \mathbb{C}^d$ is said to be N-shareable when it is possible to find a quantum state $\rho_{AC_1 \ldots C_N}$ in $\mathbb{C}^d \otimes (\mathbb{C}^d)^{\otimes N}$ such that $\rho_{AC_k} = \mathrm{tr}_{\bar{k}} \rho_{AC_1 \ldots C_N} = \rho_{AC}, \forall k$. The state $\rho_{AC_1 \ldots C_N}$ is then said to be an N-extension of ρ_{AC}. The initial correlations between subsystems A and C are now shared between A and each of the N subsystems C_i, see Fig. 6.1. It is straightforward to see that

$$\rho_{AC_1 \ldots C_N} = \sum_i q_i |\alpha_i\rangle\langle\alpha_i| \otimes |\gamma_i\rangle\langle\gamma_i|^{\otimes N} \tag{6.4}$$

gives a valid N-extension of a separable state $\rho^s_{AC} = \sum_i q_i |\alpha_i\rangle\langle\alpha_i| \otimes |\gamma_i\rangle\langle\gamma_i|$ for all N. As proven by Werner, if a state ρ_{AC} is entangled, there exists a finite number $N(\rho_{AC})$ such that no valid extension can be found.

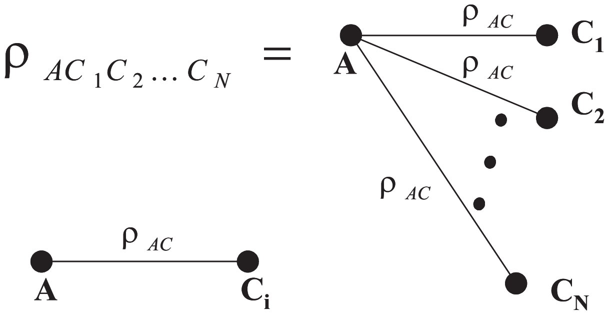

Figure 6.1: The state ρ_{AC} is said to be N-shareable when there exists a global state $\rho_{AC_1 \ldots C_N}$ such that the local state shared between A and C_i is equal to ρ_{AC}, for all i.

The second ingredient needed in what follows are the properties of EBC. A channel Υ is said to be entanglement breaking when it cannot be used to distribute entanglement. In Ref. [55] it was proven that the following three statements are equivalent: (1) Υ is entanglement breaking, (2) Υ can be written in the form

$$\Upsilon(\rho) = \sum_j \mathrm{tr}(M_j \rho) \rho_j, \tag{6.5}$$

where ρ_j are quantum states and $\{M_j\}$ defines a measurement and (3) $(\mathbb{1} \otimes \Upsilon)|\Phi^+\rangle$ is a separable state, where $|\Phi^+\rangle = \sum_i |ii\rangle/\sqrt{d}$ is a maximally entangled state in $\mathbb{C}^d \otimes \mathbb{C}^d$. The equivalence of (1) and (2) simply means that any EBC can be understood as the measurement of the input state, ρ, followed by the preparation of a new state ρ_j depending on the obtained outcome. The equivalence of (1) and (3) reflects that the intuitive strategy for entanglement distribution where half of a maximally entangled state is sent through the channel is enough to detect if Υ is entanglement breaking.

6.4 Asymptotic Cloning Is State Estimation

After collecting all these results, we are now ready to prove the following

Theorem: Asymptotic cloning corresponds to state estimation. Thus, $F_M = F_C$ for any ensemble of states.

Proof: First of all, note that, for any number of clones, we can restrict our considerations to symmetric cloning machines, $\mathrm{Ł}^s_N$, where the N clones are all in the same state. Indeed, given a machine where this is not the case, one can construct a symmetric machine achieving the same fidelity $F_C(N)$, just by making a convex combination of all the permutations of the

N clones[2]. Now, denote by Ł_N^c the effective cloning map consisting of, first, the application of a symmetric machine Ł_N^s and then tracing all but one of the clones, say the first one. The N-cloning problem can be rephrased as, see Eq. (6.2),

$$\max_{\text{Ł}_N^c} \sum_i p_i \langle \psi_i | \text{Ł}_N^c(\psi_i) | \psi_i \rangle. \tag{6.6}$$

Note that this maximization runs over all channels that can be written as $\text{Ł}_N^c = \text{tr}_{\bar{1}} \text{Ł}_N^s$. For instance, the identity map, where $\psi \to \psi$, $\forall \psi$, does not satisfy this constraint. Denote by L_N the set of these channels. These are convex sets such that $L_N \supseteq L_{N+1} \supseteq \ldots \supseteq L_\infty$. The key point of the proof is to show that all the channels in L_∞, and therefore all the channels associated to asymptotic cloning machines, are EBC. To prove this result we proceed by contradiction.

First, note that any EBC belongs to L_∞. Assume now there is a channel $\text{Ł}_\infty^c \in L_\infty$ which is not EBC, i.e. such that the state

$$\rho_{AC} = (\mathbb{1} \otimes \text{Ł}_\infty^c) |\Phi^+\rangle \tag{6.7}$$

is entangled. Since $L_N \supseteq L_\infty$ for all N, Ł_∞^c is an element of all these sets. Thus, for any finite N, there exists a symmetric channel Ł_N^s such that

$$\rho_{AC_1 \ldots C_N} = (\mathbb{1} \otimes \text{Ł}_N^s) |\Phi^+\rangle. \tag{6.8}$$

is a valid N-extension of the entangled state ρ_{AC} of Eq. (6.7). But this is in contradiction with the non-shareability of entangled states. Thus, all the channels in L_∞ have to be EBC. Since any EBC can be seen as measurement followed by state preparation, asymptotic quantum cloning, i.e. Eq. (6.6) in the limit $N \to \infty$, can be written as[3]

$$\max_{\{M_j, \phi_j\}} \sum_{i,j} p_i \, \text{tr}(M_j |\psi_i\rangle\langle\psi_i|) \, |\langle \psi_i | \phi_j \rangle|^2, \tag{6.9}$$

which defines the optimal state estimation problem. Therefore, $F_M = F_C$ for any ensemble of states. □

The same argument applies to the case in which K copies of the initial state $|\psi\rangle$ are given. The measurement and cloning fidelities now read, see Eqs. (6.1) and (6.2),

$$\begin{aligned} \bar{F}_M(L) &= \sum_{i,j} p_i \, \text{tr}(M_j |\psi_i\rangle\langle\psi_i|^{\otimes K}) \, |\langle \psi_i | \phi_j \rangle|^2 \\ \bar{F}_C(N,K) &= \sum_{i,k} p_i \, \frac{1}{N} \langle \psi_i | \text{tr}_{\bar{k}} \text{Ł}(\psi_i^{\otimes K}) | \psi_i \rangle. \end{aligned} \tag{6.10}$$

[2] Notice that this does not mean that the output of the cloning machine lives in the symmetric subspace.

[3] We can already restrict the guessed states to be pure, without any loss of optimality.

Using the same ideas as in the previous Theorem, it is straightforward to prove that

$$F_M(K) = F_C(N \to \infty, K), \tag{6.11}$$

where $F_M(K)$ and $F_C(N,K)$ denote the optimal values of $\bar{F}_M(K)$ and $\bar{F}_C(N,K)$, as above.

6.5 Asymmetric Scenario

One can also extend this result to asymmetric scenarios. An asymmetric cloning machine [75] produces N_A clones of fidelity $F_C(N_A)$ and N_B clones of fidelity $F_C(N_B)$ of a state chosen from an ensemble $\{p_i, |\psi_i\rangle\}$, the total number of clones being $N = N_A + N_B$. The machine is optimal when it gives the largest $F_C(N_A)$ for fixed $F_C(N_B)$. Extending the previous formalism, this optimal fidelity is then

$$F_C(N_A) = \max_{\mathrm{L}_{N_A,N_B}} \sum_i p_i \langle\psi_i|\mathrm{tr}_{\bar{1}}\mathrm{L}_{N_A,N_B}(\psi_i)|\psi_i\rangle, \tag{6.12}$$

where the maximization now runs over all maps $\mathbb{C}^d \to (\mathbb{C}^d)^{\otimes N}$, symmetric under permutation among the first N_A clones or among the N_B clones, and such that

$$\sum_i p_i \langle\psi_i|\mathrm{tr}_{\bar{N}}\mathrm{L}_{N_A,N_B}(\psi_i)|\psi_i\rangle = F_C(N_B). \tag{6.13}$$

In the case of measurement, we are thinking of measurement strategies where the goal is to obtain information on an unknown state introducing the minimal disturbance. As above, we consider that a guess $|\phi_j\rangle$ for the input state is done depending on the measurement outcome j. The information vs disturbance trade-off can be expressed in terms of fidelities [7]: the information gain is given by the overlap, G, between the initial and the guessed state, while the disturbance is quantified by the overlap, F, between the state after the measurement and the initial state. The whole process can be seen as a global map $\mathcal{M}$ transforming the initial state into two approximate copies of it: the state left after the measurement and the guessed state. A measurement is optimal when for fixed gain, G, it provides the minimal disturbance, i.e. the largest overlap F. So, the goal is to solve

$$\max_{\mathcal{M}} \sum_i p_i \, \langle\psi_i|\mathrm{tr}_2\mathcal{M}(\psi_i)|\psi_i\rangle, \tag{6.14}$$

where the maximization is over all channels $\mathcal{M}$ such that $\mathrm{tr}_1\mathcal{M}$ defines an EBC (6.5) with $\rho_j = |\phi_j\rangle\langle\phi_j|$[4] and $\sum_i p_i \, \langle\psi_i|\mathrm{tr}_1\mathcal{M}(\psi_i)|\psi_i\rangle = G$. The optimal trade-off between F and G is only known for the case in which the input ensemble consists of any pure state in $\mathbb{C}^d$ with uniform probability [7].

[4] We can already restrict the guessed states to be pure, without any loss of optimality.

As it happens for the symmetric case, a connection between this state estimation problem and asymmetric cloning machines can be expected when $N_A = 1$ and $N_B \to \infty$. Note that the previous measurement strategy gives a possible realization of an asymmetric cloning machine, not necessarily optimal, when N_B identical copies of the guessed state are prepared. In other words, if $G = F_C(N_B)$, then $F \leq F_C(N_A)$. Actually, this connection is indeed true for the particular case in which the input state is any pure state in $\mathbb{C}^2$, isotropically distributed on the Bloch sphere: the optimal measurement strategy of [7] turns out to saturate the optimal cloning $1 \to N_A + N_B$ fidelities of [60], when $N_A = 1$ and $N_B \to \infty$. Now, the equality between the measurement and asymptotic cloning fidelities in the asymmetric scenario can be proven in full generality exploiting the same arguments as above. Using the monogamy of entangled states, one can see that the channels (6.13), defining the $N_B \to \infty$ clones, must be EBC. This means that the set of maps L_{1,N_B} and $\mathcal{M}$ corresponding to asymmetric $1 \to 1 + N_B$ cloning machines and asymmetric measurement strategies, see Eqs. (6.12) and (6.14), coincide when $N_B \to \infty$. Therefore, the two corresponding fidelities have to be equal.

6.6 Discussion

To conclude, we have proved the long-standing conjecture on the equivalence between asymptotic cloning and state estimation. Our result represents the strongest link between these two fundamental no-go theorems of quantum theory, namely the impossibilities of perfect cloning and state estimation.

From a fundamental point of view, it would be interesting to extend these findings to more general theories. There exist several works relating the impossibility of perfect cloning to the no-signaling principle, e.g. [40]. Recently, a form of no-cloning theorem has been derived just from the no-signaling principle, without invoking any additional quantum feature [67]. In view of the strong connection between cloning and state estimation, one could wonder whether a similar link could also be established between the no-signaling principle and the impossibility of perfect state estimation, without exploiting any intrinsically quantum property such as nonorthogonality.

Chapter 7

Outlook

The present thesis studies different problems on the role of entanglement in QKD scenarios, from a new security analysis of quantum channels for QKD to the proof of equivalence between asymptotic cloning and state estimation. We would like to conclude by mentioning several open problems that naturally follow from the derived results.

First, the results of chapters 4 and 5 suggest the existence of entangled states from which no secret key can be distilled using realistic protocols. These bipartite states would have a sort of bound secrecy under SIMCAP protocols. Note however that some of these states are entanglement distillable. This also means that a secret key can be extracted out of it, simply using entanglement distillation followed by measurements. The secrecy of these states would then be distillable only if Alice and Bob are allowed to use coherent operations, but becomes bound when they are restricted to SIMCAP protocols. The existence of the gap seems plausible due to the fact that Alice and Bob are less powerful than Eve. Interestingly, some of these states become again key-distillable when Eve, as well as Alice and Bob, is assumed to apply single-copy measurements. This is, for instance, the case for individual attacks.

More in general, this type of problems is connected to the broader question of identifying those entangled states from which secret bits can be distilled. Recently, Horodecki *et al.* have proven in Ref. [56] the existence of bound entangled states from which Alice and Bob can extract a secret key. This implies that key distillability is weaker than entanglement distillability. Then, are all entangled states key distillable? If yes, do they remain key distillable when Alice and Bob are restricted to incoherent operations?

Second, the thesis has proven that asymptotic cloning is equivalent to state estimation. The proof is simple and based on two known results in quantum information theory, the monogamy of entangled states and the

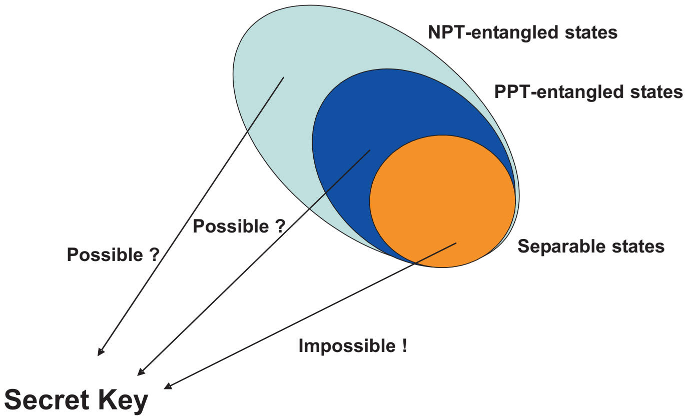

Figure 7.1: The characterization of those quantum states from which a secret key can be distilled represents a challenging open problem in Quantum Information Theory. The same question is also interesting assuming a realistic scenarios, where Alice and Bob apply SIMCAP protocols.

properties of entanglement-breaking channels. Our results imply that the fidelities F_C of quantum cloning converges to F_M, the fidelity of state estimation, in the limit of an infinite number of clones, $N \to \infty$. It is interesting to study this convergence with the number of copies, that is, how fast quantum cloning becomes equivalent to state estimation. First results in this direction have recently been obtained in Ref. [24].

Appendix A

Quantum Theory in a nutshell for quantum information theory

Quantum theory describes the physics of microscopic systems. Quantum theory formalism is grounded on algebras of hermitian operators, that define non-commuting observables. In what follows we introduce the basic mathematical structure employed in the quantum formalism.

A.1 Quantum States

Quantum states can usually be of two kinds, *pure or mixed.* A pure quantum state is represented as a ray in a Hilbert space. Given a Hilbert space $\mathcal{H}$, a quantum state is a vector in the space satisfying the following equivalence relation: $|\psi\rangle \sim |\phi\rangle$ if and only if there exists a phase $e^{i\theta}$, $\theta \in [0, 2\pi)$, such that $|\psi\rangle = e^{i\theta}|\phi\rangle$. A quantum state $|\psi\rangle$ can also be thought of as a superposition of some other states $\{|\psi_i\rangle\}$ as follows

$$|\psi\rangle = \sum_i \sqrt{p_i}|\psi_i\rangle,$$

where p_i is the probability that the system is found in the state $|\psi_i\rangle$. Explicitly the probability reads $p_i = |\langle\psi|\psi_i\rangle|^2$. Since probabilities have to sum up to one, the state is normalized under the inner product of the Hilbert space:

$$\||\psi\rangle\| = \sqrt{\langle\psi|\psi\rangle} = 1.$$

When considering a realistic situation, pure quantum states are hard (impossible) to prepare, since a quantum system is very susceptible to environment. In order to prepare a quantum system in a pure state, the system must be decoupled from any interaction with environment. Instead, any quantum state that raises in experiments results from interaction with environment. It is transformed into a *mixed state*, a probabilistic mixture of pure states.

There are two equivalent ways of interpreting mixed states. One is based on a decoherence point of view, taking into account an interaction with the environment. Suppose that a system is initially decoupled from the environment, and is in a pure state $|\psi\rangle_S|0\rangle_E$. After interacting with the environment, the system evolves into a state $|\Psi_{S+E}\rangle$, that is a pure state over system plus environment. The system alone is in a mixed state

$$\rho_S = \mathrm{tr}_E|\Psi_{S+E}\rangle\langle\Psi_{S+E}|.$$

Here the partial trace operation is applied to sum over the degrees of freedom of the environment and look at the system state.

Definition 8 (Partial trace) *The partial trace, denoted by* $\mathrm{tr}_E[\rho_{S+E}]$ *of a state* ρ_{S+E} *of a system plus an environment, is an operation to discard the environment part. If* $|e_k\rangle$ *is a basis for the environment and* $\rho_{S+E} = |\Psi\rangle_{SE}\langle\Psi|$ *where* $|\Psi\rangle_{SE} = \sum_i \sqrt{p_i}|\psi_i\rangle_S|e_i\rangle_E$*, the partial trace fulfills*

$$\mathrm{tr}_E[\rho_{S+E}] = \sum_k \langle e_k|\Psi\rangle_{SE}\langle\Psi|e_k\rangle = \sum_i p_i|\psi_i\rangle\langle\psi_i|. \tag{A.1}$$

If a system has experienced an interaction with environment, then the resulting state becomes a classical mixture of other quantum states as shown in (A.1).

This gives the second interpretation of a mixed state, as an imperfect preparation: if a system is prepared in a state $|\psi_i\rangle$ with probabilities p_i, the resulting state is again the classical mixture of quantum states, explicitly

$$\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|. \tag{A.2}$$

Both descriptions of mixed states are of course equivalent.

Given a mixed state, one can always find a pure state over an extended Hilbert space in such a way that the mixed state is recovered after tracing the environment. The global pure state is called purification.

Definition 9 (Purification) *When the system is in a mixed state* ρ_S*, there exists a pure state* $|\Psi\rangle_{SE}$ *such that*

$$\rho_S = \mathrm{tr}_E|\Psi\rangle_{SE}\langle\Psi|.$$

The purified quantum state $|\Psi\rangle_{SE}$ *is unique up to local unitary operators on the environment.*

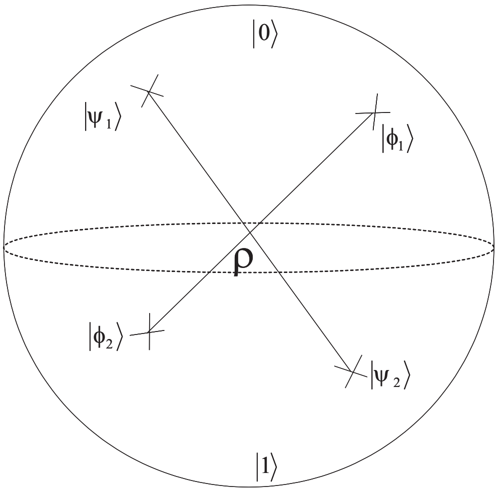

Figure A.1: A single qubit can be represented the a Bloch sphere. A pure state corresponds to a point on the surface of the sphere, and a mixed state resides inside the sphere. A mixed state ρ can be expressed as a mixture of $|\psi_1\rangle$ and $|\psi_2\rangle$ or equivalently $|\phi_1\rangle$ and $|\phi_2\rangle$.

For instance, a purification of a mixed state ρ in (A.2) can be

$$|\psi\rangle = \sum_i \sqrt{p_i}|\psi_i\rangle|i\rangle$$

with orthonormal basis $|i\rangle \in \mathcal{K}$ so that $\rho = \mathrm{tr}_{\mathcal{K}}|\psi\rangle\langle\psi|$. A mixed state does not have a unique decomposition. If a mixed state is written as a convex combination of $|v_j\rangle$ with probabilities p_j, there can be another states $|w_j\rangle$ with different probabilities q_j, i.e.

$$\rho = \sum_{j=1}^{n} p_j |v_j\rangle\langle v_j| = \sum_{j=1}^{m} q_j |w_j\rangle\langle w_j|.$$

In this case, there exists a transformation M from $|v_j\rangle$ to $|w_j\rangle$, that satisfies

$$\sqrt{q_j}|w_j\rangle = \sum_{k=1}^{n} M_{kj}\sqrt{p_k}|v_j\rangle.$$

Because of unit trace, it also satisfies that $MM^\dagger = \mathbb{1}$.

Qubit. A *qubit* is the abbreviated word of *quantum bit*, which is the unit of quantum information. Any two-level quantum system can encode a qubit,

$$|\psi\rangle = a|0\rangle + b|1\rangle,$$

Here a and b are complex numbers in $\mathcal{C}^2$, while $|0\rangle$ and $|1\rangle$ defines a basis. The state must be normalized, i.e. $|a|^2 + |b|^2 = 1$ and satisfy the equivalence relation, i.e. $|\psi\rangle$ and $e^{i\theta}|\psi\rangle$ are equivalent. These conditions reduce the degrees of freedom, and finally two parameters θ and φ completely describe a qubit state as follows,

$$a = \cos\frac{\theta}{2}, \qquad b = e^{i\varphi}\sin\frac{\theta}{2}.$$

One can depict the state on a sphere of unit radius, called Bloch sphere, where the basis $|0\rangle$ and $|1\rangle$ elements correspond to the north and south poles of the sphere. Any point on the surface represents a pure state, and a point inside the ball represents a mixed state. As said, the decomposition of a mixed state is not unique, see the figure (A.1).

A.2 Quantum Operation

Quantum states evolve in time, and often this is called as the *Schrodinger picture*. The ideal dynamics of quantum states is governed by unitary operators U generated by Hamiltonian H,

$$U_t = \mathcal{T}\exp[\int^t dt' H(t')],$$

where $\mathcal{T}$ is time ordering. Unitary operators transforms a pure state into another pure state, $|\psi(t)\rangle = U_t|\psi(0)\rangle$, and they form a group with the product, $U_{s+t} = U_s U_t$, so that $|\psi(s+t)\rangle = U_s|\psi(t)\rangle$. If a mixed state is prepared, it will be evolved by U as follows,

$$\mathfrak{S} : \rho(0) \longrightarrow \rho(t) = U_t \rho(0) U_t^\dagger.$$

$\mathfrak{S}$ is called a superoperator.

The general quantum dynamics also includes non-unitary dynamics, by which a pure state can result in a mixed state. Note that this is due to interaction with an environment during evolution. However the global state over the system plus environment remains pure at any time of the evolution. This is because the whole state is governed by the unitary evolution U_{SE}. Then, the general quantum operation reads as follows: the evolution of the state of the system plus environment is governed by the global unitary operation U_{SE}. The system state is recovered after the environment is traced out. This can be expressed as follows,

$$\mathfrak{S} : |\psi_S\rangle\langle\psi_S| \longrightarrow \mathrm{tr}_E[U_{SE}(|\psi_S\rangle\langle\psi_S| \otimes |0_E\rangle\langle 0_E|)U_{SE}^\dagger], \tag{A.3}$$

where $|0_E\rangle\langle 0_E|$ can be the arbitrary initial state of the environment and U_{SE} is for both the system and environment.

Quantum operations can be in general described with the Kraus representation that takes into account the environment interaction. This can be derived easily from (A.3) as follows. Let us denote the basis vectors of environment by $\{|\Xi_{\mathcal{K}}(j)\rangle\}$. The explicit expansion of (A.3) is then straightforward:

$$\begin{aligned}(A.3) &= \sum_j \langle \Xi_{\mathcal{K}}(j)|U(\rho \otimes |0_{\mathcal{K}}\rangle\langle 0_{\mathcal{K}}|)U^\dagger|\Xi_{\mathcal{K}}(j)\rangle \\ &= \sum_j \langle \Xi_{\mathcal{K}}(j)|U|0_{\mathcal{K}}\rangle \rho (\langle \Xi_{\mathcal{K}}(j)|U|0_{\mathcal{K}}\rangle)^\dagger.\end{aligned}$$

Here let us denote each operator by $V_j = \langle \Xi_{\mathcal{K}}(j)|U|0_{\mathcal{K}}\rangle$ satisfying $\sum_j V_j^\dagger V_j = \mathbb{1}$, which are called the Kraus operators [65].

Collorary 1 (Kraus Representation) *There exists a set of operators V_j that describes a quantum operation Λ as follows*

$$\Lambda(\rho) = \sum_j V_j \rho V_j^\dagger, \tag{A.4}$$

satisfying $\sum_j V_j^\dagger V_j = \mathbb{1}$.

The Kraus representation gives an interpretation to quantum operation as follows. Suppose ρ evolves to ρ_i which is proportional to $V_i \rho V_i^\dagger$. Actually, $\mathrm{tr}[V_i \rho V_i^\dagger]$ is the probability that the initial state ρ transforms to ρ_i, so is denoted by p_i. When $\sum_i p_i = 1$, the quantum operation is called trace-preserving. Kraus representation describes that ρ evolves to

$$\rho_i = \frac{V_i \rho V_i^\dagger}{p_i}$$

with probability p_i, and after evolution the state remains in the ensemble of ρ_i, $\Lambda(\rho) = \sum_i p_i \rho_i$.

Measurement

Measurement is a particular quantum operation, and in general is formalized through the so-called Positive-Valued-Operator-Measure (POVM). Any measurement apparatus can be described by POVMs, $\{M_\alpha\}$ satisfying $\sum_{\alpha \in \mathcal{A}} M_\alpha = \mathbb{1}$. Here it is identified $M_\alpha = V_\alpha^\dagger V_\alpha$. Suppose that the system is in the state ρ_β, then measurement by the POVM provides measurement outcomes α with probability

$$p(\alpha|\beta) = \mathrm{tr}[M_\alpha \rho_\beta]$$

In the sense that quantum measurement provides probabilities, these general measurements are also called as Probability-Operator-Measure(POM).

The most basic measurement strategy is the computational basis measurement. Quantum states $|0\rangle$ and $|1\rangle$ are called computational basis, and when POVM is constructed by those states, it is computational basis measurement, $M_\alpha = |\alpha\rangle\langle\alpha|$, $\alpha = 0, 1$. In high dimensions, this is naturally extended with M_α with $\alpha = 0, \cdots, d-1$. The general form of the computational basis measurement is the projective measurement, where each measurement operators are projectors

$$M_\alpha M_\beta = \delta_{\alpha,\beta} M_\alpha$$

satisfying $\sum_\alpha M_\alpha = \mathbb{1}$.

Measuring quantum system uncovers only a part of the full information of the system, and also causes the state of a system to evolve to some other state by the interaction.

Axiomatic approach

Finally, quantum state evolution in general can be understood in terms of a mapping from quantum states to quantum states. Those mappings includes interaction with environment and fulfills that unitarity is recovered after extending the system into system plus environment. These mappings are quantum operations, which mathematically can be identified exactly by *the completely positive maps* [76].

Definition 10 (Completely Positive Maps) *Consider a quantum state ρ and a linear map Λ.*

1. *Λ is said to be positive if $\Lambda(\rho) > 0$ for all ρ.*

2. *Λ is said to be k-positive if $(\Lambda \otimes id_k)$, where id_k is the identity operator over k-dimensional Hilbert space, is positive. The map is said to be completely positive if $(\Lambda \otimes id_k)$ is positive for all k.*

3. *Λ is said to be trace-preserving if $\mathrm{tr}\Lambda(\rho) = 1$.*

4. *Λ is said to be unital if $\Lambda(\mathbb{1}) = \mathbb{1}$.*

Each completely positive map corresponds to a quantum operation, and vice versa. This can be seen clear by the following Stinespring dilation theorem [84].

Theorem 8 (Stinespring dilation theorem) *For every completely positive map Λ, there exist a finite dimensional Hilbert space $\mathcal{K}$ and a suitable unitary operation U such that*

$$\Lambda(\rho) = \mathrm{tr}_{\mathcal{K}}[U(\rho \otimes |0_{\mathcal{K}}\rangle\langle 0_{\mathcal{K}}|)U^{\dagger}] \tag{A.5}$$

for any quantum state ρ.

The theorem gives a tool to study quantum operation: adding an ancillary space $\mathcal{K}$ and knowing the whole unitary evolution U, a quantum evolution can be completely described.

Alternative to the *Schrodinger picture*, quantum dynamics can also be seen in the view of observables, which is often called as *Heisenberg picture.* It is the dual mapping of quantum operation from bounded operators over $\mathcal{H}_2$ to bounded operators over $\mathcal{H}_1$, i.e. $\Lambda^* : \mathfrak{B}(\mathcal{H}_2) \longrightarrow \mathfrak{B}(\mathcal{H}_1)$, while keeping quantum states constant. Two pictures are constrained by the duality relation, for any observable $O \in \mathfrak{B}(\mathcal{H}_2)$

$$\mathrm{tr}[\Lambda(\rho)O] = \mathrm{tr}[\rho\Lambda^*(O)],$$

so that both Schrodinger and Heisenberg pictures equivalently describe quantum dynamics. The relationship between Λ and Λ^* is summarized as:

1. Λ is linear $\iff$ Λ^* is linear
2. Λ is completely positive $\iff$ Λ^* is completely positive
3. Λ is trace-preserving $\iff$ Λ^* is unital

Appendix B

Cloning Based Attacks

Asymmetric cloning machines have been proven to be a useful tool in the study of optimal eavesdropping attacks. In a cryptographic scenario, the input state to the cloning machine is the one sent by Alice, while one of the outputs is forwarded by Eve to Bob, keeping the rest of the output state. For instance, in the BB84 case, where Alice uses states from the x and z bases, the optimal eavesdropping attack is done by a $1 \rightarrow 1 + 1$ phase-covariant cloning machine [17] that clones the xz equator. The output states for Bob and Eve are

$$\begin{aligned}\rho_B &= \frac{1}{2}(I + \eta_{xz}^B(n_x^B\sigma_x + n_z^B\sigma_z) + \eta_y^B n_y^B\sigma_y) \\ \rho_E &= \frac{1}{2}(I + \eta_{xz}^E(n_x^E\sigma_x + n_z^E\sigma_z) + \eta_y^E n_y^E\sigma_y),\end{aligned}$$

where η_i are usually called the shrinking factors.

In the entanglement picture, this attack corresponds to the Bell diagonal state

$$\begin{aligned}\rho_{AB} &= \lambda_1|\Phi_1\rangle\langle\Phi_1| + \lambda|\Phi_2\rangle\langle\Phi_2| \\ &+ \lambda|\Phi_3\rangle\langle\Phi_3| + \lambda_4|\Phi_4\rangle\langle\Phi_4|.\end{aligned}$$

Here $\lambda_2 = \lambda_3 = \lambda$, which implies that the error rate is the same in both bases. The normalization condition is $\lambda_1 + 2\lambda + \lambda_4 = 1$. When compared to the cloning machine, the shrinking factor are $\eta_{xz}^B = \lambda_1 - \lambda_4$ and $\eta_{xz}^E = 2\sqrt{\lambda}(\sqrt{\lambda_1} + \sqrt{\lambda_4})$. Note that $\eta_y^B = 1 - 4\lambda + 4\lambda_4$ and $\eta_y^E = 2(\lambda + \sqrt{\lambda_4(1 - 2\lambda - \lambda_4)})$.

In the case of using one-way communication distillation protocols, Eve's goal is to maximize, for a given QBER, her Holevo information with Alice (see Eq. (3.5)). The optimal coefficients, or cloning attack, are $\lambda_1 = (1-Q)^2$, $\lambda = Q - Q^2$, and $\lambda_4 = Q^4$, where Q is the QBER. When considering two-way communication protocols, as shown in Chapter 4, the security condition is given in Sec. 4.1.1. According to this condition, the optimal coefficients are $\lambda_1 = 1 - 2Q$, $\lambda = Q$, and $\lambda_4 = 0$.

Appendix C

Eve's information in the case of pre-processing

In this appendix, we show how to compute Eve's information in the case Alice applies pre-processing before the CAD protocol, for large blocks. In this limit, Eve is faced with two possibilities, $\rho_{0,0}^{\otimes N}$ and $\rho_{1,1}^{\otimes N}$, that read

$$\begin{aligned} \rho_{0,0} &= u|e_{0,0}\rangle\langle e_{0,0}| + v|e_{0,1}\rangle\langle e_{0,1}| \\ \rho_{1,1} &= u|e_{1,1}\rangle\langle e_{1,1}| + v|e_{1,0}\rangle\langle e_{1,0}| \end{aligned} \tag{C.1}$$

Indeed, if $N \gg 1$, there are almost no errors in the symbols accepted by Alice and Bob. Eve's Holevo bound then reads

$$\chi(A:E) \approx S(\sigma_E) - Nh(u), \tag{C.2}$$

where we used the fact that $S(\rho_{0,0}^{\otimes N}) = S(\rho_{1,1}^{\otimes N}) = Nh(u)$.

The main problem, then, consists of the diagonalization of σ_E. Note however that the states $\rho_{0,0}$ and $\rho_{1,1}$ have rank two and their eigenvectors belong to different two-dimensional subspaces. This implies that σ_E decomposes into two-dimensional subspaces that can be easily diagonalized. The corresponding eigenvalues are

$$\lambda_r = u^r v^{N-r} \frac{1 \pm |\langle e_{0,0}|e_{1,1}\rangle|^r |\langle e_{0,1}|e_{1,0}\rangle|^{N-r}}{2} \tag{C.3}$$

for $r = 0, \ldots, N$, with degeneracy $N!/(r!(N-r)!)$. Replacing these eigenvalues into the von Neumann entropy, one gets

$$\begin{aligned} S(\sigma_E) = Nh(u) + \sum_{r=0}^{N} \binom{N}{r} u^r v^{N-r} \\ h\left(\frac{1 + |\langle e_{0,0}|e_{1,1}\rangle|^r |\langle e_{0,1}|e_{1,0}\rangle|^{N-r}}{2}\right). \end{aligned} \tag{C.4}$$

For large N and nonzero u, the only relevant terms in the previous sum are such that $|\langle e_{0,0}|e_{1,1}\rangle|^r|\langle e_{0,1}|e_{1,0}\rangle|^{N-r} \ll 1$. One can then approximate $h((1+x)/2) \approx 1 - x^2/\ln 4$, having

$$S(\sigma_E) \approx Nh(u) + 1 - \frac{(u|\langle e_{0,0}|e_{1,1}\rangle|^2 + v|\langle e_{0,1}|e_{1,0}\rangle|^2)^N}{\ln 4},$$

where we used the binomial expansion. Collecting all the terms, Eve's information reads

$$\chi(A:E) \approx 1 - \frac{(u|\langle e_{0,0}|e_{1,1}\rangle|^2 + v|\langle e_{0,1}|e_{1,0}\rangle|^2)^N}{\ln 4}. \tag{C.5}$$

Appendix D

Properties of geometrically uniform states

A set of d quantum states $\{|\psi_0\rangle, ..., |\psi_{d-1}\rangle\}$ is said to be geometrically uniform if there is a unitary operator U that transforms $|\psi_j\rangle$ into $|\psi_{j+1}\rangle$ for all j, where the indices read modulo d. All sets of geometrically uniform states, if the cardinality is the same, are isomorphic. Therefore, we do not lose any generality when assuming that those states are of the form:

$$|\psi_\alpha\rangle = \sum_{n=0}^{d-1} c_n e^{\frac{2\pi i}{d} n\alpha} |x_n\rangle$$

where α runs from 0 to $d-1$ and $|x_n\rangle$ are orthonormal basis. Each state $|\psi_\alpha\rangle$ translates to $|\psi_{\alpha+\beta}\rangle$ by applying β times the unitary $U = \sum_{m=0}^{d-1} e^{\frac{2\pi i}{d} m} |x_m\rangle\langle x_m|$. These states satisfy the following properties, that are used in our computations:

- Given a set of geometrically uniform states $\{|\psi_0\rangle, ..., |\psi_{d-1}\rangle\}$, an orthonormal basis spanning the support of those states can explicitly obtained as follows:

$$|x_n\rangle = \frac{1}{dc_n} \sum_\alpha e^{-\frac{2\pi i}{d} n\alpha} |\psi_\alpha\rangle. \tag{D.1}$$

- The uniform mixture of geometrically uniform states gives the orthogonal decomposition in the basis defined above $\{|x_n\rangle\}$:

$$\rho \;=\; \frac{1}{d} \sum_\alpha |\psi_\alpha\rangle\langle\psi_\alpha| = \sum_n c_n^2 |x_n\rangle\langle x_n|.$$

Therefore, the eigenvalues of the equal mixture of geometrically uniform state are c_n^2. Using (D.1), these eigenvalues can be written as:

$$c_n^2 = \frac{1}{d^2} \sum_{\alpha,\beta} e^{\frac{2\pi i}{d} n(\beta-\alpha)} \langle\psi_\beta|\psi_\alpha\rangle. \tag{D.2}$$

In our case, we are interested in the eigenvalues of the state

$$\rho = \frac{1}{d}\sum_{\alpha} |e_\alpha\rangle\langle e_\alpha|^{\otimes N},$$

which approximates Eve's state after CAD in the limit of large N. The states $|e_\alpha\rangle^{\otimes N}$ are geometrically uniform, so the searched eigenvalues are:

$$\lambda_\mu = \frac{1}{d^2}\sum_{\alpha,\beta} e^{\frac{2\pi i}{d}\mu(\beta-\alpha)}\langle e_\beta|e_\alpha\rangle^N.$$

Appendix E

Square-Root Measurement(SRM)

We describe the so-called square-root measurement along the lines given in Ref. [35]. Suppose that Alice encodes a classical random variable i that can take l different values into a quantum state $|\phi_i\rangle \in \mathbb{C}^d$, with $l \leq d$, and sends the state to Bob. Suppose the l states are non-orthogonal and span an m dimensional subspace of $\mathbb{C}^d$. Denote by Π_m the projection into this subspace, i.e. $\Pi_m|\phi_i\rangle = |\phi_i\rangle$ for all i. Bob has to read out the encoded value from the quantum state in an "optimal" way. There exist several "optimal" measurements depending on the figure of merit to be optimized. Here, following [35], we consider that Bob applies a measurement consisting of l rank-one operators $|m_i\rangle\langle m_i|$, satisfying $\sum_i |m_i\rangle\langle m_i| = \Pi_m$. The figure of merit to be optimized is the squared error $E = \sum_{i=0}^{l-1}\langle E_i|E_i\rangle$, where $|E_i\rangle = |\phi_i\rangle - |m_i\rangle$ are the error vectors. As shown in [35], the measurement strategy minimizing E is the so-called SRM, also known as pretty-good measurement. The construction of this optimal measurement works as follows.

Denoted by Φ the matrix whose columns are $|\phi_i\rangle$. The SRM is constructed from the structure of the matrix Φ. Applying singular value decomposition to $\Phi = UDV^\dagger$, the optimal measurement matrix is [35]

$$M = \sum_i |u_i\rangle\langle v_i|$$

where $|u_i\rangle$ and $|v_i\rangle$ are the column vectors of the two unitary matrices U and V, respectively. Here the column vectors of M define the optimal choice of measurement projectors $|m_i\rangle$.

Moving to our cryptography problem, the states Eve has to discriminate are the geometrically uniform states

$$|e_\gamma\rangle = \sum_{n=0}^{d-1} \beta_n e^{2\pi i(\gamma n/d)}|x_n\rangle$$

where $|x_n\rangle$ is an orthonormal basis in a d-dimensional Hilbert space, and γ runs from 0 to $d-1$. Each $|e_\gamma\rangle$ is normalized. In our problem, Eve aims at minimizing her error probability. Interestingly, in the case of geometrically uniform state, the previous measurement strategy turns out to minimize the error probability as well [35]. So, we only have to derive the optimal measurement matrix from $\Phi = \sum_\gamma |e_\gamma\rangle\langle x_\gamma|$. Using relations $\Phi^\dagger\Phi = VDV^\dagger$, the unitary V is the d-dimensional Fourier transform $\mathcal{F}|x_u\rangle = \frac{1}{\sqrt{d}}\sum_w \exp(-\frac{2\pi i}{d}wu)|x_w\rangle$, and the diagonal matrix is $D = diag(\sqrt{d}|\beta_n|)$. Therefore, the optimal measurement matrix is

$$M = \sum_i |m_i\rangle\langle x_i|$$

where

$$|m_j\rangle = \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1} e^{\frac{2\pi i}{d}jk}|x_k\rangle$$

Using this measurement, the probability of guessing correctly a given state $|e_j\rangle$ is $|\langle m_j|e_j\rangle|^2$. Then, the average success probability is

$$P^{success} = \sum_{j=0}^{d-1} p(j)\,|\langle m_j|e_j\rangle|^2 = \frac{1}{d}\Big|\sum_n \beta_n\Big|^2 \tag{E.1}$$

The last equality is obtained taking into account that all $|e_j\rangle$ are equally probable, $p(j) = 1/d$. In particular, for the $d+1$- or 2-bases protocols, the success probability reads, in terms of v and z, $P^{success} = (v+(d-1)z)^2/dF$.

When N copies of the states are given, $|e_j\rangle^{\otimes N}$, we can apply a collective measurement strategy. The SRM is constructed in the same way as above, and the success probability, assuming that all states are equi-probable, is

$$P_N^{success} = \frac{1}{d^2}\left|\sum_\eta \sqrt{\sum_m e^{2\pi i(\eta m/d)}\langle e_m|e_0\rangle^N}\right|^2. \tag{E.2}$$

Bibliography

[1] A. Acín, N. Gisin, and V. Scarani, Quantum Information and Computation. **3** No. 6, 563 (2003).

[2] A. Acín, Ll. Masanes, and N. Gisin, Phys. Rev. Lett. **91**, 167901 (2003).

[3] A. Acín and N. Gisin Phys. Rev. Lett. **94**, 020501 (2005).

[4] A. Acín, J. Bae, E. Bagan, M. Baig, Ll. Masanes, and R. Muñoz-Tapia, Phys. Rev. A **73**, 012327 (2006).

[5] J. Bae and A. Acín, Phys. Rev. Lett. **97** 030402 (2006).

[6] J. Bae and A. Acín, Phys. Rev. A **75**, 012334 (2007).

[7] K. Banaszek, Phys. Rev. Lett. **86**, 1366 (2001).

[8] C. H. Bennett and G. Brassard, Proceedings of International Conference on Computer Systems and Signal Processing, p. 175 (1984).

[9] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett, **68** 557(1992).

[10] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[11] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, W. K. Wootters, Phys.Rev. A **54** 3824-3851 (1996).

[12] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin, and W. Wootters, Phys. Rev. Lett, **76** 722(1996).

[13] S. L. Braunstein and A. K. Pati, eds., *Quantum Information with Continuous Variables*, Kluwer Academic, Dordrecht, 2003.

[14] D. Brody and B. Meister. Phys. Rev. Lett. **76**, 1 (1996); A. Acín, E. Bagan, M. Baig, Ll. Masanes, and R. Muñoz-Tapia, Phys. Rev. A **71** 032338 (2005).

[15] D. Bruß, A. Ekert and C. Macchiavello, Phys. Rev. Lett. **81**, 2598 (1998).

[16] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998); H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev A, **59**, 4238 (1999).

[17] D. Bruß, M. Cinchetti, G. M. D'Ariano, and C. Macchiavello, Phys. Rev. A **62**, 12302 (2000).

[18] D. Bruß M. Christandl, A. Ekert, B.-G. Englert, D. Kaszlikowski, and C. Macchiavello, Phys. Rev. Lett. **91**, 097901 (2003).

[19] V. Bužek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).

[20] N. Cerf, Phys. Rev. Lett. **84**, 4497 (2000); J. Mod. Opt. **47**, 187 (2000); Acta Phys. Slov. **48**, 115 (1998).

[21] N. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).

[22] H. F. Chau, Phys. Rev. A **66**, 060302 (2002).

[23] H. F. Chau, IEEE Trans. Inf. Theory **51**, 4 (2005).

[24] G. Chiribella and G. M. D'Ariano, Phys. Rev. Lett. **97**, 250503 (2006).

[25] M. Christandl, R. Renner and A. Ekert, quant-ph/0402131.

[26] J. I. Cirac, A. K. Ekert, and C. Macchiavello, Phys. Rev. Lett. **82** 4344-4347 (1999).

[27] I. Csiszár and J. Körner, Vol. **IT-24**, pp. 339-348, (1978).

[28] M. Curty, M. Lewenstein and N. Luetkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).

[29] R. Demkowicz-Dobrzanski, Phys. Rev. A **71**, 062321 (2005).

[30] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).

[31] I. Devetak and A. Winter, Phys. Rev. Lett. **93**, 080501 (2004); R. Renner and R. Koenig, quant-ph/0403133.

[32] L.-M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **84**, 2722; R. Simon, *ibid*, 2726.

[33] J. Eisert, S. Scheel and M. B. Plenio, Phys. Rev. Lett. **89**, 137903 (2002); J. Fiurasek, *ibid*, 137904.

[34] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[35] Y. C. Eldar and G. D. Forney, IEEE Trans. Inf. Theory **47**, 3 (2001).

[36] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, E. S. Polzik , Science **282**, 706 (1998).

[37] G. Giedke, L.-M. Duan, J.I. Cirac, and P. Zoller, Quant. Inf. Comp. **1**, 79 (2001).

[38] G. Giedke and J. I. Cirac, Phys. Rev. A **66**, 032316 (2002).

[39] N. Gisin and S. Massar, Phys. Rev. Lett. **79**, 2153 (1997).

[40] N. Gisin, Phys. Lett. A **242**, 1 (1998).

[41] N. Gisin and S. Wolf, Phys. Rev. Lett **83**, 4200 (1999).

[42] N. Gisin and S. Wolf, Advances in Cryptology - CRYPTO '00, Lecture Notes in Computer Science, Springer-Verlag, pp. 482-500 (2000).

[43] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[44] D. Gottesman and J. Preskill, Phys. Rev. A **63**, 022309 (2001).

[45] D. Gottesman and H.-K. Lo, IEEE Trans. Inf. Theory **49**, 457 (2003).

[46] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002); Ch. Silberhorn *et al.*, Phys. Rev. Lett. 89, 167901 (2002).

[47] O. Guehne, P. Hyllus, D. Bruss, A. Ekert, M. Lewenstein, C. Macchiavello, and A. Sanpera, Phys. Rev. A **94**, 062305 (2002).

[48] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature **421**, 238 (2003).

[49] L. Gurvits, Proceedings of the 35th ACM Symposium on Theory of Computing ACM Press, New York, 2003 p.10 (2003), quant-ph/0303055.

[50] P. Hausladen and W. K. Wootters, J. Mod. Opt., **41**, 2385 (1994).

[51] C. Helstrom, Quantum Detection and Estimation Theory, Academic Press, New York, 1976.

[52] A. S. Holevo and R. F. Werner, Phys. Rev. A **63**, 032312 (2001); A. Botero and B. Reznik, Phys. Rev. A **67**, 052311 (2003).

[53] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).

[54] M. Horodecki and P. Horodecki, Phys. Rev. A **59**, 4206 (1999).

[55] M. Horodecki, P. W. Shor and M. B. Ruskai, Rev. Math. Phys **15**, 629 (2003).

[56] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. **94**, 160502 (2005).

[57] http://www.imaph.tu-bs.de/qi/problems/.

[58] B. Huttner, A. Muller, J. D. Gautier, H. Zbinden and N. Gisin, Phys. Rev. A **54**, 3783 (1996).

[59] S. Iblisdir, G. Van Assche and N. J. Cerf, quant-ph/0312018.

[60] S. Iblisdir, A. Acín, N. J. Cerf, J. Fiurášek, R. Filip and N. Gisin, Phys. Rev. A **72**, 042328 (2005).

[61] D. Kaszlikowski, J. Y. Lim, L. C. Kwek, and B.-G. Englert, quant-ph/0312172.

[62] M. Keyl and R. F. Werner, J. Math. Phys. **40**, 3283 (1999).

[63] B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005); R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).

[64] B. Kraus, C. Branciard and R. Renner, quant-ph/0610151.

[65] K. Kraus, States effects and operations. Springer, Berlin (1983).

[66] H.-K. Lo, Quant. Inf. Comp **1**, 81 (2001).

[67] Ll. Masanes, A. Acín and N. Gisin, Phys. Rev. A **73**, 012112 (2006); J. Barrett, quant-ph/0508211.

[68] S. Massar and S. Popescu, Phys. Rev. Lett. **74**, 1259 (1995).

[69] U. Maurer, IEEE Trans. Inf. Theory **39**, 733 (1993).

[70] U. Maurer, IEEE Trans. Inf. Theory **45**, 2 (1999).

[71] D. Mayers, Advances in Cryptology - CRYPTO '96, LNCS 1109, p. 343-357 (1996).

[72] M. Navascués, J. Bae, J. I. Cirac, M. Lewestein, A. Sanpera and A. Acín, Phys. Rev. Lett. **94** 010502 (2005).

[73] M. Navascués and A. Acín, Phys. Rev. A **72**, 012303 (2005).

[74] G. M. Nikolopoulos, K. S. Ranade, G. Alber, Phys. Rev. A. **73** 032325 (2006).

[75] C.-S. Niu and R. B. Griffiths, Phys. Rev. A **58**, 4377 (1998); N. J. Cerf, Acta Phys. Slov. **48**, 115 (1998); V. Bužek, M. Hillery and M. Bendik, *ibid*, 177 (1998); N. J. Cerf, J. Mod. Opt. **47**, 187 (2000).

[76] V. I. Paulsen, Completely bounded maps and dilations, Longman Scientific & Technical (1986).

[77] A. Peres, Phys. Rev. Lett. **76** 1413 (1997); M. Horodecki, P. Horodecki, and R. Horodecki Phys. Lett. A **223** 1 (1996).

[78] R. Renner, PhD thesis.

[79] V. Scarani, S. Iblisdir, N. Gisin and A. Acín, Rev. Mod. Phys. **77**, 1225 (2005); N. J. Cerf and J. Fiurášek, quant-ph/0512172.

[80] C. E Shannon, Vol. 27, pp. 379-423, 623-656, (1948).

[81] P. W. Shor, *Proc. of the 35th Annual Symposium on the Foundations of Computer Science*, IEEE, Los Alamitos, CA, 124 (1994).

[82] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441, (2000).

[83] G. Smith, J. M. Renes and J. A. Smolin, quant-ph/0607018.

[84] W. F. Stinespring, Proc. Amer. Math. Soc. 211 - 216 (1955).

[85] B. M. Terhal, IBM J. Res. Dev. **48**, No.1, 71 (2004).

[86] F. Verstraete, J. Dehaene, and B. De Moor, Phys. Rev. A **64**, 010101(R) (2001).

[87] F. Verstraete and M. Wolf. Phys. Rev. Lett, **89** 170401(2002).

[88] R. Werner, Phys. Rev. A **40**, 4277 (1989).

[89] R. F. Werner, Lett. Math. Phys. **17**, 359 (1989); another, and somehow extended, proof of this result can also be found in A. C. Doherty, P. A. Parrilo and F. M. Spedalieri, Phys. Rev. A **69**, 022308 (2004). Recently, a beatifully simple proof of the same result has been given in D. Yang, quant-ph/0604168.

[90] R. F. Werner and M. M. Wolf, Phys. Rev. Lett. **86**, 3658 (2001).

[91] W. Wootters and W. Zurek Nature **299** 802-803 (1982); for review, V. Scarani, S. Iblisdir, N. Gisin, and A. Acín, Rev. Mod. Phys. **77**, 1225 (2005).

[92] W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).

[93] W. K. Wootters, Phys. Rev. Lett. **80** 2245-2248 (1998).

[94] H.P. Yuen, Phys. Lett. **113A**, 405 (1986).