Capítol 1

Esquemes per a compartir secrets

L'objectiu que es persegueix és modelitzar i estudiar la situació següent: dintre d'un conjunt de participants només certes agrupacions d'aquests estan autoritzades per accedir a un secret, però de forma que tota reunió de participants no autoritzada no ha de poder obtenir cap informació de quin pot ser el secret. Una variant en aquest plantejament és quan el secret s'entén com la desencadenació d'una acció: en aquest cas només la conjunció de determinades circumstàncies o bé la presència de determinades persones pot desencadenar l'acció. La criptologia de clau privada i de clau pública està basada en la intractabilitat d'un problema i per tant, depèn dels avenços en aquest tema o en la capacitat de computació de les parts que intervenen. En canvi, els esquemes per a compartir secrets s'han dissenyat sota una premisa de seguretat independent dels recursos computacionals i dels avenços matemàtics en el tema. Veiem situacions diferents en les quals intervé un esquema per a compartir secrets.

En un dipòsit monetari de propietat compartida entre un cert número de beneficiaris, l'accés està restringit normalment a que s'ajuntin un número prefixat de signatures de beneficiaris. Aquest número mínim es diu llindar. D'aquesta forma es defineixen els conjunts autoritzats de participants com aquells que tenen cardinal més gran o igual que aquest llindar. Aquesta manera de definir una estructura d'accés s'anomena *estructura de llindar*, la qual és una de les més estudiades. Un altre cas és el de decidir sobre la conveniència de prendre una decisió greu o no, com per exemple el llençament d'un míssil nuclear. Sovint el criteri és que si es donen una sèrie de circumstàncies preestablertes, llavors es pren la decisió. També a [82] s'ha proposat a l'hora de

mantenir de forma segura una informació (per exemple un disc dur d'un ordinador) dividir-la en n fragments segons una estructura de llindar (t, n) de forma que si molts dels fragments es fessin malbé, només caldria que almenys t d'aquests no es fessin malbé per tal de poder recuperar la informació. En aquest cas no és el secret de la informació el que més importa, si no la pròpia integritat de la informació. També s'ha proposat de la mateixa manera, establir línees segures de transmissió d'informació a base d'enviar la informació fragmentada en n porcions de forma que només calgui que t d'aquestes arribin sense perturbació amb la finalitat de poder recuperar la informació correcta. També s'han fet propostes d'utilització dels esquemes per a compartir secrets com a peça constituent d'un protocol criptogràfic. Aquest és el cas de la generació compartida de signatures digitals o la verificació de l'autenticitat d'un document [40, 84]. De fet la motivació inicial amb la qual van néixer els esquemes per a compartir secrets va ser un problema comú a tots els criptosistemes: els problemes de distribució i de gestió de claus [90]. També té la seva aplicació en els protocols segurs multipart [42] o a la computació amb tolerància a fallides [75].

1.1 Esquema per a compartir secrets perfecte

Descriurem tot seguit les diferents parts que intervenen en un esquema per a compartir secrets. Sigui un conjunt de secrets o de claus secretes $\mathcal{K}$. Disposem d'un *algorisme distribuïdor* que a partir d'un secret fixat $k \in \mathcal{K}$ assigna a cada participant $p_i \in P$ un *fragment d'informació* $s_i \in \mathcal{S}_i$. Cada participant guarda en secret el seu fragment. També disposem d'un *algorisme recuperador* que a partir dels fragments dels participants d'un subconjunt autoritzat recupera el secret. Sovint direm que hi ha un participant $D \notin P$ anomenat distribuïdor que realitza el càlcul i la repartició dels fragments entre els participants. De la mateixa manera direm que una *caixa negra* fa la feina de l'algorisme distribuïdor.

De forma natural es demana que

1. si els participants d'un subconjunt autoritzat ajunten els seus fragments poden recuperar el secret,

2. si els participants d'un subconjunt no autoritzat ajunten els seus fragments de secret, llavors no poden obtenir absolutament cap informació sobre el possible valor del secret

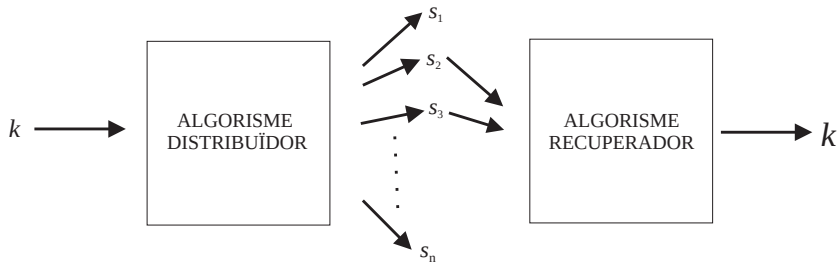

Figura 1.1: Algorisme distribuïdor i recuperador en un esquema per a compartir secrets

Per la primera condició es diu que l'esquema per a compartir secrets *realitza* l'estructura d'accés i quan es verifiquen les dues condicions es diu que es tracta d'un esquema per a compartir secrets *perfecte*. Una altra manera de definir quan un esquema per a compartir secrets és perfecte és utilitzant el concepte d'entropia com es farà notar a la Secció 2.8. Observem que l'exigència de la segona condició és que tots els secrets siguin igualment probables sota el coneixement dels fragments dels participants d'un subconjunt no autoritzat. A més a més aquest desconeixement del valor possible del secret ha de ser independent del recursos computacionals dels quals es disposi. D'aquesta manera parlem de esquemes amb seguretat *no computacional*. També es poden considerar esquemes en els quals la seguretat és *computacional*, en els quals la segona condició s'afebleix dient que si els participants d'un subconjunt no autoritzat ajunten els seus fragments de secret, llavors no poden obtenir absolutament cap informació sobre el possible valor del secret utilitzant els recursos computacionals actuals. No ens ocuparem d'aquest esquemes aquí, però es pot obtenir més informació a [32, 41]. Un estudi molt general dels esquemes per a compartir secrets *no perfectes* es pot trobar a [54]. També s'han proposat esquemes no perfectes, en els quals la seguretat depèn dels recursos computacionals dels quals es disposi [53, 5]. En el present treball tots els esquemes seran perfectes i amb seguretat no computacional, si no es diu res al contrari.

Suposem que disposem d'un conjunt finit de participants P i d'una col·lecció de subconjunts Γ de P, això és, $\Gamma \subset 2^P$ que anomenarem *estructura d'accés*. A una part Γ' d'una estructura Γ, és a dir, $\Gamma' \subset \Gamma$, se l'anomena *subestructura* de Γ. Sovint escriurem el conjunt de n participants numerant els seus elements amb subíndexos, això és, $P = \{p_1, \ldots, p_n\}$. Nosaltres només considerarem el cas en el qual el P és finit, però s'han fet estudis pel cas en el qual el conjunt de participants no és finit [33].

De forma natural, exigirem que es verifiqui que:

$$\text{si } A \in \Gamma \text{ i } A \subset B \text{ aleshores } B \in \Gamma$$

Una estructura d'accés que verifiqui aquesta condició se l'anomena *monòtona*. S'han descrit generalitzacions del concepte d'estructura monòtona d'accés a [47] que no considerarem en aquesta memòria.

La col·lecció de *subconjunts minimals* que determina l'estructura d'accés se l'anomena *base* i la representarem per Γ_0. Es pot definir quina és l'estructura generada per una col·lecció Γ_0 de subconjunts de P:

$$\text{cl}(\Gamma_0) = \{A \mid \text{ existeix } B \in \Gamma_0 \text{ tal que } B \subset A\}$$

anomenada la *clausura* de Γ_0. Evidentment si Γ_0 és la base de Γ, es té que $\text{cl}(\Gamma_0) = \Gamma$. De vegades és còmode escriure el conjunt dels participants que intervenen en una certa estructura per $P(\Gamma) = \bigcup_{A\in\Gamma} A$. Una estructura d'accés es diu *connectada* quan $P(\Gamma_0) = P$, això és, quan tot participant intervé en algun minimal. Una estructura no és connectada quan conté participants, els fragments dels quals no aporten cap informació i que figuren en els subconjunts autoritzats d'una forma supérflua. És per això que sovint considerarem estructures connectades, descartant l'existència d'aquest tipus de participants.

El *rang* de Γ es defineix com el màxim cardinal dels minimals de Γ, és a dir, $\text{rang}(\Gamma) = \max\{|A| : A \in \Gamma_0\}$. Quan tots els minimals tenen el mateix cardinal es diu que l'estructura és *uniforme* o *homogènia*.

Com ja hem comentat a la introducció, una de les estructures més estudiades ha estat la (t, n)-*estructura de llindar* en un conjunt de n participants amb $t \leq n$ definida per

$$\Gamma = \{A : |A| \geq t\}$$

és a dir, formada per tots els subconjunts d'almenys t elements d'entre n participants. Aquesta estructura és homogènia de rang t. Els esquemes de llindar han estat àmpliament estudiats ja que aconsegueixen una eficient relació entre seguretat i practicitat. Prenent, per exemple, per un llindar t, un número de participants $n = 2t - 1$ s'obté un esquema eficient ja que es pot recuperar el secret fins i tot quan s'han perdut o fet malbé $t - 1$ fragments, és a dir, pràcticament la meitat dels fragment lliurats. Qualsevol oponent no podrà obtenir cap informació sobre el valor del secret coneixent com a màxim $t - 1$ fragments.

Els esquemes que realitzen una (t, n)-estructura de llindar s'anomenen (t, n)-*esquemes de llindar*. Sovint pels (t, n)-esquemes de llindar s'escriuen les dues condicions que ens asseguren que l'esquema és perfecte, de la manera següent

1. si s'ajunten els fragments de t participants, es pot recuperar el secret
2. si s'ajunten els fragments de $t-1$ participants, llavors no es pot obtenir absolutament cap informació sobre el possible valor del secret

Condicions que són equivalents a les anteriors pel cas de les estructures de llindar.

Les estructures de llindar van ser considerades per primera vegada per Shamir en el seu article [83] de 1979 en el qual comenta una generalització: les *estructures definides per pesos i llindar*. Es pot trencar la uniformitat en la rellevància de cada participant a l'estructura de llindar, assignant a cada participant $p \in P$ un cert pes $\omega(p) \in \mathbb{R}$ de forma que un subconjunt serà autoritzat quan la suma dels pesos dels seus participants és almenys el llindar t, això és

$$A \in \Gamma \text{ si i només si } \sum_{p \in A} \omega(p) \geq t$$

Aquestes estructures també han estat anomenades *estructures intrínseques* per en Simmons a [90].

Una altra de les famílies d'estructures d'accés més estudiades han estat les homogènies de rang 2, les anomenades *estructures determinades per un graf*. Aquestes estructures es poden representar mitjançant un graf amb conjunt de vèrtexs P i conjunt d'arestes Γ_0. I a l'inrevés, tot graf $G = (V(G), E(G))$ determina una estructura d'accés en el conjunt de participants $P = V(G)$ determinada per $\Gamma = cl(E(G))$.

També s'han considerat *estructures d'accés basades en codis lineals correctors d'errors* a partir del treball de McEliece i Sarwate [60], podent-se estudiar la seva estructura en funció dels paràmetres del codi [76].

1.2 Exemples d'esquemes per a compartir secrets

Veiem en primer lloc un exemple d'esquema per a compartir secrets perfecte que realitza una (n, n)-estructura de llindar degut a Karnin, Greene i Hellman [51]. Sigui el conjunt de participants $P = \{p_1, \ldots, p_n\}$ i el conjunt de secrets $\mathcal{K} = \mathbb{Z}_m$ amb $m \geq n$. Donat un secret $k \in \mathcal{K}$, escollim aleatòriament $n-1$ elements $r_1, \ldots, r_{n-1} \in \mathbb{Z}_m$ que assignarem als participants $p_1, \ldots, p_{n-1}$ i pel darrer participant calcularem el seu fragment com a $k - r_1 - \ldots - r_{n-1}$. Per recuperar el secret només cladrà sumar tots els fragments per així poder determinar el secret. Aquest procediment el resumirem en el quadre següent

Esquema de Karnin, Greene i Hellman
Algorisme distribuïdor: sigui $k \in \mathcal{K} = \mathbb{Z}_m$ amb $m \geq n$
escollim aleatòriament $n-1$ elements
$r_1, \ldots, r_{n-1} \in \mathbb{Z}_m$ i procedim:
$p_1 \longmapsto s_1 = r_1$
$\ldots$
$p_{n-1} \longmapsto s_{n-1} = r_{n-1}$
$p_n \longmapsto s_n = k - r_1 - \ldots - r_{n-1}$
Algorisme recuperador: es recupera amb
$k = s_1 + \ldots + s_n$

S'observa que l'únic subconjunt autoritzat, format per tots els participants, recupera fàcilment el secret a partir dels seus fragments, fent la suma de tots ells. D'altra banda tot subconjunt de menys de n participants no pot obtenir cap informació sobre el valor possible del secret, atès que tot secret és igualment probable a partir de menys de n fragments. Aquest fet és degut a l'aleatorietat amb la qual han estat escollits els fragments. De fet la implementació d'aquest esquema només requereix tenir un conjunt de n o més elements amb estructura de grup.

L'*esquema polinomial de Shamir* [83] va ser històricament la primera proposta d'un esquema per a compartir secrets. En aquest mateix treball de l'any 1979 s'exposen les bases de la teoria dels esquemes per a compartir secrets. L'esquema el resumim en el quadre següent:

Esquema polinomial de Shamir
Algorisme distribuïdor: sigui $k \in \mathcal{K} = GF(q)$.
Generem els nombres aleatoris
$a_1, \ldots, a_{t-1} \in GF(q)$
A partir del polinomi
$A(x) = k + a_1 x + \ldots + a_{t-1} x^{t-1}$
es reparteix
$p_1 \longmapsto s_1 = A(x_1)$
$\ldots$
$p_n \longmapsto s_n = A(x_n)$
Algorisme recuperador: es fa
interpolació polinòmica, recuperant
el secret amb $k = A(0)$

Aquest esquema realitza una (t, n)-estructura de llindar. En efecte, sigui el conjunt de secrets $\mathcal{K} = GF(q)$, amb $q \geq n + 1$ i associem públicament a cada participant $p_i \in P$ un element $x_i \in GF(q)^*$ de forma que $x_1, \ldots, x_n$ siguin diferents dos a dos. A partir d'un polinomi $A(x)$, de grau menor o igual que $t - 1$, lliurem el fragment $s_i = A(x_i)$ al participant p_i. En aquest esquema tota reunió de t participants pot recuperar el secret a partir d'interpolació polinòmica. Recordem que donades t parelles de punts $(x_1, y_1), \ldots, (x_t, y_t) \in GF(q) \times GF(q)$ amb $x_1, \ldots, x_t$ diferents dos a dos, hi ha un únic polinomi de grau menor o igual que $t - 1$ que passa per tots ells. Així doncs, si una reunió de t participants ajunten els seus punts, poden recuperar l'únic polinomi $B(x)$ de grau menor o igual que $t - 1$ que passa per tots ells. Com que el polinomi $A(x)$ verifica que és de grau menor o igual que $t - 1$ i passa per aquests punts, tindrem que $A(x) = B(x)$ per a tot $x \in GF(q)$ i d'aquí $k = B(0)$. D'altra banda tota reunió de $t - 1$ participants no pot obtenir cap informació sobre el valor del possible secret. Sigui k' un element qualsevol de $GF(q)$. Raonem que amb la informació de la qual disposen els $t - 1$ participants es pot haver repartit el secret k'. Sabem que a partir dels $t - 1$ punts dels participants i del punt $(0, k')$ existeix un polinomi $B(x)$ de grau menor o igual que $t - 1$ que passa per tots els punts inclós el punt $(0, k')$. Per tant, amb la informació de que disposen els $t - 1$ participants, el secret k' és possible. A la Figura 2.2 es mostra com en el cas $t = 3$ tot secret és possible a partir de la informació de dos punts per on passa el polinomi.

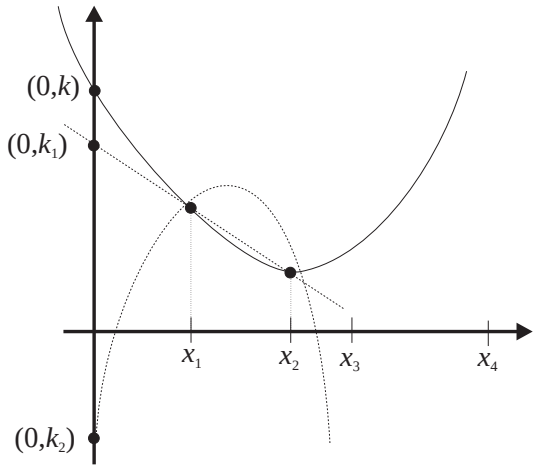

Figura 1.2: Tots els secrets són possibles a l'esquema polinomial de Shamir per $t = 3$

Shamir en el mateix treball proposa de lliurar més d'un fragment a determinats participants, de forma que defineix una estructura de llindar en la qual no tots els participants tenen el mateix pes. Aquestes estructures són les anomenades *estructures definides per pesos i llindar*.

L'esquema que presentem ara és el primer esquema que es va proposar per realitzar una estructura d'accés qualsevol. La versió que exposarem aquí és la que es coneix com la construcció de l'*esquema circuital* de Ito, Saito i Nishizeki [44] amb algunes modificacions presentades a [8] per Benaloh i Leichter. Sigui el conjunt de secrets $\mathcal{K} = \mathbb{Z}_m$ i un secret $k \in \mathcal{K}$. L'esquema es basa en la repartició del secret k sobre els participants de cada minimal $A \in \Gamma_0$ mitjançant l'esquema de $(|A|, |A|)$-llindar de Karnin, Greene i Hellman, això és:

Esquema de Ito, Saito i Nishizeki modificat
Algorisme distribuïdor: sigui $k \in \mathcal{K}$.
Per a cada $A = \{p_1, \ldots, p_\ell\} \in \Gamma_0$ generem els nombres aleatoris $r_{A1}, \ldots, r_{A\ell-1}$

$$\begin{array}{lcl} p_1 & \longmapsto & s_{A1} = r_{A1} \\ & \cdots & \\ p_{\ell-1} & \longmapsto & s_{A\ell-1} = r_{A\ell-1} \\ p_\ell & \longmapsto & s_{A\ell} = k - r_{A1} - \ldots - r_{A\ell-1} \end{array}$$

Algorisme recuperador: si $A \in \Gamma_0$
$k = \sum_{p_i \in A} s_{Ai}$

Aquest esquema per a compartir secrets va ser proposat per Ito, Saito i Nishizeki [44] en forma d'un circuit que reconeix quan un subconjunt és autoritzat. A partir de la col·lecció de minimals Γ_0 i del conjunt de participants $P = \{p_1, \ldots, p_n\}$ es pot construir el circuit que vé donat per la fórmula booleana:

$$\widetilde{\Gamma_0}(p_1, \ldots, p_n) = \bigvee_{A \in \Gamma_0} \Big(\bigwedge_{p_i \in A} p_i \Big)$$

fent l'abús de llenguatge d'escriure amb el mateix símbol el participant p_i i l'entrada i-èssima de la fórmula. Es verifica que $A \in \Gamma$ si i només si $\widetilde{\Gamma_0}(p_1, \ldots, p_n) = 1$ quan es dóna el valor $p_i = 1$ si $p_i \in A$ i $p_i = 0$ si $p_i \notin A$. Per exemple l'estructura de minimals $\Gamma_0 = \{\{p_1, p_2\}, \{p_1, p_3, p_4\}, \{p_2, p_3, p_4\}\}$ té associada la fórmula $\widetilde{\Gamma_0}(p_1, p_2, p_3, p_4) = (p_1 \wedge p_2) \vee (p_1 \wedge p_3 \wedge p_4) \vee (p_2 \wedge p_3 \wedge p_4)$. A la Figura 2.3 es pot observar el circuit representat amb les portes *and* i *or*

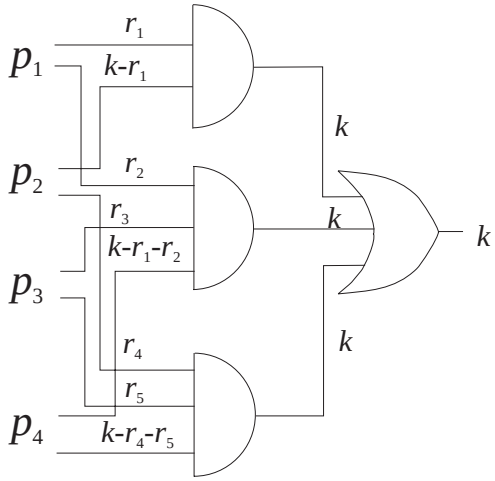

Figura 1.3: Circuit associat a la forma normal conjuntiva per l'estructura $\Gamma_0 = \{\{p_1, p_2\}, \{p_1, p_3, p_4\}, \{p_2, p_3, p_4\}\}$

corresponents, així com els fragments que s'assignen quan un secret $k \in \mathcal{K}$ es reparteix.

S'observa que la manera de calcular els fragments en el circuit és la següent: s'assigna el secret k a la línia de sortida i es va fent una construcció cap endarrera fent servir les regles:

- Per a cada porta *or* es posa el mateix a la seva sortida que a les seves entrades.
- En una porta *and* a partir de la seva sortida k' es construeixen les seves ℓ entrades a partir de $\ell - 1$ nombres aleatoris $r_1, \ldots, r_{\ell-1}$ de $\mathbb{Z}_m$ i la darrera entrada és $k' - r_1 - \ldots, r_{\ell-1}$.

Pel nostre exemple cada participant rep:

- $p_1 \longmapsto (r_1, r_2)$
- $p_2 \longmapsto (k - r_1, r_4)$
- $p_3 \longmapsto (r_3, r_5)$
- $p_4 \longmapsto (k - r_2 - r_3, k - r_4 - r_5)$

És molt fàcil comprovar que cada subconjunt de participants autoritzat pot recuperar el secret, simplement sumant part dels seus fragments. Per exemple

els participants de $\{p_1, p_3, p_4\}$ tenen entre els seus fragments r_2, r_3, i $k - r_2 - r_3$, amb els quals poden determinar el secret. Per veure que tot subconjunt no autoritzat no pot obtenir cap informació sobre el valor del secret, només cal veure-ho pels no autoritzats maximals: $\{\{p_1, p_3\}, \{p_1, p_4\}, \{p_3, p_4\}, \{p_2, p_3\}, \{p_2, p_4\}\}$. Per exemple $\{p_3, p_4\}$ no pot obtenir cap informació sobre el valor del secret ja que a partir dels seus fragments només pot calcular $r_3, r_5, k - r_2, k - r_4$ i pel caràcter aleatori dels nombres r_2 i r_4 qualsevol secret és possible.

De fet la proposta inicial que Ito, Saito i Nishizeki van fer a [44] utilitzava la mateixa fórmula $\widetilde{\Gamma_0}$ però expressada en forma normal conjuntiva. Pel nostre cas s'obté $\widetilde{\Gamma_0}(p_1, p_2, p_3, p_4) = (p_1 \vee p_2) \wedge (p_1 \vee p_3) \wedge (p_1 \vee p_4) \wedge (p_2 \vee p_3) \wedge (p_2 \vee p_4)$ i el circuit és el de la Figura 2.4 de forma que els fragments repartits són

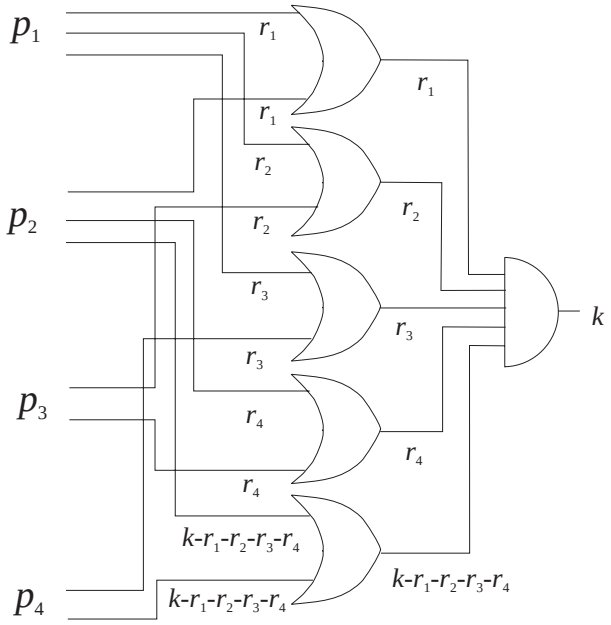

Figura 1.4: Circuit associat a la forma normal disjuntiva per l'estructura $\Gamma_0 = \{\{p_1, p_2\}, \{p_1, p_3, p_4\}, \{p_2, p_3, p_4\}\}$

- $p_1 \longmapsto (r_1, r_2, r_3)$
- $p_2 \longmapsto (r_1, r_4, k - r_1 - r_2 - r_3 - r_4)$
- $p_3 \longmapsto (r_2, r_4)$
- $p_4 \longmapsto (r_3, k - r_1 - r_2 - r_3 - r_4)$

El darrer exemple que presentem és degut a Salomaa [79]. Es tracta d'un esquema que se surt bastant del tipus d'esquemes als quals es refereix la present tesi, ja que realitza una (t, n)-estructura d'accés de forma no perfecte. Siguin $m_1, \ldots, m_n$ nombres enters no nuls primers dos a dos. Anomenem $\min(t)$ al producte dels t nombres més petits d'entre els $m_1, \ldots, m_t$. Denotarem per $\max(t-1)$ el producte dels $t-1$ nombres més grans. Escollim els valors $m_1, \ldots, m_n$ de forma que $\min(t) - \max(t-1) \geq 3\max(t-1)$. Aquests valors es fan públics. El conjunt de secrets és $\mathcal{K} = \{\max(t-1)+1, \max(t-1)+2, \ldots, \min(t)-1\}$ pel qual es defineix l'esquema

Esquema de Salomaa
Algorisme distribuïdor: sigui
$k \in \mathcal{K} = \{\max(t-1)+1, \max(t-1)+2, \ldots, \min(t)-1\}$
$p_1 \longmapsto s_1 = k \bmod m_1$
$\ldots$
$p_n \longmapsto s_n = k \bmod m_n$
Algorisme recuperador:
A partir dels fragments $s_{i_1}, \ldots, s_{i_t}$,
es resol el sistema d'equacions

$$\left.\begin{array}{l} x \equiv s_{i_1} \bmod m_{i_1} \\ \ldots \\ x \equiv s_{i_t} \bmod m_{i_t} \end{array}\right\}$$

Pel teorema xinès del residus sabem que quan s'ajunten t participants a partir dels seus fragments $s_{i_1}, \ldots, s_{i_t}$ s'obté una solució $x = k' \bmod m_{i_1} \ldots m_{i_t}$ del sistema

$$\left.\begin{array}{l} x \equiv s_{i_1} \bmod m_{i_1} \\ \ldots \\ x \equiv s_{i_t} \bmod m_{i_t} \end{array}\right\}$$

amb $0 \leq k' < m_{i_1} \ldots m_{i_t}$. Aquesta solució verifica que $k' \equiv k \bmod m_{i_1}, \ldots, k' \equiv k \bmod m_{i_t}$ però $0 \leq k, k' < m_{i_1} \ldots m_{i_t}$, per tant $k = k'$. És a dir, aquest esquema realitza la (t, n)-estructura de llindar. Ara bé, si $t-1$ participants ajunten els seus fragments, s'obté una solució $x = k' \bmod m_{i_1} \ldots m_{i_{t-1}}$ del sistema corresponent, obtenint com a possibles valors x en el conjunt $\mathcal{K} = \{\max(t-1)+1, \max(t-1)+2, \ldots, \min(t)-1\}$ els $x = k' + \lambda m_{i_1} \ldots m_{i_{t-1}}$ per valors de λ que facin que $x \in \mathcal{K}$. En total són la part entera de:

$$\frac{\min(t) - \max(t-1) - 1}{m_{i_1} \ldots m_{i_{t-1}}}$$

Com que hem escollit els valors $m_1, \ldots, m_n$ de tal manera que fos $\min(t) - \max(t-1) \geq 3\max(t-1)$, el valor del secret queda indeterminat per a aquest conjunt de $t-1$ participants. De tota manera aquest esquema no és perfecte ja que un conjunt de $t-1$ participants no pot saber quin és el secret, però sí obtenir certa informació sobre el valor possible del secret.

1.3 Taxa d'informació

L'eficiència d'un esquema per a compartir secrets es pot mesurar avaluant diversos paràmetres. El principal d'aquests és la quantitat d'informació que un participant ha de mantenir en secret. Aquesta vessant es mesura amb la taxa d'informació en les seves diferents modalitats.

Hem designat per $\mathcal{S}_i$ el conjunt de fragments que un participant $p_i \in P = \{p_1, \ldots, p_n\}$ pot rebre en repartir-se un secret $k \in \mathcal{K}$ fent servir un esquema per a compartir secrets Σ. Ara tractarem de mesurar l'"economicitat" de l'esquema Σ, en quant a la quantitat d'informació que ha de rebre cada participant. El conjunt $\mathcal{K}$ dels possibles secrets i els conjunts $\mathcal{S}_i$ dels possibles fragments del participant p_i es poden representar mitjançant una tira de bits de longitud $\log_2 |\mathcal{K}|$ i $\log_2 |\mathcal{S}_i|$, respectivament. Així per a avaluar la proporció de bits que s'han de donar al participant p_i perquè junt amb d'altres recuperi $\log_2 |\mathcal{K}|$ bits de secret és:

$$\rho_i(\Sigma, \Gamma, \mathcal{K}) = \frac{\log_2 |\mathcal{K}|}{\log_2 |\mathcal{S}_i|}$$

anomenada *taxa d'informació del participant* p_i per l'esquema Σ. Pel que fa a tot l'esquema es defineix la *taxa d'informació de l'esquema* com a:

$$\rho(\Sigma, \Gamma, \mathcal{K}) = \min\{\rho_i \mid i = 1, \ldots, n\}$$

que de fet mesura la taxa del participant que necessita més informació per a poder accedir al secret, és a dir, el cas pitjor. Aquests paràmetres van ser proposats per primera vegada per Brickell i Stinson a [27]. Es fa servir el terme taxa d'informació per la semblança amb la taxa d'informació d'un codi corrector d'errors. També s'escriuen com a ρ_i i ρ quan no hi ha ambigüitat sobre quin esquema i quin conjunt de secrets estem considerant.

Per tant, el primer paràmetre indica la quantitat de bits que ha de guardar en secret el participant per tal de recuperar un bit de secret. El segon paràmetre indica quina és aquesta quantitat en el pitjor dels casos. Els inversos d'aquests pàrametres també tenen el seu significat. Per exemple $1/\rho_i$ representa el número de bits del secret que es recuperen per cada bit de fragment.

Hem de tenir present que la seguretat d'un sistema criptogràfic disminueix quan la quantitat d'informació que s'ha de mantenir en secret augmenta. També hem de tenir en compte que quan més petits siguin els fragments lliurats als participants més manipulables seran aquests. S'han proposat variants d'aquesta definició [45] com és la de considerar el vector dels inversos de les raons $convec(\Sigma) = (1/\rho_1, \ldots, 1/\rho_n)$ anomenat *vector de contribució*.

Un altre dels paràmetre associats a un esquema per a compartir secrets és la *taxa mitjana d'informació* definida com la mitjana harmònica de les taxes dels participants

$$\tilde{\rho}(\Sigma, \Gamma, \mathcal{K}) = \frac{|P|}{\sum_{p_i \in P} \frac{1}{\rho_i(\Sigma, \Gamma, \mathcal{K})}}$$

que correspon a la idea intuïtiva de calcular en mitjana quina és la taxa dels participants, perquè

$$\tilde{\rho}(\Sigma, \Gamma, \mathcal{K}) = \frac{\log_2 |\mathcal{K}|}{\sum_{p_i \in P} \frac{\log_2 |\mathcal{S}_i|}{|P|}}$$

Aquest concepte va ser proposat simultàniament per Blundo [13] i per Martin [59]. Com en els anteriors paràmetres obviarem l'esquema, l'estructura i el conjunt de claus, escrivint només $\tilde{\rho}$ quan no hi hagi cap problema de confusió.

Trivialment es verifica que $0 \leq \rho \leq \tilde{\rho}$. A més a més aquests indicadors són menors o iguals que 1. En efecte, sigui $p_i \in P$, i suposem que existeix un $A \in \Gamma_0$ tal que $p_i \in A$. Posem $A' = A - \{p_i\} \notin \Gamma$ per ser A minimal. Si Σ és un esquema perfecte, llavors a partir dels fragments de que disposen els participants de A' no poden obtenir cap informació sobre el valor del secret. És a dir, que tot secret és possible amb els fragments dels quals disposen. Per tant, per a cada secret $k \in \mathcal{K}$ hi ha una repartició de fragments en A que coincideix amb la que tenen els participants de A'. Ara bé, si $k \neq k'$ llavors el fragment que rep p_i ha de ser també diferent, perquè si no tindríem $k = k'$ per ser $A \in \Gamma$. D'aquí podem deduir que $|\mathcal{S}_i| \geq |\mathcal{K}|$ i per tant l'afirmació. Resumint tenim que

$$0 \leq \rho \leq 1$$

També es verifica que $\rho = 1$ si i només si $\tilde{\rho} = 1$.

La millor situació és quan $\rho = 1$, en el qual cas es diu que l'*esquema és ideal*. Evidentment serà desitjable implementar un esquema amb ρ alta, ja que així donarem relativament poca informació a cada participant, obtenint una major eficiència.

Aquest dos paràmetres també es poden definir mitjançant el concepte d'entropia com es detallarà a la Secció 2.8. De tota manera la definició que s'ha fet aquí és sota la hipòtesi que el secret està uniformement escollit dins

de $\mathcal{K}$. Pel cas que no se suposi això caldrà recòrrer a la definició més general de la Secció 2.8. La particularització d'aquestes definicions més generals dóna com a resultat les definicions que acabem de fer.

Quan per una estructura d'accés existeix un esquema ideal que la realitza, es diu que és una *estructura ideal*. Per a una estructura d'accés poden haver esquemes que la realitzen amb una taxa d'informació més alta que d'altres. Per exemple per l'estructura $\Gamma_0 = \{\{p_1, p_2\}, \{p_1, p_3, p_4\}, \{p_2, p_3, p_4\}\}$ s'han trobat dos esquemes donats pels circuits de les Figures 2.3 i 2.4 que porten a taxes d'informació $\rho_1 = 1/2$, $\rho_2 = 1/2$, $\rho_3 = 1/2$, $\rho_4 = 1/2$ de forma que pel primer esquema tenim $\rho = 1/2$, i pel segon esquema tenim $\rho = 1/3$ ja que $\rho_1 = 1/3$,$\rho_2 = 1/3$, $\rho_3 = 1/2$, $\rho_4 = 1/2$. Aquest fenòmen ens porta a definir ρ^*, la *taxa d'informació òptima*, com el suprem de les taxes d'informació d'entre tots els possibles esquemes que realitzin Γ i entre tots els conjunts possibles de secrets $\mathcal{K}$ amb $|\mathcal{K}| \geq 2$, això és

$$\rho^*(\Gamma) = \sup_{\Sigma,\mathcal{K}} \rho(\Sigma, \Gamma, \mathcal{K})$$

Per a les taxes mitjanes d'un esquema es defineix la *taxa mitjana d'informació òptima* com

$$\tilde{\rho}^*(\Gamma) = \sup_{\Sigma,\mathcal{K}} \tilde{\rho}(\Sigma)$$

De la mateixa manera que les anteriors taxes, obviarem l'estructura d'accés si no hi ha cap ambigüitat. Aquests nous paràmetres verifiquen $0 \leq \rho^* \leq \tilde{\rho}^* \leq 1$. A més també es verifica que $\rho^* = 1$ si i només si $\tilde{\rho}^* = 1$.

1.4 Esquema d'espai vectorial

La *construcció d'espai vectorial* és un mètode util per a construir esquemes ideals que va ser introduïda per Brickell [24]. Sigui Γ una estructura d'accés en P i $D \notin P$ el distribuïdor. Es diu que Γ és una *estructura d'accés d'espai vectorial* si, per algun espai vectorial $E = GF(q)^r$ sobre un cos finit $GF(q)$, existeix una funció

$$\psi : P \cup \{D\} \longrightarrow E$$

tal que $A \in \Gamma$ si i només si el vector $\psi(D)$ pot ser expressat com a combinació lineal dels vectors del conjunt $\psi(A) = \{\psi(p) \,|\, p \in A\}$. Si Γ és una estructura d'accés d'espai vectorial d'aquest tipus, podem construir un esquema per a compartir secrets per Γ amb conjunt de secrets $\mathcal{K} = GF(q)$:

Esquema d'espai vectorial de Brickell
Algorisme distribuïdor: sigui un secret $k \in \mathcal{K} = GF(q)$.
El distribuïdor agafa aleatòriament un element $\mathbf{v} \in E$, tal que $\mathbf{v} \cdot \psi(D) = k$.
$p_i \longmapsto s_i = \mathbf{v} \cdot \psi(p_i)$
Algorisme recuperador: per un subconjunt autoritzat $A = \{p_1, \ldots, p_\ell\} \in \Gamma$ s'expressa $\psi(D) = \lambda_1\psi(p_1) + \lambda_2\psi(p_2) + \ldots + \lambda_\ell\psi(p_\ell)$ i d'aquí s'obté: $k = \lambda_1 s_1 + \lambda_2 s_2 + \ldots + \lambda_\ell s_\ell$

Cal remarcar que el producte entre vectors és el producte component a component i que $\psi(D) \neq 0$, cas que correspon a $\Gamma \neq 2^P$. Aquest càlcul del secret és correcte perquè $k = \mathbf{v}\cdot\psi(D) = \mathbf{v}\cdot(\lambda_1\psi(p_1)+\lambda_2\psi(p_2)+\ldots+\lambda_\ell\psi(p_\ell)) = \lambda_1 s_1 + \lambda_2 s_2 + \ldots + \lambda_\ell s_\ell$. La funció ψ és una funció pública, és a dir, a la qual pot accedir tothom.

L'esquema construït d'aquesta manera s'anomena un *esquema per a compartir secrets d'espai vectorial*. Aquest és un esquema per a compartir secrets perfecte (veure [24] o [93] per demostracions). L'esquema polinomial de Shamir [83] pot ser vist com a un esquema per a compartir secrets d'espai vectorial [93] amb l'aplicació ψ definida per $\psi(D) = (1, 0, 0, \ldots, 0)$ i $\psi(p_i) = (1, x_i, x_i^2, \ldots, x_i^{r-1})$ fixant per a cada participant un valor diferent x_i no nul. D'aquesta forma es generen els mateixos fragments que amb l'esquema polinomial de Shamir.

Les estructures d'espai vectorial admeten una generalització. Aquesta generalització consisteix en associar un subespai en lloc d'un vector, per cada participant i pel distribuïdor. Sigui el conjunt de secrets $\mathcal{K} = GF(q)$ un cos finit i $E = (GF(q))^r$ un espai vectorial sobre aquest cos. Sigui una aplicació

$$\psi : P \cup \{D\} \longrightarrow \mathsf{S}(E)$$

amb $\mathsf{S}(E)$ el conjunt dels subespais vectorials de E, tal que per a tot $A \subset P$ o bé $\psi(D) \subset \langle \bigcup_{p\in A} \psi(p) \rangle$ o bé $\psi(D) \cap \langle \bigcup_{p\in A} \psi(p) \rangle = \{0\}$. Un cas en el que es verifica trivialment aquesta condició és quan la dimensió de la imatge del distribuïdor és 1. Definirem l'estructura d'espai vectorial generalitzat a partir de ψ de la manera següent: un subconjunt A és autoritzat si i només si el subespai $\psi(D) \subset \langle \bigcup_{p\in A} \psi(p) \rangle$. Una estructura definida d'aquesta manera per a una certa funció ψ se l'anomena *estructura d'espai vectorial generalitzada*. Aquest tipus d'estructura d'accés és una generalització de les estructures

d'espai vectorial. L'esquema que proposem tot seguit és una generalització de l'esquema d'espai vectorial proposada per Jackson i Martin a [45] . Fixem una base $\mathbf{v}_{p1}, \ldots, \mathbf{v}_{pr_p}$ de $\psi(p)$ per $p \in P$ i amb $\dim \psi(p) = r_p$. També fixem una base $\mathbf{v}_{D1}, \ldots, \mathbf{v}_{Dr_D}$ de $\psi(D)$, amb $\dim \psi(D) = r_D$. L'esquema es pot definir així:

Esquema d'espai vectorial generalitzat
Algorisme distribuïdor: sigui un secret
$\mathbf{k} = (k_1, \ldots, k_{r_D}) \in \mathcal{K} = GF(q)^{r_D}$.
El distribuïdor agafa aleatòriament un vector
$\mathbf{v} \in E$, tal que $\mathbf{v} \cdot \mathbf{v}_{Di} = k_i$.
Sigui $\mathbf{v}_{p1}, \ldots, \mathbf{v}_{pr_p}$
la base fixada per a cada $p \in P$.
Repartim:
$p \longmapsto s_{p1} = \mathbf{v} \cdot \mathbf{v}_{p1}, \ldots, s_{pr_p} = \mathbf{v} \cdot \mathbf{v}_{pr_p}$
Algorisme recuperador: per un subconjunt
autoritzat $A = \{p_1, \ldots, p_\ell\} \in \Gamma$ s'expressa cada
$\mathbf{v}_{Di} = \sum \lambda_j^{(i)} \mathbf{v}_{pj}$ i d'aquí s'obté:
$k = (\sum \lambda_j^{(1)} s_{pj}, \ldots, \sum \lambda_j^{(r_D)} s_{pj})$

Igual que en el cas de l'esquema d'espai vectorial usual, el càlcul del secret que ha fet la caixa negra (o els participants que ajunten els seus fragments) és correcte perquè $k_i = \mathbf{v} \cdot \mathbf{v}_{Di} = \mathbf{v} \cdot \sum \lambda_j^{(i)} \mathbf{v}_{pj} = \sum \lambda_j^{(i)} \mathbf{v} \cdot \mathbf{v}_{pj} = \sum \lambda_j^{(i)} s_{pj}$. Recordem que la funció ψ és pública.

Simultàniament al treball de Shamir de l'any 1979, Blakley [11] proposa un esquema per una (t, n)-estructura de llindar de caire geomètric. Més tard Simmons [89, 90, 91] va generalitzar aquesta construcció a l'esquema que anomenem *esquema geomètric*. Aquest esquema realitza les mateixes estructures que les d'espai vectorial. Les estructures geomètriques generalitzades es poden definir amb la mateixa idea que s'ha fet amb les estructures d'espai vectorial generalitzat [46], realitzant d'aquesta manera les estructures d'espai vectorial generalitzat.

Seguidament farem una descripció del concepte d'estructura dual i de la seva utilització per definir una estructura qualsevol com a estructura d'espai vectorial generalitzat. L'estructura dual associada a una estructura d'accés té els seus antecedents a l'esquema circuital de M. Ito, A. Saito i T. Nishizeki [44] i

més tard va ser tractada per G.J. Simmons, W.A. Jackson i K.M. Martin a [91].

Recordem primer l'esquema circuital, el qual va ser el primer esquema per a compartir secrets proposat per a una estructura d'accés qualsevol i en el que està inspirat el concepte d'estructura dual.

Per tal de definir l'estructura dual, en tot el raonament que segueix prescindirem dels participants que no intervenen en cap subconjunt minimal autoritzat, ja que són redundants. Per tant suposarem que es tracta d'una estructura connectada. L'expressió de l'estructura Γ com a fórmula booleana es pot detallar de la manera següent: suposem que $\Gamma_0 = \{C_1, \ldots, C_c\}$ i considerem per a cada subconjunt C_i una fórmula booleana $\tilde{C}_i$ formada per la juxtaposició dels seus participants considerats com a variables booleanes. D'aquesta manera si es forma la conjunció d'aquestes expressions booleanes obtenim $\tilde{\Gamma}_0 = \tilde{C}_1 + \ldots + \tilde{C}_c$ fórmula que verifica que $A \in \Gamma$ si i només si $\tilde{\Gamma}_0$ és certa quan les variables que intervenen en A valen 1 (*cert*). Tota fórmula booleana defineix també una estructura d'accés amb conjunt de participants igual al conjunt de variables.

A partir de la doble expressió d'una fórmula booleana en forma normal conjuntiva i en forma normal disjuntiva es defineix per a una estructura d'accés Γ l'*estructura dual* Γ^* com aquella determinada pel resultat d'intercanviar "+" i "·" a la fórmula $\tilde{\Gamma}$. Quan el resultat de fer el dual és la mateixa estructura, es diu que l'estructura és *autodual*.

G.J. Simmons, W.A. Jackson i K.M. Martin fan notar a [91] que $(\Gamma^*)^* = \Gamma$ i troben que una de les propietats més importants de l'estructura dual és la següent:

Proposició 1.4.1 [91] *Sigui Γ una estructura monòtona d'accés i considerem Γ_0, Γ_0^* la col·lecció de subconjunts minimals de Γ i de Γ^*, respectivament, així com Γ_M la col·lecció de subconjunts no autoritzats maximals de Γ. Aleshores es verifica que*

$$\Gamma_0^* = \{P - A | A \in \Gamma_M\}$$

Una altra de les propietats importants que W.A. Jackson i K. Martin han provat que verifiquen les estructures duals és que si una estructura d'espai vectorial generalitzat té una certa taxa d'informació aleshores la dual també per a una certa definició de l'estructura com a estructura d'espai vectorial generalitzat:

Proposició 1.4.2 [45] *Sigui Γ una estructura d'accés d'espai vectorial generalitzat. Suposem que aquesta estructura té una taxa d'informació ρ i una taxa d'informació mitjana $\tilde{\rho}$ amb l'esquema usual associat a l'estructura d'espai*

vectorial generalitzat. En aquestes condicions podem assegurar que existeix un esquema d'espai vectorial generalitzat que defineix Γ^* *amb taxa d'informació* ρ *i una taxa d'informació mitjana* $\tilde{\rho}$*.*

La construcció de l'estructura dual ens dóna un mecanisme per expressar qualsevol estructura d'accés com a una estructura d'espai vectorial generalitzada definida per una aplicació ψ amb $\dim \psi(D) = 1$ [91].

Aquest procediment es pot sintetitzar en l'algorisme següent. Per Γ calculem Γ_0^* que suposarem que és $\Gamma_0^* = \{S_1, \ldots, S_s\}$. A partir d'aquesta nova estructura definim l'*aplicació cumulativa* $\alpha : P \longrightarrow 2^{\{1,\ldots,s\}}$ definida per $p \in P$ com $\alpha(p) = \{i | p \in S_i\}$. Aquesta aplicació verifica que [91]:

$$A \in \Gamma \text{ si i només si } \bigcup_{p \in A} \alpha(p) = \{1, \ldots, s\}$$

Podem escollir $s+1$ vectors $D_1, \ldots, D_s, W \in GF(q)^s$ de manera que agafats de s en s siguin linealment independents. Amb aquests vectors definirem Γ com a una estructura d'espai vectorial generalitzat mitjançant l'aplicació

$$\psi : P \cup \{D\} \longrightarrow \mathsf{S}(GF(q)^s)$$

definida per $\psi(p) = \langle \{D_i | i \in \alpha(p)\} \rangle$ i amb $\psi(D) = \langle W \rangle$. Es pot demostrar [91] que Γ ve definida com a estructura d'espai vectorial generalitzat a partir de ψ. Cal fer notar que $\dim \psi(D) = 1$. D'aquesta forma tenim que,

Proposició 1.4.3 [91] *Tota estructura d'accés és una estructura d'accés d'espai vectorial generalitzat amb dimensió de la imatge del distribuïdor igual a 1.*

L'expressió d'una estructura qualsevol com a una estructura d'espai vectorial generalitzada fent ús del dual, no dóna en general una taxa d'informació molt bona. Una altra via per a obtenir una expressió és l'ús de recobriments d'estructures d'espai vectorial clàssiques que formen una 1-descomposició.

Ja hem comentat que la construcció d'una 1-descomposició (Corol·lari 3.1 de [95]) consisteix en repartir el secret segons cadascun dels esquemes que coneixem per a cada subestructura d'accés. En el cas particular que l'esquema associat a cada subestructura sigui un esquema d'espai vectorial clàssic, la construcció de la 1-descomposició és un esquema d'espai vectorial generalitzat amb dimensió de la imatge del distribuïdor igual a 1.

Proposició 1.4.4 *Sigui* $\Gamma_1, \ldots, \Gamma_n$ *estructures d'espai vectorial que formen una* 1*-descomposició de* $\Gamma = \Gamma_1 \cup \ldots \cup \Gamma_n$ *amb* $P_h = P(\Gamma_h)$ *per a tota* $h =$

$1, \ldots, n$. *Aleshores existeix un esquema d'espai vectorial generalitzat per* Γ *amb dimensió de la imatge del distribuïdor igual a* 1, *taxa d'informació*

$$\rho = \min_{p \in P} \frac{1}{|\{h : p \in P_h\}|}$$

i taxa mitjana d'informació

$$\tilde{\rho} = \frac{|P|}{\sum_{h=1}^{n} |P_h|}$$

Demostració: Aplicant el Corol·lari 3.1 de [95] (Corol·lari 2.7.1) en aquest cas particular obtenim un esquema per a compartir secrets que realitza Γ. Falta veure que efectivament la repartició de fragments de la construcció de la 1-descomposició coincideix amb la d'un esquema d'espai vectorial generalitzat que defineix Γ. Veiem que Γ és una estructura d'espai vectorial generalitzat i que l'esquema coincideix amb el de la 1-descomposició. Suposem que cada Γ_i està definida com a estructura d'espai vectorial per $\psi_i : P \cup \{D\} \longrightarrow E_i$ amb $E_i = (GF(q))^{d_i}$. Aplicant un automorfisme de E_i, podem suposar que per a tota $i = 1, \ldots, n$ tenim $\psi_i(D) = (1, 0, \ldots, 0)$. Sigui l'espai vectorial $E = (GF(q))^d$ amb $d = d_1 + \ldots + d_n - n + 1$ i els monomorfismes

$$i_k : E_k \longrightarrow E$$

amb $i_k(x_1, \ldots, x_{d_k}) = (x_1, 0, \ldots, 0, x_2, \ldots, x_{d_k}, 0, \ldots, 0)$, col·locant la component x_2 en el lloc $d_1 + \ldots + d_{k-1} - k + 3$. Definim $\psi : P \cup \{D\} \longrightarrow \mathsf{S}(E)$ amb $\mathsf{S}(E)$ el conjunt dels subespais vectorials de E per

$$\psi(p) = \langle \{ i_k(\psi_k(p)) | p \in P_k \} \rangle$$

i $\psi(D) = \langle (1, 0, \ldots, 0) \rangle$. S'observa que $\psi(D) = \langle i_k(\psi_k(D)) \rangle$ per a tota $k = 1, \ldots, n$. Raonem ara que ψ defineix $\Gamma_1 \cup \ldots \cup \Gamma_n$.

Si $A \in \Gamma_k$ per a certa k llavors $\psi_k(D) = \sum_{p \in A} \lambda_p \psi_k(p)$ per certs valors de λ_p amb $p \in A$. D'aquí aplicant el monomorfisme i_k obtenim $i_k(\psi_k(D)) = \sum_{p \in A} \lambda_p i_k(\psi_k(p))$ com volíem veure.

D'altra banda si per cert conjunt $A \subset P$ tenim que $\psi(D) \subset \langle \sum_{p \in A} \lambda_p^1 i_1(\psi_1(p)) + \ldots + \sum_{p \in A} \lambda_p^n i_n(\psi_n(p)) \rangle$, llavors dient $u_k = \sum_{p \in A} \lambda_p^k i_k(\psi_k(p))$ tenim que $u_k = (\alpha_1^k, 0, \ldots, 0, \alpha_2^k, \ldots, \alpha_{d_k}^k, 0, \ldots, 0)$ i com que $\psi(D) = \langle (1, 0, \ldots, 0) \rangle$ llavors $\alpha_2^k = \ldots = \alpha_{d_k}^k = 0$ per $k = 1, \ldots, n$. Ara bé, $\alpha_1^k \neq 0$ per alguna k i llavors $(1, 0, \ldots, 0) = \lambda u_k$ per certa $\lambda \in GF(q)$. Com que i_k és injectiva i $i_k(\psi_k(D)) = i_k(\sum_{p \in A} \lambda \lambda_p^k \psi_k(p))$ obtenim $\psi_k(D) = \sum_{p \in A} \lambda \lambda_p^k \psi_k(p)$, és a dir $A \in \Gamma_k$ per cert k.

S'observa que els fragments que es reparteixen amb l'esquema d'espai vectorial generalitzat associat a ψ coincideixen amb els que proporciona la construcció de la 1-descomposició. □

1.5 Model general de les regles de distribució

Un dels models matemàtics més generals per expressar un esquema per a compartir secrets és el de les regles de distribució. Hem d'aclarir que aquest no és un nou esquema per a compartir secrets, si no que es tracta d'un model sota la perspectiva del qual es pot veure qualsevol esquema per a compartir secrets. Aquest model pot semblar una bona via per implementar un esquema per a compartir secrets, però no és eficient a la pràctica atès que fa servir molta memòria.

Donat un conjunt de secrets $\mathcal{K}$ i un conjunt de fragments $\mathcal{S}$, anomenarem *regla de distribució* a una funció

$$f : P \cup \{D\} \longrightarrow \mathcal{K} \cup \mathcal{S}$$

de forma que $f(D) \in \mathcal{K}$ i $f(p) \in \mathcal{S}$ per a tot $p \in P$. Aquesta funció representa la idea d'una possible distribució del secret $f(D)$ en porcions $f(p)$ para cada participant $p \in P$. Donat un conjunt $\mathcal{F}$ de regles de distribució i fixada una clau secreta $k \in \mathcal{K}$, totes les maneres possibles de distribuir k amb aquestes regles de distribució queden determinades pel subconjunt de regles de distribució:

$$\mathcal{F}_k = \{f \mid f(D) = k\}$$

Els algorismes de distribució i de recuperació se sintetitzen en el quadre:

Esquema de les regles de distribució
Algorisme distribuïdor: sigui un secret $k \in \mathcal{K}$.
El distribuïdor agafa aleatòriament una regla $f \in \mathcal{F}_k$
i assigna a cada participant
$p_i \longmapsto s_i = f(p_i)$
Algorisme recuperador: a partir dels fragments
s_i dels participants d'un subconjunt autoritzat,
es determina una
$f \in \mathcal{F}$
tal que $f(p_i) = s_i$ i d'aquí s'obté:
$k = f(D)$

Fem notar que $\mathcal{F}$ és un conjunt públic.

Veiem un exemple de conjunt de regles de distribució per a l'estructura d'accés $\Gamma_0 = \{\{p_1, p_2, p_3\}, \{p_2, p_4\}\}$ en el conjunt $P = \{p_1, p_2, p_3, p_4\}$:

	D	p_1	p_2	p_3	p_4
f_1	1	1	1	1	1
f_2	1	2	1	2	4
f_3	1	1	2	2	2
f_4	1	2	2	1	3
f_5	2	1	1	2	2
f_6	2	2	1	1	3
f_7	2	1	2	1	1
f_8	2	2	2	2	4

amb $\mathcal{K} = \{1, 2\}$ i $\mathcal{S} = \{1, 2, 3, 4\}$. Així si el distribuïdor vol repartir el secret $k = 1$, escull una regla de distribució a l'atzar que tingui $f(D) = 1$, i assigna a cada participant p_i el fragment $f(p_i)$. Per exemple pot fer servir la regla f_3 i assignar en privat $s_1 = 1$, $s_2 = 2$, $s_3 = 2$, $s_4 = 2$. Si els participants p_1 , p_2, p_3 ajunten els seus fragments, buscaran la distribució que coincideixi amb aquests valors (en aquest cas només f_3) i obtindran el secret $k = 1$ mirant el valor $f_3(D)$. El mateix passarà si s'ajunten els participants p_2, p_4.

En general ens podem trobar amb el problema que a partir dels fragments d'una sèrie de participants, hi hagi més d'una regla de distribució per aquests fragments. En aquest punt és important demanar que les regles de distribució sempre portin al mateix secret si el conjunt de participants és autoritzat. D'altra banda voldrem també que surtin tots els possibles secrets amb la mateixa freqüència, si el conjunt de participants no és autoritzat. Aquestes dues exigències es resumeixen en:

1. si $A \in \Gamma$ i $f, g \in \mathcal{F}$ qualssevol tals que $f(p) = g(p)$ per a tot $p \in A$ llavors $f(D) = g(D)$

2. si $A \notin \Gamma$ i $\varphi : A \longrightarrow \mathcal{S}$ és una assignació qualsevol de fragments als elements de A, llavors existeix un natural $\lambda(\varphi, A) > 0$, tal que per a tota $k \in \mathcal{K}$:

$$|\{f \in \mathcal{F}_k : f(p) = \varphi(p), \quad \text{per a tot } p \in A\}| = \lambda(\varphi, A)$$

independentment del valor de k.

D'aquesta manera, el requeriment 1) fa que tot subconjunt autoritzat pugui recuperar la clau secreta a partir del coneixement de $\mathcal{F}$. El requeriment 2) fa que tot subconjunt no autoritzat vegi tots els secrets amb la mateixa probabilitat. Els participants d'un subconjunt no autoritzat poden consultar $\mathcal{F}$ per tal de buscar les regles de distribució que concorden amb els seus fragments. De totes aquestes regles de distribució n'hi ha exactament λ que porten a cada secret $k \in \mathcal{K}$, per la qual cosa tots els secrets són igualment probables per ells. Quan aquestes dues condicions es verifiquen, es pot provar que l'esquema definit per les regles de distribució és un esquema perfecte [27].

A l'exemple de les regles de distribució per l'estructura $\Gamma_0 = \{\{p_1, p_2, p_3\}, \{p_2, p_4\}\}$ s'observa que a partir dels fragments d'un subconjunt autoritzat sempre hi ha una regla de distribució coincident amb aquests fragments que ens porta al secret repartit. A partir d'un subconjunt no autoritzat es poden trobar regles de distribució coincidents amb els fragments, que determinen tots els secrets amb el mateix número de regles de distribució. Si s'ha fet servir la tercera regla de distribució obtenim que a partir de només $s_4 = 2$ els dos secrets són igualment possibles, com també passa pel cas de conéixer $s_2 = 2$ i $s_3 = 2$.

Sovint el conjunt de regles de distribució $\mathcal{F}$ s'escriu en forma de matriu amb les columnes indexades en el conjunt $\{D\} \cup P$. Aquesta matriu $M = \{M(r,p)\}_{p \in P \cup \{D\}, r}$ en la qual el conjunt de fragments d'informació que es poden donar a un participant $p_i \in P$ és $\mathcal{S}_i = \{M(r, p_i) \mid r \text{ fila de } M\}$. Així també el conjunt de claus és $\mathcal{K} = \{M(r, D) \mid r \text{ fila de } M\}$. A l'exemple anterior s'obté $\mathcal{S}_1 = \mathcal{S}_2 = \mathcal{S}_3 = \{1, 2\}$, $\mathcal{S}_4 = \{1, 2, 3, 4\}$ i $\mathcal{K} = \{1, 2\}$.

A tall d'exemple determinem un conjunt de regles de distribució associades a una estructura d'espai vectorial generalitzada. Donada una estructura d'espai vectorial Γ definida per $\psi : P \cup \{D\} \longrightarrow \mathsf{S}(E)$ amb $\mathsf{S}(E)$ el conjunt dels subespais de l'espai vectorial $E = GF(q)^r$ sobre el cos finit $GF(q)$, podem definir

$$\mathcal{F} = \{f_{\mathbf{a}} \mid \mathbf{a} \in E\}$$

amb $f_{\mathbf{a}}(p) = (\mathbf{a} \cdot \mathbf{v}_{p1}, \ldots, \mathbf{a} \cdot \mathbf{v}_{pr_p}) \in GF(q)^r$ si $\mathbf{v}_{p1}, \ldots, \mathbf{v}_{pr_p}$ és la base fixada pel subespai vectorial $\psi(p)$ de dimensió $r_p = \dim \psi(p)$. Pel distribuïdor tenim $f_{\mathbf{a}}(D) = (\mathbf{a} \cdot \mathbf{v}_{D1}, \ldots, \mathbf{a} \cdot \mathbf{v}_{Dr_D})$ amb $r_D = \dim \psi(D)$. El conjunt de regles realitza l'estructura Γ definida per ψ, ja que verifica les dues condicions. Veiem-ho:

1. En primer lloc si A és autoritzat llavors $\langle \psi(D) \rangle \subset \bigcup_{p \in A} \psi(p)$ aleshores

$$\mathbf{v}_{Dj} = \sum_{p \in A, i = 1, \ldots, r_p} \lambda_{pi}^{(j)} \mathbf{v}_{pi} \text{ per } j = 1, \ldots, r_D$$

però si $f_{\mathbf{a}}(p) = f_{\mathbf{a}'}(p)$ per a tot $p \in A$ llavors $\mathbf{a} \cdot \mathbf{v}_{pi} = \mathbf{a}' \cdot \mathbf{v}_{pi}$ per a tot $p \in A$ i per a tot $i = 1, \ldots, r_p$, per tant

$$\mathbf{a} \cdot \mathbf{v}_{Dj} = \sum_{p \in A, i=1,\ldots,r_p} \lambda_{pi}^{(j)} \mathbf{a} \cdot \mathbf{v}_{pi} = \sum_{p \in A, i=1,\ldots,r_p} \lambda_{pi}^{(j)} \mathbf{a}' \cdot \mathbf{v}_{pi} = \mathbf{a}' \cdot \mathbf{v}_{Dj}$$

d'aquí obtenim $f_{\mathbf{a}}(D) = f_{\mathbf{a}'}(D)$, és a dir, que el secret recuperat és el mateix.

2. En segon lloc, si A no és autoritzat llavors $\psi(D) \cap \langle \bigcup_{p \in A} \psi(p) \rangle = \{0\}$ i per tant si $\dim \langle \bigcup_{p \in A} \psi(p) \rangle = d$, llavors $d + r_D \leq r$. Sigui φ una assignació de fragments i $\mathbf{k} = (k_1, \ldots, k_{r_D}) \in GF(q)^{r_D}$ un secret per repartir amb aquestes regles de distribució. Amb la finalitat de calcular $\lambda(\varphi, A)$, ens plantejem el sistema d'equacions lineals

$$\left.\begin{array}{ll} f_{\mathbf{a}}(p) = \varphi(p), & p \in A \\ f_{\mathbf{a}}(D) = \mathbf{k} & \end{array}\right\} \Rightarrow \left.\begin{array}{ll} \mathbf{a} \cdot \mathbf{v}_{pi} = s_{pi}, & p \in A, i = 1, \ldots, r_p \\ \mathbf{a} \cdot \mathbf{v}_{Dj} = k_j, & j = 1, \ldots, r_D \end{array}\right\}$$

Aquest sistema d'equacions amb r incògnites $\mathbf{a} = (a_1, \ldots, a_r)$ té per rang $d + r_D$ i per tant el conjunt de les solucions s'obté com a una solució particular (existeix per construcció) més un subespai de dimensió $r - d - r_D$, per tant $\lambda(\varphi, A) = q^{r-d-r_D}$, quantitat independent del secret $\mathbf{k}$ escollit.

1.6 Caracterització dels esquemes ideals

La caracterització de les estructures ideals, és a dir, aquelles en les quals el conjunt de secrets i el dels fragments tenen el mateix cardinal, és un problema encara obert que ha estat estudiat per diversos autors. Destaquen els resultats de Brickell i Davenport a [25], en els quals mostren una estreta relació entre les estructures ideals i els matroides.

Sigui $\mathcal{V}$ un conjunt finit i una col·lecció de subconjunts $\mathcal{I} \subset 2^{\mathcal{V}}$. Direm que $\mathcal{M} = (\mathcal{V}, \mathcal{I})$ és un *matroide* si i només si es verifica

- $\emptyset \in \mathcal{I}$
- si $X \in \mathcal{I}$ i $Y \subset X$ aleshores $Y \in \mathcal{I}$
- si $X, Y \in \mathcal{I}$ amb $|X| = |Y| + 1$ llavors existeix un $x \in X - Y$ tal que $Y \cup \{x\} \in \mathcal{I}$

Els elements de $\mathcal{V}$ els anomenarem *punts*, els elements de $\mathcal{I}$ *subconjunts independents* i els de $2^{\mathcal{V}} - \mathcal{I}$ *subconjunts dependents*. Un minimal dels dependents (respecte la inclusió) es denomina *circuit*. Un matroide es diu *connectat* quan per tot parell de punts $x, y \in \mathcal{V}$ existeix un circuit C que els conté. Es defineix el concepte de *rang d'un matroide* com el màxim cardinal dels conjunts independents, això és, $\mathrm{r}(X) = \max\{|A| : A \subset X, A \in \mathcal{I}\}$ per $X \subset \mathcal{V}$, i pel matroide es diu $\mathrm{r}(\mathcal{M}) = \mathrm{r}(\mathcal{V})$.

Un matroide $\mathcal{M} = (\mathcal{V}, \mathcal{I})$ es diu que es *representable* sobre un cos K quan existeix una aplicació $f : \mathcal{V} \longrightarrow K^r$ per a cert r de forma que $\{x_1, \ldots, x_n\} \in \mathcal{I}$ si i només si els vectors $f(x_1), \ldots, f(x_n)$ són linealment independents a l'espai vectorial K^r.

La primera relació entre matroides i esquemes per a compartir secrets ideals és el teorema següent:

Teorema 1.6.1 [25] *Si $\mathcal{M} = (\mathcal{V}, \mathcal{I})$ és un matroide representable sobre el cos K i fixem $x \in \mathcal{V}$, aleshores existeix un esquema per a compartir secrets ideal per l'estructura d'accés ideal connectada definida per la base $\Gamma_0 = \{C - \{x\} \mid x \in C, C$ circuit de $\mathcal{M}\}$*

Teorema fàcil de justificar observant que a partir de l'aplicació $f : \mathcal{V} \longrightarrow K^r$ que sabem que existeix, podem expressar Γ_0 com a una estructura d'espai vectorial mitjançant $\psi : \mathcal{V} \cup \{D\} \longrightarrow K^r$ en el conjunt $P = \mathcal{V} - \{x\}$ i $D = x$ definint $\psi(p) = f(p)$ per a tot $p \in P \cup \{D\}$. Aquest resultat també es pot resumir dient que una condició suficient per ser estructura ideal és ser estructura d'espai vectorial. Però encara no se sap si és necessària. Per certes famílies d'estructures, com per exemple les estructures representables per un graf, se sap que és equivalent. D'altra banda tampoc s'ha trobat cap estructura ideal que no sigui d'espai vectorial.

Com hem comentat el resultat recíproc no està establert però, sí que tenim que tot esquema ideal determina un matroide connectat:

Teorema 1.6.2 [25] *Sigui $\mathcal{F}$ un conjunt de regles de distribució d'un esquema ideal per l'estructura d'accés Γ. Diem $\mathcal{V} = P \cup \{D\}$ i*

$$\mathcal{D} = \{A \subset \mathcal{V} \mid \text{ existeix } x \in A \text{ tal que si } f, g \in \mathcal{F} \text{ verifiquen}$$

$$f_{|A-\{x\}} = g_{|A-\{x\}} \text{ llavors } f(x) = g(x)\}$$

En aquestes condicions $\mathcal{D}$ és la col·lecció de subconjunts dependents d'un matroide connectat.

La idea és que els elements de $\mathcal{D}$ són tots els subconjunts $A \subset \mathcal{V}$ pels quals hi ha una certa dependència entre els valors de $f(x)$ per $x \in A$.

Una altra qüestió que es pot plantejar és si tot matroide determina un esquema per a compartir secrets ideal. La resposta és que no, ja que a [90] es mostra el matroide de Vamos que no determina un d'aquests.

Els matroides també s'han fet servir per estudiar els esquemes per a compartir secrets no perfectes [54].

Una altra de les estratègies per estudiar les estructures ideals és intentar caracteritzar-les dins de famílies particulars d'estructures. Brickell i Davenport es van plantejar aquest problema per la família de les estructures representables per un graf. Van demostrar a [25] que una estructura definida per un graf connexe és ideal si i només si és un graf multipartit complet. El resultat complet sobre la caracterització de les estructures ideals representables per un graf és el següent:

Teorema 1.6.3 [25, 15] *Sigui* Γ *una estructura d'accés representable per un graf. Llavors, les afirmacions següents són equivalents:*

1. Γ *és una estructura d'accés representable per un graf multipartit complet.*
2. Γ *és una estructura d'accés d'espai vectorial.*
3. Γ *és una estructura d'accés ideal.*
4. $\rho^*(\Gamma) > 2/3$.

Per acabar aquesta secció dedicada a la caracterització de les estructures ideals volem fer una breu ressenya del problema de quan una estructura es pot realitzar sobre qualsevol conjunt de secrets. Sabem que quan es determina l'existència d'un esquema per a una estructura d'accés, sovint es deixa en un segon pla quin és el cardinal del conjunt de secrets. A la pràctica el conjunt de secrets ha de ser molt gran amb la finalitat d'evitar el mètode de la força bruta per trobar el secret. Però per a una estructura donada en la qual es pot realitzar repartint un cert número de secrets, hi haurà un esquema que reparteixi un número de secrets diferent? Tot això ha motivat l'estudi d'una subfamília d'estructures que ha estat completament caracteritzada a [6]: les estructures universalment ideals. Una estructura d'accés es diu *universalment ideal* si per a tot conjunt finit de secrets existeix un esquema per a compartir secrets ideal que la realitza. Aquesta subfamília d'estructures coincideix exactament amb les que es poden realitzar en un conjunt de 2 i de 3 secrets.

1.7 Fites inferiors de la taxa d'informació òptima

S'han estudiat algunes tècniques amb la finalitat de trobar fites inferiors de la taxa d'informació. Hi ha un doble interès per estudiar les fitacions inferiors de la taxa d'informació. D'una banda trobar resultats teòrics al respecte de les fitacions d'aquest paràmetre, però també com a generador d'esquemes raonablement pràctics ja que en general els teoremes que s'han generat són constructius, és a dir, la prova de les fites es fa via la construcció d'un esquema.

La principal tècnica feta servir per tal de fitar inferiorment la taxa d'informació ha estat la d'expressar l'estructura d'accés com a reunió d'una família de subestructures de les quals coneixem un esquema que les realitzi. Per repartir un secret es reparteix segons tots els esquemes emprats i cada participant rep tants fragments com número d'estructures en les quals està present. Diverses modificacions d'aquesta idea s'han treballat. La més completa de totes és la construcció per descomposició de D.R. Stinson, exposada a [95] que engloba totes les anteriors.

Definim a continuació què s'entèn per *construcció per descomposició*, deguda a D.R. Stinson [95]. Una λ-*descomposició* de Γ és una colecció $\Gamma_1, \ldots, \Gamma_n$ de subestructures $\Gamma_h \subset \Gamma_0$ per $h = 1, \ldots, n$ de tal manera que per a cada $B \in \Gamma_0$ existeixi almenys λ subestructures $\Gamma_{i_1}, \ldots, \Gamma_{i_\lambda}$ tal que $B \in \Gamma_{i_j}$ per $j = 1, \ldots, \lambda$. Siguin P_h els subconjunts de participants apareixent a Γ_h (per $h = 1, \ldots, n$), i P_0 el subconjunt de participants apareixent a Γ_0, és a dir, $P_h = P(\Gamma_h)$ per a tota $h = 0, 1, \ldots, n$. En aquestes condicions el Corol·lari 3.1 de [95] estableix

Corol·lari 1.7.1 [95] *Si $\Gamma_1, \ldots, \Gamma_n$ és una λ-descomposició de Γ i per a cada Γ_h $(h = 1, \ldots, n)$ existeix un esquema per a compartir secrets amb taxa mitjana d'informació $\tilde{\rho}_h$ i cada participant de $P_h = P(\Gamma_h)$ té taxa d'informació $\rho_h(p)$, llavors la taxa d'informació òptima verifica*

$$\rho^* \geq \min_{p \in P} \frac{\lambda}{\sum_{\{h:\, p \in P_h\}} 1/\rho_h(p)}$$

i la taxa mitjana d'informació òptima verifica

$$\tilde{\rho}^* \geq \frac{\lambda |P|}{\sum_{h=1}^{n} |P_h|/\tilde{\rho}_h}$$

Fem un esbós de com es construeix l'esquema per a compartir secrets a partir dels esquemes coneguts per a cada subestructura. Sigui una col·lecció

de vectors $\{L_h\}_{h=1}^n$ de $GF(q)^\lambda$ de tal manera que agafats de λ en λ siguin linealment independents, i per tant base de $GF(q)^\lambda$. Sigui un secret $K \in GF(q)^\lambda$. Amb l'esquema que realitza l'estructura Γ_h repartim el secret $K \cdot L_h \in GF(q)$, rebent cada participant $p \in P$ el fragment

$$s_p = (a_{p1}, a_{p2}, \ldots, a_{pn})$$

amb a_{ph} el fragment que li correspon al repartir $K \cdot L_h$ si $p \in P_h$, i és buit altrament. Un subconjunt autoritzat $A \in \Gamma$ estarà en almenys λ subestructures $\Gamma_{h_1}, \ldots, \Gamma_{h_\lambda}$, per tant es podran recuperar $K \cdot L_{h_1}, \ldots, K \cdot L_{h_\lambda}$ i com que $L_{h_1}, \ldots, L_{h_\lambda}$ formen base de $GF(q)^\lambda$ podrem recuperar el secret $K \in GF(q)^\lambda$. El coneixement dels fragments d'un subconjunt no autoritzat no dóna cap informació sobre el valor possible del secret. El participant $p \in P$ rebrà tants fragments com estructures en les quals surt, d'una longitud total

$$\sum_{\{h:\, p \in P_h\}} \frac{\log q}{\rho_h(p)}$$

d'aquí que la taxa d'informació del participant $p \in P$ sigui

$$\rho(p) = \frac{\log q^\lambda}{\sum_{\{h:\, p \in P_h\}} \log q / \rho_h(p)} = \frac{\lambda}{\sum_{\{h:\, p \in P_h\}} 1/\rho_h(p)}$$

i la taxa mitjana de l'esquema sigui

$$\tilde{\rho} = \frac{|P|}{\sum_{p \in P} 1/\rho(p)} = \frac{\lambda |P|}{\sum_{p \in P} \sum_{\{h:\, p \in P_h\}} 1/\rho_h(p)} =$$

$$\frac{\lambda |P|}{\sum_{h=1}^n \sum_{\{h:\, p \in P_h\}} 1/\rho_h(p)} = \frac{\lambda |P|}{\sum_{h=1}^n \sum_{\{h:\, p \in P_h\}} 1/\rho_h(p)} = \frac{\lambda |P|}{\sum_{h=1}^n |P_h| / \tilde{\rho}_h}$$

Un dels resultats trobat per Stinson [95] fent servir directament la tècnica de la λ-descomposició, és el següent: per a qualsevol graf la taxa d'informació òptima és més gran o igual que $2/(d+1)$ amb d el grau màxim del graf. Aquesta fita s'ha trobat fent servir una λ-descomposició en la qual es recobreix amb la família de grafs estrella de cadascun dels vèrtexs. Una *estrella* de centre $p \in P$ és el subgraf de G definit per $S_p = \{\{p, q\} | \{p, q\} \in E(G)\}$. Sabem que les estructures definides per grafs que són ideals són els grafs multipartits complets, per la qual cosa les estrelles tenen taxa d'informació igual a 1. Aquesta fita inferior és ajustada, ja que a [20] es troba un graf amb taxa d'informació òptima igual a $2/(d+1)$. Evidentment, això no treu que, per un graf en concret, es pugui trobar un recobriment que doni una taxa d'informació millor.

S'observa que les subestructures amb les quals recobrim poden estar repetides. Aquest fet ens pot donar la idea d'intentar trobar quantes vegades s'ha de repetir cada subestructura de forma que la taxa d'informació ens quedi el més gran possible. Aquest plantejament condueix a un problema de programació lineal que descrivim ara mateix.

Suposem que amb la notació que hem introduït per a les λ-descomposicions, cada $\rho_h(p)$ és racional. De fet en les construccions fetes amb els esquemes coneguts sempre arribem a taxes racionals. Denotem $\Gamma_0 = \{A_1, \ldots, A_v\}$. Utilitzarem $\mathbf{B}$, la matriu d'incidència $v \times n$ definida per

$$b_{jh} = \begin{cases} 1 & \text{si} \quad A_j \in \Gamma_h \\ 0 & \text{si} \quad A_j \notin \Gamma_h \end{cases}$$

També farem servir $\mathbf{C}$, la matriu d'incidència modificada de dimensions $|P| \times n$ definida per

$$c_{ph} = \begin{cases} 1/\rho_h(p) & \text{si} \quad p \in P_h \\ 0 & \text{si} \quad p \notin P_h \end{cases}$$

Denotarem per $\alpha \geq x$ amb $\alpha = (\alpha_1, \ldots, \alpha_m)$ si i només si la desigualtat es verifica per a cada component, és a dir, $\alpha_i \geq x$ per a tot $i = 1, \ldots, m$. De la mateixa manera es defineix la desigualtat $\alpha \leq x$. Amb aquesta notació el problema de programació lineal que cal resoldre és

Problema de programació lineal per ρ^* associat a una $\lambda-$descomposició
Maximitzar R amb les restriccions
$\alpha \geq 0$
$\mathbf{C} \cdot \alpha^t \leq 1$
$\mathbf{B} \cdot \alpha^t \geq R$

Si R és solució d'aquest problema llavors $\rho^* \geq R$. Per obtenir els factors de repetició de cada subestructura només caldrà multiplicar el vector α per un nombre enter adient, de forma que el resultat sigui un vector amb components enteres. El mateix problema per la taxa mitjana ens condueix al següent problema de programació lineal a on el vector $\mathbf{d} = (d_1, \ldots, d_m)$ ve definit per $d_h = |P_h|/\tilde{\rho}_h$:

Problema de programació lineal per $\tilde{\rho}^*$ associat a una $\lambda-$descomposició
Maximitzar $R|P|$ amb les restriccions
$\alpha \geq 0$
$\mathbf{d} \cdot \alpha^t \leq 1$
$\mathbf{B} \cdot \alpha^t \geq R$

Si R és solució d'aquest problema llavors $\rho^* \geq R|P|$.

Casos particulars d'aquesta construcció condueixen a tècniques de descomposició que s'havien estudiat anteriorment [27, 18, 93, 58, 59, 92]. Pel cas d'una 1-descomposició, el mètode es redueix a repartir el secret a cadascuna de les subestructures mitjançant l'esquema associat. D'aquest tipus són les tècniques desenvolupades per a les estructures homogènies de rang 2, és a dir, les definides per un graf. Aquestes descomposicions s'anomenen recobriments per grafs multipartits complets. Tota aquesta construcció per descomposició particular va ser proposada abans de la formulació de la λ-descomposició. Així Blundo, De Santis, Stinson i Vaccaro a [18] anomenen *recobriment multipartit complet* de G a una família de subgrafs $\Pi = \{G_1, \ldots, G_n\}$ del graf G pels quals cada G_i és un graf multipartit complet i cada aresta de G apareix en almenys un dels grafs G_i. El Teorema 3.1 de [18] afirma

Teorema 1.7.2 [18] *Per a cada vèrtex de G considerem $R_v = |\{i \,|\, v \in V(G_i)\}|$ i $R = \max\{R_v \,|\, v \in V(G)\}$. Existeix un esquema per a compartir secrets amb estructura d'accés donada per G i taxa d'informació $\rho = 1/R$.*

Per tant $\rho^*(G) \geq 1/R$. De fet com a cas particular de la λ-descomposició només cal observar que es tracta d'una 1-descomposició i que per a cada vèrtex v tenim $\rho(v) = 1/R_v$ i d'aquí $\rho^* \geq 1/R$. També en el mateix treball el Teorema 3.2 utilitza una família de recobriments multipartits complets:

Teorema 1.7.3 [18] *Per una família de recobriments multipartits complets $\Pi_j = \{G_{j1}, \ldots, G_{jn_j}\}$ per $1 \leq j \leq \ell$, es defineix per a qualsevol vèrtex v i per a qualsevol $j = 1, \ldots, \ell$, $R_{jv} = |\{i \,|\, v \in V(G_{ij})\}|$, $R_v = \sum_{j=1}^{\ell} R_{jv}$ i $R = \max\{R_v \,|\, v \in V(G)\}$, llavors existeix un esquema per a compartir secrets amb estructura d'accés donada per G i taxa d'informació $\rho = \ell/R$.*

Per a aquest cas només cal fixar-se que estem davant d'una ℓ-descomposició i que $\rho(v) = 1/\sum_{j=1}^{\ell} R_{jv}$ i d'aquí $\rho^* \geq 1/R$ amb $R = \max\{R_v \,|\, v \in V(G)\}$.

També s'han proposat adaptacions dels problemes de programació lineal pel cas de recobriments multipartits complets [18]. Aquestes tècniques (junt amb d'altres que veurem a l'apartat següent) van fer que en aquest mateix treball [18] es determinessin exactament les taxes d'informació per camins i per cicles de longitud parella, i certes fitacions per arbres i cicles de longitud senar, tot això abans que la tècnica de la λ-descomposició fos formulada. També s'estudien les taxes d'informació per a tots els grafs de menys de 5 vèrtexs, obtenint exactament els valors per a la pràctica totalitat dels casos.

L'estudi del problema de la fitació de la taxa d'informació restringit a famílies particulars d'estructures d'accés s'ha fet per estructures definides per grafs i per estructures homogènies.

Per estructures d'accés definides per grafs C. Blundo, A. De Santis, D.R. Stinson i U. Vaccaro van proposar a [18] una manera de fitar la taxa d'informació. D. R. Stinson a [92] generalitza per estructures d'accés qualssevol la tècnica trobada per grafs aplicant aquesta amb sistemes de Steiner i amb coloracions d'arestes de grafs bipartits. El resultat d'aplicar aquestes tècniques va suposar una millora de les fites de Benaloh i Leichter per la taxa d'informació òptima per estructures d'accés homogènies de rang r en un factor de r (asimptòticament).

Per estructures d'accés generals Benaloh i Leichter van trobar una fita de la taxa d'informació utilitzant un circuit booleà per a una forma normal disjuntiva [8]. Com s'ha comentat a la Secció 2.2, per a tota estructura d'accés es pot construir un esquema per a compartir secrets fent ús de l'esquema circuital. Aquest esquema proporciona per a una estructura homogènia de rang r una taxa d'informació que en el pitjor dels casos arriba a

$$\rho = \frac{1}{\binom{n-1}{r-1}}$$

Aquest cas es dóna quan hi ha un participant que figura en tots els subconjunts possibles de r elements que es poden fer amb els n participants i per tant rebrà un fragment per cada minimal.

Tenint en compte que tota estructura d'accés es pot posar com a reunió d'estructures homogénies, obtenim que la taxa d'informació òptima és més gran que $1/2^n$. Aquesta ha estat la primera fita inferior per la taxa d'informació òptima d'una estructura qualsevol. Per la qual cosa podem afirmar que la taxa d'informació òptima és més gran o igual que aquest valor trobat.

Una altra de les particularitzacions de la construcció per descomposició es pot trobar a [92]. En aquest treball s'aplica aquesta construcció fent servir coloracions d'arestes de grafs bipartits obtenint

$$\rho^* \geq \frac{r}{(2r-1)\binom{N-1}{r-2} + d}$$

per la taxa d'informació òptima d'estructures homogènies de rang r en un conjunt de N participants i amb d el número màxim de minimals als quals pertany un participant. Per la taxa mitjana òptima:

$$\tilde{\rho}^* \geq \frac{rN}{N(2r-1)\binom{N-1}{r-2} + r|\Gamma_0|}$$

Totes aquestes fites van suposar la millora de les fites obtingudes amb l'esquema circuital en un factor de r (asimptòticament). També en el mateix treball i fent

servir aquesta vegada sistemes de Steiner troba fites per a la taxa d'informació òptima per estructures homogènies de rang $r = 3$, la principal de les quals és

$$\rho^* \geq \frac{6}{(N-1)(N-2)}$$

si $N \equiv 2, 4 (\mathrm{mod}\, 6)$. Per la mitjana:

$$\tilde{\rho} \geq \frac{24}{5(N-1)(N-2)}$$

si $N \equiv 2, 4 (\mathrm{mod}\, 6)$ i de rang 3.

Finalment Sun i Shieh a [85] fan ús d'una mena de λ-descomposició, trobant que la taxa d'informació per estructures d'accés homogènies de rang r en un conjunt de N participants està fitada per

$$\rho^* \geq \frac{N-r+1}{\binom{N}{r}}$$

També troben per una estructura homogènia de rang 3 en un conjunt de N participants que

$$\rho^* \geq \frac{6}{N^2-2N+3}$$

1.8 Fites superiors de la taxa d'informació òptima

Blundo, De Santis, De Simone i Vaccaro van presentar a [20] un mètode per trobar fites superiors de la taxa d'informació òptima. Aquesta fita superior s'obté fent servir Teoria de la Informació. Aquestes tècniques van ser proposades per primera vegada per Capocelli, De Santis, Gargano i Vaccaro a [29], tècniques que han resultat molt profitoses en treballs posteriors en els quals s'han trobat fites superiors de la taxa d'informació òptima [19, 15, 20, 34, 92, 38]. Amb aquestes tècniques [15] es mostren estructures d'accés tals que la seva taxa d'informació òptima és $1/2 + \epsilon$, amb ϵ arbitràriament petit. Treballs amb les mateixes tècniques [29], van mostrar exemples d'estructures d'accés amb taxa d'informació fitada per un valor allunyat de 1. Totes aquestes estructures d'accés es van construir a partir de grafs. També fent servir el mateix tipus de raonaments es va trobar que si una estructura definida per un graf no era ideal aleshores la seva taxa d'informació havia d'estar a l'interval $0 < \rho^* \leq 2/3$ amb la qual cosa queda tot un interval de valors impossibles per a les taxes

d'informació. Exposem breument els conceptes i propietats principals que es faran servir.

Donada una distribució de probabilitat $\{p(x)\}_{x\in X}$ en un conjunt finit X definim $H(X)$ l'*entropia* de Shanon de X com

$$H(X) = -\sum_{x\in X} p(x)\log p(x)$$

amb el ben entés que els logaritmes són en base 2 i que $0\log 0 = 0$. S'observa que el conjunt X es pot considerar com a una variable aleatòria discreta a on $p(x)$ és la probabilitat que escollim el valor $x \in X$. Sota aquesta interpretació l'entropia de X és la esperança de la variable aleatòria discreta $\log 1/p(x)$.

El concepte d'entropia és molt important en Enginyeria de Telecomunicacions (Teoria de la Comunicació), Ciències de la Computació (Complexitat de Kolmogorov), Física Estadística (Termodinámica), Teoria de la Probabilitat i Estadística (taxes d'error en tests d'hipotesis òptims i estimació), Filosofia de la Ciència i inferència estadística (Navalla d'Occam), Economia (Inversió) i Disseny d'ordinadors [36]. Intuïtivament l'entropia mesura la incertesa d'una variable aleatòria. Veiem una altre manera d'interpretar l'entropia: suposem que descrivim els diferents elements del conjunt X per un número de bits més petit quant més probable sigui aquest valor i amb un número més gran de bits quan més improbable sigui aquest valor. Una manera possible és fer servir $\log 1/p(x)$ bits per descriure el valor x. D'aquesta forma l'entropia mesura el número de bits en mitjana que esperarem per descriure l'element $x \in X$ escollit.

L'entropia verifica

$$0 \leq H(X) \leq \log |X|$$

a més $H(X) = 0$ si i només si per un cert $x_0 \in X$ tenim que $p(x_0) = 1$ i que $p(x) = 0$ per a tot $x \in X - \{x_0\}$. També es verifica que $H(X) = \log |X|$ si i només si la probabilitat és la distribució uniforme $p(x) = 1/|X|$ per a tot $x \in X$.

Per dos conjunts X, Y i una distribució de probabilitat conjunta

$$\{p(x,y)\}_{(x,y)\in X\times Y}$$

definim $H(X|Y)$ l'*entropia condicionada* com a

$$H(X|Y) = -\sum_{y\in Y}\sum_{x\in X} p(y)p(x|y)\log p(x|y)$$

que verifica $H(X|Y) \geq 0$.

Donats $X_1, \ldots, X_n, Y$ l'entropia de $X_1, \ldots, X_n$ condicionada per Y pot ser expressada com a

$$H(X_1 \ldots X_n|Y) = H(X_1|Y) + H(X_2|X_1Y) + \ldots + H(X_n|X_1 \ldots X_{n-1}Y)$$

La *informació mútua* $I(X;Y)$ entre X i Y es defineix com a

$$I(X;Y) = H(X) - H(X|Y)$$

que verifica

$$I(X;Y) = I(Y;X) \text{ i } I(X;Y) \geq 0$$

de fet aquesta darrera propietat és equivalent a dir que

$$H(X) \geq H(X|Y)$$

També tenim que

$$H(XY) = H(X) + H(Y) - I(X;Y)$$

Donats X, Y, Z la *informació mútua condicionada* $I(X,Y|Z)$ es defineix com

$$I(X,Y|Z) = H(X|Z) - H(Y|XZ)$$

que verifica que

$$I(X,Y|Z) = I(Y,X|Z) \text{ i } I(X,Y|Z) \geq 0$$

d'on surt que

$$H(X|Z) \geq H(X|YZ) \text{ i } I(X;YZ) \geq I(X;Z)$$

Es pot definir $I(XY;Z)$ com a

$$I(XY;Z) = I(X;Z) + I(Y;Z|X)$$

També, per definició, tenim que

$$\sum_{i=1}^{n} H(X_i) = H(X_1 \ldots X_n) + \sum_{i=2}^{n} H(X_i; X_1 \ldots X_{i-1})$$

d'on es dedueix que

$$\sum_{i=1}^{n} H(X_i) \geq H(X_1 \ldots X_n)$$

Sigui un esquema per a compartir secrets Σ que reparteix secrets de $\mathcal{K}$ escollits segons una distribució de probabilitat $\{p_{\mathcal{K}}(k)\}_{k\in\mathcal{K}}$. Per simplificar la notació entendrem que $\mathcal{K}$ és el conjunt de secrets i que a la vegada és una variable aleatòria que assigna valors de $\mathcal{K}$ segons la distribució de probabilitat que hem assenyalat. Així escriurem $p_{\mathcal{K}}(k) = p(\mathcal{K} = k)$. D'aquesta forma té ple sentit parlar de $H(\mathcal{K})$, l'entropia de $\mathcal{K}$. De la mateixa manera quan el distribuïdor reparteix un secret, cada participant $p \in P$ rep un fragment de $\mathcal{S}_p$ i cada subconjunt $A = \{p_1, \ldots, p_r\} \subset P$ rep un conjunt de fragments de $\mathcal{S}_A = \mathcal{S}_{p_1} \times \ldots \times \mathcal{S}_{p_r}$ segons una certa distribució de probabilitat $\{p_{\mathcal{S}_A}(a)\}_{a\in\mathcal{S}_A}$. També, per simplificar, entendrem que $A \subset P$ és un subconjunt de participants i que a la vegada és una variable aleatòria que assigna valors de A segons la distribució de probabilitat que hem assenyalat. Així té sentit parlar de $H(A)$, l'entropia de $A \subset P$ com a subconjunt o com a variable aleatòria.

Direm que un esquema per a compartir secrets és *perfecte* si

1. Per a tot $A \in \Gamma$ es verifica que si $a \in \mathcal{S}_A$ amb $p_{\mathcal{S}_A}(a) > 0$ llavors existeix un únic secret $k \in \mathcal{K}$ tal que $p(\mathcal{K} = k|A = a) = 1$, és a dir, que tot subconjunt autoritzat pot determinar unívocament el secret a partir dels seus fragments.

2. Per a tot $A \notin \Gamma$ es verifica que per a qualsevol $k \in \mathcal{K}$ i per a qualsevol $a \in A$, $p(\mathcal{K} = k|A = a) = p_{\mathcal{K}}(k)$, és a dir, que tot subconjunt no autoritzat no pot obtenir absolutament cap informació sobre el valor del secret.

Una formulació equivalent en termes de l'entropia és la següent:

1. Per a tot $A \in \Gamma$ es verifica que $H(\mathcal{K}|A) = 0$.

2. Per a tot $A \notin \Gamma$ es verifica que $H(\mathcal{K}|A) = H(\mathcal{K})$.

El concepte de taxa d'informació en les seves diverses modalitats també ha estat traduït fent servir el concepte d'entropia. Les definicions que farem són definicions que tenen el seu més gran interès quan considerem que potser el secret no està escollit de forma uniforme dins del conjunt de secrets. Es podrà observar que tot aquest plantejament engloba el que hem fet a la Secció 2.3. Si Γ és una estructura monòtona d'accés i $p_{\mathcal{K}}$ és la distribució de probabilitats del secret, llavors la *taxa d'informació* es pot expressar fent servir el concepte d'entropia:

$$\rho(\Gamma, p_{\mathcal{K}}) = \frac{H(\mathcal{K})}{\max_{p\in P} H(p)}$$

s'observa que en el cas de distribucions de probabilitat uniformes:

$$\rho(\Gamma) = \frac{\log |\mathcal{K}|}{\max_{p \in P} \log |\mathcal{S}_p|}$$

La *taxa mitjana d'informació* es defineix per:

$$\widetilde{\rho}(\Gamma, p_{\mathcal{K}}) = \frac{H(\mathcal{K})}{\sum_{p \in P} H(p)/|P|}$$

que per distribucions de probabilitats uniformes queda:

$$\widetilde{\rho}(\Gamma) = \frac{|P| \log |\mathcal{K}|}{\sum_{p \in P} \log |\mathcal{S}_p|}$$

Presentem aquí una generalització del mètode exposat a [20], la qual es farà servir més tard.

En primer lloc recordem dos lemes tècnics, la demostració dels quals es pot trobar a [29].

Lema 1.8.1 [29] *Sigui* Γ *una estructura d'accés i siguin* $X, Y \subset P$ *tals que* $Y \notin \Gamma$ *i que* $X \cup Y \in \Gamma$. *Llavors*

$$H(X|Y) = H(\mathcal{K}) + H(X|Y\mathcal{K}).$$

Lema 1.8.2 [29] *Sigui* Γ *una estructura d'accés i siguin* $X, Y \subset P$ *tals que* $Y \in \Gamma$ *o bé* $X \cup Y \notin \Gamma$. *Llavors*

$$H(X|Y) = H(X|Y\mathcal{K}).$$

El lema següent es pot trobar a [38]:

Lema 1.8.3 [38] *Sigui* Γ *una estructura d'accés i siguin* $X, Y, Z \subset P$ *tals que* $X \cup Z \in \Gamma$, $Y \cup Z \in \Gamma$ *i que* $Z \notin \Gamma$. *Llavors*

$$I(X; Y|Z) \geq H(\mathcal{K}).$$

Blundo, De Santis, De Simone i Vaccaro a l'article [20] defineixen el que s'entén per una successió d'elements independents. Nosaltres estenem aquest concepte a una successió de subconjunts. Sigui Γ una estructura d'accés en un conjunt de participants P. Direm que una successió $B_1, B_2, \ldots, B_m$, a on

$$\emptyset \neq B_1 \subset B_2 \subset \cdots \subset B_m \subset P,$$

és *independent* si

1. $B_m \notin \Gamma$
2. Per a tot $i = 1, 2, \ldots, m$, existeix un conjunt $X_i \subset P$ tal que $B_i \cup X_i \in \Gamma$ i $B_{i-1} \cup X_i \notin \Gamma$, amb el conveni $B_0 = \emptyset$.

Direm que un conjunt $A \supset \bigcup_{i=1}^{m} X_i$ *fa la successió* $B_1, B_2, \ldots, B_m$ *independent.*

El lema següent és un lema tècnic que ens afita inferiorment la informació mútua en funció de la entropia del conjunt de secrets. Aquest lema és una generalització fàcil del corresponenet lema del treball [20].

Lema 1.8.4 *Sigui* Γ *una estructura d'accés i sigui* $B_1, \ldots, B_m$ *successió de subconjunts independents tals que* $A \subset P$ *fa independent la successió. Aleshores*

$$I(A; B_m) \geq \begin{cases} mH(\mathcal{K}) & si\ A \in \Gamma \\ (m-1)H(\mathcal{K}) & si\ A \notin \Gamma \end{cases}$$

Demostració: Per $m = 1$ i $A \notin \Gamma$ és cert perquè la informació mútua és positiva. Si $m = 1$ i $A \in \Gamma$ llavors

$$I(A; B_1) = H(B_1) - H(B_1|A) \geq H(B_1|X_1) - H(B_1|A) =$$

$$= H(\mathcal{K}) + H(B_1|X_1\mathcal{K}) - H(B_1|A\mathcal{K}) \geq H(\mathcal{K})$$

aplicant el Lema 2.8.1 a X_1, B_1 i el Lema 2.8.2 a $A \in \Gamma$ i fent servir que $X_1 \subset A$.

Si $m \geq 2$ i per $i = 1, \ldots, m$ podem posar $C_i = B_i - B_{i-1}$ llavors per $i = 1, \ldots, m-1$ tenim

$$H(A|B_i) - H(A|B_{i+1}) = I(B_{i+1} - B_i; A|B_i) = I(C_{i+1}; A|B_i) = H(C_{i+1}|B_i) - H(C_{i+1}|B_iA)$$

$$\geq H(C_{i+1}|X_{i+1}B_i) - H(C_{i+1}|B_iA) = H(\mathcal{K}) + H(C_{i+1}|X_{i+1}B_i\mathcal{K}) - H(C_{i+1}|B_iA)$$

$$= H(\mathcal{K}) + H(C_{i+1}|X_{i+1}B_i\mathcal{K}) - H(C_{i+1}|B_iA\mathcal{K}) \geq H(\mathcal{K})$$

Per tant,

$$\sum_{i=1}^{m-1} (H(A|B_i) - H(A|B_{i+1})) = H(A|B_1) - H(A|B_m) \geq (m-1)H(\mathcal{K})$$

i llavors

$$H(A|B_1) \geq (m-1)H(\mathcal{K}) + H(A|B_m)$$

Així doncs,

$$I(A;B_m) = H(A) - H(A|B_m) \geq H(A|B_1) - H(A|B_m) \geq (m-1)H(\mathcal{K})$$

A més si $A \in \Gamma$ llavors hem raonat que $I(A;B_1) = H(A) - H(A|B_1) \geq H(\mathcal{K})$ i per tant

$$I(A;B_m) = H(A) - H(A|B) \geq H(\mathcal{K}) + H(A|B_1) - H(A|B_m) \geq mH(\mathcal{K})$$

□

Com a corol·lari d'aquest lema obtenim una afitació equivalent per les entropies que torna a ser una generalització del corol·lari corresponent de [20]:

Corol·lari 1.8.5 *Sigui Γ una estructura d'accés i sigui $B_1, \ldots, B_m$ successió de subconjunts independents tals que $A \subset P$ fa independent la successió. Aleshores*

$$H(A) \geq \begin{cases} (m+1)H(\mathcal{K}) & \textit{si } A \in \Gamma \\ mH(\mathcal{K}) & \textit{si } A \notin \Gamma \end{cases}$$

Demostració: Utilitzant el Lema 2.8.1 obtenim $H(A|B_m) = H(\mathcal{K}) + H(A|B_m\mathcal{K})$ atès que $B_m \notin \Gamma, A \cup B_m \in \Gamma$. D'aquí i fent servir el Lema 2.8.4:

$$H(A) = H(A|B_m) + I(A;B_m) \geq H(\mathcal{K}) + I(A;B_m) \geq \begin{cases} (m+1)H(\mathcal{K}) & \text{si } A \in \Gamma \\ mH(\mathcal{K}) & \text{si } A \notin \Gamma \end{cases}$$

□

El teorema següent ens dóna una fita superior de la taxa d'informació òptima per una estructura d'accés, coneguda una successió de subconjunts independents i un subconjunt que la fa independent. La importància d'aquest teorema radica en que és la primera vegada que es troba una fita superior per a la taxa d'informació òptima per a una estructura d'accés qualsevol. Aquesta fita general s'expressa només en funció de qüestions combinatòries de l'estructura. Aquest resultat és una generalització fàcil del teorema corresponent de [20].

Teorema 1.8.6 *Sigui Γ una estructura d'accés en un conjunt de participants P. Sigui $\emptyset \neq B_1 \subset B_2 \subset \cdots \subset B_m \subset P$ una successió independent i $A \subset P$ un conjunt que fa aquesta successió independent. Aleshores,*

- *Si $A \in \Gamma$, $\rho^*(\Gamma) \leq \dfrac{|\,A\,|}{m+1}$.*
- *Si $A \notin \Gamma$, $\rho^*(\Gamma) \leq \dfrac{|\,A\,|}{m}$.*

Demostració: Com que

$$\sum_{a\in A} H(a) \geq H(A) \geq \begin{cases} (m+1)H(\mathcal{K}) & \text{si } A \in \Gamma \\ mH(\mathcal{K}) & \text{si } A \notin \Gamma \end{cases}$$

aleshores existeix un $a \in A$ tal que

$$H(a) \geq \begin{cases} \frac{(m+1)H(\mathcal{K})}{|A|} & \text{si } A \in \Gamma \\ \frac{mH(\mathcal{K})}{|A|} & \text{si } A \notin \Gamma \end{cases}$$

per la qual cosa podem afirmar que $\frac{H(\mathcal{K})}{H(a)} \leq \frac{|A|}{m+1}$ si $A \in \Gamma$ i que $\frac{H(\mathcal{K})}{H(a)} \leq \frac{|A|}{m}$ si $A \notin \Gamma$ quedant provat el resultat. □

El resultat obtingut per a una successió de subconjunts independents és una generalització de la tècnica de la successió de participants independents de [20]. Una *successió de participants* $b_1 \dots b_m \in P$ *és independent* si

1. $\{b_1, \dots, b_m\} \notin \Gamma$
2. Per a tot $i = 1, 2, \dots, m$, existeix un conjunt $X_i \subset P$ tal que $\{b_1, \dots, b_i\} \cup X_i \in \Gamma$ i $\{b_1, \dots, b_{i-1}\} \cup X_i \notin \Gamma$, amb $X_1 \notin \Gamma$.

Direm que un conjunt $A \supset \bigcup_{i=1}^{m} X_i$ *fa la successió de participants* $b_1, b_2, \dots, b_m$ *independent.*

El Teorema 2.8.6 és una generalització del teorema que es pot trobar a [20] i que ara es pot veure com a cas particular agafant una successió de subconjunts que va augmentant en un element, això és $|B_{i+1}| = |B_i| + 1$ amb $|B_1| = 1$. L'enunciem ja que el farem servir en aquest format:

Teorema 1.8.7 [20] *Sigui* Γ *una estructura d'accés en un conjunt de participants* P*. Sigui* B *una successió independent de participants de longitud* m *i* $A \subset P$ *un conjunt que fa aquesta successió independent. Aleshores,*

- *Si* $A \in \Gamma$, $\rho^*(\Gamma) \leq \dfrac{|\,A\,|}{m+1}$.
- *Si* $A \notin \Gamma$, $\rho^*(\Gamma) \leq \dfrac{|\,A\,|}{m}$.

Fent servir la tècnica de la successió de participants independents i amb l'ús dels corol·laris i lemes anteriors es pot demostrar [20] que la fita inferior $2/(d+1)$ per a la taxa d'informació òptima (amb d grau màxim del graf) es ajustada. En concret es justifica a [20] que per a tot $d \geq 2$ es troba un graf d-regular amb $\rho^* \geq 2/(d+1)$. Per tant la fita inferior donada per Stinson és ajustada.

1.9 Esquemes segurs enfront de mentiders

S'han proposat nombroses variants del concepte d'esquemes per a compartir secrets totes elles motivades per un aspecte a perfeccionar del plantejament clàssic dels esquemes i materialitzades en algun requeriment addicional. La variant més estudiada fins ara han estat els esquemes segurs enfront l'acció de mentiders. Repassarem els principals conceptes junt amb les propostes fetes sobre esquemes segurs enfront l'acció de mentiders i després un breu repàs d'altres variants que s'han proposat.

La variant que més s'ha estudiat ha estat la dels *esquemes segurs enfront l'acció de mentiders*. Aquests esquemes són els que incorporen algun sistema amb la finalitat d'anul·lar, detectar en el grau que es pugui l'acció de mentiders o de coalicions d'aquests o fins i tot identificar-los. Un *mentider* és un participant que lliura un fragment fals per tal de sabotejar el procés de reconstrucció del secret. Poden actuar en solitari o en forma de coalició. Tenim diferents tipus segons l'efecte del seu sabotatge. Un participant $p_i \in P$ és un *boicotejador* si és un mentider que, en lliurar a la caixa negra un fragment fals s_i^*, aconsegueix que es retorni com a secret vàlid un de fals $k^* \in \mathcal{K}$ en lloc del vertader $k \in \mathcal{K}$ de forma que només el boicotejador sap que el secret recuperat és fals (veure Figura 2.5).

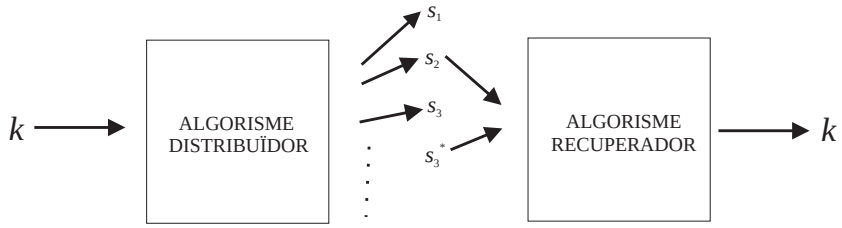

Figura 1.5: Acció d'un boicotejador

Una variant dels boicotejadors són els *estafadors*, els quals ja coneixen el secret i l'únic que pretenen és aconseguir que la resta de participants que intervenen en el procés de reconstrucció del secret marxi amb un secret fals. Es comet una *apropiació indeguda* quan el mentider $p_i \in P$ lliura a la caixa negra un fragment fals s_i^* aconseguint que es retorni com a secret vàlid un de fals $k^* \in \mathcal{K}$ en lloc del vertader $k \in \mathcal{K}$, però de tal manera que a partir del fragment fals s_i^*, el fragment correcte s_i i el secret fals k^* pot recuperar el secret correcte k. Aquesta manera de procedir queda esquematitzada a la Figura 2.6

L'apropiació indeguda és possible en una família tan extensa d'esquemes

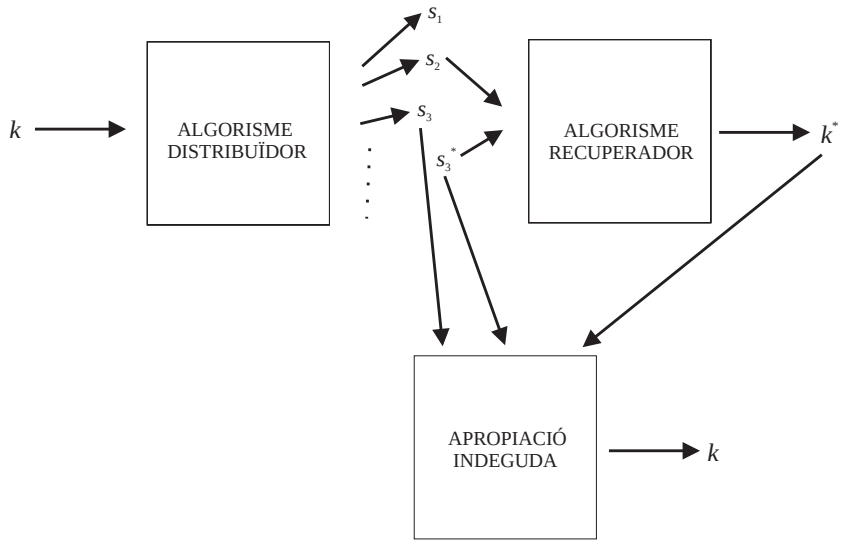

Figura 1.6: Apropiació indeguda

per a compartir secrets com són els esquemes d'espai vectorial, i de retruc, també a l'esquema polinomial de Shamir. Veiem com és possible que sigui tan vulnerable aquest esquema. Si per exemple el participant p_1 de $\{p_1, p_2, \ldots, p_r\} \in \Gamma$ menteix, lliurant un fragment fals $s_1^* = s_1 + \epsilon$, es recupera un secret fals,

$$k^* = \lambda_1(s_1 + \epsilon) + \lambda_2 s_2 + \ldots + \lambda_r s_r = k + \lambda_1 \epsilon$$

si $\psi(D) = \lambda_1\psi(p_1) + \lambda_2\psi(p_2) + \ldots + \lambda_r\psi(p_r)$. Llavors p_1 pot apropiar-se indegudament del secret calculant $k = k^* - \lambda_1\epsilon$.

Cal remarcar que tot esquema ideal és vulnerable enfront l'acció de mentiders i fins i tot és possible fer una apropiació indeguda. Justifiquem-ho fent servir el model de les regles de distribució. Sigui $A = \{p_1, \ldots, p_r\}$ un subconjunt autoritzat minimal amb $r \geq 2$. Suposem que $A - \{p_r\}$ és una coalició de mentiders que intenten enganyar p_r. Suposem que cada participant p_i ha rebut un fragment s_i quan s'ha repartit k. Com que l'esquema és ideal, fixats $r-1$ fragments hi ha una bijecció entre els fragment que pot rebre el participant que no té fixat el fragment i els secrets possibles per repartir. Si la coalició de mentiders modifica un fragment en la fase de recuperació, posem per cas $s_1^* \neq s_1$, l'algorisme de recuperació obté $k^* \neq k$ a partir dels fragments $s_1^* s_2 \ldots s_{r-1} s_r$, per tant aconsegueix enganyar al participant p_r. A més, a partir dels fragments $s_1^* s_2 \ldots s_{r-1}$ i de k^* els mentiders poden calcular s_r, simplement consultant la taula formada per les regles de distribució. A partir d'aquest darrer fragment i dels seus es pot calcular el secret k.

Parlarem de *seguretat incondicional contra mentiders* quan la probabilitat de mentir sense ser detectat no depèn de la capacitat computacional dels mentiders. Quan aquesta probabilitat depengui dels recursos computacionals dels mentiders es parla de *seguretat condicional contra mentiders*. Nosaltres ens ocuparem dels esquemes amb seguretat incondicional contra mentiders.

Davant del problema de l'actuació de mentiders s'han fet algunes propostes d'esquemes que detecten aquestes accions. A totes aquestes propostes s'augmenta la llargària del fragment que es lliura a cada participant. S'han fet estudis de com en un esquema de llindar, una exigència més alta en la seguretat fa disminuir la taxa d'informació. Els aspectes que cal observar són, junt amb la taxa d'informació, si l'esquema detecta la presència de mentiders, si els pot identificar o si no els detecta ni els identifica, si pot fer una apropiació indeguda. Fem un breu resum de les propostes que s'han fet.

Els primers que van considerar esquemes per tal de frenar l'acció de mentiders van ser McEliece i Sarwate a [60]. El seu esquema realitza una estructura de (t, n)-llindar fent ús de codis correctors d'errors. En aquest esquema qualsevol associació de com a màxim e mentiders dins d'un subconjunt de $t + 2e$ participants són descoberts i el secret es recupera correctament.

Cal remarcar que Rabin a [74] va fer la proposta de que el distribuïdor signés cadascun dels fragments lliurats als participants amb la finalitat de detectar quan un participant lliurava un fragment fals. Aquesta és una proposta condicionalment segura enfront l'atac de mentiders.

Tompa i Woll van formalitzar a [98] la primera modificació de fons de l'esquema per tal d'adaptar-se a l'existència de mentiders. La seva proposta és:

Esquema de Tompa i Woll
Algorisme distribuïdor: sigui $k \in \mathcal{K} = \{0, 1, \ldots, s-1\}$
s'escull un primer $p > \max\{\frac{(s-1)(k-1)}{\epsilon+t}, n\}$.
Generem els nombres aleatoris $a_1, \ldots, a_{t-1} \in GF(q)$
uniforme i independentment.
S'escullen $(x_1, \ldots, x_n)$ aleatoris entre les permutacions de
n elements de $\{1, \ldots, p-1\}$ de forma uniforme.
A partir del polinomi $A(x) = k + a_1 x + \ldots + a_{t-1} x^{t-1}$ es reparteix
$p_i \longmapsto s_i = (x_i, A(x_i))$
Algorisme recuperador: es fa interpolació polinòmica,
recuperant el secret amb $k = A(0)$ si $A(0) \in \mathcal{K}$,
altrament es dóna un avís de l'existència de mentiders.

Aquest esquema és el que ells van anomenar com a (t, n, ϵ)-*esquema de*

llindar robust, una modificació del que s'entén per (t, n)-esquema de llindar. A part de les dues condicions que es demanen a un esquema de (t, n)-llindar s'exigeix que com a màxim amb una probabilitat ϵ una coalició de $t-1$ participants (que coneixen el secret) pot enganyar a un tercer. Això és, aquests participants poden calcular $t-1$ fragments falsos de forma que junt amb un fragment correcte determinen un secret sense ser detectada l'existència de mentiders. La seva proposta és una modificació de l'esquema polinomial de Shamir consistent fonamentalment en lliurar a cada participant l'abscissa del punt com a fragment secret (en lloc de fer-lo públic) i en marcar part dels secrets com a no correctes.

L'esquema així definit és un (t, n, ϵ)-esquema de llindar segur. El temps d'execució d'aquest algorisme és polinomial en t, n, $\log s$ i $\log(1/\epsilon)$. La probabilitat de mentir sense ser detectat per aquest esquema és com a màxim $1-ts/p$. Desgraciadament si els mentiders no són detectats, obtenen el secret. Amb la finalitat d'evitar aquest fenòmen Tompa i Woll van proposar en el mateix treball una sofisticació de l'anterior esquema de forma que la recuperació del secret per a una coalició de mentiders és difícil. La taxa d'informació és $\rho = s/(2p)$

Rifà-Coma proposa a [77] dos esquemes per esquemes de llindar, basats en interpolació racional. El primer s'assegura que en el cas d'haver-hi un mentider, aquest no pot fer una apropiació indeguda. El segon esquema proposat és un esquema que a més detecta si hi ha mentiders. Fem una breu descripció d'aquests algorismes.

Primer esquema de Rifà-Coma
Algorisme distribuïdor: sigui $k \in \mathcal{K} = GF(q)$ i $t = 2p$.
Generem els nombres aleatoris $a_1, \ldots, a_{t-1}, c_1, \ldots, c_{t-1} \in GF(q)$ amb $a_i = 0$ per $i \geq p$, i $c_i = 0$ per $i > p$ (públics) que determinen els polinomis
$A(x) = k + a_1 x + \ldots + a_{t-1} x^{t-1}, \quad C(x) = 1 + c_1 x + \ldots + c_{t-1} x^{t-1}$
de graus $\deg(A(x)) < p$, $\deg(C(x)) \leq p$.
S'escullen $x_1, \ldots, x_n$ aleatoris no nuls de forma que $C(x_i) \neq 0$ per a tot i.
A partir de la funció racional $B(x) = A(x)/C(x)$ es reparteix
$p_i \longmapsto s_i = B(x_i)$
Algorisme recuperador: es recupera $B(x)$ fent ús de l'algorisme de Berlekamp-Massey, l'algorisme euclidià equivalent o el sistema lineal d'equacions $A(x_i) = C(x_i)s_i$
Es calcula el secret amb $k = A(0)$.

Aquest esquema és un esquema ideal que realitza una estructura de (t, n)-llindar amb $t = 2p$ en el qual l'apropiació indeguda no és possible.

El segon esquema és un (t, n)-esquema de llindar construït a partir d'un $(2t-1, 2n)$-esquema de llindar com els anteriors en el qual s'assignen dos fragments per a cada participant

Segon esquema de Rifà-Coma
Algorisme distribuïdor: sigui $k \in \mathcal{K} = GF(q)$.
Generem els nombres aleatoris $a_1, \ldots, a_{t-1}, c_1, \ldots, c_{t-1}$
que determinen els polinomis
$A(x) = k + a_1 x + \ldots + a_{t-1}x^{t-1}$ i $C(x) = 1 + c_1 x + \ldots + c_{t-1}x^{t-1}$
de graus menor o iguals que $t-1$.
Considerem la funció racional:
$B(x) = \frac{A(x)}{C(x)}$
S'escullen $x_1, \ldots, x_{2n}$ aleatoris no nuls (públics) tals que $C(x_i) \neq 0$
per a tot i. A partir de la funció racional es reparteix
$p_i \longmapsto s_i = (B(x_i), B(x_{i+n}))$
Algorisme recuperador: es recupera $B(x)$ fent ús de l'algorisme de Berlekamp-Massey, l'algorisme euclidà equivalent o el sistema lineal d'equacions
$A(x_i) = C(x_i)s_i$
Es calcula el secret amb $k = A(0)$ si $C(0) \neq 0$ i $\deg(C(x)) < t$,
i es dóna un avís de l'existència de mentiders si
$C(0) = 0$ o $\deg(C(x)) = t$.

La probabilitat de mentir sense ser detectat en aquest esquema és $1/q$. La taxa d'informació és $\rho = 1/2$.

També s'han proposat esquemes en els quals no només l'existència de mentiders és detectada, si no que a més són identificats. Aquest és el cas del treball [9] de Ben-Or i Rabin que utilitza una prova de coneixement zero basada en vectors de verificació. Carpentieri a [30] proposa un esquema per a compartir secrets que millora la taxa d'informació del de Ben-Or i Rabin. Brickell i Stinson a [26] proposen una variant de l'esquema geomètric de Blakley [11], de forma que també poden identificar mentiders. La probabilitat de mentir amb èxit és $(n-t+1)/(q-1)$.

Ja hem comentat que tots els esquemes que s'han proposat amb la finalitat de protegir-se de l'actuació dels mentiders es fonamenten en afegir certa redundància als fragments (és a dir, allargar els fragments) o equivalentment, com en el cas de Tompa i Woll, marcar part dels secrets com a *il·legals* (és a dir, escurçar l'expressió en bits dels secrets). Carpentieri, De Santis i Vaccaro [31] van establir per esquemes de (t, n)-llindar que si la probabilitat de mentir amb

èxit és $\epsilon > 0$, aleshores la longitud dels fragments ha de ser com a mínim la mesura del secret més $\log(1/\epsilon)$.

Ogata i Kurosawa a [64] van presentar un esquema per una estructura de llindar basat en l'ús d'un conjunt de diferències planar. Un *conjunt de diferències planar* mòdul $N = \ell(\ell-1)+1$ és un conjunt de ℓ nombres $B = \{d_0, d_1, \ldots, d_{\ell-1}\}$ verificant que les $\ell(\ell-1)$ diferències $d_i - d_j$ per $d_i \neq d_j$ coincideixen amb els nombres $1, 2, \ldots, N-1$ mòdul N. Aquest esquema està definit a partir de la suposició de l'existència d'un cert conjunt de diferències planar, de la manera següent:

Esquema d'Ogata i Kurosawa
Algorisme distribuïdor: sigui $k \in \mathcal{K} = B$ amb
$B = \{d_0, d_1, \ldots, d_{\ell-1}\}$ conjunt de diferències
planar mòdul un primer de la forma $N = \ell(\ell-1)+1$
Generem un polinomi $A(x)$ amb coeficients aleatoris presos a
$\mathbb{Z}_N$ de grau $t-1$ tal que $A(0) = k$
Es reparteix
$p_i \longmapsto s_i = A(i)$
Algorisme recuperador: es recupera $A(x)$ fent ús
d'interpolació polinòmica i a partir de $A(0)$ es calcula
el secret $k = A(0)$ si $A(0) \in B$. Altrament es dóna un missatge
de detecció de mentiders.

Fent servir que el conjunt de secrets és un conjunt de diferències planar, es pot veure [64] que aquesta generalització de l'esquema polinomial de Shamir és un esquema amb la taxa màxima entre els que realitzen un esquema de (t,n)-llindar amb l'exigència que la probabilitat de que una coalició de $t-1$ menteixi amb èxit és menor o igual que $1/\ell$. Aquest esquema té una taxa d'informació $\rho = \log(\ell)/\log(\ell^2 - \ell + 1)$. En aquest mateix treball es demostra, amb un raonament de tipus probabilístic, que tot esquema de llindar en el qual una coalició de $t-1$ mentiders (que no coneixen el secret) menteixi amb èxit amb una probabilitat menor o igual que ϵ, té una taxa d'informació menor o igual que

$$\log q / \log(1 + (q-1)/\epsilon)$$

amb $q = |\mathcal{K}|$. Un resultat semblant es dóna per un esquema en el qual la probabilitat és per una coalició que coneix el valor del secret. En aquest cas es troba que la taxa d'informació és menor o igual que

$$\log q / \log(1 + (q-1)/\epsilon^2)$$

També es pot donar el cas que sigui mentider el distribuïdor que lliura fragments falsos a alguns participants. D'aquesta forma pot passar que certs subconjunts autoritzats recuperin secrets correctament però diferents. Nosaltres no hem considerat aquesta possibilitat de forma que suposem que el distribuïdor serà en tot moment honest.

Un dels inconvenients dels esquemes classics és el de la gran longitud dels fragments que es lliuren als participants en realitzar certes estructures. Una possibilitat per aconseguir fragments de menor longitud és la de condicionar la seguretat del sistema a la capacitat de càlcul dels participants. Així s'estan considerant esquemes computacionalment segurs que reparteixen fragments menors que els incondicionalment segurs. Els esquemes *computacionalment segurs* són aquells en els quals l'obtenció d'informació sobre el valor del secret, per part de participants no autoritzats, depén dels recursos computacionals dels quals disposin.

Dos problemes més que pateixen els esquemes per a compartir secrets és el de la *renovació* dels fragments, consistent en que no es pot renovar el secret compartit sense modificar els fragments repartits i el de la *reutilització* consistent en que no es poden fer servir els fragments lliurats per tal de recuperar un nou secret després d'haver recuperat el secret en curs. Per resoldre tots dos problemes s'han proposat els *esquemes dinàmics* [55]. Una variant dels esquemes dinàmics és l'esquema *totalment dinàmic* presentat a [14], en el qual un únic missatge enviat a tots els participants permet reconstruir diferents secrets en diferents moments. També s'han estudiat *esquemes per a compartir diversos secrets no independents* de forma simultània a [21]. Un altre plantejament és el dels *esquemes multi secret* en els quals diferents secrets estan associats amb diferents famílies de subconjunts autoritzats [48, 50]. Esquemes en els quals es reparteixen diferents secrets de forma que es poden reconstruir per separat s'anomenen esquemes per a compartir secrets de *multi-estat* i són tractats en [43]. Una altra variant de la mateixa idea de repartir diferent secrets és la dels *preposicionats* [88]. Els *esquemes per a compartir secrets anònims* van ser proposats a [96] com a intent de modelar un esquema per a compartir secrets en el qual no cal que els participants que intenten recuperar el secret s'identifiquin davant de la caixa negra que computarà el secret. La identificació de cada participant es fa normalment amb un fragment públic. Un estudi d'aquest tipus d'esquemes es pot trobar a [22]. També s'han proposat esquemes en els quals no és necessària l'acció d'un distribuidor [49].

La darrera extensió del concepte d'esquema per a compartir secrets és la *criptografia visual*, en la qual es construeix un esquema per a compartir secrets que reparteix una imatge secreta en diferents imatges, cadascuna com

a fragment d'un participant. L'algorisme recuperador de l'esquema consisteix en superposar les imatges dels participants com si fossin transparències amb la finalitat de definir el grau de gris que correspon a cada pixel. L'ull humà s'ocuparà de recuperar la imatge secreta fent la composició total [62, 2, 3]. Un dels camps d'aplicació de la criptografia visual és la *identificació humana* [52].

S'han proposat esquemes en els quals certes minories de participants poden vetar la reconstrucció del secret [10, 17], els anomenats *esquemes amb capacitat de vet*. Els esquemes que estan preparats per la sortida de participants sense que això faci el sistema vulnerable són els anomenats *esquemes per a compartir secrets amb capacitat de desenrolament*, estudiats a [12] per esquemes de llindar.