Capítol 3

Esquemes segurs enfront de mentiders

En un esquema per a compartir secrets pot donar-se el fenòmen de l'existència de mentiders. Els *esquemes segurs enfront de mentiders* són esquemes per a compartir secrets en els quals l'algorisme recuperador avisa de l'existència de mentiders. Un *mentider* és un participant que lliura un fragments fals.

Dintre dels possibles sabotatges que es poden esperar d'un mentider, o d'una coalició d'aquests, s'han distingit dues situacions: sabotatge quan coneixen el secret i sabotatge quan no el coneixen. Com a paràmetres per a avaluar les prestacions de l'esquema hem de destacar unes quantes. La primera d'elles és si detecta els mentiders i amb quina probabilitat els detecta. També en el cas que els detecti si els pot identificar. En el cas que no els detecti, si es pot fer una apropiació indeguda o no.

S'han fet diverses propostes d'esquemes amb seguretat contra l'acció de mentiders, les més importants de les quals, s'han destacat a la Secció 2.9. Tots aquests esquemes realitzen estructures de llindar, per la qual cosa ens hem proposat de trobar esquemes amb certs nivells de seguretat per estructures més àmplies. Per la seva manejabilitat, hem escollit les estructures d'espai vectorial (veure Secció 2.4), les quals generalitzen les estructures de llindar. El primer dels esquemes és un esquema que detecta mentiders amb una certa probabilitat si no coneixen el secret. El segon és un esquema que detecta mentiders fins i tot en el cas que coneguin quin és el secret repartit. L'ús d'estructures d'espai vectorial ens ha permés fer una generalització per estructures qualssevol.

Abans de fer la descripció dels tres esquemes proposats hem fet la definició formal de probabilitat de mentir i de la seguretat en esquemes en els quals els mentiders no coneguin el secret repartit i en el cas que sí el coneguin. Hem

trobat una fita per a la taxa òptima d'informació pel primer cas. Aquests resultats han estat estudiats per altres autors només per estructures de llindar.

Els dos primers esquemes han estat l'objecte d'estudi del Projecte Final de Carrera de l'*Escola Tècnica Superior d'Enginyeria de Telecomunicacions de Barcelona* [65]. En aquest projecte s'han implementat aquests esquemes i s'han estudiat diverses propietats d'ells.

3.1 Esquemes (Γ, δ)-segurs i (Γ, ϵ)-robustos

Entendrem que un participant $p \in A$ amb $A \in \Gamma$ és *enganyat amb uns fragments* que lliuren $A - \{p\}$, si l'algorisme recuperador no identifica aquests fragments com a invàlids i es recupera un secret incorrecte.

Seguint [64], direm que un esquema per a compartir secrets amb estructura d'accés Γ és (Γ, δ)-*segur* si per a qualsevol subconjunt minimal autoritzat $A \in \Gamma$ i per a qualsevol $p \in A$, la probabilitat que els participants de $A - \{p\}$, que no coneixen el secret, enganyin el participant p és com a màxim δ, això és,

$$\Pr_1(A - \{p\} \text{ enganyin }) \leq \delta$$

aquesta *probabilitat d'enganyar* quan els mentiders no coneixen el secret és, per definició,

$$\Pr_1(A - \{p\} \text{ enganyin }) = E_b\left(\max_{b'}\left(\Pr\left(p \text{ és enganyat amb } b' | A - \{p\} \text{ tenen } b\right)\right)\right)$$

on b denota el conjunt de fragments rebuts pels participants de $A - \{p\}$ i b' denota els fragments modificats utilitzats pels participants de $A - \{p\}$ per tal d'enganyar el participant p. Notem que la probabilitat d'enganyar és el valor esperat d'una variable aleatòria que, per a cada b assigna la probabilitat màxima d'enganyar al participant p amb uns fragments b'. La idea que hi ha al darrera de la definició de probabilitat d'enganyar és la següent: la coalició de mentiders, amb el coneixement dels seus fragments (b), busquen quin és el conjunt de fragments modificat b' que poden lliurar per tal d'aconseguir que la probabilitat que s'enganyi al participant p sigui el més gran possible; el valor esperat d'aquesta probabilitat màxima és la probabilitat d'enganyar.

Si suposem que els participants de $A - \{p\}$ coneixen el secret, definim seguint [31], la probabilitat que els participants de $A - \{p\}$ enganyin el participant p, denotada per $\Pr_2(A - \{p\} \text{ enganyar })$, com

$$E_{b,k}\left(\max_{b'}\left(\Pr\left(p \text{ és enganyat amb } b' | A - \{p\} \text{ tenen } b, \text{ el secret és } k\right)\right)\right).$$

Direm que un esquema per a compartir secrets amb estructura d'accés Γ és (Γ, ϵ)-*robust* si per a qualsevol subconjunt minimal autoritzat $A \in \Gamma$, per a qualsevol $p \in A$, la probabilitat que els participants de $A - \{p\}$, que coneixen el secret, enganyin el participant p és com a màxim ϵ, això és, $\Pr_2(A - \{p\} \text{ enganyin }) \leq \epsilon$.

Quan l'estructura d'accés Γ és una (r, n)-estructura d'accés de llindar (Γ, δ)-segura llavors es diu que un esquema és (r, n, δ)-*segur*. El mateix es defineix quan l'esquema per l'estructura de llindar Γ és robust: per una (r, n)-estructura d'accés de llindar es diu que un esquema és (r, n, ϵ)-*robust* quan és un esquema (Γ, ϵ)-robust.

Ogata i Kurosawa han trobat fitacions per a la taxa d'informació d'esquemes de llindar (r, n, δ)-segurs [64]. La proposició següent troba la fita màxima per a la taxa d'informació òptima d'un esquema (Γ, δ)-segur. Aquesta fita va ser provada a [64] per estructures de llindar.

Proposició 3.1.1 *Qualsevol esquema per a compartir secrets (Γ, δ)-segur amb $q = |\mathcal{K}|$ té taxa d'informació menor o igual que*

$$\frac{\log q}{\log(1 + \frac{q-1}{\delta})}$$

Demostració: Sigui $A = \{p_1, p_2, \ldots, p_r\} \in \Gamma$ amb $r \geq 2$, un subconjunt minimal autoritzat. Siguin $s_i \in \mathcal{S}_i$, amb $1 \leq i \leq r$, els fragments que reben quan es reparteix un secret k. Considerem la funció

$$\chi : \mathcal{S}_r \longrightarrow \mathcal{K} \cup \{w\}$$

tal que $\chi(s'_r) = k' \in \mathcal{K}$ si $s_1, s_2, \ldots, s_{r-1}, s'_r$ determinen un secret $k' \in \mathcal{K}$ i $\chi(s'_r) = w \notin \mathcal{K}$ altrament. Atès que no es pot obtenir cap informació dels fragments $s_1, s_2, \ldots, s_{r-1}$, per a tot $k^* \in \mathcal{K} - \{k\}$, existeix almenys un $s_r^* \in \mathcal{S}_r - \{s_r\}$ tal que $\chi(s_r^*) = k^*$. Conseqüentment, $|\chi^{-1}(\mathcal{K} - \{k\})| \geq q - 1$.

Els participants de $A - \{p_1\}$ poden enganyar el participant p_1 simplement escollint aleatòriament un fragment fals $s_r^* \in \mathcal{S}_r - \{s_r\}$. En aquest cas,

$$\Pr(\chi(s_r^*) = k^* \in \mathcal{K} - \{k\}) = \frac{|\chi^{-1}(\mathcal{K} - \{k\})|}{|\mathcal{S}_r| - 1} \geq \frac{q-1}{|\mathcal{S}_r| - 1}$$

A partir d'aquí, per qualssevol fragments $b = (s_2, \ldots, s_r)$ pels participants de $A - \{p_1\}$, la màxima probabilitat d'enganyar p_1, entre tots els fragments possibles b', és almenys $(q-1)/(|\mathcal{S}_r| - 1)$. Com que el valor esperat d'aquesta probabilitat màxima és com a molt δ, tenim que $\delta \geq (q-1)/(|\mathcal{S}_r| - 1)$. Llavors,

atès que p_r pot ser qualsevol participant, per a tot participant $p_i \in P$, $|\mathcal{S}_i| \geq 1 + (q-1)/\delta$.□

Pels esquemes (r, n, ϵ)-robustos, Carpentieri, De Santis i Vaccaro a [31] proven que si la probabilitat de mentir és menor que $\epsilon > 0$ aleshores cal lliurar als participants fragments de longitud com a mínim la del secret més $\log(1/\epsilon)$. Ogata i Kurosawa a [64] i també Blundo i De Santis a [16] han donat fitacions per a la taxa òptima d'informació. Aquesta fitació afirma que tot esquema (r, n, ϵ)-robust té taxa òptima d'informació menor igual que $\log q / \log(1 + (q-1)/\epsilon^2)$.

3.2 Un esquema vectorial (Γ, δ)-segur

En aquesta secció, presentem un esquema (Γ, δ)-segur per a compartir secrets que pot ser implementat en qualsevol estructura d'accés d'espai vectorial. En aquest esquema, la probabilitat de mentir és $\delta = 1/q$, a on $q = |\mathcal{K}|$. La taxa d'informació d'aquest esquema és igual a 1/2. Suposem que el distribuïdor és honest i que utilitzem per a computar el secret una caixa negra completament segura. La descripció de l'esquema que presentem queda condensada al quadre següent:

Esquema (Γ, δ)-segur
per una estructura d'espai vectorial
Algorisme distribuïdor: sigui un secret $k \in \mathcal{K} = GF(q)$.
El distribuïdor agafa aleatòriament
$\mathbf{v}_1, \mathbf{v}_2 \in E$, tals que $\mathbf{v}_1 \cdot \psi(D) = k$, i $\mathbf{v}_2 \cdot \psi(D) = k^2$.
$p_i \longmapsto (s_i, t_i) = (\mathbf{v}_1 \cdot \psi(p_i), (\mathbf{v}_2 \cdot \psi(p_i))$
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:
$k_1 = \lambda_1 s_1 + \lambda_2 s_2 + \ldots + \lambda_\ell s_\ell$ i
$k_2 = \lambda_1 t_1 + \lambda_2 t_2 + \ldots + \lambda_\ell t_\ell$
Si $k_1^2 = k_2$ la caixa negra retorna k_1
com a valor correcte del secret.
Altrament informa de l'existència de mentiders.

Sigui $E = K^r$ un espai vectorial sobre un cos finit de q elements $K = GF(q)$ de característica diferent de 2. Sigui Γ l'estructura d'accés d'espai vectorial

definida per la funció

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

El distribuïdor D agafa aleatòriament un secret $k \in K$ i els vectors $\mathbf{v}_1, \mathbf{v}_2 \in E$ tals que $k = \mathbf{v}_1 \cdot \mathbf{x}_0$ i $k^2 = \mathbf{v}_2 \cdot \mathbf{x}_0$, on $\mathbf{x}_0 = \psi(D)$ i $\mathbf{x}_i = \psi(p_i)$ $(1 \leq i \leq n)$. Després d'això, D calcula $s_i = \mathbf{v}_1 \cdot \mathbf{x}_i$, $t_i = \mathbf{v}_2 \cdot \mathbf{x}_i$ i dóna el fragment (s_i, t_i) al participant p_i, per a cada $i = 1, \ldots, n$.

Sigui $A = \{p_1, \ldots, p_\ell\} \in \Gamma$ un subconjunt autoritzat i $\mathbf{x}_0 = \lambda_1 \mathbf{x}_1 + \lambda_2 \mathbf{x}_2 + \ldots + \lambda_\ell \mathbf{x}_\ell$. Quan els participants de A introdueixen els seus fragments, la caixa negra computa $k_1 = \lambda_1 s_1 + \lambda_2 s_2 + \ldots + \lambda_\ell s_\ell$ i $k_2 = \lambda_1 t_1 + \lambda_2 t_2 + \ldots + \lambda_\ell t_\ell$. Si $k_1^2 = k_2$, la caixa negra retorna k_1 com a valor correcte del secret. Els participants són avisats de l'existència de mentiders si $k_1^2 \neq k_2$. En aquest segon cas, els valors k_1 i k_2 han de mantenir-se en secret, això és, cal que la caixa negra els destrueixi.

El primer dels resultats sobre aquest esquema afirma que es tracta d'un esquema perfecte de taxa d'informació 1/2.

Proposició 3.2.1 *Aquest esquema és un esquema perfecte per a compartir secrets amb estructura d'accés* Γ *i taxa d'informació igual a* $\frac{1}{2}$.

Demostració: És fàcil veure que els participants de qualsevol subconjunt $A \in \Gamma$ poden reconstruir el secret a partir dels seus fragments. D'altra banda, si els participants de $A = \{p_1, p_2, \ldots, p_\ell\} \notin \Gamma$ intenten reconstruir el secret a partir dels seus fragments, han de deduir el valor de $k = \mathbf{v}_1 \cdot \mathbf{x}_0$ a partir del sistema d'equacions

$$\left.\begin{array}{l} s_1 = \mathbf{v}_1 \cdot \mathbf{x}_1 \\ s_2 = \mathbf{v}_1 \cdot \mathbf{x}_2 \\ \ldots \\ s_\ell = \mathbf{v}_1 \cdot \mathbf{x}_\ell \end{array}\right\}, \quad \left.\begin{array}{l} t_1 = \mathbf{v}_2 \cdot \mathbf{x}_1 \\ t_2 = \mathbf{v}_2 \cdot \mathbf{x}_2 \\ \ldots \\ t_\ell = \mathbf{v}_2 \cdot \mathbf{x}_\ell \end{array}\right\}, \quad (\mathbf{v}_1 \cdot \mathbf{x}_0)^2 = \mathbf{v}_2 \cdot \mathbf{x}_0$$

on les incògnites són $\mathbf{v}_1$ i $\mathbf{v}_2$. A partir de $\mathbf{x}_0 \notin \langle \mathbf{x}_1, \ldots, \mathbf{x}_\ell \rangle$, no és difícil comprovar que $k = \mathbf{v}_1 \cdot \mathbf{x}_0$ pot prendre tots els valors de K amb la mateixa probabilitat. Per tant els participants de qualsevol $A \notin \Gamma$ no tenen absolutament cap informació sobre el secret. La taxa d'informació es troba fàcilment si es té en compte que els secrets estan presos uniformement a K i els fragments estan presos uniformement a K^2.□

La seguretat enfront de mentiders d'aquest esquema està determinada a la proposició següent

Proposició 3.2.2 *L'esquema és* (Γ, δ)*-segur amb* $\delta = 1/q$.

Demostració: Sigui $A = \{p_1, p_2, \ldots, p_\ell\} \in \Gamma$ un subconjunt minimal autoritzat i sigui $T = \{p_1, \ldots, p_{\ell-1}\} \subset A$, una coalició de mentiders. Evidentment, $T \notin \Gamma$. Suposem que els participants de T no coneixen el secret. Si els participants de T donen fragments falsos $(s_i^*, t_i^*) = (s_i + \epsilon_i, t_i + \delta_i)$, la caixa negra computa

$$k_1 = \sum_{i=1}^{\ell} \lambda_i s_i + \sum_{i=1}^{\ell-1} \lambda_i \epsilon_i = k + \sum_{i=1}^{\ell-1} \lambda_i \epsilon_i$$

i

$$k_2 = \sum_{i=1}^{\ell} \lambda_i t_i + \sum_{i=1}^{\ell-1} \lambda_i \delta_i = k^2 + \sum_{i=1}^{\ell-1} \lambda_i \delta_i.$$

Això és, els participants poden escollir qualsevol parell d'elements $\epsilon, \delta \in K$, $\epsilon \neq 0$, i modificar els seus fragments de tal manera que els valors calculats per la caixa negra són $k_1 = k + \epsilon$ i $k_2 = k^2 + \delta$. Els mentiders no seran detectats si i només si $k_1^2 = k_2$, això és, si i només si $2k\epsilon + \epsilon^2 = \delta$. Com que no coneixen el valor de k, la probabilitat de trobar un parell de valors adients (ϵ, δ) és $1/q$. Per tant,

$$\max_{b'} \Pr(p_\ell \text{ és enganyat amb } b' | T \text{ tenen } b) = \frac{1}{q}$$

per a qualsevol valor b dels fragments dels participants de T. □

Aquest primer esquema que hem proposat només és capaç de detectar mentiders que no coneguin el secret. A partir de l'equació $2k\epsilon + \epsilon^2 = \delta$, podem veure que una coalició de mentiders que coneguin el secret k poden trobar fragments falsos per tal d'enganyar el participant honest sense ser detectats.

S'observa que el nostre esquema és (Γ, δ)-segur amb $\delta = 1/q$ i té taxa d'informació $1/2$, la qual és molt propera a la fita inferior $\log q / \log(q^2 - q + 1)$ donada a la Proposició 4.1.1. De fet, és asimptòticament òptima perquè

$$\lim_{q \to \infty} \frac{\log q}{\log(q^2 - q + 1)} - \frac{1}{2} = 0.$$

Quan K és un cos de característica 2, no podem proposar una modificació similar de l'esquema d'espai vectorial per a compartir secrets per tal de obtenir un esquema $(\Gamma, 1/q)$-segur. Suposem que el distribuïdor assigna fragments (s_i, t_i) corresponents a un parell $(k, f(k))$ per certa $f : K \longrightarrow K$ (a l'esquema que hem proposat, $f(k) = k^2$). Si una coalició de mentiders tracta de mentir, la caixa negra obtindrà $k_1 = k + \epsilon$, $k_2 = f(k) + \delta$ tot seguit comprovant si $f(k_1) = k_2$, això és, si $f(k + \epsilon) = f(k) + \delta$. Si f és tal que la probabilitat de mentir és

$1/q$, aleshores, per a qualsevol $\epsilon \neq 0$ fixat, l'aplicació $\delta(k) = f(k+\epsilon) - f(k)$ ha de ser bijectiva, en contradicció amb el fet que $\delta(k+\epsilon) = f(k) - f(k+\epsilon) = \delta(k)$.

Ogata i Kurosawa [64] van proposar un esquema (Γ, δ)-segur amb $\delta = 1/q$, i taxa d'informació òptima, això és, igual a la fita inferior donada a la Proposició 4.1.1. Malgrat que Ogata i Kurosawa consideren només estructures d'accés de llindar, el seu esquema pot ser realitzat en qualsevol estructura d'accés d'espai vectorial.

Si volem comparar el temps de computació d'ambdós esquemes, hem de tenir en compte que treballen per valors diferents de q. En el nostre esquema, q ha de ser una potència de primer diferent de 2 mentre que a l'esquema de Ogata i Kurosawa q ha de ser tal que $q-1$ sigui una potència de primer i $q^2 - q + 1$ sigui un primer. Això no obstant, podem comparar el temps de computació d'aquests esquemes quan tenen un cardinal similar els conjunts de secrets i realitzen la mateixa estructura d'accés d'espai vectorial. Això és, compararem, per a una estructura d'accés d'espai vectorial donada, l'esquema de Ogata i Kurosawa amb q_1 secrets i el nostre esquema amb q_2 secrets, on q_1 i q_2 són similars (per exemple, tenen la mateixa longitud en bits).

A l'esquema de Ogata i Kurosawa el conjunt de secrets és un conjunt de diferències planar a $\mathbb{Z}_{q_1^2-q_1+1}$. La manera coneguda per a obtenir aquest conjunt de diferències planar és prendre els q_1 punts en una recta en el pla projectiu $PG(2, q_1 - 1)$ (veure [61]). Si considerem aquests punts com a elements de $GF((q_1-1)^3)$, els podrem escriure com $\alpha^{d_0}, \alpha^{d_1}, \ldots, \alpha^{d_{q_1-1}}$, on α és un element primitiu de $GF((q_1-1)^3)$. Llavors $\{d_0, d_1, \ldots, d_{q_1-1}\}$ és un conjunt de diferències planar mòdul $q_1^2 - q_1 + 1$.

Per a valors grans de q_1, és inefectiu emmagatzemar tots els elements del conjunt de diferències planar. Aleshores, podem prendre una recta $Ax + By + Cz = 0$ en el pla projectiu $PG(2, q_1-1)$ com a conjunt de secrets. A l'algorisme distribuïdor, el distribuïdor pren el punt $(x, y, z) = \alpha^k$ de la recta $Ax + By + Cz = 0$, calcula k mòdul $q_1^2 - q_1 + 1$ i calcula fragments corresponents a k en l'esquema per a compartir secrets d'espai vectorial sobre el cos $\mathbb{Z}_{q_1^2-q_1+1}$. S'observa que, per tal de trobar k, n'hi ha prou en calcular un logaritme discret en base α d'un element de $GF((q_1-1)^3)$. Per tal d'evitar el càlcul del logaritme discret, podem procedir de la manera següent: donat un secret $k \in \mathbb{Z}_{q_1^2-q_1+1}$, el distribuïdor agafa aleatòriament $A, B, C \in GF(q_1-1)$ tals que α^k pertanyi a la recta $Ax + By + Cz = 0$, distribueix com abans els fragments corresponents a k, i fa públics els valors de A, B i C.

A l'algorisme de reconstrucció, la validesa del secret k ha de ser verificada. Aleshores, α^k ha de ser calculada per tal de comprovar si és un punt de la recta $Ax + By + Cz = 0$.

Per tant, en el millor cas, el temps de computació de l'esquema de Ogata i Kurosawa és igual que el temps de computació de l'esquema per a compartir secrets d'espai vectorial sobre el cos $\mathbb{Z}_{q_1^2-q_1+1}$ més una exponenciació adicional en el cos $GF((q_1-1)^3)$ en els algorismes de distribució i de reconstrucció.

El temps de computació en el nostre esquema és, en els algorismes de distribució i reconstrucció, dues vegades el temps de computació de l' espai vectorial esquema per a compartir secrets d'espai vectorial sobre el cos $GF(q_2)$ més els temps de càlcul d'un quadrat.

Utilitzant que $\log(q_1^2-q_1+1)$ és aproximadament $2\log q_2$ les multiplicacions en $GF(q_1^2-q_1+1)$ són quatre vegades més que les multiplicacions en $GF(q_2)$. Llavors, el temps de computació a causa de l'aplicació de l'esquema per a compartir secrets d'espai vectorial és en el nostre esquema dues vegades més ràpid que el de Ogata i Kurosawa. La mitjana de temps de computació de la exponenciació modular és equivalent a $1.5\log_2(q_1^2-q_1+1)$ multiplicacions en el cos amb $(q_1-1)^3$ elements, que és aproximadament $27\log_2(q_2)$ multiplicacions en el cos amb q_2 elements. Aleshores, la part de verificació dels algorismes és en el nostre esquema aproximadament $27\log_2(q_2)$ vegades més ràpid que el de Ogata i Kurosawa.

3.3 Un esquema de llindar (r, n, ϵ)-robust

El segon esquema que presentem en aquesta secció és un esquema de llindar (r, n, ϵ)-robust on la probabilitat de mentir ϵ és com a màxim $(2r-3)/(q-r)$.

Descriurem l'esquema de llindar (r, n) que proposem com a modificació de l'esquema de llindar (r, n) de Shamir. Al començament, el distribuïdor escull aleatòriament i independentment n diferents i no nuls elements $x_1, x_2, \ldots, x_n$ del cos finit $K = GF(q)$. Aquests valors són guardats en secret. Per a qualsevol valor donat del secret $k \in K$, el distribuïdor pren independentment i aleatòriament dos polinomis $\phi_1(x)$ i $\phi_2(x)$ amb grau com a màxim $r-1$ tals que $k = \phi_1(0)$ i $k^2 = \phi_2(0)$. Llavors, el participant p_i rep el fragment (x_i, s_i, t_i), on $s_i = \phi_1(x_i)$ i $t_i = \phi_2(t_i)$, per $1 \leq i \leq n$. Això és, dos secrets, k i k^2 són distribuïts seguint l'esquema polinomial de Shamir i, a més, els valors x_i, els quals són públics a l'esquema de Shamir, són guardats en secret. Resumim l'esquema per a compartir secrets:

Esquema (r, n, ϵ)-robust
Algorisme distribuïdor:
S'escullen aleatòria i independentment n
diferents i no nuls elements$x_1, x_2, \ldots, x_n \in GF(q)$
Sigui un secret $k \in \mathcal{K} = GF(q)$.
Generem els nombres aleatoris
$a_1, \ldots, a_{r-1} \in GF(q)$
A partir dels polinomis
$\phi_1(x) = k + a_1 x + \ldots + a_{r-1} x^{r-1}$
$\phi_2(x) = k + a_1 x + \ldots + a_{r-1} x^{r-1}$
es reparteix
$p_i \longmapsto (x_i, s_i, t_i) = (x_i, \phi_1(x_i), \phi_2(x_i))$
Algorisme recuperador: es fa
interpolació polinòmica, recuperant k_1, k_2
Si $k_1^2 = k_2$ la caixa negra retorna k_1
com a valor correcte del secret.
Altrament informa de l'existència de mentiders.

Aquest esquema pot ser vist com a una variació de l'esquema presentat a la Secció 4.2. L'única diferència és que, en aquest segon esquema, la funció

$$\begin{array}{rccl} \psi: & P \cup \{D\} & \longrightarrow & K^r \\ & D & \longmapsto & \mathbf{x}_0 = (1, 0, 0, \ldots, 0) \\ & p_i & \longmapsto & \mathbf{x}_i = (1, x_i, x_i^2, \ldots, x_i^{r-1}) \end{array}$$

no és coneguda públicament, perquè el distribuïdor guarda en secret els valors $x_1, x_2, \ldots, x_n \in K$.

Degut a aquesta similitud, les dues proposicions següents són conseqüències de la Proposició 4.2.1 i de la Proposició 4.2.2.

Proposició 3.3.1 *Aquest esquema és un esquema perfecte de llindar (r, n) amb taxa d'informació igual a $\frac{1}{3}$.*

Proposició 3.3.2 *L'esquema és (r, n, δ)-segur amb $\delta = 1/q$.*

En aquest esquema els mentiders poden ser detectats també si coneixen el secret i intenten enganyar a un participant honest. Necesitem el lema següent, el qual es prova utilitzant interpolació de Lagrange.

Lema 3.3.3 *Si $x_1, \ldots, x_{r-1}, x_r$ són elements de K diferents i no nuls i $\phi(x)$ és un polinomi de grau com a màxim $r-1$ tal que $\phi(x_i) = s_i$, $(1 \leq i \leq r)$, aleshores tenim*

$$\phi(0) = x_r \gamma_r(0) \left(\sum_{i=1}^{r-1} \frac{s_i}{(x_i - x_r)\Gamma_r'(x_i)} + \frac{s_r}{\Gamma_r(x_r)} \right),$$

on $\gamma_r(x) = (x - x_1) \cdots (x - x_{r-1})$ i $\Gamma_r(x) = x\gamma_r(x)$.

Demostració: A partir de la fórmula d'interpolació de Lagrange,

$$\phi(x) = \sum_{i=1}^{r} s_i \prod_{k=1, k\neq i}^{r} \frac{x - x_k}{x_i - x_k}$$

Tenint en compte que $\gamma_r(0) = \prod_{k=1}^{r-1}(-x_k)$, $\Gamma_r'(x_i) = x_i \prod_{k=1,k\neq i}^{r-1}(x_i - x_k)$, on $1 \leq i \leq r-1$, és fàcil comprovar que

$$\phi(0) = \sum_{i=1}^{r} s_i \prod_{k=1, k\neq i}^{r} \frac{-x_k}{x_i - x_k} = x_r \gamma_r(0) \left(\sum_{i=1}^{r-1} \frac{s_i}{(x_i - x_r)\Gamma_r'(x_i)} + \frac{s_r}{\Gamma_r(x_r)} \right) \square$$

Proposició 3.3.4 *L'esquema és (r, n, ϵ)-robust amb $\epsilon \leq (2r-3)/(q-r)$.*

Demostració: Suposem que una coalició $T = \{p_1, p_2 \ldots, p_{r-1}\}$ de participants intenten enganyar al participant p_r donant fragments falsos (x_i^*, s_i^*, t_i^*), $(1 \leq i \leq r-1)$ a l'hora de reconstruir el secret. A partir dels seus fragments i el secret, els participants de T poden trobar els polinomis $\phi_1(x)$ i $\phi_2(x)$ que van ser utilitzats pel distribuïdor per generar els fragments. Malgrat tot, com que ells no coneixen el valor de x_r, no poden determinar el fragment del participant p_r.

Per tal de trobar una fita superior per la probabilitat d'enganyar amb èxit, considerem els polinomis ϕ_1^* i ϕ_2^* amb grau com a màxim $r-1$ tal que $\phi_1^*(0) = k$, $\phi_2^*(0) = k^2$, $\phi_1^*(x_i^*) = s_i^*$ i $\phi_2^*(x_i^*) = t_i^*$, $1 \leq i \leq r-1$. A més a més, siguin $s_r^* = \phi_1^*(x_r)$ i $t_r^* = \phi_2^*(x_r)$. Pel Lema 4.3.3 se segueix que

$$k = x_r \gamma_r(0) \left(\sum_{i=1}^{r-1} \frac{s_i^*}{(x_i^* - x_r)\Gamma_r'(x_i^*)} + \frac{s_r^*}{\Gamma_r(x_r)} \right)$$

i

$$k^2 = x_r \gamma_r(0) \left(\sum_{i=1}^{r-1} \frac{t_i^*}{(x_i^* - x_r)\Gamma_r'(x_i^*)} + \frac{t_r^*}{\Gamma_r(x_r)} \right),$$

on $\gamma_r(x) = (x - x_1^*) \cdots (x - x_{r-1}^*)$ i $\Gamma_r(x) = x\gamma_r(x)$. Si p_r és honest, la caixa negra calcularà

$$k_1 = x_r\gamma_r(0)\left(\sum_{i=1}^{r-1} \frac{s_i^*}{(x_i^* - x_r)\Gamma_r'(x_i^*)} + \frac{s_r}{\Gamma_r(x_r)}\right) = k + \frac{x_r\gamma_r(0)}{\Gamma_r(x_r)}(s_r - s_r^*)$$

i

$$k_2 = k^2 + \frac{x_r\gamma_r(0)}{\Gamma_r(x_r)}(t_r - t_r^*).$$

L'engany no serà detectat si i només si $\gamma_r(x_r) \neq 0$ i $k_1^2 = k_2$, això és, si i només si $\gamma_r(x_r) \neq 0$ i

$$2k\frac{\phi_1(x_r) - \phi_1^*(x_r)}{\gamma_r(x_r)} + \frac{\gamma_r(0)}{\gamma_r^2(x_r)}(\phi_1(x_r) - \phi_1^*(x_r))^2 = \frac{\phi_2(x_r) - \phi_2^*(x_r)}{\gamma_r(x_r)}.$$

Aleshores, els mentiders són detectats si i només si $\gamma_r(x_r) \neq 0$ i x_r és una arrel del polinomi

$$\Phi(x) = 2k\gamma_r(x)(\phi_1(x) - \phi_1^*(x)) + \gamma_r(0)(\phi_1(x) - \phi_1^*(x))^2 - \gamma_r(x)(\phi_2(x) - \phi_2^*(x)).$$

Com que $\deg(\Phi) \leq 2r - 2$ i 0 és una arrel de Φ, x_r pot prendre com a màxim $2r - 3$ valors. Per tant, la probabilitat de mentir amb èxit és com a màxim $(2r - 3)/(q - r)$.□

L'esquema (r, n, ϵ)-robust que hem presentat aquí millora el proposat per Tompa i Woll [98] en dos punts: aquest té millor taxa d'informació i és computacionalment més eficient.

Considerem l'esquema (r, n, ϵ)-robust de Tompa i Woll amb $\epsilon = (2r - 3)/(q - r)$, on q és el nombre de secrets. En aquest esquema, el cardinal del conjunt de fragments de qualsevol participant és p^2, on p és una potència de primer tal que

$$p \geq \frac{(q-1)(q-r)(r-1)}{2r-3} + r.$$

En el nostre esquema, el conjunt de fragments té q^3 elements. A partir de $r \geq 2$, tenim que $p^2 > (q - r)^4/4$ i, llavors, $p^2 > q^3$ si $q > \max\{2r, 64\}$. Aleshores, el nostre esquema té en general millor taxa d'informació que la de l'esquema de Tompa i Woll. A més, per valors grans de q, la taxa d'informació de l'esquema de Tompa i Woll és proper a $1/4$ i la taxa d'informació del nostre esquema és $1/3$.

Per tal comparar el temps de computació d'ambdós esquemes, observem que en el nostre esquema hem d'executar dues vegades l'esquema de Shamir

sobre $GF(q)$ i que l'esquema de Tompa i Woll és bàsicament l'esquema Shamir sobre $GF(p)$. Com que $\log p$ és proper a $2\log q$ per valors grans de q, les multiplicacions en $GF(p)$ són quatre vegades el nombre de multiplicacions en $GF(q)$. Per tant, el temps de computació de l'esquema de Tompa i Woll és aproximadament dues vegades el temps de computació del nostre esquema.

Ogata i Kurosawa [64] van trobar una fita en el nombre possible de fragments per a un esquema (r, n, ϵ)-robust. Aquesta fita és

$$|\mathcal{S}_p| \geq \frac{|\mathcal{K}| - 1}{\epsilon^2} + 1.$$

Ells no proposen cap esquema robust. En el nostre esquema $\epsilon = (2r-3)/(q-r)$ i el valor corresponent de la fita és

$$|\mathcal{S}_p| \geq \frac{(q-1)(q-r)^2}{(2r-3)^2} + 1 = O(q^3).$$

Aquest esquema també ha estat objecte d'estudi del Projecte Final de Carrera realitzat a l'*Escola Tècnica Superior d'Enginyeria de Telecomunicacions de Barcelona* [65].

3.4 Esquema (Γ, δ)-segur per estructures qualsevol

En aquesta secció, a partir de l'expressió de tota estructura com a estructura d'espai vectorial generalitzat amb $\dim \psi(D) = 1$ (fent servir la Proposició 2.4.3), hem obtingut un esquema (Γ, δ)-segur per a qualsevol estructura d'accés Γ. Aquest esquema és una generalització de l'esquema presentat a la Secció 4.2.

Sigui Γ una estructura d'accés qualsevol. Segons hem fet notar a la Secció 2.2 pot ser realitzada per un esquema d'espai vectorial generalitzat amb dimensió de la imatge del distribuïdor igual a 1. Aquesta construcció es fa amb la tècnica dels duals de Martin, Jackson i Simmons[91] que hem condensat a la Proposició 2.4.3. També hem comentat a la Proposició 2.4.4 que una manera d'expressar qualsevol estructura d'accés com a estructura d'espai vectorial generalitzat amb dimensió de la imatge del distribuïdor igual a 1 és recobrint amb estructures d'espai vectorial clàssiques la nostra estructura. Una possible via per generar aquestes estructures és anar recobrint per estrelles tal com s'han definit a la Secció 3.4.1.

La implementació del recobriment per estrelles d'una estructura i la resolució del conseqüent problema de programació lineal ha estat motiu de la realització d'un Projecte Final de Carrera a l'*Escola Tècnica Superior d'Enginyeria de Telecomunicacions de Barcelona* [28].

Podem generalitzar l'esquema segur enfront de mentiders presentat a la Secció 4.2 per la nostra estructura d'espai vectorial generalitzat amb $\dim \psi(D) = 1$. Així tindrem construït un esquema (Γ, δ)-segur per un estructura d'accés qualsevol.

Sigui el conjunt de secrets $\mathcal{K} = GF(q)$ un cos finit de característica diferent de 2, $E = (GF(q))^r$ un espai vectorial, $\mathsf{S}(E)$ el conjunt dels subespais de E i Γ una estructura d'accés que ve definida per

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

com a estructura d'espai vectorial generalitzada. Fixem una base per a cada $\psi(p)$ per $p \in P \cup \{D\}$. Donat un secret $k \in \mathcal{K} = GF(q)$ el distribuïdor agafa aleatòriament dos vectors de $\mathbf{v}_1, \mathbf{v}_2 \in E$, tals que $k = \mathbf{v}_1 \cdot \mathbf{v}_D$, $k^2 = \mathbf{v}_2 \cdot \mathbf{v}_D$ amb $\mathbf{v}_D$ la base fixada de $\psi(D)$.

Per a cada participant $p \in P$ amb $\mathbf{v}_{p1}, \ldots, \mathbf{v}_{pr}$ la base fixada de $\psi(p)$, el distribuïdor calcula i lliura en privat $s_{p1} = \mathbf{v}_1\mathbf{v}_{p1}, \ldots, s_{pr} = \mathbf{v}_1\mathbf{v}_{pr}$, i $t_{p1} = \mathbf{v}_2\mathbf{v}_{p1}, \ldots, t_{pr} = \mathbf{v}_2\mathbf{v}_{pr}$. Si A és un subconjunt autoritzat de participants, $\mathbf{v}_D$ es pot expressar com a combinació lineal dels vectors de $\langle \cup_{p\in A}\psi(p)\rangle$ i llavors es podrà recuperar k com a combinació lineal dels fragments $\{s_{pi}\}_{pi}$. Aquest esquema és un esquema perfecte amb $\mathcal{S}_p = (GF(q))^{\dim \psi(p)}$ per a tot $p \in P$. Sigui $A \in \Gamma$ un subconjunt autoritzat. Quan els participants de A introdueixen els seus fragment en la caixa negra aquesta calcula k_1 i k_2. Si $k_1^2 = k_2$, la caixa negra retorna k_1 com a valor correcte del secret. Els participants reben un avís de l'existència de mentiders si $k_1^2 \neq k_2$. En aquest segon cas els valors k_1 i k_2 han de romandre secrets, això és, la caixa negra els ha de destruir.

Proposició 3.4.1 *Sigui Γ una estructura d'accés qualsevol realitzada per un esquema d'espai vectorial generalitzat amb dimensió de la imantge del distribuïdor igual a 1 i taxa d'informació ρ. L'esquema proposat és un esquema per a compartir secrets perfecte que realitza l'estructura d'accés Γ i té taxa d'informació igual a $\rho/2$.*

Demostració: És fàcil veure que els participants de qualsevol subconjunt autoritzat $A \in \Gamma$ poden reconstruir el secret a partir dels seus fragments. D'altra banda, si els participants de $A \notin \Gamma$ tracten de reconstruir els secret a partir

dels seus fragments, han de deduir el valor de $k = \mathbf{v}_1 \cdot \mathbf{v}_D$ a partir del sistema d'equacions

$$\left.\begin{array}{l} s_1 = \mathbf{v}_1 \cdot \mathbf{x}_1 \\ s_2 = \mathbf{v}_1 \cdot \mathbf{x}_2 \\ \cdots \\ s_\ell = \mathbf{v}_1 \cdot \mathbf{x}_\ell \end{array}\right\}, \quad \left.\begin{array}{l} t_1 = \mathbf{v}_2 \cdot \mathbf{x}_1 \\ t_2 = \mathbf{v}_2 \cdot \mathbf{x}_2 \\ \cdots \\ t_\ell = \mathbf{v}_2 \cdot \mathbf{x}_\ell \end{array}\right\}, \quad (\mathbf{v}_1 \cdot \mathbf{v}_D)^2 = \mathbf{v}_2 \cdot \mathbf{v}_D$$

on les incògnites són $\mathbf{v}_1$ i $\mathbf{v}_2$ i $s_1, \ldots, s_\ell, t_1, \ldots, t_\ell$ són els fragments dels participants de A i $\mathbf{x}_1, \ldots, \mathbf{x}_\ell$, és una base de $\langle \cup_{p \in A} \psi(p) \rangle$. A partir de $\mathbf{v}_D \notin \langle \mathbf{x}_1, \ldots, \mathbf{x}_\ell \rangle$, no és difícil comprovar que $k = \mathbf{v}_1 \cdot \mathbf{v}_D$ pot prendre tots els valors de $GF(q)$ amb la mateixa probabilitat. A més a més els participants de qualsevol $A \notin \Gamma$ no tenen absolutament cap informació sobre el valor del secret. □

S'observa que la taxa d'informació d'aquest esquema és $1/(2 \max_{p \in P} \dim \psi(p))$.

Com en el cas de l'esquema proposat per estructures d'espai vectorial, la seguretat enfront de mentiders d'aquest esquema es determina per la proposició següent, que es demostra de la mateixa manera que la Proposició 4.2.2

Proposició 3.4.2 *L'esquema és (Γ, δ)-segur amb $\delta = 1/q$.*