Introducció

Un esquema per a compartir secrets és un sistema criptogràfic que permet que l'obtenció d'un cert valor secret només pugui ser materialitzada per la conjunció de certs grups pre-establerts de persones. A diferència d'altres criptosistemes que depenen dels recursos computacionals dels quals es disposa, els esquemes per a compartir secrets són considerats en un marc en el qual no es depèn d'aquest factor.

Els esquemes per a compartir secrets són útils per a qualsevol acció important que requereixi la participació de diverses persones (o màquines), com ara obrir la cambra cuirassada d'un banc, accedir a una informació reservada o prendre una decisió compartida. Els esquemes per a compartir secrets són utilitzats també en l'administració de claus criptogràfiques [37, 90], en protocols multipart segurs [42] o en transmissió segura d'informació [82]. També s'utilitzen en votacions electròniques [23, 7] a l'hora de fer la constitució de la mesa electoral i en el recompte de vots. S'han proposat aplicacions a la compartició de funcions de forma segura [80] així com a la compartició segura d'imatges (l'anomenada *criptografia visual*) [62, 2, 3]. A [93] i a [94] es pot trobar una introducció als principals temes estudiats a la teoria d'esquemes per a compartir secrets.

En un *esquema per a compartir secrets*, es reparteix un secret en un conjunt de participants de manera que cada participant té una peça d'informació anomenada *fragment*. Tanmateix, el valor del secret només es podrà conèixer si els participants d'un *subconjunt autoritzat* ajunten els seus fragments d'informació.

L'esquema es diu *perfecte* quan

1. Els membres d'un subconjunt autoritzat poden recuperar el secret.
2. Els membres d'un subconjunt no autoritzat no poden obtenir absolutament cap informació sobre el valor del secret

Dit d'una altra manera, els subconjunts autoritzats poden recuperar el secret i amb els fragments dels participants d'un conjunt no autoritzat, tots els

secrets són igualment probables. A més, això s'ha de complir independentment dels recursos computacionals dels quals disposi. L'estudi de la present tesi està centrat en els esquemes perfectes sense considerar d'altres possibilitats.

La col·lecció de subconjunts autoritzats s'anomena *estructura d'accés*. Sovint ens trobarem amb el problema següent: determinar un esquema per a compartir secrets que realitzi una estructura d'accés donada. Així doncs, l'estructura d'accés és, en general, una dada del problema. Aquesta ha de ser *monòtona*, això és, ha de verificar que tot conjunt de participants que contingui a un subconjunt autoritzat sigui a la vegada autoritzat. L'estructura d'accés queda perfectament determinada a partir dels subconjunts autoritzats minimals (respecte a la inclusió).

La seguretat de qualsevol sistema criptogràfic és menor com més gran és la quantitat d'informació que s'ha de mantenir en secret. Com que en un esquema per a compartir secrets cada participant ha de mantenir el seu fragment d'informació en secret, aquest ha de ser el més petit possible. La *taxa d'informació* d'un esquema per a compartir secrets és la raó entre la longitud en bits del secret i la longitud en bits dels fragments que es donen als participants. La taxa d'informació és un nombre entre 0 i 1. Un esquema per a compartir secrets és *ideal* si la taxa d'informació és òptima, és a dir, igual a 1. Per a tota estructura existeix un esquema que la realitza, però només algunes l'admeten ideal. Per aquesta raó es considera la millor de les taxes d'informació d'entre tots els esquemes que realitzen l'estructura, l'anomenada *taxa d'informació òptima*. Si la mida dels fragments no és la mateixa per a tots els participants, és interessant considerar també la *taxa mitjana d'informació* [59], com el quocient entre la llargària en bits del secret i la llargària mitjana dels fragments. La *taxa d'informació òptima* d'una estructura d'accés és el suprem de les raons d'informació d'entre tots els esquemes que realitzen l'estructura d'accés. Una definició anàloga es fa per la *taxa mitjana d'informació òptima*

En un esquema per a compartir secrets poden existir participants que lliurin un fragment fals, els *mentiders*, de forma que sabotegin el procés de recuperació del secret. En alguns esquemes per a compartir secrets el sabotejador pot arribar fins i tot a conèixer el secret autèntic a partir del secret fals recuperat, del fragment fals lliurat i del fragment autèntic (*apropiació indeguda*). Els esquemes protegits contra l'acció de mentiders [26, 31] és una de les variants més importants que s'han considerat del concepte d'esquema per a compartir secrets, malgrat que s'han considerat d'altres requeriments addicionals.

En aquesta tesi es tracten diversos problemes relacionats amb l'estudi de la taxa d'informació i dels esquemes segurs enfront de l'acció de mentiders. També hem dedicat un capítol a l'estudi del problema de l'existència i el

càlcul de l'arrel cúbica a $\mathbb{Z}_m$. Pel que fa a la taxa d'informació els problemes principals són la caracterització de les estructures ideals i l'afitació de la taxa d'informació. En aquesta tesi es tracten aquests problemes per a diverses famílies d'estructures d'accés desde un punt de vista combinatori per obtenir propietats d'elles i a partir d'aquestes trobar fites per a la taxa òptima d'informació. Les estructures que més ens han interessat són les estructures de llindar amb pesos, les bipartites i les homogènies. El principal problema teòric que hi ha al darrera de l'estudi de la taxa d'informació és el de trobar la taxa òptima d'informació i generar esquemes amb aquesta taxa. Un altre dels problemes teòrics més interessants és el de la caracterització de les estructures ideals. Ens hem plantejat aquestes dues qüestions per a certes famílies d'estructures. Hem estudiat la taxa d'informació sota certes condicions de seguretat pels esquemes segurs enfront l'acció de mentiders. Ens hem plantejat el disseny d'esquemes per a compartir secrets que assoleixin les condicions de seguretat requerides amb taxa d'informació el més alta possible.

El problema de l'estudi de famílies particulars d'estructures d'accés és un dels primers que s'ha plantejat històricament. El primer esquema proposat és l'anomenat *esquema polinomial de Shamir* [83] basat en interpolació polinòmica sobre cossos finits i el segon és *l'esquema geomètric de Blakley* [11], basat en l'ús de geometries finites. L'estructura d'accés d'aquests esquemes és *l'estructura de llindar*. En un esquema de llindar t, la reunió de t participants qualssevol poden desvetllar el secret però menys de t participants no poden obtenir-ne cap informació sobre el seu valor. En el treball de Shamir [83] es generalitzen les estructures de llindar assignant a cada participant un pes en funció de la seva rellevància. D'aquesta manera es van definir les *estructures de llindar amb pesos*. Després d'aquesta primera definició no s'ha fet cap més esment en tots els treballs posteriors.

Cal destacar el darrer problema relacionat amb la taxa d'informació: caracterització de les estructures ideals. Brickell i Davenport [25] van estudiar la relació entre estructures ideals i *matroides*. Aquests autors fan servir un esquema que s'ha mostrat molt útil, l'esquema d'espai vectorial de Brickell [24] vàlid per certes estructures ideals.

Pel que fa a l'estudi de la taxa d'informació òptima per a una estructura d'accés qualsevol, aquest és un problema no resolt, encara que s'ha estudiat buscant fites superiors i inferiors de la taxa d'informació. Les fites de la taxa d'informació òptima per a estructures d'accés en general que s'han trobat, no són en general ajustades. Per un conjunt de n participants i una estructura d'accés qualsevol [8, 44] una fita inferior de la taxa d'informació òptima és de l'ordre de $\Omega(1/2^n)$ i una fita superior és de l'ordre de $\Omega(\log n/n)$. S'han descrit

diversos mètodes per trobar fites inferiors basats en recobriments i per les fites superiors s'han utilitzat tècniques de Teoria de la Informació.

És difícil fitar la taxa d'informació òptima en general. Molts treballs han anat dirigits a fer aquestes fitacions per famílies particulars d'estructures d'accés.

Una de les famílies d'estructures d'accés més estudiada són les *estructures d'accés determinades per un graf*. En aquestes els participants són els vèrtexs del graf i els subconjunts autoritzats són els que contenen una aresta. Aquestes estructures admeten un esquema ideal si i només si el graf és multipartit complet [25]. A més a més, si no és d'aquest tipus, la taxa d'informació òptima està entre 0 i 2/3.

També les estructures en les quals els minimals tenen tots el mateix cardinal, anomenades *homogènies*, han estat objecte d'estudi. No s'ha fet cap estudi de la taxa superior per estructures homogènies de rang més gran que 2.

La primera fita inferior per la taxa d'informació es va trobar a partir de mètodes per implementar esquemes per a compartir secrets per a qualsevol estructura d'accés [44, 8, 91, 59]. Cal destacar el primer d'aquests: l'*esquema circuital* de Ito, Saito i Nishizeki [44]. La tècnica més potent per determinar fites inferiors de la taxa d'informació òptima és la λ-*descomposició* [95] que engloba la majoria de les propostes anteriors. Una de les tècniques que engloba és la tècnica per trobar fites inferiors de la taxa d'informació òptima per estructures basades en grafs utilitzant recobriments per grafs multipartits complets [18]. Fent ús de la λ-descomposició es prova que 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. La taxa d'informació i la taxa mitjana d'informació de les estructures d'accés obtingudes a partir de tots els grafs connexos amb com a molt 5 vèrtexs es determinen a [18]. S'han utilitzat sistemes de Steiner i coloracions d'arestes de grafs bipartits per obtenir fites inferiors de la taxa d'informació òptima en [92].

Per les fites superiors s'han obtingut resultats recents [20] que utilitzen tècniques de Teoria de la Informació que permeten trobar fites superiors de la taxa d'informació òptima per a una estructura d'accés en general, a partir de propietats combinatòries de l'estructura. Aquests estudis de fitació superior de la taxa d'informació es van iniciar amb el treball [29], en el qual es van donar els primers exemples d'estructures d'accés amb taxa d'informació fitada per un valor allunyat de 1. En el treball [15] es mostren estructures d'accés tals que la seva taxa d'informació òptima és $1/2+\epsilon$, amb ϵ arbitràriament petit. Totes aquestes estructures d'accés es construeixen a partir de grafs. També amb aquestes tècniques es demostra que la fita inferior $2/(d+1)$ per la taxa

d'informació òptima d'un graf és ajustada ja que a [20] es troba un graf amb taxa d'informació òptima igual a $2/(d+1)$ per $d \geq 2$.

Pel que fa a l'estudi dels esquemes segurs enfront l'acció de mentiders cal destacar que els treballs sobre aquest tema han anat dirigits cap a la proposta d'esquemes de llindar segurs enfront de l'acció de mentiders com són el de Tompa i Woll [98], el de Rifà-Coma [77], el de Carpentieri [30] i el de Ogata i Kurosawa [64]. Les úniques solucions possibles es basen en la disminució de la taxa d'informació com van demostrar per esquemes de llindar Carpentieri, De Santis i Vaccaro [31]. Ogata i Kurosawa fiten superiorment la taxa d'informació per esquemes de llindar amb una certa seguretat [64].

Els nostres objectius han estat la caracterització de les estructures ideals i la fitació de la taxa d'informació òptima per a certes famílies d'estructures d'accés. A l'inici del present treball es defineixen les estructures d'accés que estan definides per pesos i llindar. Hem trobat que totes es poden expressar mitjançant pesos i llindar naturals. Hem obtingut una caracterització completa de les de rang 2, és a dir, les que estan determinades per un graf que hem anomenat k-graf. Hem dissenyat un algorisme que les identifica a partir dels graus de cadascun dels vèrtexs. Hem determinat els pesos i llindar mínims per a aquestes estructures. A partir de l'estructura d'aquests grafs hem determinat una fita inferior de la taxa d'informació òptima que és de l'ordre de $1/\log n$ millorant la fita $1/2^{n/2}$ trobada amb l'únic esquema proposat fins ara per a aquestes estructures, degut a Shamir. A partir d'aquests resultats i mitjançant l'ús del dual d'una estructura hem extés els resultats de caracterització i de càlcul dels pesos i llindar mínims a noves famílies d'estructures definides per pesos i llindar així com el valor de les fites per la taxa d'informació òptima. Per estructures de rang superior hem obtingut fites superiors i inferiors per les estructures definides per dos pesos. S'han generalitzat els resultats per estructures definides per més de dos pesos.

Les *estructures bipartites* són aquelles en les quals els participants estan subdividits en dos col·lectius de tal manera que un subconjunt és autoritzat només depenent de quants participants té de cadascun dels col·lectius. Per les estructures bipartites, hem aconseguit caracteritzar totalment les que són ideals. Aquestes són la família d'estructures de *quasi-llindar*. Aquesta caracterització de les estructures ideals fa que les estructures de quasi-llindar juguin un paper dins de les estructures bipartites anàleg al paper que juguen els grafs multipartits complets dins de les estructures definides per grafs. Així és equivalent dir que una estructura bipartita és ideal a dir que és de quasi-llindar o a dir que és pot definir amb un esquema d'espai vectorial o a dir que la seva taxa d'informació òptima és més gran que 2/3. Per les estructures bipartites

descrivim tècniques típiques de recobriment per tal de trobar fites inferiors de la taxa d'informació. Determinem un algorisme que permet trobar una fita superior de la taxa d'informació òptima que per certes estructures coincideix amb la inferior. Justifiquem que aquestes fites són ajustades.

Hem estudiat la fitació de la taxa d'informació per estructures homogènies. Hem proposat dues construccions d'esquemes per a compartir secrets per les estructures homogènies basats en les tècniques de recobriments. La segona d'elles ens dóna un esquema amb una taxa d'informació millor que la primera, però a canvi la primera utilitza un conjunt de secrets de mesura més realista. Per avaluar les taxes d'informació hem definit el concepte de k-grau d'un participant en una estructura homogènia. Aquest paràmetre és la clau de tots els càlculs de fites fetes, així com de les comparacions entre elles. Amb aquest concepte hem expressat les nostres taxes d'informació i hem millorat les taxes proposades fins ara per d'altres autors. El resultat de la comparació de les nostres fites amb les proposades anteriorment mostra que les nostres són millors en la majoria dels casos. Pel que fa al càlcul de fites superiors per les estructures homogènies hem encetat el seu estudi amb les de rang 3, trobant una primera fita superior per una família d'estructures que és del mateix ordre que la fita inferior obtinguda per les nostres construccions.

Pels esquemes segurs enfront l'acció de mentiders hem generalitzat els conceptes de seguretat que s'havien utilitzat fins ara només per estructures de llindar per a una estructura qualsevol, tant pel cas en el qual els mentiders no coneixen el secret, com pel cas que sí el coneixen. Hem trobat una fita superior de la taxa d'informació òptima per un esquema en el que una coalició de mentiders és detectada amb una certa probabilitat. Després d'aquest estudi general hem proposat un esquema per a compartir secrets per a una estructura d'accés de tipus vectorial que detecta l'acció de coalicions de mentiders, que no coneixen el secret, amb una certa probabilitat. La taxa d'informació d'aquest esquema és $1/2$, la qual és asímptòticament òptima. Per una estructura de llindar hem proposat un esquema que detecta l'acció de coalicions de mentiders (que sí que coneixen el secret) amb una certa probabilitat. Finalment hem trobat el primer esquema per a una estructura qualsevol que detecta l'acció de coalicions de mentiders (que no coneixen el secret) amb una certa probabilitat.

Pel que fa a l'arrel cúbica en un $\mathbb{Z}_m$ es coneixen algorismes per tal de calcular efectivament l'arrel quadrada, però cap algorisme hi ha publicat pel càlcul de l'arrel cúbica. El que sí es coneixen són mètodes no específics que es poden aplicar, com són els mètodes generals per trobar arrels de polinomis [35].

L'organització de la memòria de la tesi és la següent: el Capítol 1 és una

introducció als principals conceptes sobre esquemes per a compartir secrets que tenen a veure amb el nostre treball (també es pot trobar alguna generalització de resultats ja coneguts). En el Capítol 2 estan exposats tots els nostres resultats sobre la taxa d'informació. En el Capítol 3 hem tractat els esquemes segurs enfront l'acció de mentiders. En el Capítol 4 hi ha descrit tota la nostra feina sobre les arrels cúbiques a $\mathbb{Z}_m$. Fem, a continuació, un breu resum de cada capítol i de les publicacions a que han donat lloc.

El Capítol 1 de la memòria està pensat com una introducció i presentació del tema, exposant els principals resultats coneguts fins ara. Fem esment, sobretot, dels conceptes que tenen a veure amb el nostre treball, fent un breu comentari dels conceptes que són colaterals al nostre estudi. També hem inclòs algun resultat que és generalització de treballs previs que es demostren sense fer un esforç exagerat a partir del treball prèviament publicat. L'organització d'aquest capítol és com la de tota la memòria: després de la introducció als conceptes bàsics (amb la introducció de les estructures més estudiades), s'enuncien els resultats sobre la taxa d'informació i els dedicats als esquemes segurs enfront l'acció de mentiders.

El Capítol 2 està dedicat a detallar els resultats que nosaltres hem aportat pel que fa a la taxa d'informació. Estudiem les estructures definides per pesos i llindar caracteritzant-les totalment pel cas de rang 2 i determinant els pesos i llindar mínims. Per aquestes estructures trobem una fita inferior per la taxa d'informació òptima. Generalitzem els resultats sobre caracterització i càlcul de pesos i llindar mínims a una altra família d'estructures fent ús del dual d'una estructura. A la segona secció ens ocupem de les estructures bipartites, estudiant en primer lloc quines ens donen estructures ideals i veient que són exactamet les definides per una subfamília d'estructures: les estructures de quasi-llindar. Després ens dediquem a fitar superior i inferiorment la taxa d'informació òptima. A la tercera secció hem trobat fites per a la taxa d'informació per estructures definides per pesos i llindar, principalment pel cas de dos pesos diferents. A la quarta secció hem descrit dues formes de construir esquemes per a compartit secrets per estructures homogènies, de forma que millorem gairebé totes les fites conegudes fins al moment pel càlcul de les taxes d'informació amb l'ús d'un nou paràmetre, el *k-grau*. Fem les corresponents comparacions entre elles i amb les conegudes fins al moment. Acabem el capítol determinant una fita superior de la taxa d'informació per una família d'estructures homogènies de rang 3 que resulta ser del mateix ordre que la fita inferior obtinguda amb les construccions exposades anteriorment. Part dels resultats obtinguts per estructures definides per pesos i llindar de rang 2 s'han recollit en un article que està en procés de referenciat [78] i que ha estat

exposat a la *XV British Combinatorial Conference*. Part dels resultats per les estructures bipartites seran presentats a *Eurocrypt'98* amb la conseqüent publicació en els *Proceedings* [70]. Els resultats referents a la taxa d'informació per estructures homogènies serà presentat en el *MFCS'98 Workshop on Communications* i serà publicat a [71].

En el Capítol 4 presentem els nostres resultats sobre esquemes per a compartir secrets segurs enfront l'acció de mentiders. La primera proposta és un esquema per una estructura d'espai vectorial que detecta (amb una certa probabilitat) l'acció de mentiders que no coneguin el secret, a fi i efecte d'evitar el sabotatge i l'apropiació indeguda. Es defineix, seguint els treballs de Tompa i Woll [98], Carpentieri, De Santis i Vaccaro [31] i Ogata i Kurosawa [64], el que s'entèn per un esquema (Γ, δ)-segur i un esquema (Γ, ϵ)-robust. S'estudia en general la taxa d'informació per un esquema (Γ, δ)-segur trobant que en el nostre esquema és asimptòticament òptima. També fem la comparació amb l'únic esquema conegut que té una taxa d'informació òptima: tant a nivell de complexitat de l'algorisme de distribució dels fragments, com de l'algorisme de recuperació del secret a partir dels fragments. El segon esquema proposat, aquesta vegada per una estructura de llindar, detecta l'acció de mentiders fins i tot si coneixen el valor del secret (evitant el sabotatge). S'acaba el capítol fent la proposta del primer esquema per a compartir secrets conegut, segur enfront l'acció de mentiders (que no coneixen el secret) que realitza una estructura d'accés qualsevol. Part d'aquests resultats han estat presentats al congrés *PRAGOCRYPT'96* amb la corresponent publicació a les actes del congrés [66] i estan pendents de publicació en la seva versió definitiva [67]. El primer esquema vàlid per a qualsevol estructura d'accés està presentat en el treball [68] en procés de referenciat.

El Capítol 5 està dedicat a l'estudi del càlcul d'arrels cúbiques en el conjunt dels enters mòdul un nombre. Tot i que aquest és un tema que diferent del tema de la tesi, ens ha interessat per la seva possible aplicació en Criptografia i en Teoria de Nombres. En aquest capítol es fa resenya de la qüestió de l'existència i del número d'aquestes, per a la qual cosa es defineix un símbol cúbic. A partir d'aquí s'estudia el cas en el qual la base del $\mathbb{Z}$ mòdul és un primer. Es comenta per a quins valors del primer és molt fàcil trobar les arrels cúbiques d'un nombre i pels casos que no es proposen algorismes eficients que les calculen. El primer d'aquests és la generalització de l'algorisme de Peralta per fer arrels quadrades. Es fa un estudi detallat de les probabilitats que intervenen en la part no determinista de l'algorisme i s'avalua la complexitat. El segon algorisme proposat és l'extensió de l'algorisme de Tonelli-Shanks per a calcular arrels quadrades. Amb la finalitat de determinar l'algorisme s'estableix

l'expressió de l'arrel cúbica en funció del generador d'un cert subgrup de Sylow i partir d'aquí es genera aquest procediment. També s'estudia l'eficiència i es compara amb la de l'anterior algorisme. Seguidament es comenten algunes utilitats criptogràfiques. Aquest treball està en procés de referenciat a [69].

S'acaba la memòria amb un capítol de conclusions i enumeració de problemes oberts amb els que ens hem trobat.