2 szintű titokmegosztás

A titokmegosztás célja a következő: adva van egy titok (ez akármi lehet, csak képes legyen különböző értékeket fölvenni), erről akarunk úgy információt átadni, hogy ezeknek pontosan az előre meghatározott részhalmazaiból lehessen megfejteni a titkot, miközben az összes többi esetben keveset lehessen megtudni róla. (a nem elfogadott esetekben az optimális módszerrel való tippelés találati esélyét akarjuk minimalizálni)

Egy példaként legyen az a cél, hogy bármely két adatból meg lehessen határozni a titkot.

Ehhez vegyünk egy (véges test feletti) projektív síkot, ezen egy e egyenest, e-n egy P pontot (ez lesz a titok), és P-n át egy e-től különböző f egyenest. Az embereknek szétosztjuk f P-től különböző pontjait, és közzétesszük az e egyenest, és az előbbi metódust. Így két pont ismeretében az őket összekötő egyenes és e metszéspontjaként megkapható a titok, de ha legfeljebb egy pontot ismerünk, e minden pontján át ugyanannyi egyenes megy, ami tartalmazza a legfeljebb 1 ismert pontot, tehát semmi információnk nincs a titokról.

Hasonló a helyzet, ha 2 helyett n adatot várunk el. Ekkor egy n dimenziós projektív teret veszünk, e rögzített egyenes, P e egy pontja (a titok), H egy olyan hipersík, ami e-t P-ben metszi. Az emberek között szétosztjuk egy H-beli, P-t tartalmazó ívnek a P-től különböző pontjait, és közzétesszük az e egyenest, és az előbbi metódust. (Egy ponthalmaz ív, ha bármely részhalmaza vagy feszíti az egész teret, vagy egy elemszám-1 dimenziós alteret feszít.) A megfejtéshez a kapott pontok által feszített alteret kell elmetszeni e-vel. (Itt − ahogy a korábbi példában és a későbbiekben is − e-t választhatjuk egy k dimenziós altérnek egy $k-1$-gyel nagyobb dimenziós térben, és ha így növeljük a titok lehetséges értékeinek számát, azzal kevesebb pontú teret kaphatunk, mint amit az alaptest növelésével kapnánk.)

A 2 szintű titokmegosztásnál az embererket 2 csoprtba osztjuk, és a titok megfejtéséhez vagy az elsőből kell m ember, vagy a kettőből összesen $n(> m)$. Itt csak az $m = 2$ esettel foglalkozunk.

Ehhez egy az előzőek után természetes konstrukció a következő: legyen e, P és H mint az előző példában, f egy P-n átmenő egyenes H-ban, K pedig egy olyan ív H-ban, amire $f \cap K$ üres, és $K \cup \{P\}$ is ív. Az első csoportnak szétosztjuk f pontjainak egy F részét ($P \notin F$), a másodiknak pedig K pontjait. Ez akkor fog az előzőekhez hasonlóan működni, ha minden $Q \in F$-re $K \cup \{P, Q\}$ is ív. (A konstrukció általánosítható $m > 2$-re is, de az utolsó feltétel nehezen ellenőrizhető/kezelhető.) Azt vizsgáljuk, hogy hány emberig használható ez a módszer az alaptest rögzített q elemszáma mellett. (Tehát $|F \cup K|$ maximumára vagyunk kíváncsiak, és hogy ez $|K|$ mely értékeire

érhető el.) A továbbiakban feltesszük, hogy $|F| \geq 2$ és $|K| \geq n$. A q elemű testet jelölje $GF(q)$, annak multiplikatív csoportját $GF(q)^*$.

Kezdésnek tegyük fel, hogy $n = 3$. Ekkor az utolsó feltétel arra egyszerűsödik, hogy F semelyik pontja sincs rajta K semelyik szelőjén.

H-ból f-et elhagyva egy affin teret kapunk, amelyben K egy olyan ív, aminek a szelői kevés párhuzamossági osztályt határoznak meg (hiszen a maradékból kerülnek ki $F \cup \{P\}$ pontjai). Erre egy példát képeznek az úgynevezett affin szabályos sokszögek (egy affin sík egy ponthalmaza affin szabályos sokszög, ha a ponjainak létezik olyan bijekciója egy euklideszi síkbeli szabályos sokszög csúcsaira, ami megtartja a csúcsok közt futó egyenesek párhuzamosságát): ha K-t egy affin szabályos sokszögnek választjuk, F-et pedig azon P-től kül. pontoknak, amik nincsenek rajta K semelyik szelőjén, akkor $|F \cup K| = q$. Ennél jobbra pedig általában nem is számíthatunk, ugyanis könnyen bizonyítható, hogy $|F \cup K| \leq q + 1$, és egyenlőség esetén q páros.

Páratlan q-ra karakterizálták az affin szabályos sokszögeket: (mindegyik átvihető affinitással a következők valamelyikébe)

1. A test 1 által generált additív H részcsoportjára $\{(h^2, h) | h \in H\}$
   (Ez bármely additív részcsoportra a célnak megfelelő K-t ad.)

2. A test multiplikatív csoportjának egy tetszőleges H részcsoportjára $\{(h, \frac{1}{h}) | h \in H\}$

3. Legyen $GF(q^2)$-ben i az $x^2 - k$ ($GF(q)$ fölött) irreducibilis polinom egyik gyöke. Ekkor minden elem egyértelműen áll elő $a + bi$ alakban, ahol $a, b \in GF(q)$. Azon elemek, amelyekre
   $a^2 - kb^2 = 1$, csoportot alkotnak a szorzásra nézve; vegyük ennek egy H részcsoportját. Az $(a, b) \leftrightarrow a + bi$ azonosítással élve H pontjai affin szabályos sokszöget alkotnak.

Az első kettő páros q-ra is jó K-t ad, és a csúcsszámuk prímosztója q-nak, tetszőleges osztója $q - 1$-nek, illetve $q + 1$-nek. Bizonyítható, hogy ha q páratlan, és $|F \cup K| = q$, akkor $|K|$ osztja q-t, $q - 1$-et vagy $q + 1$-et.

Ezeket általánosítva térjünk vissza $n - 1$ dimenzióba.

A második pontjainak a koordinátái a projektív síkon $(h : 1 : \frac{1}{h}) = (h^2 : h : 1)$, a hozzátartozó egyenes pedig az $(x : 0 : y)$ pontokból álló. Ez úgy általánosodik $n - 1$ dimenzióra, hogy K a $(h^{n-1} : h^{n-2} : ... : h : 1)$ alakú pontokból áll, f pedig az $(x : 0 : 0 : ... : 0 : y)$ alakúakból.

Def.: $(n-1)$-dimenziós momentumgörbének nevezzük az $\{M(x) = (x^{n-1} : x^{n-2} : ... : x : 1) | x \in GF(q)\} \cup \{M(\infty) = (1 : 0 : 0 : ... : 0)\}$ halmazt. Ezzel a jelöléssel $K = \{M(h) | h \in H\}$, $f = \overline{M(0)M(\infty)}$. Azt állítom,

hogy minden n-re és H-ra kiválasztható a feltételeknek megfelelő $q - |H|$ pontú F.

Nézzük meg, hogy mikor lesz $M(x_1), M(x_2), ..., M(x_{n-1}), (x : 0 : ... : 0 : y)$ összefüggők. Pontosan akkor, ha a koordinátáikból alkotott mátrix determinánsa 0:

$$\det \begin{pmatrix} x & 0 & ... & 0 & y \\ x_1^{n-1} & x_1^{n-2} & ... & x_1 & 1 \\ \vdots & \vdots & & \vdots & \vdots \\ x_{n-1}^{n-1} & x_{n-1}^{n-2} & ... & x_{n-1} & 1 \end{pmatrix} =$$

$$= x \cdot \det \begin{pmatrix} x_1^{n-2} & ... & x_1 & 1 \\ \vdots & & \vdots & \vdots \\ x_{n-1}^{n-2} & ... & x_{n-1} & 1 \end{pmatrix} + (-1)^{n-1} y \cdot \begin{pmatrix} x_1^{n-1} & x_1^{n-2} & ... & x_1 \\ \vdots & \vdots & & \vdots \\ x_{n-1}^{n-1} & x_{n-1}^{n-2} & ... & x_{n-1} \end{pmatrix}$$

Mivel a második mátrix minden sorából kiemelve a megfelelő változót visszakapjuk az első mátrixot, ez pontosan akkor lesz 0, ha $x = (-1)^n y \prod x_i$. Tehát ha minden x_i H-beli, és ezek összefüggők, akkor $\frac{x}{y} = (-1)^n \prod x_i \in (-1)^n H$, így $|F \cup \{P\}| = q + 1 - |H|$ adódik, és ezt állítottuk.

Az első típus homogén koordinátái $(h^2 : h : 1)$, az egyenes pedig az $(x : y : 0)$. Ez az előzőhöz hasonlóan akadálymentesen általánosítható $n - 1$ dimenzióba.

Végül a harmadik típusban az egyenletet homogenizálva $(a^2 - kb^2 = c^2)$, majd átrendezve $k(a + c)(a - c) = (kb)^2$ adódik, tehát az $(a : b : c) \to (k(a+c) : kb : a-c)$ transzformáció az egyenlet gyökeit éppen az $(x^2 : x : 1)$ alakúakba viszi át. Mivel az eredeti egyenletnek nem volt gyöke semelyik ideális pont, az ilyen alakú pontok között a $c = 0$ egyenletnek nem lehet megoldása... az alaptestben, de a bővítettben kettő is van: $(i^2 : i : 1)$ és $((-i)^2 : -i : 1)$. Ez azt jelenti, hogy az általunk keresett f egyenes igazából $GF(q^2)$-ben az ezeken átmenő szelő. Ezt átvive nagyobb dimenzióba azt tapasztaljuk, hogy az $\overline{M(i)M(-i)}$ egyenes azon pontjai, amiknek minden koordinátája $GF(q)$-beli, mindig egy egyenest alkotnak a $GF(q)$ fölötti projektív térben (ez lesz f). Most az eddigiek alapján a logikus lépés az lenne, hogy $GF(q^2)^*$ $q + 1$ elemű részcsoportját illesztjük rá M pontjaira (és ez is megoldható), de az azonos elemszámú faktorral könnyebb dolgozni, ugyanis az nem más, mint $GF(q^2)^*/GF(q)^*$. Ezen faktor elemei: $\{k(a + bi)|k \in GF(q)^*\}$. Ezek párba állíthatóak (relatíve természetes módon) a momentumgörbe pontjaival:$\{k(a + bi)\} \to M(\frac{a}{b})$. (Ezzel gyakorlatilag egy szorzást kaptunk M-en.) Mindezek után némi (igazából elég sok) számolás után az ember azt tapasztalja, hogy az $M(x_1), M(x_2), ...M(x_{n-1})$ pontok által generált altérbe f pontjai közül pontosan egy esik bele (ez még nyilvánvaló),

és hogy melyik, az csak előbb nekik megfeleltetett értékek szorzatától függ. Ez pedig azt jelenti, hogy ha ebből veszünk egy K részcsoportot, akkor ez f-ről csak $|K|$ pontot zár ki, így $|K \cup F \cup \{P\}| = q + 1$, és ez volt a cél.

Ez a konstrukció páros q-ra is működik, két módosítással: az első az, hogy mivel $x^2 - k$ alakú irreducibilis polinom nincs, ezért helyette egy $x^2 + x - k$ alakút kell venni; a második pedig az, hogy ahol $-i$ szerepel, oda ezen polinom másik gyökét kell írni: $i + 1$-et. (Ez a számolásokban komoly változás, de végül ugyanez az eredmény.)

Végül néhány eredmény arról, hogy ezeket mennyire (nem) lehet javítani (csak felsorolás-szinten, mert ezekkel nem foglalkoztam):

$|K| \leq \frac{q}{2} + n - 2$, ha q páros, és $|K| \leq \frac{2q-5}{3} + n$ egyébként.

Feltéve, hogy K-t a momentumgörbéről választjuk, az első becslés vonatkozik a páratlan esetre is.

És, ha emellett még azt is feltesszük, hogy q nem 3 vagy 5 hatvány, akkor $|K| \leq \frac{q+1}{2}$.

Hivatkozások:

A. Beutelspacher, F Wettl, On 2-level secret sharing, Des Codes Cryptogr. 3 (2) (1993) 127-134.

J.W.P. Hirschfeld, Projective geometries over finite fields, second ed., in: Oxford Mathematical Monographs, The Clarendon Press. Oxford University Press, New York, 1998.