

Titokmegosztás

Csirmaz László

Több résztvevő között egy titkot akarunk szétszítani a következő feltételekkel:

- a résztvevők bizonyos halmazai, az úgynevezett *kvalifikált* vagy megbízott részei magát a titkot a részekből vissza tudják állítani
- a nem kvalifikált részhalmazok a lehető legkevesebb információt tudják meg a titokról, ha lehet akkor ez az információ nulla legyen.

A titokmegosztás önmagában is érdekes, de nagyon sok más kriptográfiai protokollnak a részeként is előjön. Erre fogunk példákat is látni. Gyakran nem magát a titokmegosztási protokollt használják, hanem annak elkészítésekor használt ötleteket.

1 Első ötlet

A legegyszerűbb esetben a titok egyetlen bit, és két résztvevő van. A titokmegosztást könnyen elvégezhetjük: a két résztvevőnek egy-egy bitet adunk úgy, hogy a titok a két bit xor-ja (mod 2 összege) legyen.

A szétszítást az alábbi táblázat mutatja:

titok	A	B
0	0	0
0	1	1
1	0	1
1	1	0

Maga a táblázat szinte mindent megmutat. Aki a titkot elosztja (szakszóval a *dealer*) véletlenül választ egy sort a táblázatból, és a sornak megfelelően határozza meg a titkot valamit az egyes résztvevők értékeit. Persze a táblázatot mindenki ismeri, csak azt nem, hogy a dealer melyik sorát választotta ki.

Ha most A szempontjából nézzük, akkor A annyit tud, hogy ő 0-t vagy 1-et kapott-e. Mondjuk 0-t. Ekkor a dealer a táblázat első vagy harmadik sorát kellett választania, de mindkettőre ugyanakkor esély van. Következésképp A nem tud semmit arról, hogy mi a titok: az A által látott érték és a titok értéke *független* (a szó valószínűségszámítási értelmében).

Az eljárást könnyen általánosíthatjuk kettő helyett akárhány résztvevőre is. Mindenki 0-t vagy 1-et kap, és a titok a résztvevők által kapott értékek mod 2 összege. Ha mindenki összejön és megmondja saját értékét, akkor érsze a titkot is könnyen kiszámíthatják. Ha viszont akár egyetlen résztvevő is hiányzik, *semmi információjuk nincs a titokról*. Ez utóbbi annak következménye, hogy a hiányzó résztvevők miatt a titok pontosan ugyanannyi esetben lesz 0 mint amennyi esetben 1 (ha egy ember hiányzik, akkor 1-1, ha ketten hiányoznak, akkor 2-2, ha hárman, akkor 4-4, stb., kettőhatványok szerint megy a dolog előre).

Az így definiált titokmegosztás speciális esete a *küszöb-rendszereknek*, ahol az n résztvevő közül bármely k vissza tudja állítani a titkot, viszont k -nál kevesebb résztvevőnek nincs információja a titokról. A küszöb rendszerekre később visszatérünk.

2 Általános eset

Mindjárt felmerül a kérdés: ha akárhogyan, össze-vissza adom meg a kvalifikált csoportokat, létezik-e mindig megfelelő titokmegosztás? Vagy ha nem, milyen feltételek mellett? Egy nagyon szép eredmény azt mutatja, hogy bizonyos triviális feltételek mellett mindig létezik tökéletes titokmegosztás. Lássuk ezeket a feltételeket.

Először is nyilvánvaló, hogy ha a résztvevők egy csoportja *kvalifikált*, vagyis vissza tudja állítani a titkot, akkor bárkit is adunk a csoporthoz, ez a lehetőség továbbra is megmarad. Másrészt ha egy csoportnak együttesen sincs semmi információja a titokról, akkor a csoport egy részének sincs.

1. Definíció: A résztvevők részhalmazainak egy \mathcal{A} családja *elérési struktúra* ha

- ha $A \in \mathcal{A}$ és $A \subseteq B$, akkor $B \in \mathcal{A}$;
- ha $C \notin \mathcal{A}$ és $D \subseteq C$, akkor $C \notin \mathcal{A}$.

Az \mathcal{A} halmazrendszer elemei a *kvalifikált* részhalmazok, vagyis azon részhalmazok, melyek résztvevő együttesen vissza tudják állítani a titkot. A többi részhalmaz, mármint azok, melyek nincsenek \mathcal{A} -ban, viszont semmi információval nem szabad hogy rendelkezzen a titokról.

Egy elérési struktúrát tipikusan úgy adunk meg, hogy megmondjuk mik a *minimális kvalifikált részek*, vagyis melyek azok a lehető legkevesebb résztvevőből álló halmazok, amiknek vissza kell tudni fejteni a titkot. Vagy úgy is megadhatjuk \mathcal{A} -t, hogy megadjuk a *maximális nem kvalifikált* részeket, vagyis azon részhalmazokat, amik még nem tudnak semmit a titokról, ámde ha bárki csatlakozik hozzájuk, már mindent tudnak.

1. Tétel: Minden \mathcal{A} elérési struktúrához létezik titokmegosztási rendszer.

Az állítás a 90-es évekből származik. Két konstrukciót fogunk ismertetni, mindkettőnek vannak előnyei és hátrányai is. Az elsőt talán parányit könnyebb megérteni.

2.1 Első konstrukció

Mindkét konstrukcióban a szétosztandó titok egyetlen bit lesz, vagyis 0 vagy 1. Az első konstrukcióhoz felsoroljuk \mathcal{A} (minimális) elemeit, vagyis a résztvevőknek azokat a (minimális) részhalmazait melyeknek vissza kell tudni fejteni a titkot. Egy táblázatot készítünk, melynek oszlopai a résztvevők, sorai pedig a minimális kvalifikált részhalmazok:

halmaz	A	B	C	D	E	F
Q_1	?	•	•	?	•	•
Q_2	•	?	•	?	?	?
Q_3	•	•	•	?	•	?
Q_4	?	•	?	•	?	•
Q_5	?	?	?	•	?	•
Q_6	?	•	•	?	•	?
Q_7	?	•	?	•	?	•

A táblázatban a • azt jelzi, hogy az illető résztvevő nem tagja a kvalifikált résznek, a kérdőjelek helyére pedig majd a 0 és 1 számok kerülnek. Ezt a táblázatot természetesen mindenki ismeri, hiszen nem tartalmaz mást, mint a kvalifikált halmazok leírását.

A táblázatot az titok szétosztó *titokban* kitölti a következőképpen. Kiváasztja a titkot, ami vagy 0 vagy 1, mindkettőt 1/2 valószínűséggel. Utána a táblázat *sorait* kitölti független 0/1 értékekkel úgy, hogy minden sorban a beírt bitek mod 2 összege éppen a titkot adja ki. Ezek után a táblázatot egy ollóval szétvágja az oszlopaira, és mindenki megkapja a saját (kitöltött) oszlopát.

Ezek után ha egy kvalifikált részhalmaz jön össze, akkor persze ki tudják számítani a titkot. Egymás mellé teszik a kapott csíkjaikat, és valamelyik sorban az összes beírt számot ismerik, nevezetesen abban a sorban, ami éppen az összejtött kvalifikált részhalmaznak felel meg.

Másrészt ha egy nem kvalifikált részhalmaz jön össze, és egymás mellé teszik a cetlijeiket, abból semmilyen következtetést nem tudnak levonni a titokra nézve. Ugyanis minden sorból hiányzik valamelyik szám, és a hiányzó számokat pontosan ugyanígyélekképpen tudta a szétosztó kitölteni akkor is ha a titok 0, meg akkor is ha a titok 1.

Tessék észrevenni, hogy ez a konstrukció éppen megegyezik a bevezetésben adott konstrukcióval ha egyetlen kvalifikált részhalmaz van, az, amelyik az összes résztvevőt tartalmazza.

2.2 Második konstrukció

Második konstrukciónk bizonyos értelemben az első duálisa. Előbb a minimális kvalifikált részhalmazokat használtuk, most a maximális nem kvalifikált részhalmazokat fogjuk használni.

Legyenek tehát N_1, N_2, \dots, N_t az összes maximális **nem kvalifikált** részhalmazai a résztvevőknek. Most is elkészítünk egy a fentihez hasonló táblázatot. A sorokat most az N_1, \dots halmazok címkézik, az oszlopok a résztvevők, csak hogy most a táblázat egy elemébe \bullet kerül ha a résztvevő benne van az illető halmazban, és $?$ ha nincs:

halmaz	A	B	C	D	E	F
N_1	\bullet	$?$	\bullet	$?$	\bullet	\bullet
N_2	\bullet	\bullet	\bullet	$?$	$?$	$?$
N_3	$?$	\bullet	\bullet	$?$	\bullet	$?$
N_4	$?$	\bullet	$?$	\bullet	$?$	\bullet
N_5	\bullet	$?$	$?$	\bullet	$?$	\bullet
N_6	\bullet	$?$	\bullet	\bullet	$?$	$?$

Esetünkben például A benne van N_1 -ben, N_2 -ben, N_5 -ben és N_6 -ban, de nincs benn N_3 -ban és N_4 -ben. Hasonlóan, E csak N_1 -ben és N_3 -ban van, a többiben nincs benne.

A titokszétosztó kiválasztja a titok, ami most is 0 vagy 1, valamint kiválaszt annyi darab véletlen bitet úgy, hogy azok mod 2 összege éppen a titok legyen amennyi sora van a táblázatban (esetünkben 6 bitet). Minden sorban a kérdőjelek helyére beírja a sorhoz tartozó bitet (minden helyre ugyanazt), majd felvágja a táblázatot oszlopokra és az oszlopokat szétosztja a résztvevők között.

Ha most egy nem kvalifikált halmaz jön össze, akkor van olyan sor, amelyik címkéjének mindannyian tagjai. Következésképp abban a sorban mindnek \bullet van, tehát a csoport nem fogja tudni az ehhez a sorhoz tartozó véletlen bitet, így a titokról sem lesz semmilyen információja.

Ha viszont egy kvalifikált halmaz tagjai jönnek össze, akkor mindegyik N_i halmazhoz van a csoportnak olyan tagja, aki nincs benne N_i -ben (egyébként mindegyikük tagja volna N_i -nek, ezért ők együttesen is nem kvalifikáltak lennének). Ez a személy viszont tudja mennyi az N_i sorához tartozó szám, ezért az összes sorhoz tartozó számot ismerik. Ebből pedig a titkot ki is lehet számítani.

3 Mennyit kell megjegyezni?

A titokmegosztás egyik fontos kérdése hogy az egyes résztvevőknek mennyi információk kell megjegyeznie. Az első benyomásunk az, hogy nem sokat, hiszen tobben vannak, és együttesen kell annyit tudniuk, mint amennyi információ a titokban van. Ha a titok egy 10 jegyű szám és tizen vannak, akkor mindenkinek elegendő 1 számjegyet megjegyezni, abból a titkot már össze tudják rakni. Így mindenki csak a teljes információ 1/10-ét jegyzi meg. Ekkor azonban mindenki tud valamit a titokról – nevezetesen valamelyik jegyét –, és ha például kilencen összejönnek, akkor bár nem tudják helyreállítani a titkot, de összesen 10 lehetőséget kell kipróbálniuk. Azért ez sokkal kevesebb, mintha semmit nem tudnának a titokról amikor is mind a 10^{10} lehetőséget ki kell próbálniuk.

Az alábbi okoskodás mutatja, hogy a résztvevőknek bizony meg kell jegyezniük annyi információt, amennyi a titokban van, nem lehet kevesebbet. Legyen A egy résztvevő, és keressünk olyan nem kvalifikált részhalmazt, amiben A nincs benne, de ha A -t hozzávesszük, akkor

a részhalmaz kvalifikálttá válik. Ha ilyen részhalmaz nincs, akkor A -nak nem kell semmit sem tudnia, őrá úgy sincs szükség a titok visszaállítására.

Egy nem kvalifikált részhalmaz együttesen semmilyen információt nem tud a titokról. Ha viszont A csatlakozik hozzájuk, hirtelen ki tudják számítani a titkot, vagyis a teljes információ birtokába jutnak. Mivel információ nem keletkezik, az extra információ csak abból az ismeretből jöhet, aminek A birtokában van. Így A -nak legalább annyi információval kell rendelkeznie, amennyi a titokban van.

Magyarul, ha a titok 100 bites, akkor minden résztvevőnek legalább 100 bitnyi információt meg kell jegyeznie. Nézzük mi történik a fenti esetekben.

Az első konstrukcióban – amikor csak a teljes halmaz volt kvalifikált – a titok egy bit, és mindenki pontosan egy bitet jegyez meg. Ez optimális ennél jobbat nem lehet csinálni.

A két általános konstrukciónál azonban nem ez a helyzet. A titok mindkét esetben továbbra is egy bit, viszont egy-egy résztvevőnek több bitet is meg kell jegyeznie (igazán csak a biteket, mivel azok elhelyezkedése a papíron visszanyerhető a táblázatból, amit viszont mindenki ismer, így nem is kell megjegyezni). Mégpedig annyi bitet, ahány kérdőjel van a résztvevő oszlopában. Az első konstrukciónál ez az a szám, ahány minimális kvalifikált halmazban van benne a résztvevő, a második konstrukciónál viszont ahány maximális nem kvalifikált részhalmazban *nincs* benne. Ha mondjuk a résztvevők száma 20, és a kvalifikált részhalmazok az összes 10 elemű részhalmaz (azaz bármely 10 vissza tudja állítani a titkot, de semelyik 9 semmilyen információval nem rendelkezik a titokról), akkor az első konstrukcióban a táblázat $\binom{20}{10}$ soros, és mindenkinek az oszlopában

$\binom{19}{9} = 92378$ kérdőjele van, tehát ennyi bitet kell megjegyeznie!

A másik konstrukció sem jobb. Most a táblázatunk “mindössze” $\binom{20}{9}$ soros (a maximális nem kvalifikált halmazok kilenc eleműek), és persze egy résztvevő ezek közül pontosan $\binom{19}{9}$ -ban nincs benne, ami ugyanazt a számot adja mint előbb.

Kérdés: lehet ezt jobban csinálni?

Meglepő módon nem tudjuk a választ. Annyit azért sikerült megmutatni, hogy bizonyos esetekben egyes résztvevőknek tényleg több információt kell megjegyezniük mint amennyi a titokban van, sőt, ennek mértéke arányos tud lenni a résztvevők számával. Ugyanakkor nincs olyan általános módszer, ami tetszőleges elérést struktúra esetén a fenti konstrukciónál jobban tudna. Igazán nincs is másfajta *általános* konstrukció. Természetesen vannak fontos speciális esetek, amikor a titokmegosztást a lehető legjobban lehet megcsinálni. Erről szól a következő rész.

4 Köszöbös titokmegosztás

Kicsit szerencsétlen elnevezés, egészen pontosan arról van szó, hogy n résztvevő közül bármely (legalább) t meg tudja határozni a titkot, viszont bármely $t - 1$ vagy annál kevesebb semmilyen információval ne rendelkezzen a titokról. Az ilyen titokmegosztás szokásos jelölése T_n^t , ahol a T betű az angol *threshold* szóra utal. Ilyen esetekben egy nagyon ravasz módszerrel tökéletes titokmegosztást tudunk csinálni.

A módszerhez szükségünk van a *Lagrange interpoláció* ismeretére.

4.1 Lagrange interpoláció

Egy (legfeljebb) d -edfokú polinom így néz ki:

$$p(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_2 x^2 + a_1 x + a_0.$$

Az a_i számok a polinom együtthatói, ha a_d nem nulla, akkor a polinom d -edfokú. A legmagasabb kitevőhöz tartozó nem-nulla együttható a polinom főegyütthatója.

Jól ismert, hogy egy nem azonosan nulla d -edfokú polinomnak legfeljebb d gyöke van. Ez azt jelenti, hogy ha két legfeljebb d -edfokú polinom $d + 1$ helyen megegyezik, akkor a két polinom minden helyen megegyezik (azonosan az együtthatóik). Valóban, ekkor a két polinom különbsége is legfeljebb d -edfokú, de van $d + 1$ gyöke, így az azonosan nulla polinomnak kell lennie.

Ebből következik, hogy ha megadunk $d + 1$ helyet és ott $d + 1$ értéket, akkor legfeljebb egy olyan polinom létezik, amelyik a megadott helyeken a megadott értékeket veszi fel. De létezik-e ilyen polinom, és ha igen, hogyan lehet azt megtalálni?

Ez utóbbi feladatra való a *Lagrange interpolációs polinom*. Első lépésként olyan polinomot állítunk elő, ami az adott a_1, a_2, \dots, a_n helyeken nulla értéket vesz fel. Ez persze nem nehéz:

$$q(x) = (x - a_1)(x - a_2) \dots (x - a_n)$$

megfelelő polinom.

Másodszor olyan polinomra vagyunk kíváncsiak, ami az a_1, a_2, \dots, a_n helyek közül az a_i kivételével nulla, az a_i helyen pedig az 1 értéket veszi fel.

Az előző lépésből tudjuk, hogy érdemes az

$$(x - a_1)(x - a_2) \dots (x - a_{i-1})(x - a_{i+1}) \dots (x - a_n)$$

polinomból kiindulni. Ez legalább nulla értéket vesz fel mindenhez, ahol szükséges. Az a_i helyen pedig valamilyen értéket felvesz. Ahhoz, hogy ott 1-et vegyen fel, egyszerűen leosztjuk az ott felvett értékével. A kapott $n - 1$ -edfokú polinomot $L_i(x)$ -szel jelöljük:

$$L_i(x) = \prod_{\substack{1 \leq j \leq n \\ j \neq i}} \frac{x - a_j}{a_i - a_j}.$$

Innen könnyű dolgunk van. Az a polinom, ami az a_1, \dots, a_n helyek közül az elsőn b_1 -et, a többi helyen nullát vesz fel, $b_1 L_1(x)$. Az, ami az a_2 helyen b_2 -t, a többi helyen nullát, az pedig $b_2 L_2(x)$. Így a $b_1 L_1(x) + b_2 L_2(x)$ az a_1 helyen b_1 -et, az a_2 helyen b_2 -t vesz fel. Következésképp

$$L(x) = \sum_{i=1}^n b_i L_i(x)$$

egy olyan legfeljebb $n - 1$ -edfokú polinom, amely az a_i helyen a b_i értéket veszi fel. Ezt a polinomot hívják Lagrange interpolációs polinomnak.

4.2 Titokmegosztás polinominterpolációval

Hogyan használhatjuk a polinomokat titokmegosztásra? A válasz nagyon egyszerű, eszfantasztikus ötlet, ami *Adi Shamir*től (az S betű az RSA-ban) származik. A titok egy polinom értéke a 0 helyen. A résztvevőknek szétesztott értékek ugyanennek a polinomnak a helyettesítési értékei különböző (a résztvevőktől függő) helyeken. Ha annyi résztvevő összejön, amennyi a polinom fokánál eggyel nagyobb, akkor a fenti eljárással meg tudják határozni a polinomot, és így annak a 0 helyen felvett értékét, vagyis a titkot.

Ha viszont (legfeljebb) annyian vannak mint amennyi a polinom foka, akkor még hozzávesznek tetszőleges értéket a 0-nál (vagyis elhatározzák mennyi is legyen a titok értéke), és akkor is találnak megfelelő polinomot ami előállítja az ő általuk ismert értékeket, a titokra meg azt az értéket mondja amit ők gondoltak ki. Vagyis nem tudják meghatározni a titkot.

Sajnos ez a megfontolás csak azt adja, hogy *lehetséges* hogy nem tudják meghatározni a titok értékét, azt az erősebb feltételt, miszerint semmi információjuk ne legyen a titok értékéről, még nem. Ugyanis nagyon sok függ attól, hogyan választhá ki az osztó a polinomot. (Magyarul: a polinomokon van egy valószínűségi eloszlás, és annak megfelelően választ egy polinomot véletlenszerűen.) Namármost, ezt az eloszlást valamint a polinom értékét itt-ott ismerve pontosabban megtippelhetjük a polinom nullában felvett értékét mintha a polinom értékét sehol sem ismernénk. Pontosán az ilyen helyzetek elkerüléséhez van szükség a "semmi információ" feltételre.

Amennyiben a polinomokat a valós számok felett használjuk, nem ismeretes hogy létezik-e megfelelő polinom választási módszer. (Ha például a polinomokat megszorítjuk a racionális számokra, akkor valami információ mindenképpen kikerül, ez nem jó választás.) A polinominterpoláció persze nem csak a valósakon működik, hanem tetszőleges testen is, és így a véges testeken is. A megoldás tehát:

Vegyünk egy kellően sok elemű (lásd később) \mathbb{F} véges testet. Minthogy \mathbb{F} véges, lehet az elemei közül egyenletes valószínűséggel véletlenül választani. A szétoztó az alábbi legfeljebb $t-1$ -edfokú polinom

$$a_{t-1}x^{t-1} + a_{t-2}x^{t-2} + \dots + a_2x^2 + a_1x + a_0$$

mind a t együtthatóját egyenletesen és függetlenül válassza \mathbb{F} -ből. A így kapott polinom 0-ban felvett értéke lesz a titok. Az első résztvevő megkapja a polinom értékét az 1 helyen, a második résztvevő a polinom értékét a 2 helyen, és így tovább. Persze ehhez az kell, hogy \mathbb{F} -nek több eleme legyen, mint ahány résztvevőnk van. (Ezért kell hogy a test kellően nagy legyen.)

Ha most t vagy annál több résztvevő összejön, akkor az általuk ismert értékek alapján meg tudják határozni a polinomot, és ki tudják számítani a polinom értékét a 0 helyen (vagyis a_0 értékét). Ezzel megkapják a titkot. Ha viszont t -nél kevesebben vannak, akkor a fenti polinomok közül csak azokat tartva meg, melyek az általuk meghatározott helyeken az általuk ismert értékeket veszik fel, továbbra is igaz, hogy ezek a nullában minden lehetséges értéket pontosan ugyanannyiszor vesznek fel, és ezért a titokról együttesen is csak nulla információjuk van. (Ahhoz hogy ez egy helyes következtetés legyen kell, hogy a test véges.)

4.3 A küszöb titokmegosztás mérete

Láttuk fent, hogy általában egy-egy résztvevőnek igen sok információt kell megjegyeznie. A Shamir-féle konstrukció esetén a titok az \mathbb{F} test egy eleme, és minden résztvevőnek ugyancsak a test egy elemét kell megjegyeznie. Ami azt teszi, hogy mindenki pontosan annyi információt fog megjegyezni, amennyi a titokban van. Ez pedig egy korábbi megjegyezésünk szerint a lehető legjobb.

Azt is láttuk, hogy a testnek több eleme kell legyen, mint ahány résztvevő van. Így ha van 1000 résztvevőnk, akkor \mathbb{F} legalább 1001 elemű kell legyen. Az \mathbb{F} egy elemének leírására körülbelül 10 bit kell. Így ha a titok legalább 10 bites, akkor jók vagyunk: mindenki a titok méretének megfelelő információt jegyez meg. Ámde ha a titok rövid, egy vagy két bites, akkor is mindenkinek nagyjából 10 bitnek megfelelő információt meg kell jegyeznie, vagyis a módszer ebben az esetben messze nem optimális. Nem ismeretes, hogy mikor lehet kevés bitet tartalmazó titkot optimálisan szétoztani.