

Titokmegosztási feladatok

Gyarmati Máté

Eötvös Loránd Tudományegyetem, Budapest
Komputeralgebra tanszék

Motiváció

- Titkos információ (pl. széf kód, jelszó, titkos kulcs, rakéta kilövő kód) elrejtése
- Nem biztonságos, ha egy helyen (egy embernél) van eltárolva
- Titokmegosztás: osszuk szét részekre, és a részeket külön tároljuk. A titkot a részekből csak a megfelelő emberek tudják visszafejteni.

Példa

- Cél: 4 jegyű szám szétosztása 4 személy között, csak 4-en tudják visszafejteni
- Rossz megoldás: Mindenki kap 1 számjegyet
- Jó megoldás: $s \in \mathbb{Z}_{10000}$ titok esetén a titokrészek $a, b, c \in \mathbb{Z}_{10000}$ és $s = a + b + c \pmod{10000}$

Motiváció

- Titkos információ (pl. széf kód, jelszó, titkos kulcs, rakéta kilövő kód) elrejtése
- Nem biztonságos, ha egy helyen (egy embernél) van eltárolva
- Titokmegosztás: osszuk szét részekre, és a részeket külön tároljuk. A titkot a részekből csak a megfelelő emberek tudják visszafejteni.

Példa

- Cél: 4 jegyű szám szétosztása 4 személy között, csak 4-en tudják visszafejteni
- Rossz megoldás: Mindenki kap 1 számjegyet
- Jó megoldás: $s \in \mathbb{Z}_{10000}$ titok esetén a titokrészek $a, b, c \in \mathbb{Z}_{10000}$ és $s = a + b + c \pmod{10000}$

Motiváció

- Titkos információ (pl. széf kód, jelszó, titkos kulcs, rakéta kilövő kód) elrejtése
- Nem biztonságos, ha egy helyen (egy embernél) van eltárolva
- Titokmegosztás: osszuk szét részekre, és a részeket külön tároljuk. A titkot a részekből csak a megfelelő emberek tudják visszafejteni.

Példa

- Cél: 4 jegyű szám szétosztása 4 személy között, csak 4-en tudják visszafejteni
- Rossz megoldás: Mindenki kap 1 számjegyet
- Jó megoldás: $s \in \mathbb{Z}_{10000}$ titok esetén a titokrészek $a, b, c \in \mathbb{Z}_{10000}$ és $s = a + b + c \pmod{10000}$

Motiváció

- Titkos információ (pl. széf kód, jelszó, titkos kulcs, rakéta kilövő kód) elrejtése
- Nem biztonságos, ha egy helyen (egy embernél) van eltárolva
- Titokmegosztás: osszuk szét részekre, és a részeket külön tároljuk. A titkot a részekből csak a megfelelő emberek tudják visszafejteni.

Példa

- Cél: 4 jegyű szám szétosztása 4 személy között, csak 4-en tudják visszafejteni
- Rossz megoldás: Mindenki kap 1 számjegyet
- Jó megoldás: $s \in \mathbb{Z}_{10000}$ titok esetén a titokrészek $a, b, c \in \mathbb{Z}_{10000}$ és $s - a - b - c \pmod{10000}$

Alkalmazások (Titokmegosztás)

Kriptográfiai protokollok

- Biztonságos többrésztvevős számítások (MPC)
- Online aukciók
- Multi-signature (BitCoin)
- Elosztott tanulás: Secure aggregation, secure shuffling
- Attribútum alapú titkosítás
- ...

Additív titokmegosztás

Konstrukció

Additív titokmegosztás

- Titok: $s \in \mathbb{Z}_m$
- Titokrészek
 - $P_i : s_i \in_R \mathbb{Z}_m \ i = 1, \dots, n-1$
 - $P_n : s_n = s - \sum_i s_i \bmod m$

Megjegyzés

An titkot csak egyszerre az összes résztvevő tudja visszafejteni, $n-1$ résztvevő nem elég.

Példa

1 bit titok, A, B, C, D , $s = 1$, $s_A = 1$, $s_B = 0$, $s_C = 1$, $s_D = 1$

Küszöb struktúrák

k -küszöb séma

- P : résztvevők halmaza, $|P| = n$
- s titok
- $A \subseteq P$ vissza tudja fejteni a titkot $\Leftrightarrow |A| \geq k$

Konstrukció (Shamir titokmegosztás)

- 1 $\mathbb{F}$ véges test, $|\mathbb{F}| > n$, $p \in \mathbb{F}[x]$, $\deg p \leq k - 1$
- 2 Titok: $s = p(0)$
- 3 Titokrészek: $s_i = p(i)$
 - Ha $A \subseteq P$ és $|A| \leq k$: Lagrange-interpoláció
 - Ha $A \subseteq P$ és $|A| < k$: semmit sem tudnak kiszámolni s -ről

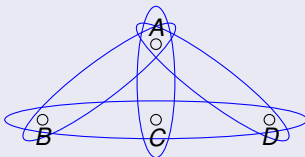
Elérési struktúra

Definíció

- *Résztvevők*: P véges halmaz
- *Elérési struktúra*: $\Gamma \subseteq 2^P$, ami monoton, azaz ha $A \in \Gamma$ és $A \subset B$, akkor $B \in \Gamma$. Γ elemeit kvalifikált halmazoknak hívjuk.

Példa

$$\Gamma_{\min} = \{\{A, B\}, \{A, C\}, \{A, D\}, \{B, C, D\}\}.$$



Hatékonyság

- A titokrészek mérete a titokhoz képest.
- Ha $s, s_i \in S \Rightarrow 1$
- Shamir és additív titokmegosztások hatékonysága 1
- Struktúra ideális, ha létezik titokmegosztás 1 hatékonysággal
- Általános struktúra esetén nagy a hatékonyság (érték nem ismert)

Gráf alapú struktúrák

Ha minden minimális kvalifikált halmaz 2 elemű $\Rightarrow$ reprezentálható gráffal:

- résztvevők $\rightarrow$ csúcsok
- min. kvalifikált halmaz $\rightarrow$ él

Példa

Γ elérési struktúra, résztvevők: A, B, C, D , minimális kvalifikáltak: AB, BC, CD , akkor a gráf egy 3 hosszú út P_3 .

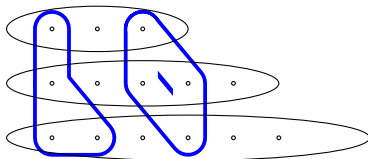
$$A - B - C - D$$

Cél

Minél jobb titokmegosztások készítése gráf alapú struktúrákhoz

Szintezett struktúrák (Hierarchikus)

- Küszöb séma általánosítása



ábra: (1,2,4)-szintezett struktúra

- m osztály, $L_1, \dots, L_m$, $L_1 \cup \dots \cup L_m = P$,
- $0 < t_1 \leq \dots \leq t_m \leq n$ küszöbök.
- $A \in \Gamma$, ha $|A \cap \bigcup_{i=1}^k L_i| \geq t_k$.

Cél

Ideális titokmegosztás, ahol $s, s_i \in S$ -re S kicsi.

1-bit titok

- Shamir titokmegosztás ideális, de titok, titokrészek mérete $\log |\mathbb{F}| > \log n$
- Ha titok 1 bit $\Rightarrow$ nem tud jobbat
- Additív titokmegosztás 1 bit $\Rightarrow$ csak n -küszöb esetén működik

Cél

Minél hatékonyabb titokmegosztás k -küszöb sémákra

Dinamikus titokmegosztás

- P résztvevő, Γ elérési struktúra
- Dinamikus struktúra, Γ változhat
 - Új résztvevő érkezhetsz
 - Résztvevő távozhatsz
 - $A \in \Gamma$, de $A \notin \Gamma'$
 - $A \notin \Gamma$, de $A \in \Gamma'$

Cél

Titokmegosztás, amire

- *Titokrészek nem (ritkán) változnak*
- *Kis titokrészek*
- *Kevés publikus érték*

Köszönetnyilvánítás

Köszönöm a figyelmet!