ELTE IK Diszkrét modellek alkalmazásai

7. gyakorlat

Koch-Gömöri Richárd

2021. október 20.

Titokmegosztás (secret sharing)

Adott egy sztring, amit n ember között akarunk szétosztani úgy hogy:
-senki nem kapja meg a teljes eredeti sztringet
-az eredeti sztring előállításához nem feltétlenül mindenki szükséges
-m-nél kevesebb ember ne tudja előállítani az eredeti sztringet ($m \leq n$)

Shamir titokmegosztás (Shamir's Secret Sharing)

Legyenek $1 \leq m \leq n$ egészek, továbbá $S \in \mathbb{N}$ a titok (secret), amit n ember (participants) között akarunk szétosztani úgy, hogy bármely m részből (threshold) a titok rekonstruálható kegyen, de kevesebből nem.

Legyen $p \in \mathbb{N}$ prímszám úgy, hogy $p > S$ és $p > n$, továbbá válasszunk véletlenszerű $a_1, a_2, ..., a_{m-1} \in \mathbb{Z}_p$ együtthatókat.

Állítsuk elő a $p(x) = a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + ... + a_1x + S \in \mathbb{Z}_p[x]$ polinomot.

Számoljuk ki $i = 1, 2, ..., n$-re az $(i, p(i))$ értékeket (titokrészletek (pieces)) és adjuk oda az i. embernek.

Ekkor bármely m db helyettesítési értékből előállítható a polinom Lagrange-interpolációval, így annak szabad tagja is, de m-nél kevesebb értékből nem.

példa

$n = 4$ ember között osztunk szét

$m = 3$ részből állítható elő

$S = 5$ a titok

ekkor $p > 5$ és $p > 4$, például $p = 7$ alkalmas prímszám

legyen $a_1 = 3, \quad a_2 = 4$

$p(x) = 4x^2 + 3x + 5 \in \mathbb{Z}_7[x]$

a titokrészletek:

$p(1) = 5$

$p(2) = 6$

$p(3) = 1$

$p(4) = 4$

példa

ha pl. a rendelkezésre álló titokrészletek $p(1) = 5, p(3) = 1, p(4) = 4$

$$l_0(x) = \frac{(x-3)\cdot(x-4)}{(1-3)\cdot(1-4)} = 6x^2 + 2 \pmod 7$$

$$l_1(x) = \frac{(x-1)\cdot(x-4)}{(3-1)\cdot(3-4)} = 3x^2 + 6x + 5 \pmod 7$$

$$l_2(x) = \frac{(x-1)\cdot(x-3)}{(4-1)\cdot(4-3)} = 5x^2 + x + 1 \pmod 7$$

$$p(x) = 5\cdot(6x^2+2) + 1\cdot(3x^2+6x+5) + 4\cdot(5x^2+x+1) = 53x^2 + 10x + 19 = 4x^2 + 3x + 5 \pmod 7$$

p szabad tagja 5, ami az eredeti titok