lec 20

Multi-level / hierarchical Secret sharing

Hermite Interpolation: some points on the poly & some points on its derivatives

Example

$x=1$ $f(1)=10$

$x=3$ $f(3)=58$

$x=2$ $f^{(1)}(2)=23$

$x=4$ $f^{(1)}(4)=67$

$$f^{(0)}(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3$$

$$\downarrow$$

$$f^{(1)}(x) = a_1 + 2a_2 x + 3a_3 x^2$$

→ 4 unknowns & 4 equations

$$\begin{cases} f^{(0)}(1) = a_0 + a_1 + a_2 + a_3 = 10 \\ f^{(0)}(3) = a_0 + 3a_1 + 9a_2 + 27a_3 = 58 \\ f^{(1)}(2) = a_1 + 4a_2 + 12a_3 = 23 \\ f^{(1)}(4) = a_1 + 8a_2 + 48a_3 = 67 \end{cases} \longrightarrow \begin{matrix} a_0 = 4 \\ a_1 = 3 \\ a_2 = 2 \\ a_3 = 1 \end{matrix}$$

$$f(x) = 4 + 3x + 2x^2 + x^3$$

Multi-level access structure

(a) each player is assigned to a certain level

(b) each level "L" is associated with a threshold t_L such that

$$t_0 < t_1 < \cdots < t_n$$

ⓐ Disjunctive secret sharing:

A group of players can recover the secret if the group contains at least t_L players at levels $\phi \sim L$ for ~~some~~ level L

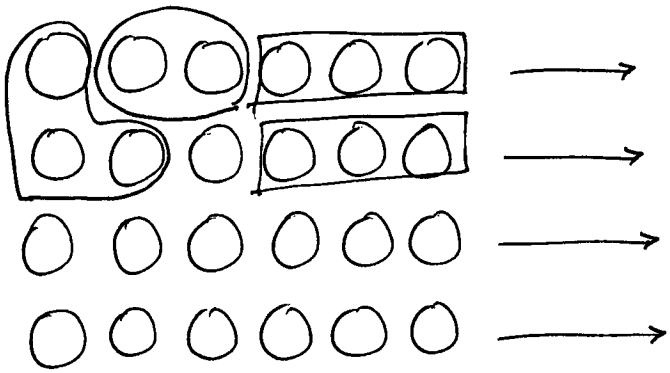
I.e., ~~at least one~~ threshold must be satisfied.

ⓑ Conjunctive Secret sharing

A group of players can recover the secret if the group contains at least t_L players at levels $\phi \sim L$ for ~~every~~ level L

I.e., ~~all~~ the thresholds must be satisfied.

Example: $t_0 < t_1 < \cdots < t_n$



L_0: $t_0 = 2$

L_1: $t_1 = 3$

L_2: $t_2 = 4$

L_3: $t_3 = 6$ max threshold

Disjunctive 1988

2 players at L_0 is enough

$\vee$ 3 players at $L_0 | L_1$

$\vee$ 4 " at $L_0 | L_1 | L_2$

$\vee$ 6 " at $L_0 | L_1 | L_2 | L_3$

* users/players at lower levels are more important & we don't need the contribution of players at all levels

Conjunctive 2004

At least 2 players at L_0

$\wedge$ " 3 " at $L_0 | L_1$

$\wedge$ " 4 " at $L_0 | L_1 | L_2$

$\wedge$ " 6 " at $L_0 | L_1 | L_2 | L_3$

Example of Disjunctive SS

$\mathbb{Z}_{19}$

$t_0 = 2 < t_1 = 3 < t_2 = 4 < t_3 = 6$ max threshold

$f(x) = 2 + 3x + x^2 + 5x^3 + 6x^4 + 13x^5$ ⟶ secret is the leading coefficient

$L_0 \Rightarrow t_0 = 2$ (14,1) (15,3) ⟷ $f^{(6-2=4)}_{(x)} = 11 + 2x$

$L_1 \Rightarrow t_1 = 3$ (11) (12) (13) ⟷ $f^{(6-3=3)}_{(x)} = 11 + 11x + x^2$

$L_2 \Rightarrow t_2 = 4$ (7) (8) (9) (10) ( ) ⟷ $f^{(6-4=2)}_{(x)} = 2 + 11x + 15x^2 + 13x^3$

$6 - t_3 = (0)$

$L_3 \Rightarrow t_3 = 6$ (1) (2) (3) (4) (5) (6) ⟷ $f_{(x)} = 2 + 3x + x^2 + 5x^3 + 6x^4 + 13x^5$

dealer does not need this poly ⊗ $f^{(1)} = 3 + 2x + 15x^2 + 5x^3 + 8x^4$

P_{14} ← (1) share

P_{15} ← (3) share

Ids are in monotonically ~~decreasing~~ order by level (Can be ~~random~~)

$f^{(0)}_{(x)} = a + bx + cx^2 + dx^3 + ex^4 + gx^5$ ⟶ secret: leading coefficient

$f^{(1)}_{(x)} = b + 2cx + 3dx^2 + 4ex^3 + 5gx^4$

$f^{(2)}_{(x)} = 2c + 6dx + 12ex^2 + gx^3$

$f^{(3)}_{(x)} = 6d + 5ex + 3gx^2$

$f^{(4)}_{(x)} = 5e + 6gx \xrightarrow[(15,3)]{(14,1)} \begin{cases} 5e + 6g(14) = 1 \\ 5e + 6g(15) = 3 \end{cases} \longrightarrow$

2 unknowns & 2 equations ⟶ $e = 6$

$\boxed{g = 13}$ ⟶ secret

Example of Conjunctive SS $\mathbb{Z}_{19}$

$t_0 = 2 < t_1 = 3 < t_2 = 4 < t_3 = 6$ Ids are in ~~increasing~~ or ~~random~~ order

$f(x) = \boxed{13} + 3x + x^2 + 5x^3 + 6x^4 + 2x^5 \longrightarrow$ secret is the constant term

$L_0 \Rightarrow t_0 = 2$: (1, 11) (2, 14)

$L_1 \Rightarrow t_1 = 3$: (3, 15)

$L_2 \Rightarrow t_2 = 4$: (6, 8)

$L_3 \Rightarrow t_3 = 6$: (10, 17) (11, 10)

$f^{(0)}(x) = 13 + 3x + x^2 + 5x^3 + 6x^4 + 2x^5$

$f^{(t_0=2)}(x) = 2 + 11x + 15x^2 + 2x^3$

$f^{(t_1=3)}(x) = 11 + 11x + 6x^2$

$f^{(t_2=4)}(x) = 11 + 12x$

$f^{(1)}(x) = 3 + 2x + 15x^2 + 5x^3 + 10x^4$ not required

$f^{(0)}(x) = \boxed{a} + bx + cx^2 + dx^3 + ex^4 + gx^5$

$\begin{cases} a+b+c+d+e+g = 11 \\ a+2b+4c+8d+16e+13g = 14 \end{cases}$

$f^{(2)}(x) = 2c + 6dx + 12ex^2 + gx^3 \longrightarrow \{ 2c + 18d + 13e + 8g = 15$

$f^{(3)}(x) = 6d + 5ex + 3gx^2 \longrightarrow \{ 6d + 11e + 13g = 8$

$f^{(4)}(x) = 5e + 6gx \longrightarrow \begin{cases} 5e + 3g = 17 \\ 5e + 9g = 10 \end{cases}$

$\longrightarrow \boxed{a = 13}$ ✓

$b = 3$ $\quad e = 6$

$c = 1$ $\quad g = 2$

$d = 5$