lecture 07

Threshold Secret sharing (TSS)

① * passive vs active ✓
- → just listen to info & try to learn secrets
- → tries to manipulate values & disrupts the protocol

② * static vs mobile ✓
- → # of corrupted players are defined ahead of time
- → adversary goes around & try to disrupt the protocol while we are executing the protocol

③ * computational vs unconditional

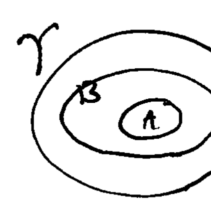
computational ↓
- # factoring 2 long integers
- # discrete log

unconditional ↓
- unlimited computational power

however, we assum less than "t" player can be compromised by the adversary

Def: Access Structure

let $\mathcal{P}$ be a finite set of "n" players $P_1 \cdots P_n$. An access structure Γ is a set of subsets of players (authorized subsets) that satisfies two conditions:



(a) if $A \in \Gamma$ and $A \subseteq B \subseteq \mathcal{P}$, then $B \in \Gamma$

(b) if $A \in \Gamma$ then $|A| > 0$

A secret sharing scheme must have the following properties:

$\boxed{\text{1. Correctness}}$: if the players in an authorized subset combine their shares (shadow), then they recover the secret.

$\boxed{\text{2. Secrecy}}$: if the players in an unauthorized subset combine their shares, then they have no information about the value of the secret.

Lagrange interpolation method

sharing → poly evaluation → $f(x) \to f(2)$

recovery → poly interpolation → $(x_1, y_1), \ldots, (x_n, y_n) \to f(x)$

let "q" be a prime number. Let $x_1 \ldots x_t$ be distinct elements in the finite field $\mathbb{Z}_q$ and let $f_1 \ldots f_t$ be arbitrary elements in $\mathbb{Z}_q$. Then, there is a unique poly $f(x) \in \mathbb{Z}_q[x]$ of degree at most "$t-1$" such that

$$f(x_i) = f_i \quad \text{for } 1 \leq i \leq t$$

$$\begin{cases} (x_1, f_1) \\ (x_2, f_2) \\ \vdots \\ (x_t, f_t) \end{cases}$$

$$f(x) = \sum_{i=1}^{t} \left(\prod_{\substack{1 \leq j \leq t \\ i \neq j}} \frac{x - x_j}{x_i - x_j} * f_i \right)$$

Lagrange Int method for bivariate polys

$f(x,y) \in \mathbb{Z}_q[x,y]$

$f(x, y_i) = f_i(x)$ for $1 \leq i \leq t$

$$f(x,y) = \sum_{i=1}^{t} \left(\prod_{\substack{1 \leq j \leq t \\ j \neq i}} \frac{y - y_j}{y_i - y_j} * f_i(x) \right)$$

* TSS [1979]

$\boxed{\text{secret sharing}}$

1. the dealer "D" selects a random polynomial $f(x) \in \mathbb{Z}_q[x]$ of degree at most $t-1$ such that its constant term is the secret, i.e., $f(0) = \alpha \leftarrow$ secret
2. He sends the share $f(i)$ to P_i for $1 \leq i \leq n$ i.e., each player receives a point on this poly $f(x)$

$(i, f(i))$ → secret value / share of P_i

public / identity of the player

$\boxed{\text{secret Recovery}}$

1. Any subset Δ of at least "t" players can send shares $f(i)$ to a selected player P_j.
2. player P_j recovers secret $f(0) = \alpha$ by LI in the absence of the dealer $f(0) = \sum_{i \in \Delta} \left(\prod_{j \in \Delta, i \neq j} \frac{j}{j-i} * f(i) \right)$

$\boxed{\text{Example of TSS :}}$

secret

$\boxed{\text{Secret sharing}}$ poly is $f(x) = 5 + 3x + 6x^2 \in \mathbb{Z}_{13}[x]$

$\{0 \sim 12\}$

public IDs

P_1, P_2, P_3, P_4

$(1,1) \to f(1) = 5 + 3(1) + 6(1)^2 = 1 \pmod{13}$

$(2,9) \to f(2) = 9 \pmod{13}$

$(3,3) \to f(3) = 3$ 〃

$(4,9) \to f(4) = 9$ 〃

secret shares

$\boxed{\text{Recovery}}$ $P_1, P_2, P_3 \in \Delta$

$$f(0) = \left(\frac{2}{2-1}\right)\left(\frac{3}{3-1}\right)\underbrace{(1)}_{f(1)} + \left(\frac{1}{1-2}\right)\left(\frac{3}{3-2}\right)\underbrace{(9)}_{f(2)} +$$

$$\left(\frac{1}{1-3}\right)\left(\frac{2}{2-3}\right)\underbrace{(3)}_{f(3)} = -21 \pmod{13} = 5$$

Note: $\frac{4}{3} \pmod 7 \equiv 4 * \underbrace{3^{-1}}_{\text{inverse of } 3 \pmod 7 \text{ is } -2 \to -2*3 \overset{7}{\equiv} 1} \pmod 7 \equiv 4 * -2 \overset{7}{\equiv} \boxed{6}$

$$\frac{11}{14} \overset{31}{\equiv} 11 * 14^{-1} \overset{31}{\equiv} 11 * 20 \overset{31}{\equiv} \boxed{3}$$

Inverse