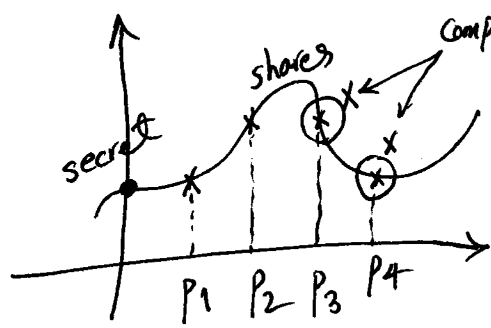
lec 11

Proactive secret sharing (PSS)

PSS is proposed to deal with a mobile adversary

static
vs
Mobile ⟶ he compromised different players while we are executing the protocol

Note: for the sake of simplicity, we assume the adv knows sh_3 & sh_4 (3rd & 4th shares)



$t = 3$

Problem

\# Mobile adv has already compromised P_3 & P_4. If we don't react, he probably compromises another player (P_1 or P_2)

\# you have to keep the same secret in your scheme while resolving this problem.

Solution

\# shares of players are updated periodically without changing the secret. This can be done by adding shares of a new poly with a zero constant term to the shares of the original secret sharing poly. As a result, the secret remains the same and the new secret sharing poly is the summation of two secret sharing polys.

Assumption → # Erasing the old shares is an inevitable assumption.

How to generat a random poly with zero constant term:

random poly

$$g(x) = 4 + 2x + 10x^2 \quad \mathbb{Z}_{13}$$

id

$P_1 \Rightarrow 3 * 1 = 3$

$P_2 \Rightarrow 9 * 2 = 5$

$P_3 \Rightarrow 9 * 3 = 1$

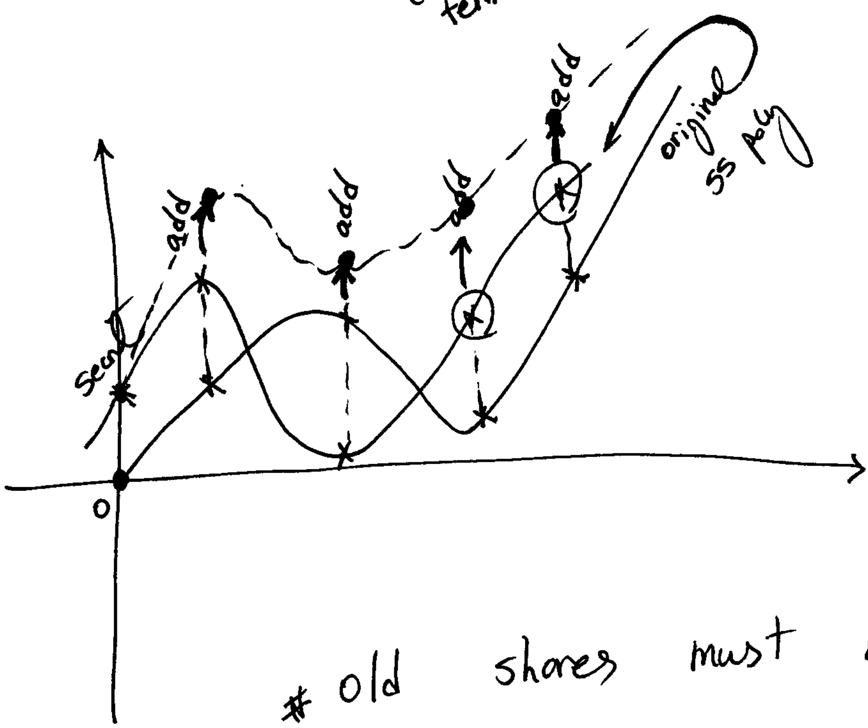
$P_4 \Rightarrow 3 * 4 = 12$

random poly

$$\underbrace{g'(x) = 4x + 2x^2 + 10x^3}_{\text{zero constant term \& degree is higher}}$$

$$\underbrace{x * g(x)}_{deg = t-1} \longrightarrow \underbrace{g'(x)}_{deg = t}$$

$$\alpha \xrightarrow{\text{constant term}} 0$$



old shares must be erased by players

The "sharing" & "recovery" phases are the same as TSS.

After each execution, shares are transformed from $f(x)$ to $\hat{f}(x)$

where $f(0) = \hat{f}(0) = \alpha$ and degrees are $t-1$.

proactive update

1. Each player P_j acts as an independent dealer and shares a polynomial $g_j(x) \in \mathbb{Z}_q[x]$ of degree at most $(t-2)$ with a random constant term.

2. Each P_j sends shares $g_j(i)$ to P_i for $1 \leq i \leq n$, $i \neq j$, i.e., each player receives a point on every secret sharing poly $g_j(x)$. the following matrix shows the shares that each player P_i receives:

$$
\begin{array}{c c}
 & \begin{array}{cccc} \downarrow P_1 & & & \end{array} \\
\begin{array}{c} P_1 \rightarrow \\ P_2 \rightarrow \\ \vdots \\ P_n \rightarrow \end{array} &
\begin{bmatrix} g_1(1) & g_2(1) & \cdots & g_n(1) \\ g_1(2) & g_2(2) & \cdots & g_n(2) \\ \vdots & \vdots & \ddots & \\ g_1(n) & g_2(n) & \cdots & g_n(n) \end{bmatrix} \\
 & \begin{array}{cccc} & \uparrow P_2 & & \uparrow P_n \end{array}
\end{array}
$$

\# each col will be generated by one player

\# each row will be received by one player

3. Each P_i adds all the shares that he has received together and multiplies the result by his identity i as follows.

$$\hat{g}(i) = i * \sum_{j=1}^{n} g_j(i)$$

shares $\sum_{j=1}^{n} g_j(i)$ are on a random poly of degree $(t-2)$ with a random constant term. After multiplying by "i", $\hat{g}(x)$ is a random poly with $\boxed{\text{zero}}$ constant term & its degree is $(t-1)$

④. Now, each P_i has two shares $f(i)$ and $g(i)$ on two polys of degree $(t-1)$ where $f(0) = \alpha$ (secret) and $g(0) = 0$.
Each P_i therefor adds two shares together $\hat{f}(i) = f(i) + g(i)$
keeps $\hat{f}(i)$ and earases $f(i)$ and $g(i)$.

As a result, old shares (on $f(x)$) in the hand of adversary are useless & he has to start over...

Example:

$$f(x) = 3 + 4x + 7x^2 + 5x^3 \in \mathbb{Z}_{13}[x] \longrightarrow$$

$f(1) = 6$
$f(2) = 1$
$f(3) = 5$
$f(4) = 9$

$$g(x) = \underbrace{0 + 4x + 2x^2 + 10x^3}$$

we need 4 polys of degree 2

$g(1) = 3$
$g(2) = 5$
$g(3) = 1$
$g(4) = 12$

$\hat{f}(1) = 9$
$\hat{f}(2) = 6$
$\hat{f}(3) = 6$
$\hat{f}(4) = 8$

new shares

do it yourself $\begin{cases} g_1(x) \\ g_2(x) \\ g_3(x) \\ g_4(x) \end{cases}$

$$\hat{f}(x) = 3 + 8x + 9x^2 + 2x^3$$

New secret sharing polys