Multistage secret sharing scheme

goal may secrets are shared in such a way that all secrets can be recovered separately. Each share is of the same size as that of any single shared secret.

Motivation: almost all SS schems are one-time meaning that after secret recovery, shares & secret are known to everyone.

Contribution: may secrets are shared but only one share is kept by each player.

assumption: The secrets will be reconstructed stage-by-stage in a specific order.

Def: $g(x): \mathbb{Z}_q \longrightarrow \mathbb{Z}_q$ an aribitray one-way function.

$$x \underset{\text{hard}}{\overset{\text{easy}}{\rightleftarrows}} y = f(x)$$

$$\begin{cases} g^0(x) = x \\ g^K(x) = g\left(g^{K-1}(x)\right) \end{cases}$$

$$g^K(x) = g\left(g^{K-1}(x)\right) = g\left(g^0(x)\right) = g(x) \longrightarrow$$ the result of K successive application of "g" on "x"

$$g^{K+1}(x) = g\left(g^K(x)\right) = g\left(g(x)\right)$$

$$g^{K+2}(x) = g\left(g^{K+1}(x)\right) = g\left(g\left(g(x)\right)\right) \quad \dots$$

Secret sharing

$\mathbb{Z}_q$

① The dealer selects "n" arbitrary shares s_j

Note: he does n't use any secret sharing poly at this phase. $1 \leq j \leq n$

② the dealer selects "m" secrets α_i $1 \leq i \leq m$

2.1 $f_i(x) = \alpha_i + a_1 x + a_2 x^2 + \cdots a_{t-1} x^{t-1}$ $\longrightarrow$ we have m secret sharing poly of degree "t-1"

shift values

2.2 $sh_{ij} = f_i(j) - g^{i-1}(s_j)$ $\longrightarrow$ $m \times n$ shift values are calculated

$1 \leq i \leq m$
$1 \leq j \leq n$

③ The dealer sends master-shares $s_1, \ldots, s_n$ (s_j) to players P_j through private channels. He also publishes all shift values sh_{ij} for $1 \leq i \leq m$, $1 \leq j \leq n$ to everyone.

Secret Recovery

① We know each P_j has received S_j from the dealer. P_j is going to calculat:

$$f_i(j) = sh_{ij} + g^{i-1}(S_j)$$

his share with respect to secret α_i

i-th secret

index of P_j

private

public

function is public

As a result all players will have their shares with respect to secret α_i

② At least "t" player combine α_i-s by Lagrange Interpolation to recover secret α_i.

---

assumption: To protect the secrecy of secrets α_i, the players have to recover α_{m-i+1} at stage "i"

Example:

α_1, α_2

$m=2$

$\xrightarrow{i=1} \alpha_{2-1+1} = \alpha_2 \rightarrow$ must be recovered at stage "1"

$\xrightarrow{i=2} \alpha_{2-2+1} = \alpha_1 \rightarrow$ must " " at stage "2"

Example of Multi-stage SS

- Working in $\mathbb{Z}_{13}$.
- The one way function $g(x): \mathbb{Z}_{13} \to \mathbb{Z}_{13}$

$$g(x) = 3^x \bmod 13$$

- Threshold $t = 3$.
- Three players P_1, P_2, P_3

Secret Sharing

1.) The dealer selects three arbitrary shares s_1, s_2, s_3 which equal 1, 2; 4 respectively.

2.) The dealer selects $m = 2$ secrets α_1 and α_2 which equal 7 and 6 respectively.

2.1.) We have 2 secret sharing polys of degree 2.

$$f_1(x) = \underbrace{7}_{\alpha_1} + x + 5x^2$$

$$f_2(x) = \underbrace{6}_{\alpha_2} + 11x + 3x^2$$

2.2.) Shift values are calculated

$$sh_{ij} = f_i(j) - g^{i-1}(s_j)$$

$$1 \le i \le 2$$

$$1 \le j \le 3$$

$$sh_{11} = f_1(1) - g^{1-1}(s_1) = (7+1+5) - 1 \equiv 12 \mod 13$$
$$sh_{12} = f_1(2) - g^{1-1}(s_2) = (7+2+20) - 2 \equiv 1 \mod 13$$
$$sh_{13} = f_1(3) - g^{-1}(s_3) = (7+3+45) - 4 \equiv 12 \mod 13$$
$$sh_{21} = f_2(1) - g^{2-1}(s_1) = (6+11+3) - 3^1 \equiv 4 \mod 13$$
$$sh_{22} = f_2(2) - g^{2-1}(s_2) = (6+22+12) - 3^2 \equiv 5 \mod 13$$
$$sh_{23} = f_2(3) - g^{2-1}(s_3) = (6+33+27) - 3^4 \equiv 11 \mod 13$$

3.) The dealer sends master-shares s_1, s_2, s_3 to players P_1, P_2, P_3 resp.

$$\left.\begin{array}{l} s_1 = 1 \longrightarrow P_1 \\ s_2 = 2 \longrightarrow P_2 \\ s_3 = 4 \longrightarrow P_3 \end{array}\right\} \text{over a private channel.}$$

The dealer also publish all the shift values for all players

$$\underbrace{(sh_{11}, sh_{12}, sh_{13}, sh_{21}, sh_{22}, sh_{23}) = (12, 1, 12, 4, 5, 11)}_{\text{publically known}}$$

Secret Recovery

1.) Each P_j received s_j from the dealer.

P_j is going to calculate:

$$f_i(j) = sh_{ij} + g^{i-1}(s_j).$$

$f_i(j)$ is P_j's share with respect to the secret α_i.

First we calculate the shares for $\alpha_1 = 7$

$P_1 : f_1(1) = sh_{11} + g^{1-1}(s_1) = 12 + 1 \equiv 0 \mod 13$

$P_2 : f_1(2) = sh_{12} + g^{1-1}(s_2) = 1 + 2 \equiv 3 \mod 13$

$P_3 : f_1(3) = sh_{13} + g^{1-1}(s_3) = 12 + 4 \equiv 3 \mod 13$

Now we calculate the shares for $\alpha_2 = 6$.

$P_1 : f_2(1) = sh_{21} + g^{2-1}(s_1) = 4 + 3^1 \equiv 7 \mod 13$

$P_2 : f_2(2) = sh_{22} + g^{2-1}(s_2) = 5 + 3^2 \equiv 1 \mod 13$

$P_3 : f_2(3) = sh_{23} + g^{2-1}(s_3) = 11 + 3^4 \equiv 1 \mod 13$

The shares for $\alpha_1 = 7$ are

$P_1 : (1, 0)$, $P_2 : (2, 3)$, $P_3 : (3, 3)$

The shares for $\alpha_2 = 6$ are

$P_1 : (1, 7)$, $P_2 : (2, 1)$, $P_3 : (3, 1)$

Then use Lagrange to recover the secret,

Stage i, Players recover the secret α_{m-i+1}

stage 1: $\alpha_2 = 7$ is recovered

stage 2: $\alpha_1 = 6$ is recovered.