Dealer-Free Threshold Changeability in Secret Sharing Schemes

Mehrdad Nojoumian
Department of Computer Science
Florida Atlantic University, USA

Douglas R. Stinson
David R. Cheriton School of Computer Science
University of Waterloo, Canada

ICITS 2016
Tacoma, Washington

Dynamic Secret Sharing

- **Motivation:** in a threshold scheme, the sensitivity of the secret as well as the number of players may fluctuate due to various reasons.

  - ✓ Over time, mutual trust might be decreased: perhaps due to the organizational problems or security incidents, and vise versa.

  - ✓ The structure of the organization to which the players belong might be changed: new players may join or current parties may leave.

  Therefore, modifying the threshold and/or changing the secret might be required throughout the lifetime of a secret

- **Contribution:** new dynamic secret sharing schemes.

  - ✓ Dealer-Free: protocols can be executed in the absence of the dealer.
  - ✓ Unconditionally Secure: protocols don't rely on any math assumptions.
  - ✓ Min Storage Cost: parties don't need to store extra shares beforehand.
  - ✓ Flexible: parameters can be changed to arbitrary values multiple times.

t ~> t': Passive Adv - Lagrange Method

Threshold Modification

1. A set Δ is determined such that it consists of the identifiers of at least t elected players. Each player $P_i \in \Delta$ selects a random polynomial $g_i(x)$ of degree at most $t' - 1$ such that $g_i(0) = f(i)$. He then gives $g_i(j)$ to P_j for $1 \leq j \leq n$, i.e., resharing the original shares by auxiliary shares.
2. The following public constants are computed:

$$\gamma_i^{\Delta} = \prod_{j \in \Delta, j \neq i} \frac{j}{j - i} \quad \text{for all } i \in \Delta.$$

3. Each player P_j $(1 \leq j \leq n)$ erases his old shares, and then combines the auxiliary shares he has received from other players to compute his new share as follows:

$$\varphi_j = \sum_{i \in \Delta} \left(\gamma_i^{\Delta} \times g_i(j) \right).$$

the threshold is now t'

Secret Recovery

- Now, if a set Δ' of at least t' players P_j cooperate, they can recover α by using Lagrange interpolation method:

$$\alpha = \sum_{j \in \Delta'} \left(\gamma_j^{\Delta'} \times \varphi_j \right).$$

$t=3 \sim> t'=4$

➢ **Example:** using Lagrange method, let $f(x) = 3+2x+x^2 \in \mathbb{Z}_{19}$

1. Players re-share their shares with new polynomials of degree three, i.e., $t' = 4$.

$$f_1(x) = 6 + x + x^2 + 2x^3 \qquad f_3(x) = 18 + 3x + 2x^2 + x^3$$
$$f_2(x) = 11 + 2x + x^2 + 3x^3 \qquad f_4(x) = 8 + 2x + 2x^2 + 2x^3$$

2. The $\mathcal{E}_{n\times n}$, where each P_i generates a row and receives a column, is as follows:

$$\mathcal{E}_{n\times n} = \begin{pmatrix} 10 & 9 & 15 & 2 \\ 17 & 5 & 12 & 18 \\ 5 & 2 & 15 & 12 \\ 14 & 17 & 10 & 5 \end{pmatrix} \leftarrow \text{P}_3 \text{ generates}$$

3. At this stage, each P_i has to store four shares or players need to define a set Δ in order to convert these shares to a single share. Suppose $\Delta = \{P_1, P_2, P_3\}$

$$\gamma_1 = \frac{(0-2)(0-3)}{(1-2)(1-3)} = 3 \qquad \gamma_2 = \frac{(0-1)(0-3)}{(2-1)(2-3)} = -3 \qquad \gamma_3 = \frac{(0-1)(0-2)}{(3-1)(3-2)} = 1$$

4. At this step, players convert their shares to a single share based on Δ and γ_i-s, and erase their old shares, shown in $\mathcal{E}_{n\times n}$:

$$\varphi_1(x) = (3)10 + (-3)17 + (1)5 = -16 \qquad \varphi_3(x) = (3)15 + (-3)12 + (1)15 = 5$$
$$\varphi_2(x) = (3)9 + (-3)5 + (1)2 = 14 \qquad \varphi_4(x) = (3)2 + (-3)18 + (1)12 = -17$$

t ~> t': Passive Adv - Vandermonde Method

Threshold Modification

1. A set Δ is determined such that it consists of the identifiers of at least t elected players. Each player $P_i \in \Delta$ selects a random polynomial $g_i(x)$ of degree at most $t' - 1$ such that $g_i(0) = f(i)$. He then gives $g_i(j)$ to P_j for $1 \leq j \leq n$, i.e., resharing the original shares by auxiliary shares.

2. Participants then compute the first row of a public matrix $\mathcal{V}^{-1}_{n \times n} \pmod{q}$ to adjust the threshold, where $\mathcal{V}_{n \times n}$ is the Vandermonde matrix, i.e., $\mathcal{V}_{i,j} = i^{(j-1)}$ for $1 \leq i, j \leq n$. Suppose this vector is $\mathcal{V}^{-1}_{1 \times n} = (v_1, \quad v_2, \quad \ldots, \quad v_n)$.

3. Eventually, each player P_j computes his final share by multiplying $\mathcal{V}^{-1}_{1 \times n}$ by his vector of shares:

$$\varphi(j) = \sum_{i=1}^{n} v_i \, g_i(j).$$

the threshold is now t'

Secret Recovery

- To recover the secret, t' participants P_j have to collaborate in order to construct a polynomial of degree $t' - 1$:

$$\varphi(x) = \sum_{j=1}^{t'} \left(\prod_{1 \leq i \leq t', i \neq j} \frac{x - i}{j - i} \times \varphi(j) \right).$$

secret $\varphi(0)$

$t \searrow t$-1: Passive/Active Adv - Public Evaluation

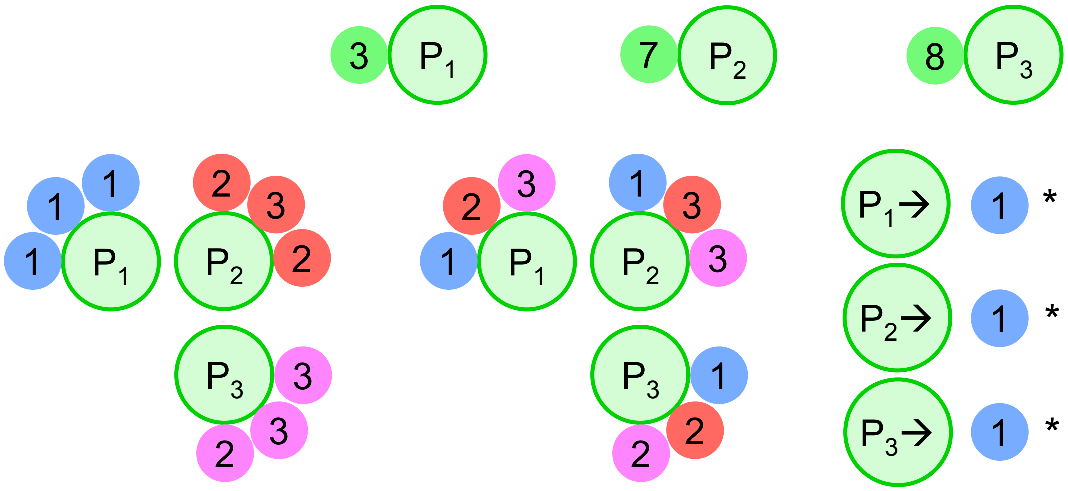
Threshold Decrease

1. The players select an *id* j such that $j \notin \mathcal{P}$. Subsequently, t players P_i are selected (e.g., $1 \leq i \leq t$). They compute Lagrange constants as follows:
$$\gamma_i = \prod_{1 \leq k \leq t, i \neq k} \frac{j-k}{i-k}.$$
2. Each P_i multiplies his share $f(i)$ by his Lagrange constant. He then randomly splits the result into t portions, i.e., $f(i) \times \gamma_i = \partial_{1i} + \partial_{2i} + \cdots + \partial_{ti}$ for $1 \leq i \leq t$.
3. The players exchange ∂_{ki}-s through pairwise channels
As a result, each P_k holds t values. He adds them together and reveals $\sigma_k = \sum_{i=1}^{t} \partial_{ki}$
4. The players add these values σ_k for $1 \leq k \leq t$ together to compute the public share $f(j) = \sum_{k=1}^{t} \sigma_k$.
5. Each P_i combines his private share $f(i)$ with the public share $f(j)$ as follows:
$$\hat{f}(i) = f(j) - j\left(\frac{f(i) - f(j)}{i-j}\right).$$
6. The shares $\hat{f}(i)$ are on a new polynomial $\hat{f}(x) \in \mathbb{Z}_q[x]$ of degree $t-2$ where $\hat{f}(0) = f(0)$. Therefore, $t-1$ players are now sufficient to recover the secret.

t=3 ~> t'=2

- **Example:** let $f(x) = 9 + 2x + 5x^2 \in Z_{13}$

*** Can be seen as the "Enrolment Protocol"**



? **P_4: Public Share**

$P_1 \rightarrow$ 1 * 1 + 2 * -3 + 3 * 3 = 4

$P_2 \rightarrow$ 1 * 1 + 3 * -3 + 3 * 3 = 1

$P_3 \rightarrow$ 1 * 1 + 2 * -3 + 2 * 3 = 1

} 6

$$\hat{f}(i) = f(j) - j\left(\frac{f(i) - f(j)}{i - j}\right)$$

$\hat{f}(1) = 6 - 4\,(3 - 6/1 - 4) = 2$

$\hat{f}(2) = 6 - 4\,(7 - 6/2 - 4) = 8 \rightarrow \hat{f}(x) = 9 + 6x \in Z_{13}$

$\hat{f}(3) = 6 - 4\,(8 - 6/3 - 4) = 1$

$t \nearrow t'$: Passive/Active Adv - Zero Addition

Threshold Increase

For every player P_i, suppose $f(i)$ is the share of an unknown secret α belonging to P_i.

1. Players use polynomial production to generate shares of an unknown secret δ on a polynomial $g(x)$ of degree $t' - 2$.

his public identity

2. Each player P_i multiplies his share $g(i)$ by i. Now, each P_i has a share of 0 on the polynomial $\hat{g}(x) = xg(x)$ of degree $t' - 1$.

3. Each player adds his share $f(i)$ of α to his share $ig(i)$ of 0. As a result, each player has a share of α, where the new threshold is $t' > t$.

Polynomial Production

1. Initially, t players P_i are selected at random in order to act as independent dealers; they each might be honest or malicious.

2. Each of the t chosen players P_i shares a secret, say δ_i, among all the players using a Shamir scheme, where the degree of the secret sharing polynomial is $t - 1$. Then all players have shares of every secret δ_i.

3. Every player adds his shares of the δ_i-s together. As a result, each player has a share on a polynomial $g(x)$ of degree $t - 1$ with a constant term $\delta = \sum \delta_i$.

Summary of Threshold Modification Techniques

Threshold Change	Passive Adversary	Active Adversary
Decrease	Re-sharing by Lagrange Method Re-Sharing by Vandermonde Matrix Public Evaluation	Public Evaluation
Increase	Re-sharing by Lagrange Method Re-Sharing by Vandermonde Matrix Zero Addition	Zero Addition

Thank You Very Much

Special Thanks to Dr. Douglas R. Stinson

More Resources:

- ✓ Nojoumian M. and Stinson D. R., On Dealer-free Dynamic Threshold Schemes, *Advances in Mathematics of Communications (AMC), American Institute of Mathematical Sciences (AIMS)*, vol. 7, no. 1, pp. 39-56, 2013.

- ✓ Nojoumian M., Novel Secret Sharing and Commitment Schemes for Cryptographic Applications, *PhD Thesis, David R. Cheriton School of Computer Science, U of Waterloo, Canada*, 2012.