# Secret Sharing Schemes

## Cryptography - CS 411 / CS 507

Erkay Savaş

Department of Computer Science and Engineering
Sabancı University

December 12, 2023

# Problem Statement

- Distribution of a secret among multiple users in a secure way such that only a coalition of users is able to construct the secret.

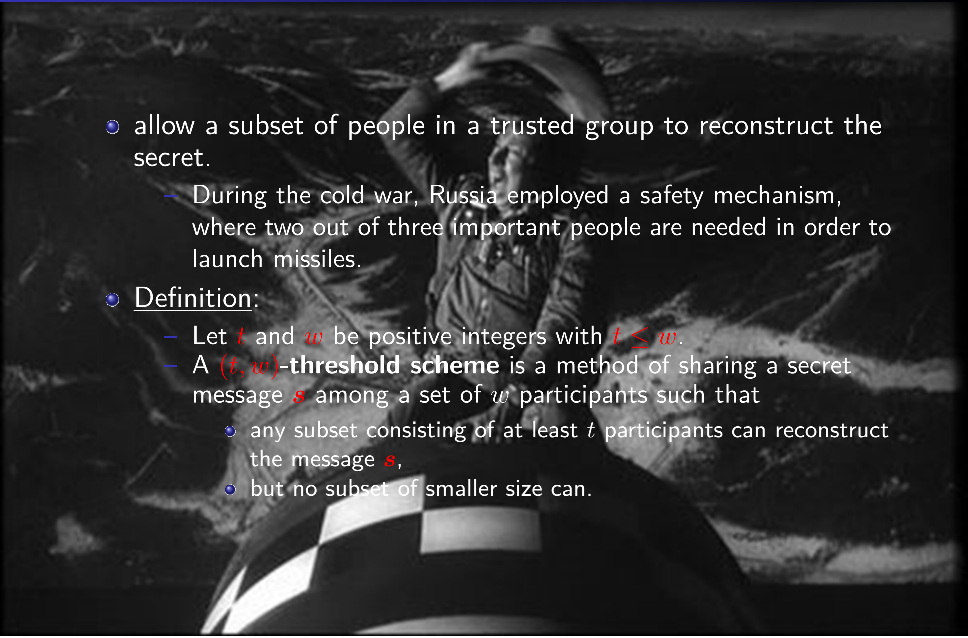
# Secret Splitting

- Consider a case where a secret message $s$ is to be shared among a group of $w$ people.
- Choose an integer $p$ larger than all possible messages. $s < p$.
- Choose $w-1$ random numbers $r_1, r_2, \ldots, r_{w-2} < p$ and give them to $w-1$ people in the group, and

$$r_{w-1} = s - \sum_{k=0}^{w-2} r_k \bmod p$$

  to the last person.
- All the people must get together to construct the secret message $s$.

# Threshold Schemes



- allow a subset of people in a trusted group to reconstruct the secret.
  - During the cold war, Russia employed a safety mechanism, where two out of three important people are needed in order to launch missiles.
- Definition:
  - Let $t$ and $w$ be positive integers with $t \leq w$.
  - A $(t, w)$-**threshold scheme** is a method of sharing a secret message $s$ among a set of $w$ participants such that
    - any subset consisting of at least $t$ participants can reconstruct the message $s$,
    - but no subset of smaller size can.

# Shamir Threshold Scheme

- Also known as Lagrange Interpolation Scheme.
  - A prime $p$, which must be larger than all possible messages, is chosen.
  - The secret message $s < p$, will be split among $w$ people in such a way that at least $t$ of them are needed to reconstruct it.
- Method
  - Select $t - 1$ integers at random,
    - $0 \leq s_1, s_2, \ldots, s_{t-1} < p$
  - Construct a secret polynomial
    - $S(x) = s + s_1 x + s_2 x^2 + \ldots + s_{t-1} x^{t-1} \bmod p$
    - $s = S(0) \bmod p = s_0$

# Shamir Threshold Scheme

- For $w$ participants,
  - Evaluate the polynomial at $w$ different values of $x$
  - $y_k = S(x_k) \bmod p \quad k = 1, 2, \ldots, w$
  - each person is given a pair $(x_k, y_k)$ (e.g., $(k, y_k)$)
- The polynomial $S(x)$ is kept secret, $p$ is known.
- Any $t$ people can reconstruct the message $s$ by using linear system approach.
  - Assume their pairs are $(x_{i_0}, y_{i_0}), \ldots, (x_{i_{t-1}}, y_{i_{t-1}})$.
  - $y_k = S(x_k) = s + s_1 x_k + s_2 {x_k}^2 + \ldots + s_{t-1} {x_k}^{t-1} \bmod p$ for $k \in \Lambda$, where $\Lambda = \{i_0, i_1, \ldots\ i_{t-1}\}$ and $|\Lambda| = t$.
  - Let us denote $s_0 = s$.

- We can come up with the following linear system

$$\begin{bmatrix} 1 & x_{i_0} & \cdots & {x_{i_0}}^{t-1} \\ 1 & x_{i_1} & \cdots & {x_{i_1}}^{t-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_{i_{t-1}} & \cdots & {x_{i_{t-1}}}^{t-1} \end{bmatrix} \cdot \begin{bmatrix} s_0 \\ s_1 \\ \vdots \\ s_{t-1} \end{bmatrix} \equiv \begin{bmatrix} y_{i_0} \\ y_{i_1} \\ \vdots \\ y_{i_{t-1}} \end{bmatrix} \bmod p$$

- If the determinant of the matrix $V$ is nonzero, the linear system has a unique solution $\mathrm{mod} p$.

$$\det V = \prod_{1 \leq j < k \leq t} (x_k - x_j) \bmod p$$

- The determinant of $V$ is nonzero, hence the system has a unique solution, as long as we have distinct $x_k$'s.

- An alternative approach that leads to a formula for the reconstruction of the polynomial.
- Our goal is to reconstruct the polynomial $S(x)$ given that we know of $t$ of its values $(x_k, y_k)$.
- Assume $k \in \Lambda \subset \{1, 2, \ldots, w\}$, where $|\Lambda| = t$ (namely, $\Lambda$ is the coalition of $t$ share holders)
- First,

$$l_k(x) = \prod_{\substack{j \in \Lambda \\ j \neq k}} \frac{x - x_j}{x_k - x_j} \bmod p \qquad k \in \Lambda$$

$$l_k(x_i) = \begin{cases} 1 & \text{when} \quad k = i \\ 0 & \text{when} \quad k \neq i \end{cases}$$

# Reconstruction of the Polynomial

- The Lagrange interpolation polynomial

  $$p(x) = \sum_{k \in \Lambda} y_k l_k(x)$$

  satisfies the requirement $p(x_k) = y_k$ for $k \in \Lambda$.
- We know $S(x) = P(x)$.
- To reconstruct the secret message we have to evaluate the polynomial at $x = 0$ (i.e., $s = P(0)$).

$$s = \sum_{k \in \Lambda} y_k \prod_{\substack{j \in \Lambda \\ j \neq k}} \frac{-x_j}{x_k - x_j} \bmod p \qquad s = \sum_{k \in \Lambda} y_k \lambda_k \bmod p$$

$$\lambda_k = \prod_{\substack{j \in \Lambda \\ j \neq k}} \frac{-x_j}{x_k - x_j} \bmod p \qquad k \in \Lambda$$

# Reconstruction of the Polynomial

- Generally,
  - $x_k = k$
  - $s = \sum_{k \in \Lambda} y_k \lambda_k \bmod p$
  - $\lambda_k = \prod_{\substack{j \in \Lambda \\ j \neq k}} \frac{j}{j-k} \bmod p \qquad k \in \Lambda$

# Example 1/3

- $(3, 8)$-threshold scheme:
  - we have $8$ people and we want any $3$ of them to be able to determine the secret.
- Let the secret message $s = 19$;
  - and we choose the next prime $p = 23$.
- Choose random integer as $s_1 = 6$ and $s_2 = 11$; hence
  - $S(x) = 19 + 6x + 11x^2 \bmod 23$.
- We now give eight people pairs $(x_k, y_k)$:
  - $(1, 13)$, $(2, 6)$, $(3, 21)$, $(4, 12)$, $(5, 2)$, $(6, 14)$, $(7, 2)$, $(8, 12)$.

## Example 2/3

- Suppose the participants 3, 5, and 6 come together and collaborate to calculate the secret (i.e., $\Lambda = \{3, 5, 6\}$).
  - $(3, 21)$, $(5, 2)$, $(6, 14)$
- They have to calculate
  $p(x) = y_3 l_3(x) + y_5 l_5(x) + y_6 l_6(x)$

$$l_3(x) = \frac{x - x_5}{x_3 - x_5} \cdot \frac{x - x_6}{x_3 - x_6} = \frac{(x-5)(x-6)}{6}$$
$$l_5(x) = \frac{x - x_3}{x_5 - x_3} \cdot \frac{x - x_6}{x_5 - x_6} = -\frac{(x-5)(x-6)}{2}$$
$$l_6(x) = \frac{x - x_3}{x_6 - x_3} \cdot \frac{x - x_5}{x_6 - x_5} = \frac{(x-3)(x-5)}{3}$$

# Example 3/3

- $y_3 = 21$, $y_5 = 2$, and $y_6 = 14$, then

$$p(x) = \frac{21}{6}(x-5)(x-6) - \frac{2}{2}(x-3)(x-6) + \frac{14}{3}(x-3)(x-5)$$
$$= \frac{21(x^2-11x+7) - 6(x^2-9x+18) + 5(x^2-8x+15)}{6}$$
$$= \frac{20x^2-10x-1}{6} \bmod 23$$

since $6^{-1} \equiv 4 \bmod 23$

$\rightarrow 4 \cdot 20x^2 - 4 \cdot 10x - 4 \cdot 1 \equiv 11x^2 + 6x + 19 \bmod 23$

# Variations on Threshold Schemes

- Hybrid schemes (Access Structures)
  - Two companies A and B share a bank vault.
  - Four employees from A and three employees from B are needed in order to obtain the secret combination ($s$) to the vault.
  - Apply, first, secret splitting: $s \equiv s_A + s_B \bmod p$.
  - Apply, then, $(t, w)$-threshold schemes
  - $(4, w_A)$-threshold scheme for $s_A$.
  - $(3, w_B)$-threshold scheme for $s_B$.
- By giving certain persons more shares, it is possible to make some people more important than the others.

# Complex Threshold Schemes

- A certain military office, which is in control of a powerful missile, consists of one general, two colonels, 5 captains.
- The following combinations can launch the missile
  1. One general
  2. Two colonels
  3. 5 captains
  4. One colonel + 3 captains.
- Describe the threshold scheme which implements this.

# Recall: ElGamal Encryption Algorithm

- Setup:
  - $p$, $q$ are two large primes with $q|p-1$ and $g$ is a generator in $G_q \subset \mathbb{Z}_p^*$
- Key Generation:
  - $s \leftarrow \mathbb{Z}_q$ (secret key)
  - $h = g^s \mod p$ (public key)
- Encryption:
  - $m$ : message
  - $k \leftarrow \mathbb{Z}_q$
  - $(c_0, c_1) = (g^k \mod p, h^k m \mod p)$ (ciphertext)
- Decryption:
  - $c_1 c_0^{-s}$

# Threshold ElGamal Encryption Algorithm

- The secret key is shared among $w$ parties, $y_k$ , $1 \leq k \leq w$
- Party $P_k$ holds $y_k$
- Let $\Lambda$ be a subset of $t$ participants;
  - e.g., $\Lambda = \{k_1, k_2, \ldots, k_t\}$
  - $s \equiv \sum_{k \in \Lambda} y_k \lambda_k \bmod q$, where $\lambda_k = \prod_{\substack{j \in \Lambda \\ j \neq k}} \frac{j}{j-k} \bmod q$
- Encryption: $(c_0, c_1) = (g^k \bmod p, h^k m \bmod p)$
- Decryption:
  - Party $P_k$ computes and publishes $\gamma_k = c_0^{y_k} \bmod p$
  - We, then, compute $c_1 (\prod_{k \in \Lambda} \gamma_k^{\lambda_k})^{-1} \bmod q$