Secret Sharing Schemes

Cryptography - CS 411 / CS 507

Erkay Savaş

Department of Computer Science and Engineering
Sabancı University

December 13, 2019

Problem Statement

- Distribution of a secret among multiple users in a secure way such that only a coalition of users is able to construct it.
- Application:
  - The secret code for nuclear arm launcher
  - The secret key for decryption of election results

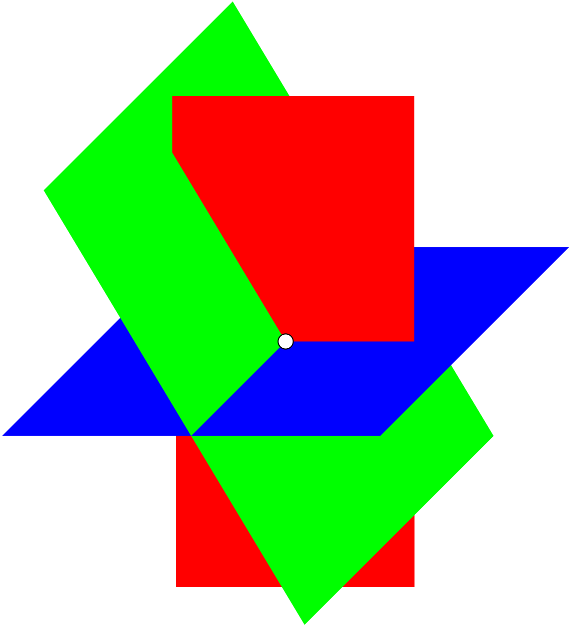
Secret Splitting

- Consider a case where a secret message M is to be shared among a group of w people.
- Choose an integer n larger than all possible messages. $M < n$.
- Choose $w-1$ random numbers $r_1, r_2, \ldots, r_{w-1} < n$ and give them to $w-1$ people in the group, and
$$r_w = M - \sum_{k=1}^{w-1} r_k \bmod n$$
to the last person.
- All the people must get together to construct the secret message M.

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.
- <u>Definition</u>:
  - Let t and w be positive integers with $t \leq w$.
  - A (t, w)-threshold scheme is a method of sharing a message M among a set of w participants such that
    - any subset consisting of at least t participants can reconstruct the message M,
    - but no subset of smaller size can.

Blakley's Method for Secret Sharing



Blakley's Method 1/4

- From 1979.
- There are several people (possibly more than three); any three people can find the secret, but no two can.
- Choose a prime p and let $x_0 < p$ be the secret.
- Choose y_0 and z_0 randomly $(y_0, z_0 < p)$.
- $Q = (x_0, y_0, z_0)$ is a point in three-dimensional space $\bmod p$.
- Each person is given the equation of a plane passing through Q.

Blakley's Method 2/4

- Choose a_i and $b_i \bmod p$ at random for each person and then compute
$$c_i = z_0 - a_i x_0 - b_i y_0 \bmod p \quad (i = 1, 2, \ldots, w)$$
- The planes
$$z = a_i x + b_i y + c_i \bmod p \quad (i = 1, 2, \ldots, w)$$
- This is done for each person.
- All planes will intersect in a point, which must be Q (whose x coordinate is the secret).
- Two planes will intersect in a line, so usually no information can be obtained concerning the secret x_0 (be careful here).

Blakley's Method 3/4

- Example: In a Blakley $(3, w)$ scheme, suppose A and B are given planes $z = 2x + 3y + 13$ and $z = 5x + 3y + 1$.
- A and B can recover the secret without the third person.
- $2x + 3y + 13 = 5x + 3y + 1 \rightarrow 3x = 12 \rightarrow x_0 = 4$.
- They cannot determine (y_0, z_0).
- The secret must be distributed among three coordinates (x_0, y_0, z_0). A proper mapping must be found between points and the messages.

Blakley's Method 4/4

- Three people who want to determine the secret can proceed as follows.
- They have three equations
  $z = a_i x + b_i y + c_i \bmod p \qquad 1 \leq i \leq 3.$
- We can have the following matrix equation
  $$\begin{pmatrix} a_1 & b_1 & -1 \\ a_2 & b_2 & -1 \\ a_3 & b_3 & -1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix} \equiv \begin{pmatrix} -c_1 \\ -c_2 \\ -c_3 \end{pmatrix} \bmod p$$
- As long as the determinant of this matrix is nonzero $\bmod p$, the matrix can be inverted and the secret is found.

Example: Blakley's Method

- $p = 73$
- Suppose users A, B, C, D, E are given the following planes:
  - A: $z = 4x + 19y + 68$
  - B: $z = 52x + 27y + 10$
  - C: $z = 36x + 65y + 18$
  - D: $z = 57x + 12y + 16$
  - E: $z = 34x + 19y + 49$
- If A, B, and C want to recover the secret, they solve

$$\begin{pmatrix} 4 & 19 & -1 \\ 52 & 27 & -1 \\ 36 & 65 & -1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix} \equiv \begin{pmatrix} -68 \\ -10 \\ -18 \end{pmatrix} \bmod 73 \to \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix} = \begin{pmatrix} 42 \\ 29 \\ 57 \end{pmatrix}$$

Generalization of Blakley's Scheme

- By using $(t-1)$-dimensional hyperplanes in t-dimensional space, we can create a (t, w)-threshold scheme for any values of t and w.
- As long as p is reasonably large, it is very likely that the matrix is invertible, although this is not guaranteed.
- It is hard to arrange ways to choose $(a_i, b_i, c_i, \ldots)$ so that the matrix is always invertible.
- Shamir's method could be regarded as a special case of the Blakley's method in this sense.
- However, Shamir's method always yields a Vandermonde matrix, which guarantees a solution.
- Shamir's method also requires less information to be carried by each person. ((x, y) vs. $(a, b, c, \ldots)$).

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 $M < p$, 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
    - $S(x) = M + s_1 x + s_2 x^2 + \ldots + s_{t-1} x^{t-1} \bmod p$
    - $S(0) \bmod p = M = s_0$

Shamir Threshold Scheme

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

- We can come up with the following linear system

$$\begin{bmatrix} 1 & x_{i_1} & \cdots & x_{i_1}^{t-1} \\ 1 & x_{i_2} & \cdots & x_{i_2}^{t-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_{i_t} & \cdots & x_{i_t}^{t-1} \end{bmatrix} \cdot \begin{bmatrix} s_0 \\ s_1 \\ \vdots \\ s_{t-1} \end{bmatrix} \equiv \begin{bmatrix} y_{i_1} \\ y_{i_2} \\ \vdots \\ y_{i_t} \end{bmatrix} \mod p$$

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

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

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

Reconstruction of the Polynomial

- 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 $k \in \Lambda \subset \{1, 2, ..., w\}$, where $|\Lambda| = t$ (namely, Λ is the colation of t share holders)
- First,

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

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

Reconstruction of the Polynomial

- The Lagrange interpolation polynomial

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

  satisfies the requirement $p(x_i) = y_i$ for $1 \leq i \leq w$.
- We know $S(x) = p(x)$.
- To reconstruct the secret message we have to evaluate the polynomial at $x = 0$.

  $$M = \sum_{k \in \Lambda}^{t} y_k \prod_{\substack{j \in \Lambda \\ j \neq k}} \frac{-x_j}{x_k - x_j} \bmod p$$

  Or, $M = \sum_{k \in \Lambda}^{t} y_k \lambda_k \bmod p$, where $\lambda_k = \prod_{\substack{j \in \Lambda \\ j \neq k}} \frac{x_j}{x_j - x_k} \bmod p$

Example 1/4

- $(3, 8)$-threshold scheme:
  - we have 8 people and we want any 3 of them to be able to determine the secret.
- Let the secret message $M = 19$;
  - 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_i, y_i):
  - $(1, 13)$, $(2, 6)$, $(3, 21)$, $(4, 12)$, $(5, 2)$, $(6, 14)$, $(7, 2)$, $(8, 12)$.

Example 2/4

- Suppose the participants 3, 5, and 6 come together and collaborate to calculate the secret.
  - $\Lambda = \{3, 5, 6\}$
  - $(3, 21)$, $(5, 2)$, $(6, 14)$
- 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 3/4

- $y_3 = 21$, $y_5 = 2$, 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 $6^{-1} \equiv 4 \bmod 23$

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

Example 4/4

- If we are looking for only the secret
- $(x_3, y_3) = (3, 21)$, $(x_5, y_5) = (5, 2)$, and $(x_6, y_6) = (6, 14)$
- $M = \sum_{k \in \Lambda}^{t} y_k \lambda_k \mod p$, where $\lambda_k = \prod_{\substack{j \in \Lambda \\ j \neq k}} \frac{j}{j-k} \mod p$
- $M = y_3\lambda_3 + y_5\lambda_5 + y_6\lambda_6 \mod 23$,
- $\lambda_3 = \frac{5}{5-3}\frac{6}{6-3} \mod 23 = 5$,
- $\lambda_5 = \frac{3}{3-5}\frac{6}{6-5} \mod 23 = 14$,
- $\lambda_6 = \frac{3}{3-6}\frac{5}{5-6} \mod 23 = 5$,
- $M = 21 \cdot 5 + 2 \cdot 14 + 14 \cdot 5 \mod 23 = 19$.

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: $s = s_A + s_B \bmod p$.
  - 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.

- **ElGamal Encryption Scheme**
  - p, q are two large primes with $q|p-1$ and g is a generator in $\mathbb{G}_q \subset \mathbb{Z}_p^*$
  - **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 Scheme

- The secret key is shared among w parties, $s_j, 1 \leq j \leq w$.
- Party P_j holds s_j
- Let Λ be a subset of t participants; e.g., $\Lambda = \{j_1, j_2, \ldots, j_t\}$
- Then, $s = \sum_{j \in \Lambda} \lambda_j s_j$, where $\lambda_j = \prod_{\substack{l \in \Lambda \\ l \neq j}} \frac{l}{l-j} \mod q$
- **Encryption:** $(c_0, c_1) = (g^k \mod p, h^k m \mod p)$
- **Decryption:**
  - Party P_j computes and publishes $\gamma_j = c_0^{s_j} \mod p$
  - We, then, compute $c_1 \left(\prod_{j \in \Lambda} \gamma_j^{-\lambda_j} \right)$