Secret Sharing Schemes

Cryptography – CS 507
Erkay Savas
Sabanci University
erkays@sabanciuniv.edu
Problem Statement

• Distribution of a secret among multiple users in a secure way s.t. only a coalition of users is able to construct the secret.

• *Example*: You are the owner of a restaurant and what makes your operation successful is a secret recipe for a specially prepared dessert. You don’t want to tell the whole recipe to one employee since s/he might quit working for you and open up her/his own restaurant. Instead, one employee is allowed to know only a small part of the recipe and to prepare the dessert takes several employee putting their pieces together.
Secret Splitting

- Consider a case where a secret message $M$ is to be shared among $m$ people.
- Choose an integer $n$ larger than all possible messages.
- Choose $m-1$ random numbers $r_1, r_2, \ldots, r_{m-1} \mod n$ and give them to $m-1$ of the people, and

$$M - \sum_{k=1}^{m-1} r_k \pmod{n}$$

to the remaining person.
- All the people must get together to construct the secret message $M$. 
Threshold Schemes

- Threshold schemes allow a subset of the people in 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 $t$, $w$ 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 s.t. any subset consisting of $t$ participants can reconstruct the message $M$, 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. All computations are done mod $p$.
- The secret message $M$, represented as an integer mod $p$, will be split among $w$ people in such a way that $t$ of them are needed to reconstruct it.
- Select randomly $t-1$ integers mod $p$, $s_1$, $s_2$, ..., $s_{t-1}$.
- The polynomial
  \[ S(x) \equiv M + s_1x + s_2x^2 + \ldots + s_{t-1}x^{t-1} \pmod{p} \]
  is a polynomial s.t. $s(0) \equiv M \pmod{p}$. 

12/18/2002  Erkay Savas
Shamir Threshold Scheme

- For \( w \) participants, distinct integers \( x_1, x_2, \ldots, x_w \) (mod \( p \)) are selected and each person is given a pair \((x_i, y_i)\) with \( y_i \equiv S(x_i) \) (mod \( p \)).
- 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 \((x_1, y_1), \ldots, (x_t, y_t)\).
- \( y_i = S(x_i) \equiv M + s_1 x_i + s_2 x_i^2 + \ldots + s_{t-1} x_i^{t-1} \) (mod \( p \)) for \( 1 \leq k \leq t \).
- Let us denote \( s_0 = M \).
- Then we can construct the following matrix.
Shamir Threshold Scheme

\[
\begin{bmatrix}
1 & x_1 & \cdots & x_1^{t-1} \\
1 & x_2 & \cdots & x_2^{t-1} \\
\vdots & \vdots & \ddots & \vdots \\
1 & x_t & \cdots & x_t^{t-1} \\
\end{bmatrix} 
\begin{bmatrix}
s_0 \\
s_1 \\
\vdots \\
s_t \\
\end{bmatrix} \equiv 
\begin{bmatrix}
y_1 \\
y_2 \\
\vdots \\
y_t \\
\end{bmatrix} \pmod{p}
\]

- The matrix, \( V \), is what is known as a Vandermonde matrix. It is known that this system has a unique solution mod \( p \) if the determinant of \( V \) is nonzero mod \( p \).

\[
\det V = \prod_{1 \leq j < k \leq t} (x_k - x_j)
\]

- 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 a polynomial \( S(x) \) given that we know of \( t \) of its values \((x_i, y_i)\).

• First,

\[
l_k(x) = \prod_{\substack{j=1 \atop j \neq k}}^{t} \frac{x - x_j}{x_k - x_j} \quad \text{(mod } p\text{)}
\]

• Where

\[
l_k(x_i) = \begin{cases} 
1 & \text{when } k = i \\
0 & \text{when } k \neq i
\end{cases}
\]
Reconstruction of the polynomial

• The *Lagrange interpolation polynomial*

\[ p(x) = \sum_{k=1}^{t} y_k l_k(x) \]

satisfies the requirement \( p(x_i) = y_i \) for \( 1 \leq i \leq t \).

• We know \( S(x) = p(x) \).

• To reconstruct the secret message we have to evaluate the polynomial at \( x = 0 \).

\[ M \equiv \sum_{k=1}^{t} y_k \prod_{\substack{j=1 \atop j \neq k}}^{t} \frac{-x_j}{x - x_j} \pmod{p} \]
Example

• (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 $s_1 = 6$ \textit{and} $s_2 = 11$; hence $S(x) = 19 + 6x + 11x^2 \pmod{23}$.

• 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

- Suppose the persons 3, 5, and 6 come together and collaborate to calculate the secret.
- They have to calculate

\[ p(x) = y_3 l_3(x) + y_5 l_5(x) + y_6 l_6(x) \]

\[ l_3(x) = \frac{x - x_5}{x_3 - x_5} \cdot \frac{x - x_6}{x_3 - x_6} = \frac{(x - 5)(x - 6)}{6} \]

\[ l_5(x) = \frac{x - x_3}{x_5 - x_3} \cdot \frac{x - x_6}{x_5 - x_6} = -\frac{(x - 3)(x - 6)}{2} \]

\[ l_6(x) = \frac{x - x_3}{x_6 - x_3} \cdot \frac{x - x_5}{x_6 - x_5} = \frac{(x - 3)(x - 5)}{3} \]
Example

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

\[
p(x) = \frac{21}{6} (x - 5)(x - 6) - \frac{2}{2} (x - 3)(x - 6) + \frac{14}{3} (x - 3)(x - 5)
\]

\[
= \frac{21(x^2 - 11x + 7) - 6(x^2 - 9x + 18) + 5(x^2 - 8x + 15)}{6}
\]

\[
= \frac{20x^2 - 10x - 1}{6} \quad \text{(mod 23)}
\]

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

\[
\Rightarrow 4 \cdot 20x^2 - 4 \cdot 10x - 4 \cdot 1 \equiv 11x^2 + 6x + 9 \quad \text{(mod 23)}
\]
Blakley Method for Secret Sharing

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

- Choose $a_i$ and $b_i \mod p$ at random for each person and then compute
  \[ c_i \equiv z_0 - a_i x_0 - b_i y_0 \pmod{p} \]
- The plane
  \[ z \equiv a_i x + b_i y + c_i \pmod{p} \]
- This is done for each person.
- Three planes will intersect in a point, which must be $Q$.
- Two planes will intersect in a line, so usually no information can be obtained concerning the secret $x_0$. 

Blakley’s Method for Secret Sharing

• But one must be careful with Blakley’s Method.
• Example: In a Blakley (3, w) scheme, suppose persons 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.
• $2x + 3y + 13 = 5x + 3y + 1 \Rightarrow 3x = 12 \Rightarrow x_0 = 4$.
• We cannot determine $(y_0, z_0)$.
• The secret can be distributed among three coordinates $(x_0, y_0, z_0)$. A proper mapping must be found between points and the meaningful messages.
Blakley’s Method for Secret Sharing

- Three persons who want to determine the secret can proceed as follows.
- They have three equations
  \[ z \equiv a_i x + b_i y + c_i \pmod{p} \quad 1 \leq i \leq 3. \]
- We can have the following matrix equation
  \[ \begin{pmatrix} a_1 & b_1 & -1 \\ a_2 & b_2 & -1 \\ a_3 & b_3 & -1 \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix} \equiv \begin{pmatrix} -c_1 \\ -c_2 \\ -c_3 \end{pmatrix} \pmod{p} \]
- As long as the determinant of this matrix is nonzero mod \( p \), the matrix can be inverted and the secret is found.
Example: Blakley Method

- \( p = 73 \). Suppose we give A, B, C, D, E the following planes:
  A: \( z \equiv 4x + 19y + 68 \)
  B: \( z \equiv 52x + 27y + 10 \)
  C: \( z \equiv 36x + 65y + 18 \)
  D: \( z \equiv 57x + 12y + 16 \)
  E: \( z \equiv 34x + 19y + 49 \)

- If A, B, and C want to recover the secret, they solve
  \[
  \begin{pmatrix}
  4 & 19 & -1 \\
  52 & 27 & -1 \\
  36 & 65 & -1 \\
  \end{pmatrix}
  \begin{pmatrix}
  x_0 \\
  y_0 \\
  z_0 \\
  \end{pmatrix}
  \equiv
  \begin{pmatrix}
  -68 \\
  -10 \\
  -18 \\
  \end{pmatrix}
  \pmod{73}
  \]
  \[(x_0, y_0, z_0) = (42, 29, 57)\]
Generalization of Blakley Scheme

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

- By giving certain persons more shares, it is possible to make some people more important than the others.
- 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 to the vault.
- Apply, first, secret splitting: \( s \equiv c_A + c_B \pmod{p} \).
- Apply, then, \((t, w)\)-threshold schemes
  - \((4, w_A)\)-threshold scheme for \(c_A\).
  - \((3, w_B)\)-threshold scheme for \(c_B\).
Designing a complex threshold scheme

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