Lecture 16-17: Secret Sharing Schemes

Thomas Johansson

Motivating examples

- (1992) Control of nuclear weapons in Russia involves a two-out-of-three mechanism.
  - In order to launch a nuclear missile, the cooperation of at least two parties out of three are needed.
  - The three parties involved are the president, the Defence Minister, and the Defence Ministry.
- Bank: a vault that must be opened every day.
  The bank employs senior tellers. We would like to design a system where any two of the senior tellers together can open the vault, but no individual alone can do so.

The above problems can be solved by means of a *secret sharing scheme*.

Threshold schemes

Definition

Let k and n be positive integers, $k \leq n$. A (k, n)-threshold scheme is a method of sharing a secret K among a set of n participants in such a way that any k participants can compute the value of the secret, but no group of $k-1$ or fewer can do so.

Threshold schemes

- Set of participants $= \mathcal{P}$.
- the secret K is chosen by the *dealer* D.
- When D wants to share the secret K among the participants in $\mathcal{P}$, D gives each participant some partial information, called a *share*.
- The shares are secret, no participant knows any other participant's share.
- At a later time, some $\mathcal{B} \subseteq \mathcal{P}$ would like to compute K. They will then pool their shares together and compute K.

Shamir Threshold Scheme

- $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$,
- $\mathcal{K}$ set of secrets, and $\mathcal{S}$ set of shares.
- $\mathcal{K} = \mathbb{Z}_p$, where $p \geq n + 1$ is a prime,
- $\mathcal{S} = \mathbb{Z}_p$.

Shamir Threshold Scheme

Initilization:

D chooses n distinct non-zero elements from $\mathbb{Z}_p$, denoted x_i, $1 \leq i \leq n$. All these values are public.

Share Distribution:

1. D wants to share the secret $K \in \mathbb{Z}_p$. D randomly chooses $k-1$ elements of $\mathbb{Z}_p$, denoted $a_1, a_2, \ldots, a_{k-1}$. Furthermore, $a_0 = K$.
2. D computes $y_i = a(x_i)$, for $1 \leq i \leq n$, where

$$a(x) = \sum_{j=0}^{k-1} a_j x^j \mod p.$$

3. D gives participant P_i the share y_i.

Shamir Threshold Scheme

- The dealer constructs a random polynomial of degree at most $k-1$ in which the constant term is the secret K, i.e., $a_0 = K$.
- Every participant obtains a point (x_i, y_i) on this polynomial.
- This works if any k participants can reconstruct the polynomial $a(x)$; and secondly if no group of $k-1$ participants can do so.

I: How k participants can reconstruct $a(x)$

- Assume that $\mathcal{B} = \{P_1, P_2, \ldots, P_k\}$.
- The participants in $\mathcal{B}$ know

$$y_i = a(x_i), \quad 1 \leq i \leq k,$$

where $a(x) \in \mathbb{Z}_p[x]$ is the secret polynomial.

- The polynomial $a(x)$ has degree at most $k-1$ and, hence, can be written

$$a(x) = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1},$$

where the coefficients $a_0, a_1, \ldots, a_k$ are unknown elements of $\mathbb{Z}_p$ and $a_0 = K$ is the secret.

- Each participant knowing $y_i = a(x_i)$ can obtain one linear equation in the k unknowns $a_0, a_1, \ldots, a_{k-1}$.

I: How k participants can reconstruct $a(x)$

- So the group $\mathcal{B}$ has k linear equations at its disposal.
- If they are all linearly independent, there will be a unique solution, and a_0 will be revealed.

The system of linear equations is the following:

$$\begin{aligned} a_0 + a_1 x_1 + a_2 x_1^2 + \cdots + a_{k-1} x_1^{k-1} &= y_1, \\ a_0 + a_1 x_2 + a_2 x_2^2 + \cdots + a_{k-1} x_2^{k-1} &= y_2, \\ \vdots \qquad\qquad\qquad\qquad\qquad\quad &\vdots \quad \vdots \\ a_0 + a_1 x_k + a_2 x_k^2 + \cdots + a_{k-1} x_k^{k-1} &= y_k, \end{aligned}$$

I: How k participants can reconstruct $a(x)$

In matrix form:

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{k-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_k & x_k^2 & \dots & x_k^{k-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_k \end{pmatrix} = \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_k \end{pmatrix}.$$

- The coefficient matrix, we call it A, is a so-called Vandermonde matrix.
- There is a well-known formula for the determinant of a $k \times k$ Vandermonde matrix, namely

$$\det A = \prod_{1 \le i < j \le k} (x_i - x_j) \mod p.$$

I: How k participants can reconstruct $a(x)$

- x_i's are all distinct, the product cannot equal 0, and $\det A \neq 0$.
- Non-zero determinant, implies a unique solution over $\mathbb{Z}_p$.
- Conclusion: any k participants can recover the polynomial $a(x)$ and, hence, the secret K.

(example)

II: Why $k-1$ participants cannot reconstruct $a(x)$

What will happen if $k-1$ participants tries to compute the secret?

- Proceeding as above, they will end up with a system of $k-1$ linear equations in k unknowns.
- Suppose $K = y_0$. Since the secret $K = a_0 = a(0)$, we have

$$y_0 = a(0),$$

  and this will yield a kth linear equation.
- As before, there is now a unique solution for $a(x)$.
- So for every possible value y_0 of the secret K, there is a unique polynomial $a_{y_0}(x)$ such that

$$y_i = a_{y_0}(x_i),$$

  for $1 \leq i \leq k-1$, and such that

$$y_0 = a_{y_0}(0).$$

- No value of the secret can be ruled out by a group of $k-1$ participants!

Alternative method of calculating $a(x)$

- **The Lagrange interpolation formula:** An explicit formula for the unique polynomial $a(x)$ of degree at most $k-1$, when the values in k different points

$$y_1 = a(x_1), y_2 = a(x_2), \ldots, y_k = a(x_k)$$

are given.

- $$a(x) = \sum_{i=1}^{k} y_i \prod_{1 \le j \le k, j \neq i} \frac{x - x_j}{x_i - x_j}.$$

Verify the correctness of the formula by substituting $x = x_i$, and all terms in the sum vanish except for the ith term, which is y_i.

Computing K by Lagrange interpolation

- The group is only interested in calculating the secret $K = a_0$.
- Since $K = a_0 = a(0)$, we substitute $x = 0$ into the Lagrange interpolation formula and get

$$K = \sum_{i=1}^{k} y_i \prod_{1 \leq j \leq k, j \neq i} \frac{x_j}{x_j - x_i}.$$

(example)

A simplified construction for (k, k)-threshold schemes

Consider the following (k, k)-threshold scheme.

1. The dealer D chooses k random shares $y_1, y_2, \ldots, y_k$ from $\mathbb{Z}_m$, and gives y_i to participant i as the share.
2. The secret K is chosen to be

$$K = \sum_{i=1}^{k} y_i \mod m.$$

The k participants can recover the key by adding all their shares.

Access structures and general secret sharing

- Let Γ be a set of subset of $\mathcal{P}$, $\Gamma \subseteq 2^{\mathcal{P}}$
- Subsets in Γ specify those subset of participants that are qualified to compute the secret.
- Γ is called an *access structure*.
- If $\mathcal{B} \subseteq \mathcal{P}$, then we denote by B the set of shares for $\mathcal{B}$.

Access structures and general secret sharing

Definition

A secret sharing scheme for the access structure Γ is a method of sharing a secret K among a set of n participants in such a way that the following two properties hold:

1. If $\mathcal{B} \in \Gamma$, then $H(K|B) = 0$.
2. If $\mathcal{B} \notin \Gamma$, then $H(K|B) \geq log\ \alpha$,

where α is a fixed value and $\alpha > 1$.

We see that a (k, n)-threshold scheme has access structure

$$\Gamma = \{\mathcal{B} \subseteq \mathcal{P}; |\mathcal{B}| \geq k\}.$$

Access structures and general secret sharing

Definition

A secret sharing scheme for which $\alpha = |\mathcal{K}|$ is called a *perfect* secret sharing scheme.

In a perfect secret sharing scheme any non-qualified subset of participants gets no information about the secret.

Definition

A secret sharing scheme is called *ideal* if it is perfect and if $|\mathcal{S}| = |\mathcal{K}|$.

An ideal secret sharing scheme is perfect and has also the smallest possible size of each participants share.

Properties of access structure Γ

- Suppose $\mathcal{B} \in \Gamma$ and we add one participant to the set $\mathcal{B}$. This set must also be qualified, since it contains a qualified subset. We have

$$\text{if } \mathcal{B} \in \Gamma \text{ and } \mathcal{B} \subseteq \mathcal{C} \subseteq \mathcal{P}, \text{ then } \mathcal{C} \in \Gamma.$$

  Such an access structure is called a *monotone access structure*.
- The *closure* of an access structure Γ, denoted $\mathrm{cl}(\Gamma)$

$$\mathrm{cl}(\Gamma) = \{\mathcal{C} \subseteq \mathcal{P}; \mathcal{B} \subseteq \mathcal{C}, \mathcal{B} \in \Gamma\}.$$

Properties of access structure Γ

- It is easy to see that an access structure is monotone if and only if

$$\Gamma = \mathsf{cl}(\Gamma).$$

- **We assume that if Γ is not monotone, we mean $\mathsf{cl}(\Gamma)$.**

Constructing a perfect secret sharing scheme for any Γ

Initilization:

D chooses any access stucture Γ such that

$$\mathsf{cl}(\Gamma) = \mathsf{cl}(\Gamma_0).$$

Write Γ in the form

$$\Gamma = \{\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_l\},$$

where $\mathcal{B}_i \subseteq \mathcal{P}$ for $1 \leq i \leq l$. $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_l$ is public information.

Share Distribution:

Let $\mathcal{K} = \mathbb{Z}_m$. For each $\mathcal{B}_j = \{P_{i_1}, P_{i_2}, \ldots, P_{i_k}\}$, D does:

1. D constructs a (k, k)-threshold scheme for $\mathcal{K}$ with participants $\mathcal{B}_j$, meaning that D chooses k random values $a_{j1}, a_{j2}, \ldots, a_{jk}$ such that

$$K = a_{j1} + a_{j2} + \cdots + a_{jk} \mod \mathbb{Z}_m.$$

2. D gives the value a_{jm} to participant P_{i_m}, $1 \leq m \leq k$, as a piece of that participant's share.

Constructing a perfect secret sharing scheme for any Γ

- The share for participant i is then the set of pieces that P_i has received.
- The number of pieces is the same as the number of times that P_i can be found in the subsets $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_l$.

(example)