Secret Sharing

Daniel Sanchez

Motivation

• Is it secure to keep private/secret information in a single central location?

• If we distribute private/secret information to multiple parties how much risk is added?
Goal of Secret Sharing Schemes

- Goal is to divide D (the secret) into n pieces D₁, ..., Dₙ such that:
  - Knowledge of any k, where k≤n, or more Dᵢ pieces allows for the feasible computation of the secret D.
  - Knowledge of k-1 or fewer Dᵢ pieces provides no information for an adversary about the secret D.

Secret Sharing Schemes

- A secret sharing scheme is a pair of two algorithms <Share, Rec>.
  - \( Share(D) \rightarrow (D₁, ..., Dₙ) \)
  - \( Rec(D₁, ..., D_k) \rightarrow D \)
  - \( Rec(Share(D)) \rightarrow D \)
N-out-of-N Secret Sharing Scheme

- Assume that $D \in G$ where G is an abelian group under addition

$\text{Share}(D)$

$S_1, S_2, ..., S_{n-1} \leftarrow_r G$

$S_n = D - (S_1 + ... + S_{n-1})$

return $(S_1, ..., S_n)$

$\text{Rec}(S'_1, ..., S'_n)$

$D' = S'_1 + ... + S'_n$

Perfect Privacy for N-out-of-N Scheme

- Assume that an adversary has obtained $N - 1$ shares and the missing share is denoted $S_i$

$S_1 + ... + S_{N-1} + S_i = D$

Case 1: $S_i$ was originally picked randomly from the group

Case 2: $S_i$ was the share constructed from $D - (S_1 + ... + S_{N-1})$
Shamir’s Secret Sharing Scheme

- Assume that $F$ is a finite field where $|F| > n$ and $D \in F$
- Choose $n$ random non-zero points, $z_1, ..., z_n \in F$
- Choose a prime $p$ such that $p > n$ and $p > |D|$

$Share(D)$

Choose $a_1, ..., a_{k-1} \leftarrow_R F$
Define $P_D(x) = D + a_1x + a_2x + ... + a_{k-1}x^{k-1} \mod p$
Let $S_i = P_D(z_i)$
Each share is $(z_i, S_i)$

Proof of Feasible Computation

- There exists a bijection from $(a_0, ..., a_{k-1}) \leftrightarrow (P_D(z_0), ..., P_D(z_{k-1}))$
  - From $a \rightarrow P_D(z)$ simply reconstruct $P_D$ and evaluate at points $z$
  - From $P_D(z) \rightarrow a$ use Lagrange Interpolation:

$$P_D(z) = \sum_{i=0}^{k-1} P_D(z_i) \prod_{0 \leq j \leq k-1}^{j \neq i} \frac{x - z_j}{z_j - z_i}$$
Proof of Feasible Computation

• There exists a bijection from \((a_0, ..., a_{k-1}) \leftrightarrow (P_D(z_0), ..., P_D(z_{k-1}))\)
  • Optimize Lagrange Interpolation by only calculating actual secret value

\[
P_D(0) = \sum_{i=0}^{k-1} P_D(z_i) \prod_{0 \leq j \leq k-1 \setminus i} \frac{z_j}{z_j - z_i}
\]

Shamir Secret Sharing Scheme

Share\((D)\)

Choose \(a_1, ..., a_{k-1} \leftarrow_R F\)
Define \(P_D(x) = D + a_1 x + a_2 x + ... + a_{k-1} x^{k-1} \mod p\)
Let \(S_i = P_D(z_i)\)
Return \(((z_1, S_1), ..., (z_n, S_n))\)

Rec\((S_i, ..., S_k)\)

\(D' = OLI(S_1, ..., S_k)\)
Return \(D'\)
Perfect Privacy of Shamir Secret Sharing

- Need to show that $P[D = d] = P[D = d | P_D(z_i) = S_i, ..., P_D(z_t) = S_t]$ for $0 \leq t \leq k$

$$P[D = d | P_D(z_{i_1}) = S_{i_1}, ..., P_D(z_{i_t}) = S_{i_t}]$$

$$= \frac{P[D = d, P_D(z_{i_1}) = S_{i_1}, ..., P_D(z_{i_t}) = S_{i_t}]}{P[P_D(z_{i_1}) = S_{i_1}, ..., P_D(z_{i_t}) = S_{i_t}]}$$

$$= \frac{P[P_D(0) = d, P_D(z_{i_1}) = S_{i_1}, ..., P_D(z_{i_t}) = S_{i_t}]}{P[P_D(z_{i_1}) = S_{i_1}, ..., P_D(z_{i_t}) = S_{i_t}]}$$

$$= P[P_D(0) = d] = P[D = d]$$

Useful Properties Shamir Secret Sharing

- You can dynamically add and remove shares of the secret without having to compute new shares for each person.

- Create a hierarchy with the distribution of keys to certain individuals based on their role in the hierarchy

- Each share does not exceed the original length of the secret
Citations
