Algorithms of Information Security: Secret sharing

Faculty of Information Technology
Czech Technical University in Prague

October 27, 2020

Secret sharing

- *Secret sharing* refers to methods for distributing a secret among a group of participants, each of whom is allocated a share of the secret. The secret can be reconstructed only when a sufficient number, of possibly different types, of shares are combined together; individual shares are of no use on their own.
- Secret sharing was invented independently by Adi Shamir and George Blakley in 1979.

Shamir's Secret Sharing (SSS)

- Shamir's Secret Sharing (SSS) is used to secure a secret in a distributed way, most often to secure other encryption keys. The secret is split into multiple parts, called *shares.* These shares are used to reconstruct the original secret. To unlock the secret via Shamir's secret sharing, you need a minimum number of shares. This is called the *threshold,* and is used to denote the minimum number of shares needed to unlock the secret.

Shamir's Secret Sharing (SSS)

- *Problem:* Company XYZ needs to secure their vault's passcode. They could use something standard, such as AES, but what if the holder of the key is unavailable or dies? What if the key is compromised via a malicious hacker or the holder of the key turns rogue, and uses their power over the vault to their benefit?
- This is where SSS comes in. It can be used to encrypt the vault's passcode and generate a certain number of shares, where a certain number of shares can be allocated to each executive within Company XYZ. Now, only if they pool their shares can they unlock the vault. The threshold can be appropriately set for the number of executives, so the vault is always able to be accessed by the authorized individuals. Should a share or two fall into the wrong hands, they couldn't open the passcode unless the other executives cooperated.

Shamir's (t, n) Threshold Scheme.

- Shamir proposed a (t, n) threshold scheme that splits a secret $s \in S$ into n shares, which are distributed to n users.
- Splitting is done by a dealer using an algorithm called *share generation algorithm.* The algorithm uses a polynomial $f(x)$ of degree $t - 1$ to generate and distribute shares.
- The secret is reconstructed based on interpolating a polynomial using Lagrange interpolation, which is reconstructed by t users.
- The users combine their shares to reconstruct a polynomial $f'(x)$ of degree t using reconstruction algorithm. The algorithm inputs the user's identity i and their share v_i, which forms a point or an ordered pair (i, v_i) for all $i = 1, 2, \ldots, t$ and outputs the secret $f'(0) = s$.

Shamir's (t, n) Threshold Scheme.

Shamir's scheme has the following important properties.

- Share size is exactly equal to secret size.
- If a new player joins or leaves, it is easy to add or delete shares without affecting the other shares.
- It is easy to change the shares of the same secret just by changing the polynomial without breaching any security.
- $t - 1$ users do not reveal any information about the secret.

Lagrange interpolation.

Theorem

Given t distinct points (x_i, y_i) of the form $(x_i, f(x_i))$, where $f(x)$ is a polynomial of degree less that t, then $f(x)$ is determined by

$$f(x) = \sum_{i=1}^{t} y_i \prod_{\substack{1 \le j \le t \\ j \neq i}} \frac{x - x_j}{x_i - x_j} \qquad (1).$$

Proof. Let $g(x)$ be the right hand side of (1). For each x_i in we verify directly that $f(x_i) = g(x_i)$, so that $f(x) - g(x)$ is divisible by $x - x_i$. It follows that

$$\prod_{i=1}^{t} (x - x_i) \mid (f(x) - g(x)) \qquad (2)$$

but since $deg(f(x) - g(x)) \le t$, the only polynomial of this degree satisfying equation (2) is $f(x) - g(x) = 0$.

Shamir's scheme.

Shamir's scheme is defined for a secret $s \in \mathbb{Z}/p\mathbb{Z}$ with p prime, by setting $a_0 = s$, and choosing $a_1, \ldots, a_{t-1}$ at random in $\mathbb{Z}/p\mathbb{Z}$. The trusted party computes $f(i)$, where

$$f(x) = \sum_{k=0}^{t-1} a_k x^k,$$

for all $1 \leq i \leq n$. The shares $(i, f(i))$ are distributed to the n distinct parties. Since the secret is the constant term $s = a_0 = f(0)$, the secret is reovered from any t shares $(i, f(i))$, for $I \subset \{1, \ldots, n\}$ by

$$s = \sum_{i \in I} c_i f(i), \text{where each } c_i = \prod_{\substack{j \in I \\ j \neq i}} \frac{i}{j - i}.$$

Shamir's scheme - example

Example. Shamir secret sharing with $p = 31$. Let the threshold be $t = 3$, and the secret be $7 \in \mathbb{Z}/31\mathbb{Z}$. We choose elements at random $a_1 = 19$ and $a_2 = 21$ in $\mathbb{Z}/31\mathbb{Z}$, and set $f(x) = 7 + 19x + 21x^2$. As the trusted part, we can now generate as many shares as we like

$$(1, f(1)) = (1, 16) \qquad (5, f(5)) = (5, 7)$$
$$(2, f(2)) = (2, 5) \qquad (6, f(6)) = (6, 9)$$
$$(3, f(3)) = (3, 5) \qquad (7, f(7)) = (7, 22)$$
$$(4, f(4)) = (4, 16) \qquad (8, f(8)) = (8, 15)$$

which are distributed to the holders of the share recipients, and the original polynomial $f(x)$ is destroyed. The secret can be recovered from the formula

$$f(x) = \sum_{i=1}^{t} y_i \prod_{\substack{1 \le j \le t \\ j \neq i}} \frac{x - x_j}{x_i - x_j} \Longrightarrow \qquad f(0) = \sum_{i=1}^{t} y_i \prod_{\substack{1 \le j \le t \\ j \neq i}} \frac{x_j}{x_j - x_i}$$

Shamir's scheme - example

Using any t shares $(x_1, y_1), \ldots, (x_t, y_t)$. If we take the first three shares (1,16), (2,5), (3,5), we compute

$$\begin{aligned} f(0) &= \frac{16 \cdot 2 \cdot 3}{(1-2)(1-3)} + \frac{5 \cdot 1 \cdot 3}{(2-1)(2-3)} + \frac{5 \cdot 1 \cdot 2}{(3-1)(3-2)} \\ &= 3 \cdot 2^{-1} + 15 \cdot (-1) + 10 \cdot 2^{-1} = 17 - 15 + 5 = 7. \end{aligned}$$

This agrees with the same calculation for the shares (1,16), (5,7), and (7,22),

$$\begin{aligned} f(0) &= \frac{16 \cdot 5 \cdot 7}{(1-5)(1-7)} + \frac{7 \cdot 1 \cdot 7}{(5-1)(5-7)} + \frac{22 \cdot 1 \cdot 5}{(7-1)(7-5)} \\ &= 2 \cdot 24^{-1} + 18 \cdot (-8)^{-1} + 17 \cdot 12^{-1} = 13 + 21 + 4 = 7. \end{aligned}$$