Secret Sharing (Threshold) Schemes
Ahmet Burak Can
Hacettepe University
abc@hacettepe.edu.tr

Secret Sharing in Real World
- A bank safe can be protected with a combination of locks, keys.

Secret Sharing in Digital World
- How would you distribute a secret among n parties, such that only t or more of them together can reconstruct it.
  - Answer: A (t, n)-threshold scheme
  - Create n keys
  - Reveal the secret by using t of the keys
- Some applications:
  - Storage of sensitive cryptographic keys
  - Command & control of nuclear weapons

A Secret Sharing Scheme
Example: An (n, n)-threshold scheme:
- To share a k-bit secret, the dealer D
  - generates n − 1 random k-bit numbers (shares) $y_i$, where $i = 1, 2, ..., n \text{−} 1$,
  - $y_k = K \oplus y_1 \oplus y_2 \oplus \ldots \oplus y_{n-1}$,
  - gives the share $y_k$ to party $P_k$.
- This is a “perfect” SSS: A coalition of less than t can not obtain information about the secret.
- Q: How to generalize to arbitrary (t, n)?
3.11.2016

Polynomials

Shamir’s (t, n)-threshold Scheme

- Preparing and distributing the keys:
  - The dealer chooses prime p such that p ≥ n+1, K ∈ Z^*_p;
  - generates distinct, random, non-zero x_i ∈ Z^*_p, i = 1, ..., n;
  - generates random a_i ∈ Z_p, i = 1, ..., t – 1;
  - a_0 = K, the secret;
  - f(x) = ∑_{i=0}^{t-1} a_i x^i mod p
  - f(x) = a_0 + a_1 x + ... + a_{t-1} x^{t-1} mod p
  - i-th person’s share is (x_i, f(x_i)).

- Combining t keys and reconstructing the secret K
  - l(x) = ∏_{i=1}^{t} 1/(x - x_i) mod p
  - f(x) = ∑_{i=1}^{t} l(x) a_i mod p
  - f(x) = K

Lagrange Interpolation

- Take a polynomial f(x)
  - f(x) = a_0 + a_1 x + ... + a_{t-1} x^{t-1}
  - Compute f(x) values for x_i ∈ Z^*_p, i = 1, ..., t;

- Given t (x_i, f(x_i)) pairs, we can reconstruct f(x) as follows:
  - l(x) = ∏_{j=1, j≠i}^{t} (x - x_j) / (x_i - x_j)
  - f(x) = ∑_{i=1}^{t} l(x_i) y_i

Example: Shamir’s (3, 6)-threshold Scheme

- This example does not use modulus operation, so it’s not a real Shamir’s scheme. The example basically shows Lagrangian interpolation.
- n = 6, t = 3, K = 1234,
  - We randomly obtain 2 numbers: a_1 = 166, a_2 = 94
  - a_0 = K = 1234
  - f(x) = 1234 + 166x + 94x²
  - We construct six points:
    - (1, 1401); (2, 1942); (3, 2578); (4, 3402); (5, 4414); (6, 5614)
  - To reconstruct the key any 3 points will be enough. Assume that we have these keys:
    - (x_1, y_1) = (2, 1942); (x_2, y_2) = (4, 3402); (x_3, y_3) = (5, 4414)
Example: Shamir’s (3, 6)-threshold Scheme-2

- From these 3 keys, we compute I values:
  \[ I_0 = \frac{x - r_1}{x_0 - x_1}, \frac{x - r_2}{x_0 - x_2}, \frac{x - r_3}{x_0 - x_3} = \frac{x - 1}{2 - 1}, \frac{x - 3}{2 - 3}, \frac{x - 5}{2 - 5} = \frac{1}{1}, \frac{1}{6}, \frac{1}{3} \]
  \[ I_1 = \frac{x - r_1}{x_1 - x_0}, \frac{x - r_2}{x_1 - x_2}, \frac{x - r_3}{x_1 - x_3} = \frac{x - 1}{4 - 1}, \frac{x - 3}{4 - 3}, \frac{x - 5}{4 - 5} = \frac{1}{3}, \frac{1}{1}, \frac{1}{4} \]
  \[ I_2 = \frac{x - r_1}{x_2 - x_0}, \frac{x - r_2}{x_2 - x_2}, \frac{x - r_3}{x_2 - x_3} = \frac{x - 1}{6 - 1}, \frac{x - 3}{6 - 3}, \frac{x - 5}{6 - 5} = \frac{1}{5}, \frac{1}{3}, \frac{1}{1} \]

- Then, we compute \( f(x) \):
  \[
  f(x) = \sum_{j=0}^{3} I_j \cdot \ell_j(x) \\
  = 1942 \left( \frac{1}{5} x^2 - \frac{1}{3} x + \frac{1}{5} \right) + 3405 \left( \frac{1}{1} x^2 + \frac{1}{3} x - 5 \right) + 4414 \left( \frac{1}{3} x^2 - 2 x + 2 \right) \\
  = 1234 + 106e + 94e^2
  \]

Secret Sharing Scenarios

- **Scenario-1**
  - 5 generals, each have a share of a key which can launch nuclear missile
  - 3 generals have to provide their shares to reconstruct the key
  - A (3,5)-threshold scheme is needed.

- **Scenario-2**
  - A bank branch with 10 bank tellers and a manager
  - 7 tellers or the manager with 4 tellers can open the safe
  - How do you define the threshold schemes?
    - (7,13)-threshold scheme: 1 key for tellers, 3 keys for manager
    - (7,10)-threshold scheme (1 key for each teller)
    - (4,10)-threshold scheme (1 key for each teller) and (2,2)-threshold scheme (1 key for manager; the other key comes from (4,10) scheme)