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

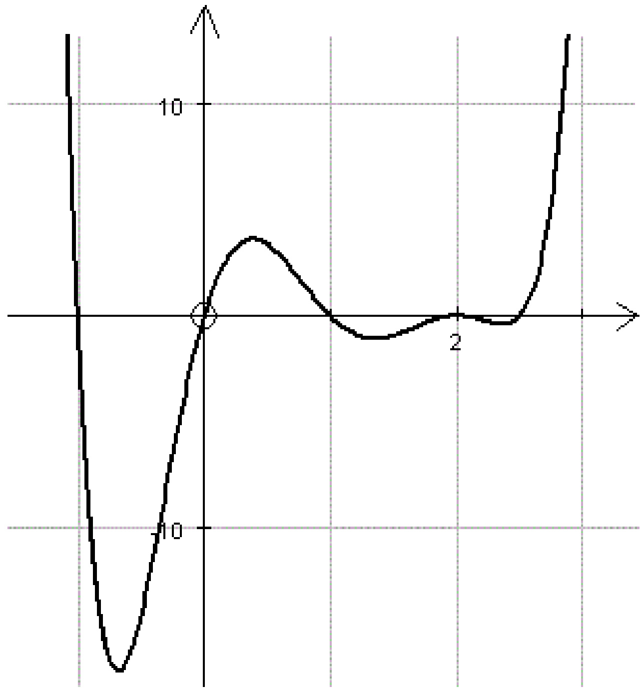
A Secret Sharing Scheme

Example: An (n, n)-threshold scheme:

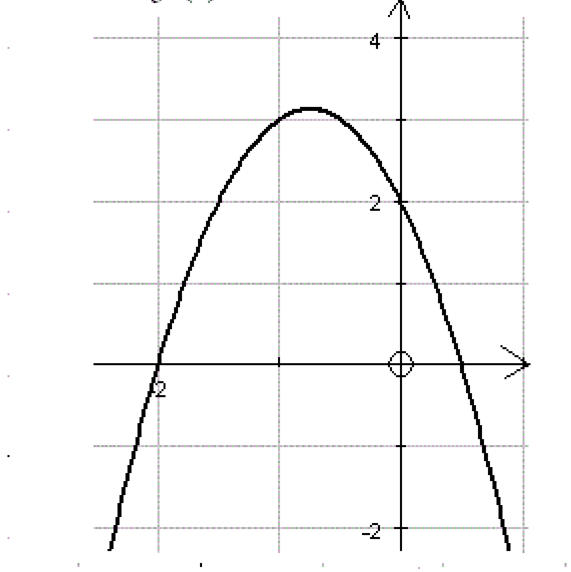
- To share a k-bit secret, the dealer D
  - generates n – 1 random k-bit numbers (shares) y_i where i = 1, 2,..., n – 1,
  - $y_n = K \oplus y_1 \oplus y_2 \oplus \ldots \oplus y_{n-1}$,
  - gives the share y_i to party P_i.
- This is a "perfect" SSS: A coalition of less than t can not obtain information about the secret.
- Q: How to generalize to arbitrary (t, n)?

Polynomials

$$f(x)=2x^6-13x^5+26x^4-7x^3-28x^2+20x$$



$$f(x)=-2x^2-3+2$$



Lagrange Interpolation

- Take a polynomial f(x)
  - $f(x) = a_0 + a_1 x + \ldots + a_{t-2} x^{t-2} + a_{t-1} x^{t-1}$
  - Compute $f(x_i)$ values for $x_i \in Z$, $i=1,\ldots,t$;

- Given t $(x_i, f(x_i))$ pairs, we can reconstruct f(x) as follows:
  - $l_i(x) = \Pi_{j=1 \text{ to } t, j \neq i} (x - x_j) / (x_i - x_j)$
  - $f(x) = \sum_{i=1 \text{ to } t} l_i(x)\, y_i$

Shamir's (t, n)-threshold Scheme

- Preparing and distributing the keys:
  - The dealer chooses prime p such that $p \geq n+1$, $K \in Z_p$;
  - generates distinct, random, non-zero $x_i \in Z_p$, $i=1,\ldots,n$;
  - generates random $a_i \in Z_p$, $i=1, 2,\ldots, t-1$;
  - $a_0 = K$, the secret;
  - $f(x) = \sum_{i=0 \text{ to } t-1} a_i x^i \mod p$
    $= a_0 + a_1 x + \ldots + a_{t-2} x^{t-2} + a_{t-1} x^{t-1} \mod p$
  - i^{th} person's share is $(x_i, f(x_i))$.

- Combining t keys and reconstructing the secret K
  - $l_i(x) = \prod_{j=1 \text{ to } t, j \neq i} (x - x_j) / (x_i - x_j) \mod p$
  - $f(x) = \sum_{i=0 \text{ to } t} l_i(x)\, y_i \mod p$
  - $f(0) = K$

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: $a_1=166, a_2=94$
  - $a_0 = K = 1234$
  - $f(x) = 1234 + 166x + 94x^2$
  - We construct six points:

$$(1, 1494); (2, 1942); (3, 2578); (4, 3402); (5, 4414); (6, 5614)$$

  - To reconstruct the key any 3 points will be enough. Assume that we have these keys:

$$(x_0, y_0) = (2, 1942); (x_1, y_1) = (4, 3402); (x_2, y_2) = (5, 4414)$$

Example: Shamir's (3, 6)-threshold Scheme-2

- From these 3 keys, we compute l_i values:

$$\ell_0 = \frac{x - x_1}{x_0 - x_1} \cdot \frac{x - x_2}{x_0 - x_2} = \frac{x - 4}{2 - 4} \cdot \frac{x - 5}{2 - 5} = \frac{1}{6}x^2 - 1\frac{1}{2}x + 3\frac{1}{3}$$

$$\ell_1 = \frac{x - x_0}{x_1 - x_0} \cdot \frac{x - x_2}{x_1 - x_2} = \frac{x - 2}{4 - 2} \cdot \frac{x - 5}{4 - 5} = -\frac{1}{2}x^2 + 3\frac{1}{2}x - 5$$

$$\ell_2 = \frac{x - x_0}{x_2 - x_0} \cdot \frac{x - x_1}{x_2 - x_1} = \frac{x - 2}{5 - 2} \cdot \frac{x - 4}{5 - 4} = \frac{1}{3}x^2 - 2x + 2\frac{2}{3}$$

- Then, we compute f(x):

$$f(x) = \sum_{j=0}^{2} y_j \cdot \ell_j(x)$$

$$= 1942 \cdot \left(\frac{1}{6}x^2 - 1\frac{1}{2}x + 3\frac{1}{3}\right) + 3402 \cdot \left(-\frac{1}{2}x^2 + 3\frac{1}{2}x - 5\right) + 4414 \cdot \left(\frac{1}{3}x^2 - 2x + 2\frac{2}{3}\right)$$

$$= 1234 + 166x + 94x^2$$

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.

Secret Sharing Scenarios

- 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)