Chapter 6.3. Secret Sharing

Def. Let $t, n \in \mathbb{Z}^+$ with $1 \le t \le n$.

An algorithm that distributes a secret among n participants s.t. t participants need to collaborate to recover the secret is called a (t,n)-threshold secret sharing scheme.

(n,n)-Threshold Secret Sharing ⇒ can do addition and multiplication by constant.

- Input: A binary number k. ← secret
- Secret Distribution:
  1. generate $n-1$ random binary numbers k_i for $1 \le i \le n-1$
  2. $k_n = k \oplus k_1 \oplus \cdots \oplus k_{n-1}$ ($k_n = k - k_1 - \cdots - k_{n-1}$)
  3. distribute k_i among n participants.
- Secret Recovery:
  1. collect all values $k_1, \cdots, k_n$
  2. $k := k_1 \oplus k_2 \oplus \cdots \oplus k_n$

(t,n)-Threshold Secret Sharing

- Input: A secret k
- Secret Distribution:
  1. generate $t-1$ random numbers $a_1, \cdots, a_{t-1} \in \mathbb{F}_p$.
  2. $f(x) := k + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}$
  3. distribute $(i, f(i))$ to participant P_i for all i.
- Secret Recovery:
  1. collect t pairs $(i, f(i))$ from at least t participants.
  2. reconstruct a polynomial $f(x)$ by Lagrange's interpolation.
  3. $k = f(0)$.