Access structures & secret sharing schemes
Secret sharing

**Goal** Share a secret $k$ among $n$ participants by distributing secret shares among the participants such that

1. authorized sets of participants can always reconstruct the secret $k$ from their shares,

2. non-authorized sets of participants learn nothing about the secret $k$ from their shares, in particular can not reconstruct secret $k$. 
Visually sharing a secret
Sharing a secret number
Sharing a secret number

- Insecurity about secret of each participant is $10^{45}$.
- Insecurity about secret of any $m$ participants is $10^{50-5m}$.

$\Rightarrow$ 9 out of 10 participants almost learn the secret number!
Access structures

U finite set, \( \mathcal{A} \subseteq 2^U \). \( \mathcal{A} \) is called monotone collection if
\[
\forall B, C \in 2^U : B \in \mathcal{A} \land B \subseteq C \Rightarrow C \in \mathcal{A}
\]

Definition 3.1 \( U = \{p_1, \ldots, p_n\} \). An access structure over \( U \) is a monotone collection \( \mathcal{A} \subseteq 2^U \). Sets in \( \mathcal{A} \) are called authorized, and sets not in \( \mathcal{A} \) are called non-authorized.

Examples

- \( \mathcal{A} = \{U\} \)
- \( \mathcal{A} = \{B \subseteq U : |B| \geq t\} \) (threshold t access structure)
- f montone Boolean formulae on n variables \( \{x_1, \ldots, x_n\} \), \( \mathcal{A} = \{B \subseteq U : \text{assignment} \ (x_i = 1 \iff p_i \in B) \text{ satisfies } f \} \)
Distribution schemes

Definition 3.2 A distribution scheme for \( U = \{p_1,\ldots,p_n\} \) with domain of secrets \( K \) is a pair \((\Pi,\mu)\), where \( \mu \) is a probability distribution on some finite set \( R \) and \( \Pi : K \times R \rightarrow K_1 \times \cdots K_n \), \( K_j \) is called the domain of shares of \( p_j \).

\[
\Pi(k,r) = s_1 \ s_2 \ s_3 \ s_4 \ s_5
\]
Secret sharing schemes

Definition 3.2 A distribution scheme for $U = \{p_1, \ldots, p_n\}$ with domain of secrets $K$ is a pair $(\Pi, \mu)$, where $\mu$ is a probability distribution on some finite set $R$ and $\Pi : K \times R \rightarrow K_1 \times \cdots K_n$, $K_j$ is called the domain of shares of $p_j$.

Definition 3.3 A distribution scheme $(\Pi, \mu)$ with domain of secrets $K$, $|K| \geq 2$, is a secret sharing scheme realizing access structure $\mathcal{A}$, if

Correctness $\forall B \in \mathcal{A}$ $\exists \text{Recon}_B : K_1 \times \cdots K_n \rightarrow K$ such that $\forall k \in K : \Pr[\text{Recon}_B(\Pi(k;r)) = k] = 1$.

Privacy $\forall T \notin \mathcal{A}$ $\forall a, b \in K$ $\forall \langle s_j \rangle_{p_j \in T}$ :

$\Pr[\forall j \in T : \Pi(a, r)_j = s_j] = \Pr[\forall j \in T : \Pi(b, r)_j = s_j]$.
n-out-of-n secret sharing

access structure $\mathcal{A} = \{U\}, U = \{p_1, \ldots, p_n\}$

domain of secrets $K = \mathbb{Z}_m, m \in \mathbb{N}$

$R = \mathbb{Z}_m^{n-1} = \mathbb{Z}_m \times \cdots \times \mathbb{Z}_m$

$\mu :=$ uniform distribution, $K_i := \mathbb{Z}_m, i = 1, \ldots, n$

$$\Pi: \mathbb{Z}_m \times \mathbb{Z}_m^{n-1} \rightarrow \mathbb{Z}_m^n$$

$$(k, s_1, \ldots, s_{n-1}) \mapsto (s_1, \ldots, s_{n-1}, s_n)$$

where $s_n := k - s_1 - \cdots - s_{n-1} \mod m$

Correctness $k = s_1 + \cdots + s_n \mod m$

Privacy $\forall a \in K, T, |T| \leq n - 1:$

$$\Pr\left[ \forall j \in T: \Pi(a, r)_j = s_j \right] = \frac{1}{m^{|T|}}.$$
t-out-of-n secret sharing – Shamir’s scheme

access structure \( \mathcal{A}_t = \{B \subseteq \{p_1, \ldots, p_n\} : |B| \geq t\} \)

domain of secrets \( K = \mathbb{Z}_q, q \in \mathbb{N} \) prime, \( q > n \).

\[ R = \mathbb{Z}_q^{t-1} = \mathbb{Z}_q \times \cdots \times \mathbb{Z}_q \]

\( \mu : \text{uniform distribution}, K_i := \mathbb{Z}_q, i = 1, \ldots, n \)

\[ \Pi : \mathbb{Z}_q \times \mathbb{Z}_q^{t-1} \rightarrow \mathbb{Z}_q^n \]

\[ (k, r_1, \ldots, r_{t-1}) \mapsto (s_1, \ldots, s_n) \]

where

- \( s_i = a(\gamma_i) \)
- \( a(x) = \sum_{i=1}^{t-1} r_i x^i + k \)
- \( \gamma_i \in \mathbb{Z}_q^* \) pairwise distinct
Lemma 3.4 Over any field $\mathbb{F}$ a polynomial $p(\cdot)$ of degree $t-1$ is uniquely determined by its value at $t$ distinct points $\gamma_j$ in $\mathbb{F}$.

Proof \[ p(x) = \sum_{i=1}^{t} \left( p(\gamma_i) \prod_{j \neq i} \frac{x - \gamma_j}{\gamma_i - \gamma_j} \right) \]
Corollary 3.5 Let $s \leq t - 1$ and $(\gamma_i, c_i) \in \mathbb{Z}_q^* \times \mathbb{Z}_q$, $i = 1, \ldots, s$, and $c_0 \in \mathbb{Z}_q$. Then there are exactly $q^{t-1-s}$ polynomials $a(x)$ of degree at most $t - 1$ over $\mathbb{Z}_q$ such that

1. $a(0) = c_0$
2. $a(\gamma_i) = c_i$, $i = 1, \ldots, s$.

Privacy \hspace{1cm} \forall a \in K, T, |T| \leq t - 1: \Pr \left[ \forall j \in T : \Pi(a, r)_j = s_j \right] = \frac{1}{q^{|T|}}.
A general scheme

access structure $\mathcal{A}$ arbitrary

domain of secrets $K = \{0,1\}$

$R = \{0,1\}^N$, where $N = \sum_{B \in \mathcal{A}} |B| - 1$,

$\mu :=$ uniform distribution,

$K_i := \{0,1\}^{N_i}$, where $N_i = \{B \in \mathcal{A} : p_i \in B\}$

$\Pi$ on input $\mathcal{A}$

for every $B \in \mathcal{A}, B = \{p_{i_1}, \ldots, p_{i_l}\}$

- choose $l-1$ bits $r_1, \ldots, r_{l-1}$,
- compute $r_l = k \oplus r_1 \oplus \cdots \oplus r_{l-1}$,
- give bit $r_j$ to $p_{i_j}$. 
A more efficient general scheme

access structure \( \{ B \subseteq U : \text{assignment } x_i = 1 \iff p_i \in B \text{ satisfies } f \} \)

\( f \) momotone Boolean formulae

domain of secrets \( K = \mathbb{Z}_m \)

\( A_0, A_1 \) access structures over \( U = \{ p_1, \ldots, p_m \} \)

\( A_0 \lor A_1 := \{ B \subseteq U : B \in A_0 \lor B \in A_1 \} \)

\( A_0 \land A_1 := \{ B \subseteq U : B \in A_0 \land B \in A_1 \} \)

\( f = f_0 \odot f_1, \odot \in \{ \land, \lor \} \)

\( f_0 \) Boolean formulae for access structure \( A_1 \)

\( f_1 \) Boolean formulae for access structure \( A_2 \)

\( \Sigma_i \) \( \Sigma_i = (\Pi_i, \mu_i) \) secret sharing scheme for \( A_i \)
A more efficient general scheme

\[ f = f_0 \text{ or } f_1, \bullet \in \{\land, \lor\} \]

- \( f_0 \): Boolean formulae for access structure \( A_1 \)
- \( f_1 \): Boolean formulae for access structure \( A_2 \)
- \( \Sigma_i \): \( (\Pi_i, \mu_i) \) secret sharing scheme for \( A_i \)

Secret sharing scheme \( \Sigma \) for \( A \)

- \( f = f_0 \text{ or } f_1 \): share secret \( k \) independently using scheme \( \Sigma_0, \Sigma_1 \)
- \( f = f_0 \text{ and } f_1 \): choose \( k_0 \in \mathbb{Z}_m \) uniformly, \( k_1 := k - k_0 \mod m \), independently share \( k_0 \) using \( \Sigma_0 \) and \( k_1 \) using \( \Sigma_1 \)
Monotone formulae construction - example

\[ f(x) = ((x \land y) \lor z)) \land ((z \land y) \lor x) \]

\[ \mathcal{A} = \{\{x,y\}, \{x,z\}, \{y,z\}, \{x,y,z\}\} \]
Attribute-based encryption (key policy)

\[ U = \{a_1, \ldots, a_n\} \] (set of attributes)

**Definition 3.6** A (key policy) attribute-based encryption scheme \( \Pi \) is a quadruple \( (\text{Setup}, \text{KeyGen}, \text{Enc}, \text{Dec}) \) of ppts such that:

1. **Setup** on input \( 1^n \) computes public parameters params and secret master key msk.
2. **KeyGen** on input \( 1^n, \text{params}, \text{msk} \) and access structure \( \mathcal{A} \) over \( U \), outputs the private key \( \text{sk}_{\mathcal{A}} \) for access structure \( \mathcal{A} \).
3. **Enc** on input a set of attributes \( \gamma \subseteq U \) and a message \( m \) outputs a ciphertext \( c \leftarrow \text{Enc}_\gamma (m) \).
4. **Dec** on input a private key \( \text{sk}_{\mathcal{A}} \) and a ciphertext \( c \in \text{Enc}_\gamma (m) \) outputs message \( m \) if and only if \( \gamma \in \mathcal{A} \). We assume \( \text{Dec} \) is deterministic and write \( m := \text{Dec}_{\text{sk}_{\mathcal{A}}} (c) \).
The next steps

- Form three groups working on
  - Modeling and implementing access structures
  - Implementing attribute-based encryption
  - Realizing distributed PKG

  - general construction
  - threshold scheme
  - monotone formulae
  - identity-based
  - fuzzy identity-based
  - secret sharing
    - Shamir
    - monotone formulae

- continue to work on your seminar topics
  ⇒ what is particularly relevant for PG?