Lecture 22: Threshold Encryption

CS 539 / ECE 526
Encryption Scheme

Alice → m ← Bob

Eve the eavesdropper
Encryption Scheme

Alice

Eve the eavesdropper

Bob
Encryption Scheme

Alice -> Safe box 

Eve the eavesdropper 

Bob
Symmetric key Encryption Scheme

Alice

Eve the eavesdropper

Bob
Asymmetric Encryption

Alice

Eve the eavesdropper

Bob

\[ sk = \text{Alice's private key} \]

\[ pk = \text{Bob's public key} \]

\[ m \leftarrow \text{Dec}(sk, c) \]

\[ c \leftarrow \text{Enc}(pk, m) \]

\[ c: \text{ciphertext} \]

- Q: Does Eve know either of the keys?
  - What if Eve knows the sk?
  - What if Eve knows the pk?
Asymmetric Encryption

Alice
sk = ☢️

Eve the eavesdropper

Bob
pk = ⚒️

c: ciphertext

m ← Dec(sk, c)
c ← Enc(pk, m)

• Allows anyone to send messages to Alice in private (an eavesdropper cannot read)
  • Alice has a private key sk
  • Everyone knows her corresponding public key pk

Symmetric vs Asymmetric Encryption?

Further reading: Key Encapsulation Mechanism (KEM).
Defining Encryption Security
Indistinguishability under Chosen Plaintext Attacks (IND-CPA)

Challenger

\( \text{pk} = \)  
\( m \)  
\( c \leftarrow \text{Enc}(\text{pk}, m) \)  
\( m' \)  
\( c' \leftarrow \text{Enc}(\text{pk}, m') \)  
\( \cdots \)  
\( m_0, m_1 \)  
\( \text{Enc}(\text{pk}, m_b) \)  
\( m'' \)  
\( c'' \leftarrow \text{Enc}(\text{pk}, m'') \)  
\( b' \)

Eve

\( b \leftarrow \{0, 1\} \)

\( \text{sk} = \)  

Secure if \( \Pr[b=b'] = \frac{1}{2} + \text{negl} \)
Indistinguishability under Chosen Plaintext Attacks (IND-CPA)

• A game with attacker Eve:
  – We (proponent of a cipher) pick a random key sk
  – Eve can ask for encryptions of any messages
    • I.e., pick any m and get back Enc(sk, m), and repeat any (feasible) number of times
  – Eve picks two messages m₀ and m₁ of equal length
  – We flip a coin b ← {0, 1} and give Eve Enc(sk, m₇)
  – Eve can ask for encryptions of any messages
  – Eve guesses b. Encryption is insecure if Eve wins with 0.5 + ε probability; secure if 0.5 probability
Is IND-CPA Too Stringent?

• What if Eve asks for \(\text{Enc}(k, m_0)\) and \(\text{Enc}(k, m_1)\) and compares with \(\text{Enc}(k, m_b)\)? An easy win?

• No. IND-CPA is achievable and necessary!

• Need \textbf{randomized} encryption
  – Encryption of the same message (under the same key) must change every time!
<table>
<thead>
<tr>
<th>Plaintext</th>
<th>randomized encryption</th>
<th>deterministic encryption</th>
</tr>
</thead>
</table>

12
Secret Sharing

• (n, t) secret sharing:
  – A dealer shares a secret s
  – Each party gets a share (n parties in total)
  – Any t shares reconstruct s
  – Any t-1 shares reveal no information about s

• Tolerate t-1 curious parties and n-t crash faults
Shamir’s Secret Sharing [Shamir 1979]

• \( y = f(x) = s + c_1 x + c_2 x^2 + c_2 x^2 + ... + c_{t-1} x^{t-1} \)
  – \( s = f(0) \) is the secret. Other coefficients are random

• Party i’s share is \( s_i = f(a_i) \)
  – \( a_1, a_2, a_3, ..., a_n \) are distinct public values

• \( t \) points fix a degree \( t-1 \) polynomial; can reconstruct using Lagrange interpolation
Lagrange Interpolation Formula

Let \((x_1, y_1), \ldots, (x_n, y_n)\) be \(n\) points with different \(x\) coordinates, then

\[
P(x) = \sum_{i=1}^{n} \left( y_i \prod_{j \neq i} \frac{(x - x_j)}{(x_i - x_j)} \right)
\]

is the only polynomial of degree \(\leq n - 1\) that goes through all of them.

\[
X = \{x_1, x_2, \ldots, x_n\}
\]

\[
L_{i,X}(x) = \prod_{j \neq i} \frac{(x - x_j)}{(x_i - x_j)}
\]

1. Degree of \(L_{i,X}(x)\)?
2. Value of \(L_{i,X}(x_i)\)
3. Value of \(L_{i,X}(x_j)\) for \(j \neq i\)
$(n, t)$ Threshold Encryption

Eve the eavesdropper

Bob

$c \leftarrow \text{Enc}(pk, m)$

$(\ldots, \ldots, \ldots, \ldots, \ldots, \ldots) = \text{Share}(n, t, \ldots)$
(n, t) Threshold Encryption

Eve the eavesdropper

Bob

pk =

\((n, t, k_1, k_2, \ldots, k_t) = \text{Share}(n, t, k)\)

\(c \leftarrow \text{Enc}(pk, m)\)

Q: How to decrypt the ciphertext?

1. \(k = \text{Reconstruct}(k_1, k_2, \ldots, k_t)\)
2. \(m \leftarrow \text{Dec}(k, c)\)

Q: Any issues with this approach?
(n, t) Threshold Encryption

Eve the eavesdropper

Bob

pk = Share(n, t, ) = Share(n, t, )

Q: How to decrypt the ciphertext?

1. m₁ ← Dec(, c), m₂ ← Dec(, c), ... , mₙ ← Dec(, c)
2. m = Combine(m₁, m₂, ..., mₙ)

We never have to reconstruct the secret at any node!
(n, t) Threshold Encryption IND-CPA

Challenger

\[ \text{sk} = \text{key} \]

\[ b \leftarrow \{0, 1\} \]

Eve

\[ \text{pk} = \text{key}, \text{key}, \text{key}, \text{key}. \]

\[ m \]

\[ c \leftarrow \text{Enc}(\text{pk}, m) \]

\[ m' \]

\[ c' \leftarrow \text{Enc}(\text{pk}, m') \]

\[ \vdots \]

\[ m_0, m_1 \]

\[ \text{Enc}(\text{pk}, m_b) \]

\[ m'' \]

\[ c'' \leftarrow \text{Enc}(\text{pk}, m'') \]

\[ b' \]

Secure if \( \Pr[b=b'] = \frac{1}{2} + \text{negl} \)
Some Basic Group Theory

- A set of elements with a binary operation • that satisfies
  - (Closure) If x, y are in G, so is x•y
  - (Associativity): (x•y)•z = x•(y•z)
  - (Identity): there exists e s.t. e•x = x•e = x
    - e=1 here
  - (Inverse): For each x, there exists x⁻¹ s.t. x•x⁻¹ = e

- \( \mathbb{Z}_p \) with mod p multiplication forms a group
Elliptic Curve Group
Some Basic Group Theory

- Can define exponentiation as repeated •, i.e., $g^a = g \cdot g \cdot g \cdot \ldots \cdot g$ (repeated a times)
  - Note that $(g^a)^b = (g^b)^a$

- Can also use notations + and $ag = g+g+\ldots+g$

- We will use a cyclic group $G$ and a generator $g$
  - You don’t need to understand these notions for this class
Important Assumptions

• The discrete-log assumption: given $g$ and $g^a$ for random $a$, infeasible to find $a$
  – Easy for real numbers (continuous case)
  – (Believed to be) hard for $\mathbb{Z}_p$ and some other groups

• Decisional Diffie-Hellman (DDH) assumption: given $g, g^a, g^b$ for random $a$ and $b$, infeasible to indistinguishable $g^{ab}$ from random
  – Stronger than the discrete-log assumption
El Gamal Encryption

• Key generation:
  – Pick a (cyclic) group $G$ and a (generator) element $g$
  – Private key: a random integer $s$; public key $g^s$
    • Cannot find $s$ from $g^s$ under the discrete-log assumption

• Encryption: $c = Enc(g^s, m)$
  – Pick random integer $r$
  – $c = (g^r, m \cdot (g^s)^r) = (c_1, c_2)$

• Decryption: $m = Dec(s, (c_1, c_2))$
  – $c_2 \cdot (c_1^s)^{-1} = m \cdot (g^s)^r \cdot (g^{rs})^{-1} = m$
El Gamal Security Intuition

- $\text{Enc}(g^s, m) = (g^r, m \cdot (g^s)^r) = (c_1, c_2)$ (random $r$)
- $\text{Dec}(s, (c_1, c_2)) = c_2 \cdot (c_1^s)^{-1} = m \cdot (g^s)^r \cdot (g^{rs})^{-1} = m$

- Given $g^s$ and $c_1 = g^r$, $(g^s)^r$ looks random due to the Decisional Diffie-Hellman assumption.
El Gamal Threshold Encryption

- Key generation: private key $s$; public key $g^s$
  - Party $i$ has $s_i = f(a_i)$
- Encryption: $c = \text{Enc}(g^s, m) = (g^r, m \cdot (g^s)^r) = (c_1, c_2)$
- Decryption share $d_i = c_1^{s_i}$
- Combine shares to decrypt
El Gamal Threshold Encryption

• Have \( t \) decryption shares \( (c_1^{s_i}) \)
• Need to compute \( c_2 \cdot (c_1^s)^{-1} \)

Lagrange Interpolation Formula

Let \( (x_1, y_1), \ldots, (x_n, y_n) \) be \( n \) points with different \( x \) coordinates, then

\[
P(x) = \sum_{i=1}^{n} \left( y_i \prod_{j \neq i} \frac{x - x_j}{x_i - x_j} \right)
\]

is the only polynomial of degree \( \leq n - 1 \) that goes through all of them
El Gamal Threshold Encryption

- Have $t$ decryption shares ($c_1^{s_i}$)
- Need to compute $c_2 \cdot (c_1^s)^{-1}$

\[
s = f(0) = \sum_{i=1}^{t} s_i L_i(0)
\]

\[
c_1^s = c_1 \sum_{i=1}^{t} s_i L_i(0) = \prod_{i=1}^{t} d_i L_i(0)
\]

- Recall $d_i = c_1^{s_i}$
- Called “interpolate in the exponent”