1 Public Key Encryption

1.1 Overview

- For Alice to send encrypted messages to Bob, Bob needs to know a secret (private key)
- Both Alice and Eve (eavesdropper) know Bob’s public key

1.2 Symmetric vs. Asymmetric Key Generation

<table>
<thead>
<tr>
<th>KG</th>
<th>Symmetric Encryption</th>
<th>Asymmetric Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Both parties hold the same key</td>
<td>Each party gets public, private key pair $\text{pub}_B$, $\text{prv}_A$</td>
</tr>
<tr>
<td>Encrypting</td>
<td>Alice performs $\text{Enc}_B(m) \rightarrow c$</td>
<td>Alice performs $\text{Enc}_{\text{pub}_B}(m) \rightarrow c$</td>
</tr>
<tr>
<td>Decrypting</td>
<td>Bob performs $\text{Dec}_B(c) \rightarrow m'$</td>
<td>Bob performs $\text{Dec}_B(\text{pub}_B(c)) \rightarrow B$</td>
</tr>
</tbody>
</table>

1.3 Basic Key Generation, Encryption, and Decryption functions

Figure 1: Key Generation, Encryption, Decryption
The key generation algorithm outputs both a public key and a private key. Data is encryption with the public key, and any ciphertext encrypted this way cannot be decrypted without the matching private key.

2 Chosen Ciphertext Security (public version)

We will modify our attacker/challenger model:

![Diagram of attacker and challenger models](image-url)

The attacker can run the PKE-DEC algorithm repeatedly to see many different ciphertexts. This model is called a Chosen Ciphertext Attack (CCA). Without the attacker having access to PKE-DEC, this attack is called Chosen Plaintext Attack (CPA).

3 El Gamal Encryption

3.1 Recall: Decisional Diffie-Hellman

\[ p = 2p' + 1, \quad < g > = \mathbb{Z}_p^*, \quad g = g^{2 \mod (p)}, \quad < g > = QR_p \]

DDH:

\[ a, b \xleftarrow{\$} \mathbb{Z}_p^* \]

\[ y_1 \leftarrow g^a \mod (p) \]

\[ y_2 \leftarrow g^b \mod (p) \]
\( y_3 \leftarrow g^{ab} \mod (p) \)

Random:
\( a, b, c \leftarrow \mathbb{Z}_p^* \)
\( y_1 \leftarrow g^a \mod (p) \)
\( y_2 \leftarrow g^b \mod (p) \)
\( y_3 \leftarrow g^c \mod (p) \)

**Distinguisher → 1/0**
The distinguisher function decides if the \( y \)'s are Diffie-Hellman or just random numbers. DDH Assumption:
\[
\forall PP + \gamma \exists s.t. Pr[\text{Dist}(y_1, y_2, y_3) = 1 | (y_1, y_2, y_3) \leftarrow \mathbb{Z}_p^* I] - Pr[\text{Dist}(y_1, y_2, y_3) = 1 | (y_1, y_2, y_3) \leftarrow \mathbb{Z}_p^* II] < \nu
\]

### 3.2 Encryption

1. Pick some \( r' \in \mathbb{Z}_{p'} \), and \( m \in \mathbb{Z}_{p'} \)
2. \( C_1 = g^{r} \mod (p) \)
3. \( C_2 = my^{r} \mod (p) \)
4. Cipher text = \( C_1 | C_2 \)

### 3.3 Decryption

Decryption Procedure: \( \text{Dec}(Dk, c) \)
1. Start with \( C_2 / C_1^x \mod (p) \)
2. \( C_2 / C_1^x = my^{r} / (g^{r})^x = m(g^x)^r / (g^x)^r = m \)

### 3.4 CCA Analysis

El Gamal is not secure under a chosen ciphertext attack. This is because, for example, given an encryption \((c_1, c_2)\) of some unknown message \( m \), one can easily construct a valid encryption \((c_1, 2c_2)\) of the message \( 2m \).

### 3.5 CPA Analysis

El Gamal satisfies Chosen Plaintext Attack security. The chances are the same for either case.
4 Rabin QR

4.1 In $\mathbb{Z}_p^*$

Quadratic Residues are exactly half of the numbers in $\mathbb{Z}_p^*$
4.2 In $\mathbb{Z}_n^*$

For $a \in \mathbb{Z}_n^*$:

$n = p \cdot q$, where $p = 2p' + 1$ and $q = 2q' + 1$)

$\mathbb{Z}_n^* \cong \mathbb{Z}_{p'}^* \times \mathbb{Z}_{q'}^*$

A number must be square both mod $p$ and mod $q$.

- (-, -) Non-square both mod $p$ and mod $q$
- (-, +) Non-square mod $p$, square mod $q$
- (+, -) Square mod $p$, non-square mod $q$
- (+, +) Square mod $p$, square mod $q$

5 Jacobi Symbol

$(a/n) = (a/q)(a/q)$

Note: There exists a fast (efficient) way to compute $(a/n)$ without having to factor $n$.

References