### Improving Stateful Encryption Schemes

**Secure Communication for Mobile Environment**

<table>
<thead>
<tr>
<th>Traditional Encryption</th>
<th>Stateful Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Device</td>
<td>Mobile Device</td>
</tr>
<tr>
<td>( \text{pk}_1 )</td>
<td>( \text{pk}_1, \text{PSt} )</td>
</tr>
<tr>
<td>( \text{sk}_1 )</td>
<td>( \text{sk}_1, \text{SSt} )</td>
</tr>
</tbody>
</table>

**Example: Stateful PKE**

- **DHIES:** (DH-StEnc, USK-CCA-secure with RO)
  - Public parameter: DSA group or elliptic curve group with prime order \( p \), with generator \( g \)
  - \( \text{PK}: \langle g, \langle y \rangle \rangle, \text{SK}: \langle x \rangle \)
  - Enc: \( t \leftarrow \mathbb{Z}_q, (c_0, c_1) \leftarrow (g^t, h^t) \), \( c_1 = \text{E}_{\text{sym}}(K,m) \)
  - Ciphertext: \( \langle c_0, c_1 \rangle \)
  - Dec: \( c_0 = g^t \) is independent from \( y \) (Receiver’s PK)
  - Notice that \( c_0 = g^t \) is independent from \( y \) (Receiver’s PK)
  - Encryption: it is sufficient to compute \( K \) for each Receiver
  - For decryption, it remains unchanged

**Security Notions**

- **Indistinguishability against Adaptive Chosen Ciphertext Attack (IND-CCA)**
  - Multi-Receiver setting
    - Each Receiver sets up his public key
    - Known Secret Key (KSK)
    - Unknown Secret Key (USK)
    - Attacker may not know the secret key of its public key

**Efficiency Improvement**

- Modular exponentiations dominate the computational cost of public key encryption
  - Power consumption / Bandwidth
- Stateful encryption can improve the computational cost of traditional PKE dramatically

**Our Results**

1. **Improving efficiency of DH-StEnc**:
   - Underlying assumption
     - Gap-DH (Strong) \( \Rightarrow \) Computational DH (Weak)
     - Idea: twin public keys
   - Implementation (80-bit security)
     - Elliptic curve: 512 bit \( \rightarrow \) 160 bit
     - Public key size: 512 bit \( \rightarrow \) 320 bit
     - Slightly worse computational cost
       - \( 1 \rightarrow 1.5 \) modular exponentiation

2. **Generalization of the model**:
   - Stateful Key Encapsulation Mechanism (KEM)
   - Tag-based Stateful KEM

3. **ID-based Setting**:
   - Generic construction from Identity-Based Non-Interactive Key Exchange (IBNIKE)
     - With (additional) mild assumptions
   - Satisfied by all known schemes
     - Stateful IBE without pairings (inefficient)
   - Avoiding the gap-BDH assumption
     - No known implementation for Gap-BDH assumption exists

---

**RUI ZHANG**
Improving Stateful Encryption Schemes

Rui Zhang
Research Team for Physical Analysis
RCIS, AIST
Secure Communication

Traditional Encryption

Mobile Device

\( K_1 \)

\( K_2 \)

\( pk_1 \)

\( pk_2 \)

\( sk_1 \)

\( sk_2 \)

Stateful Encryption

Mobile Device

\( pk_1 \)

\( pk_2 \)

\( sk_1 \)

\( sk_2 \)

State = \(<PSt, SSt>\)
Stateful encryption can improve the computational cost of the sender dramatically.
Results

• Weakening assumptions of known schemes
  – Stateful PKE/IBE
  – Easier design

• Generalization of the model and generic constructions