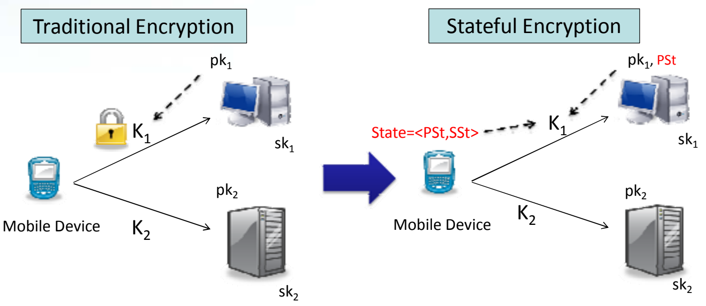
Improving Stateful Encryption Schemes

RUI ZHANG

Secure Communication for Mobile Environment



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

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"
  - ❖ PK: $<y\ (=g^x), H>$ SK: $<x>$
  - ❖ Enc: $r \leftarrow Zq, (c_0 = g^r)\ K=H(c_0,y,y^r),\ c_1=E_{sym}(K,m)$
  - ❖ Ciphertext: $<c_0,c_1>$
  - ❖ Dec: $K=H(c_0,\ y,\ c_0^x),\ m = D_{sym}(K,c_1)$
- Noticing that $c_0=g^r$ is independent from y (Receiver's PK)
  - ❖ $PSt = <c_0>$ $SSt = <r>$
  - ❖ For 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
    - o Each Receiver sets up his public key
  - ❖ Known Secret Key (KSK)
    - o Attacker knows
  - ❖ Unknown Secret Key (USK)
    - o Attacker may not know the secret key of its public key

Our Results

1. Improving efficiency of DH-StEnc:

- ❖ Underlying assumption
  - o Gap-DH (Strong) ➔ Computational DH (Weak)
  - o Idea: twin public keys
- ❖ Implementation (80-bit security)
  - o Elliptic curve: 512 bit -> 160 bit
  - o Public key size: 512 bit -> 320 bit
  - o Slightly worse computational cost
    - ▪1 -> 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)
  - o With (additional) mild assumptions
    - ❑ Satisfied by all known schemes
  - o Stateful IBE without pairings (inefficient)
- ❖ Avoiding the gap-BDH assumption
  - o No known implementation for Gap-BDH assumption exists

National Institute of Advanced Industrial Science and Technology AIST

Research Center for Information Security

Improving Stateful Encryption Schemes

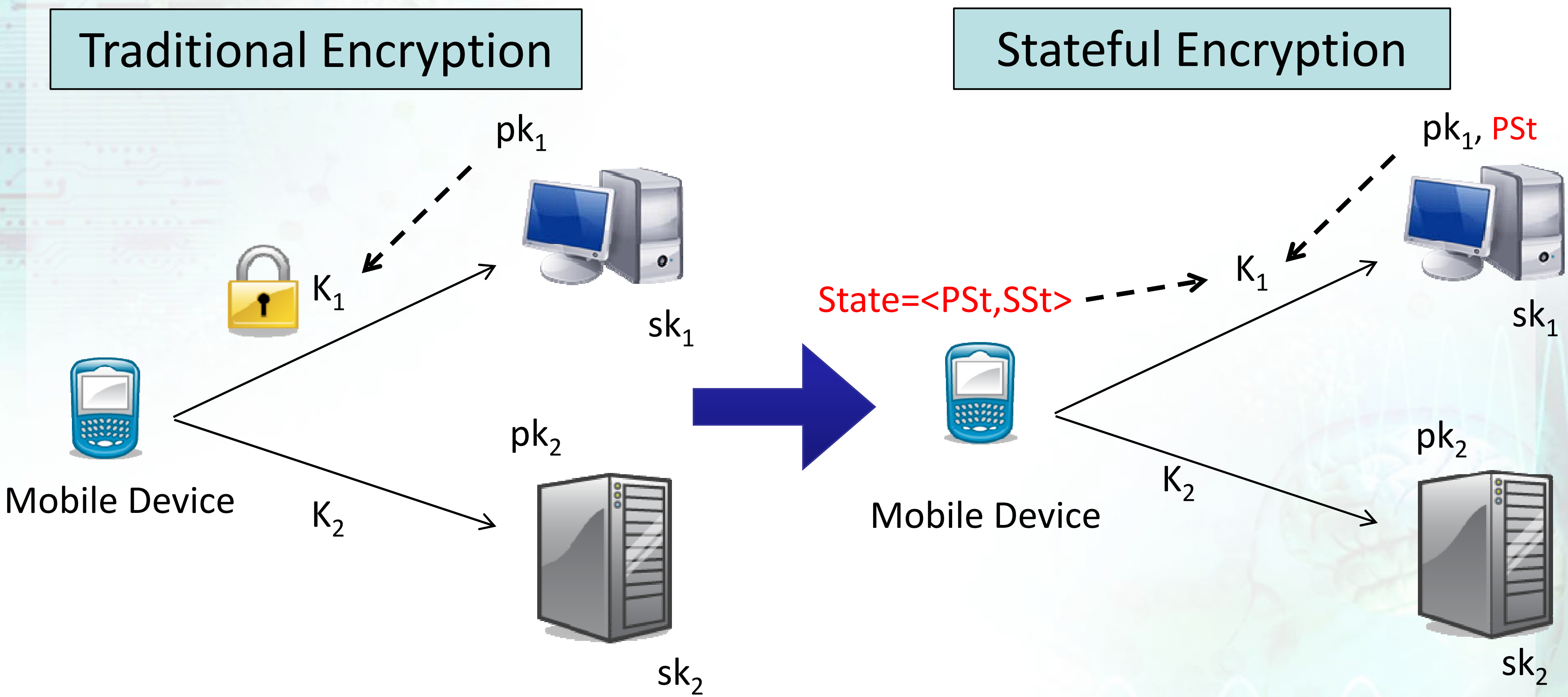
Rui Zhang

Research Team for Physical Analysis

RCIS, AIST

RCIS Workshop 2009

Secure Communication



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