ETSI
The Standards People

Security Conference

Efficient Quantum-Safe Communication using Hybrid Encryption

Rei Safavi-Naini

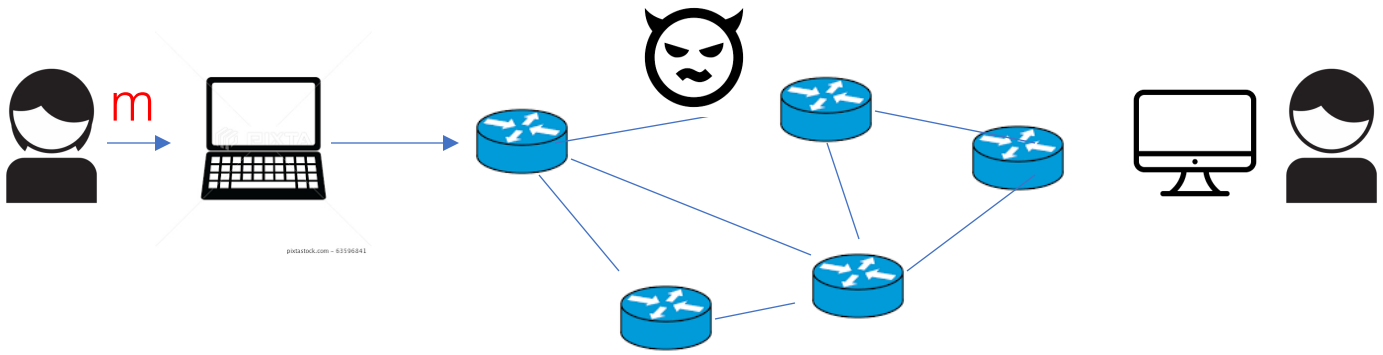
UNIVERSITY OF CALGARY

17/10/2023

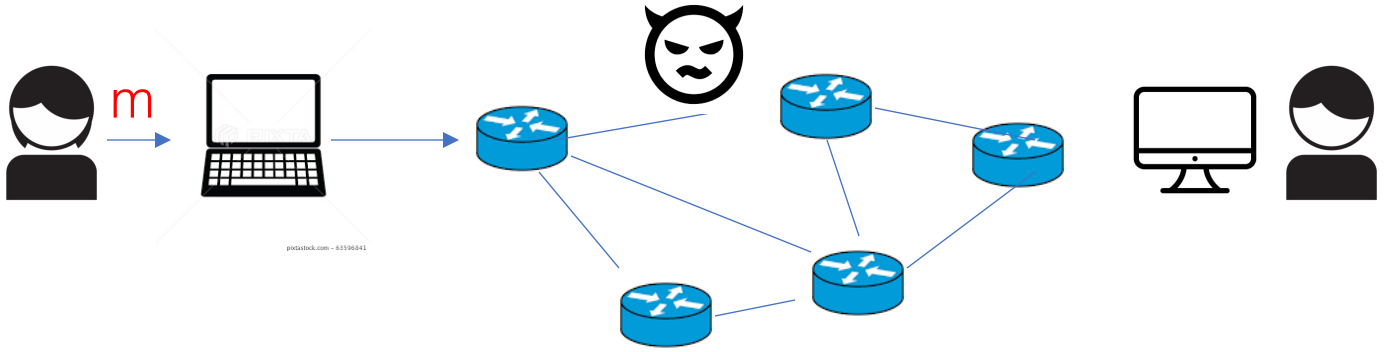
Plan of the talk

- Establishing a confidential channel (storage)
  - Approaches
- Hybrid encryption (KEM/DEM)
  - Confidential channel with proved security
- A new approach to HE
  - Correlated randomness model
- Combing KEMs
- Concluding

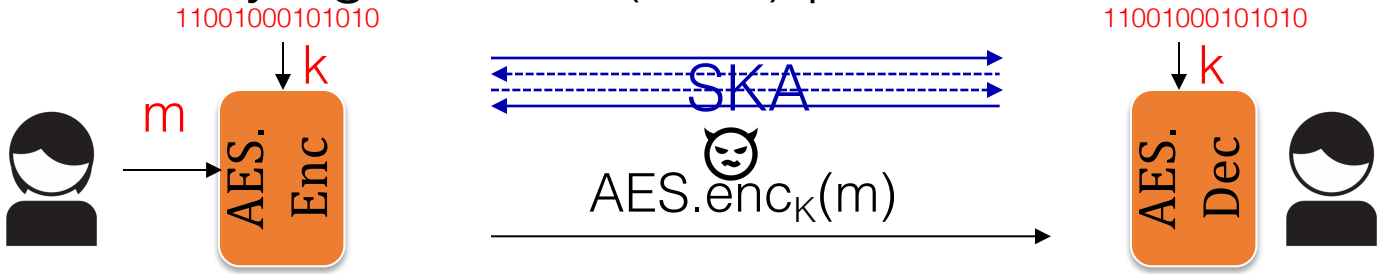
Confidential communication over Internet



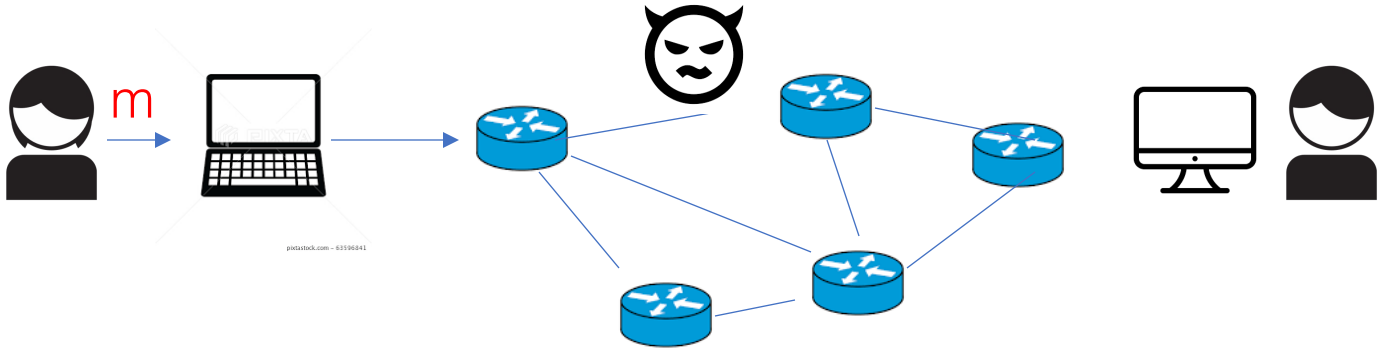
Confidential communication over Internet



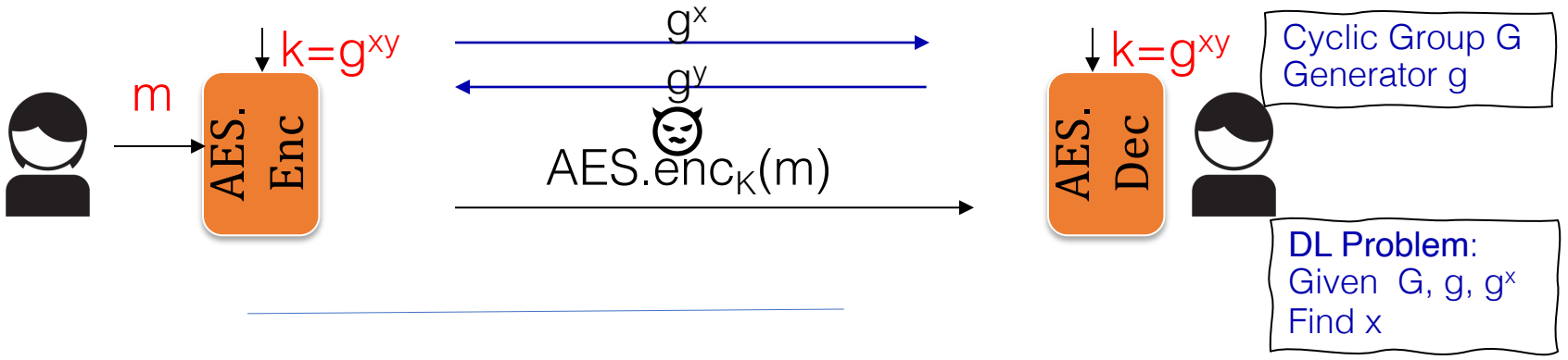
A secure key agreement (SKA) protocol establishes a key.



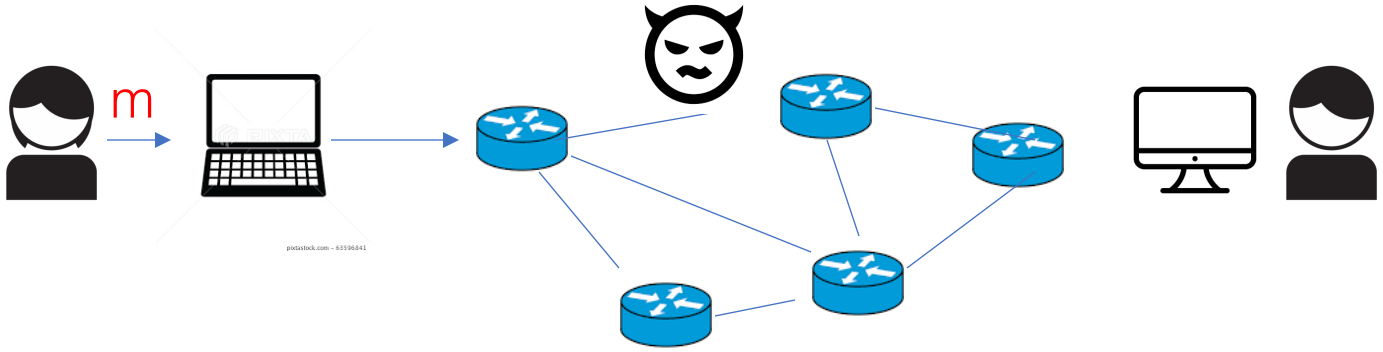
Confidential communication over Internet



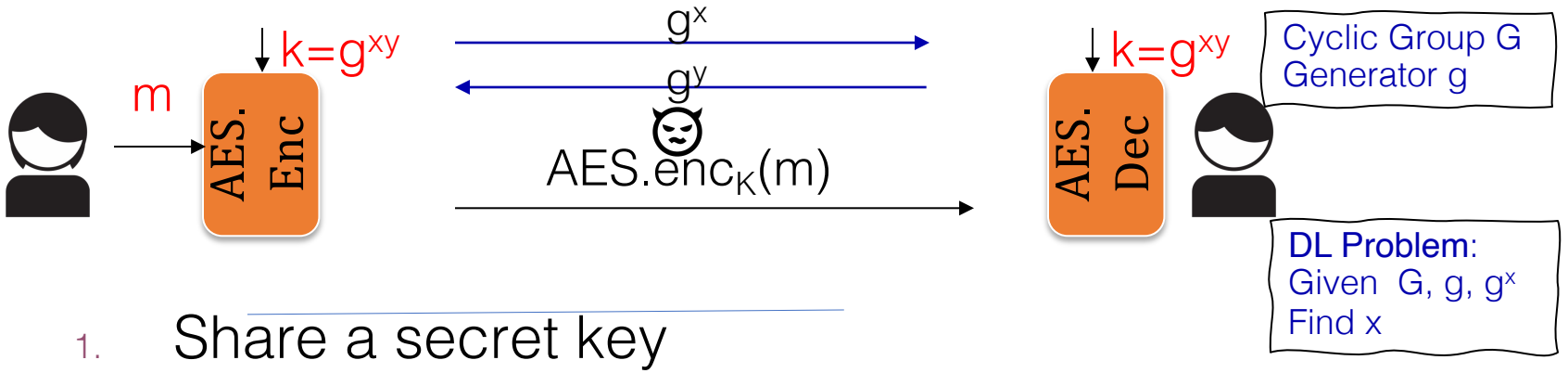
A secure key agreement (SKA) protocol establishes a key.



Confidential communication over Internet

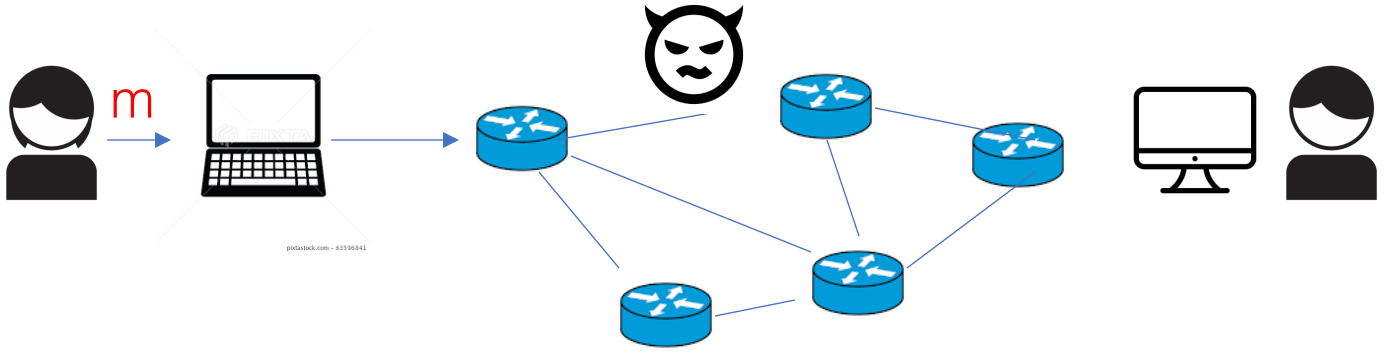


A secure key agreement (SKA) protocol establishes a key.

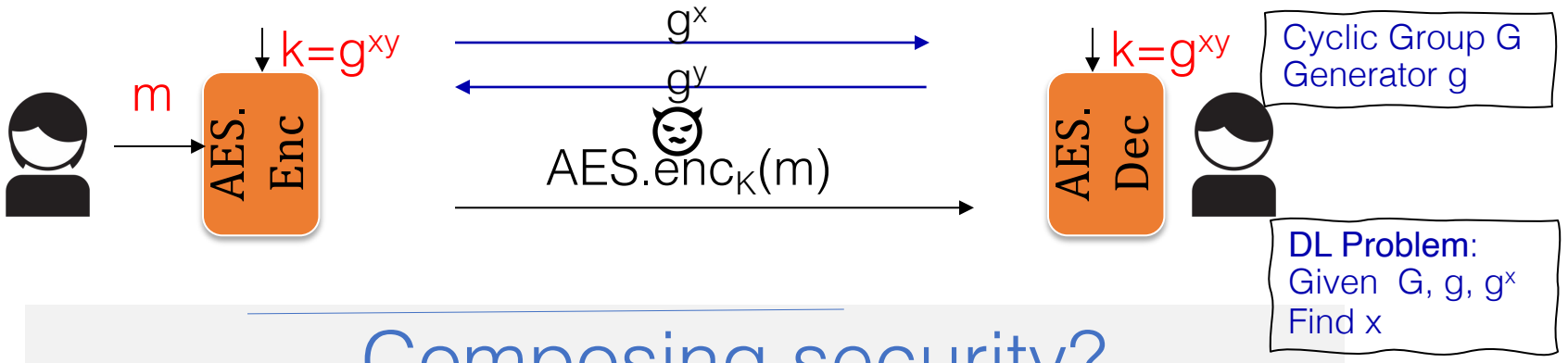


1. Share a secret key
2. Encrypt using a symmetric key cipher

Confidential communication over Internet

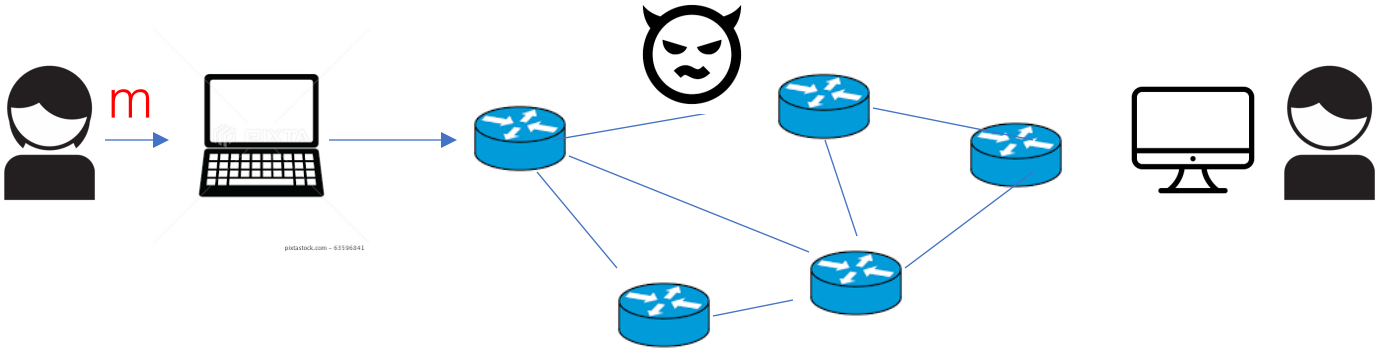


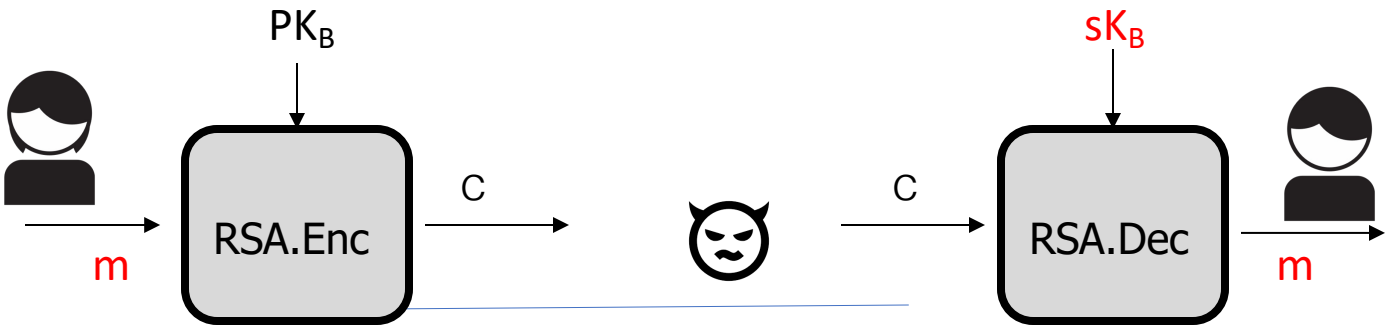
A secure key agreement (SKA) protocol establishes a key.



Composing security?

Confidential communication over Internet

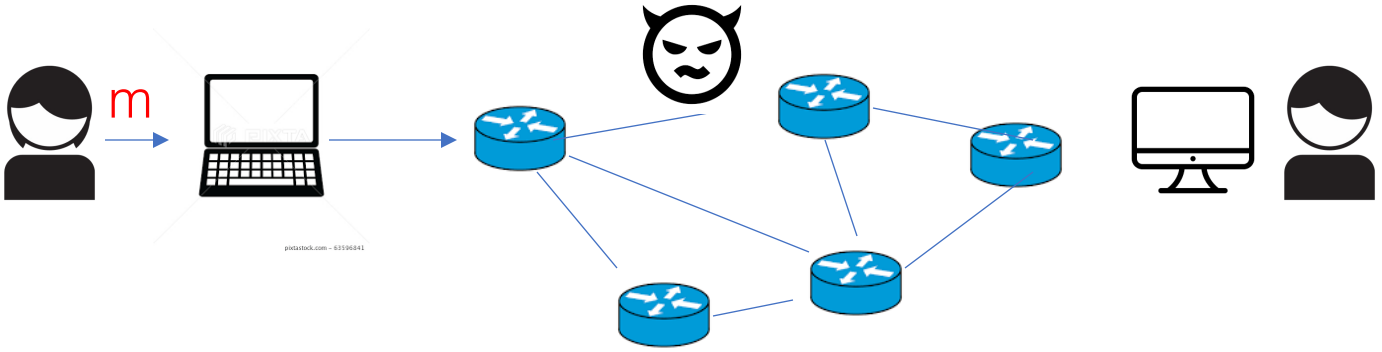


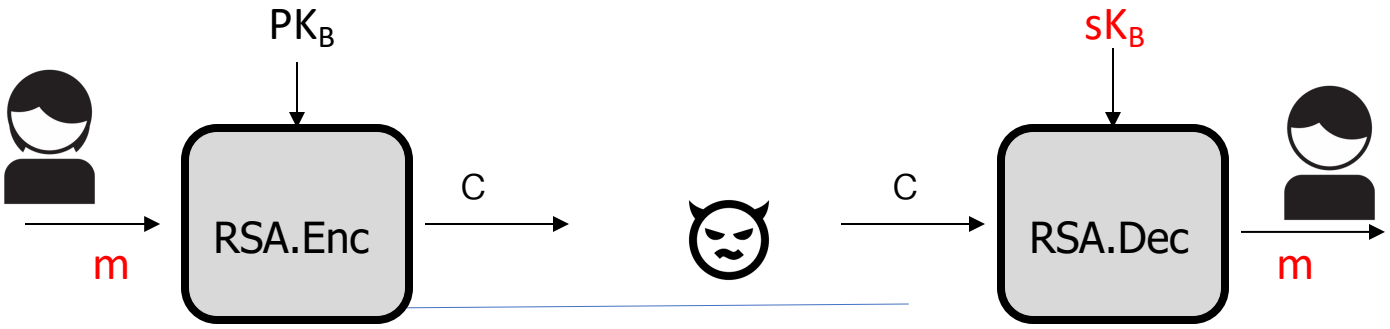


Public key encryption : No key sharing

Computationally Inefficient

Confidential communication over Internet

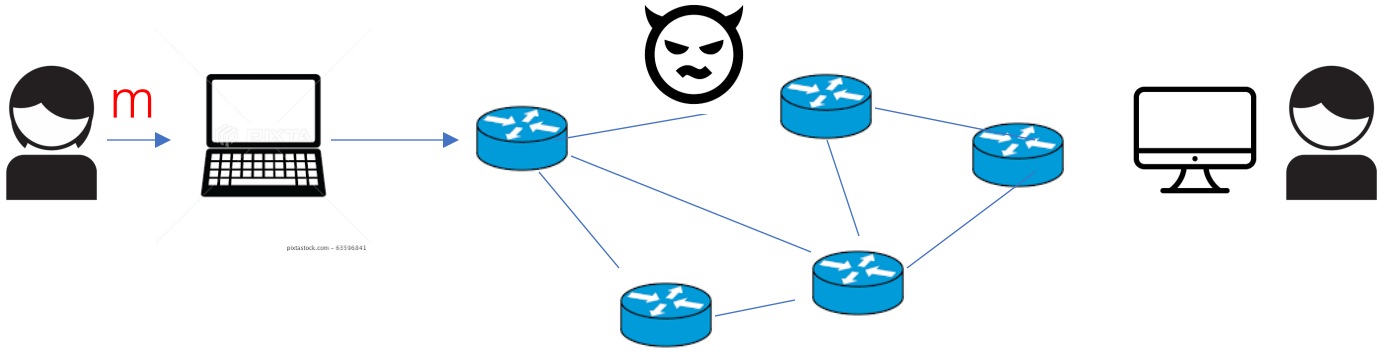


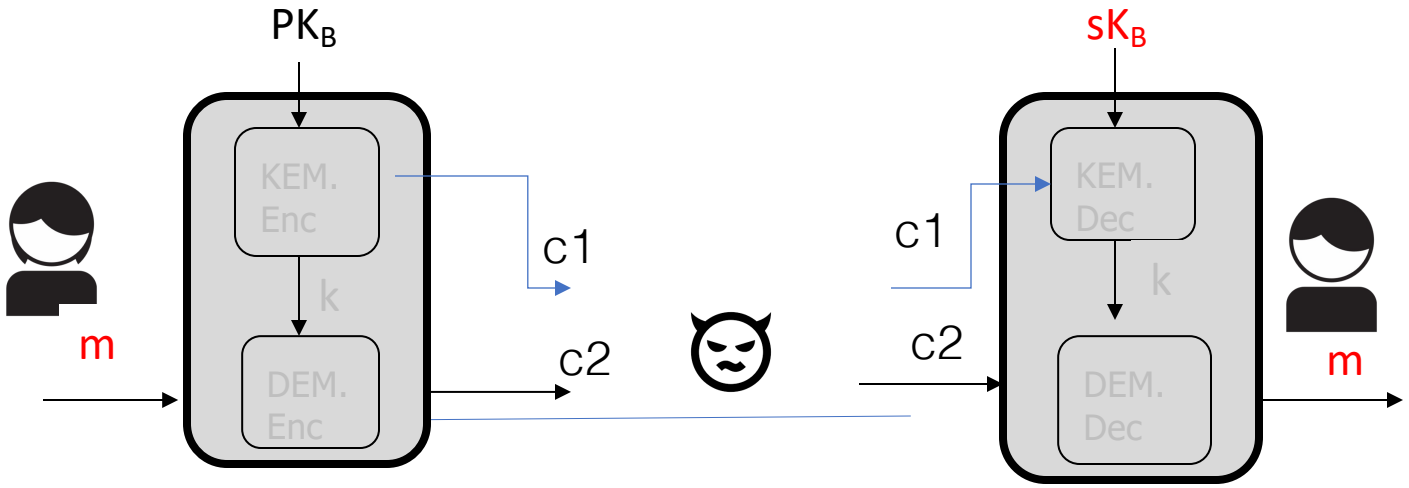


Public key encryption : No key sharing

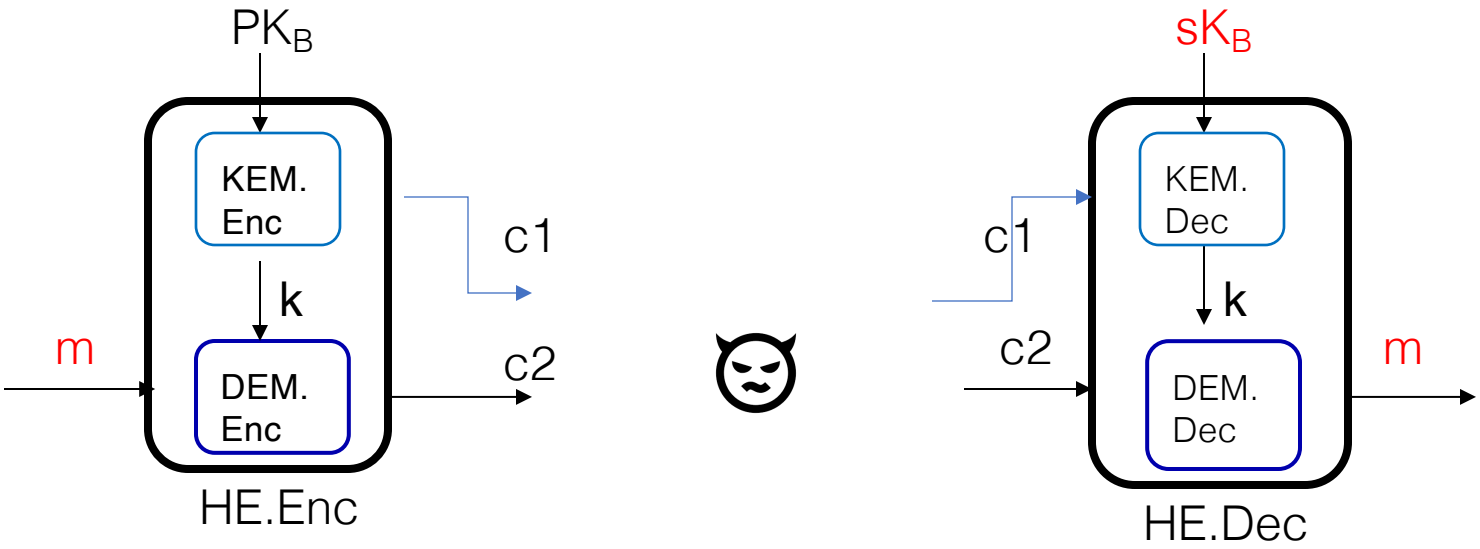
Computationally Inefficient

Hybrid Encryption: SKA + Encryption





Hybrid Encryption: KEM + DEM



KEM = (KEM.KGen, KEM.Enc, KEM.Dec)

Key Generation: $(PK,sK) \leftarrow KEM.KGen(1^\lambda)$

Key Encapsulation: $(k, c_1) \leftarrow KEM.Enc(1^\lambda, PK)$

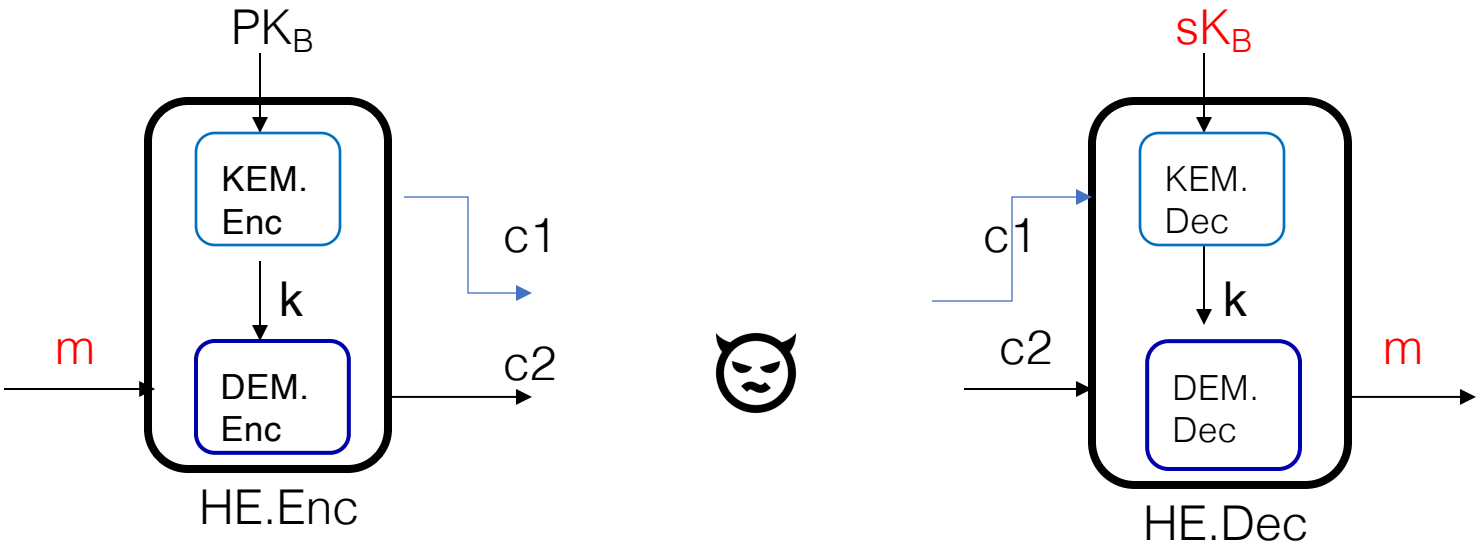
Key Decapsulation: $k \leftarrow KEM.Dec(1^\lambda, sK, c_1)$

DEM= (DEM.Enc, DEM.Dec)

Data Encapsulation: $c_2 \leftarrow DEM.Enc(1^\lambda, k, m))$

Data Decapsulation: $m \leftarrow DEM.Dec(1^\lambda, k, c_1)$

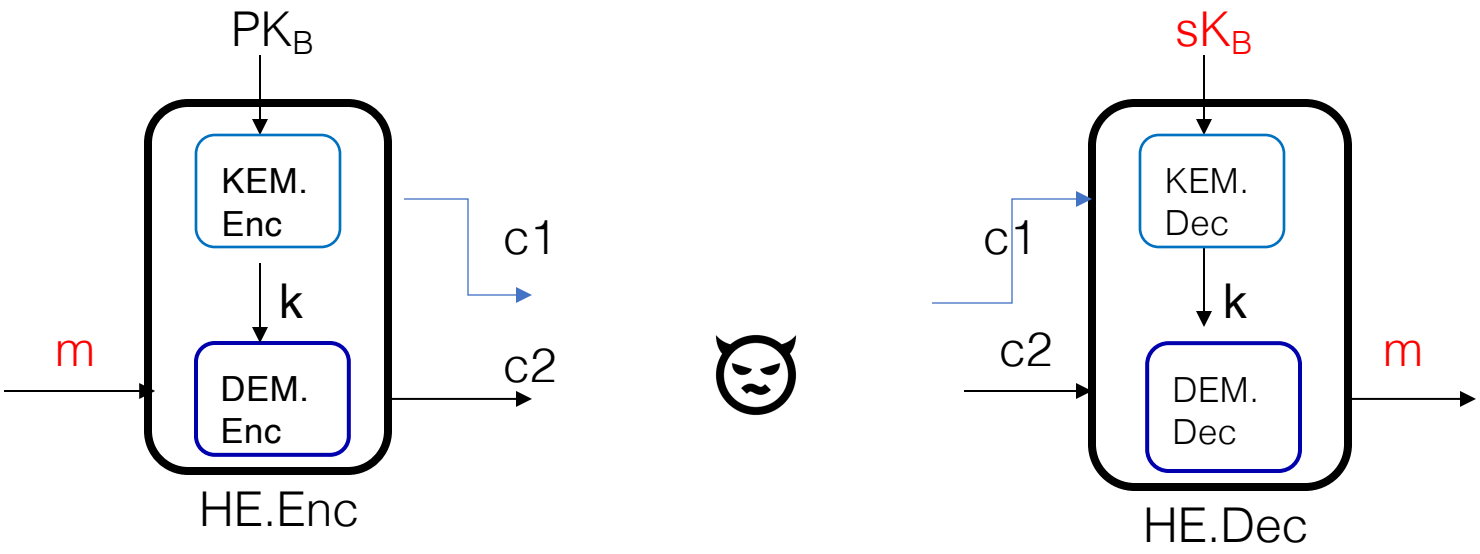
Hybrid Encryption: KEM + DEM



Security Theorem (Cramer & Shoup, Siam J of Comput, 2003)

If KEM and DEM are secure against adaptive chosen ciphertext attacks, then so is HPKE.

Hybrid Encryption: KEM + DEM

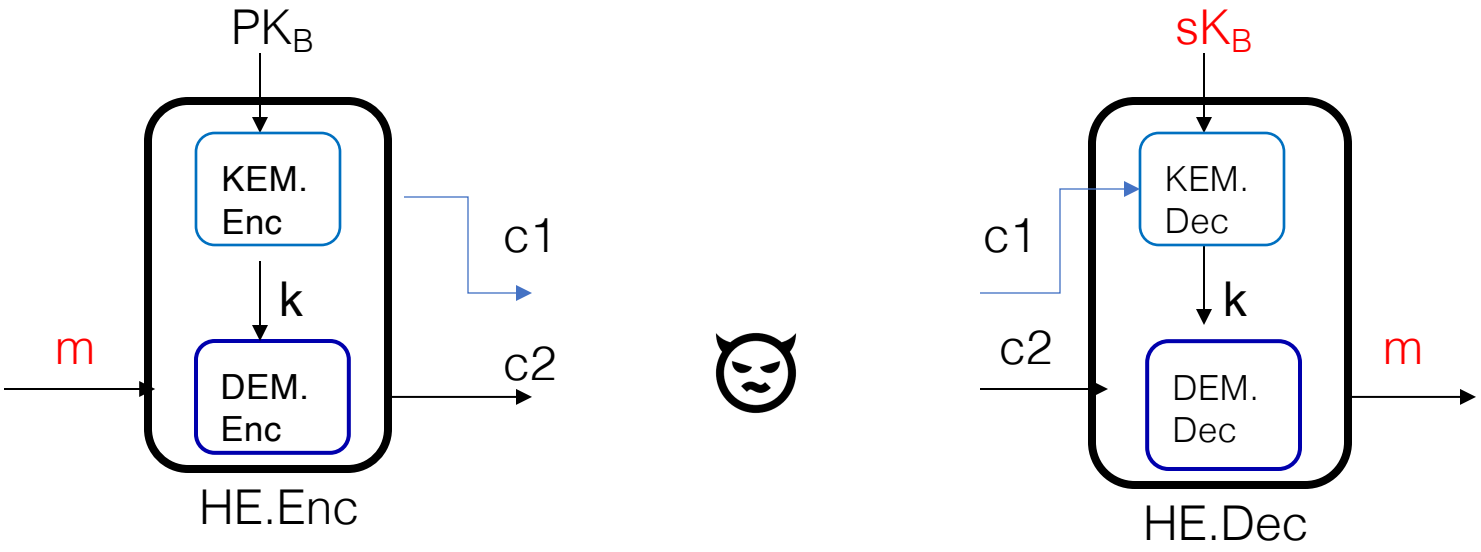


Kyber is a quantum-resistant IND-CCA2-secure KEM

- Security is based on LWE problem over module lattices
- Standardized by NIST.

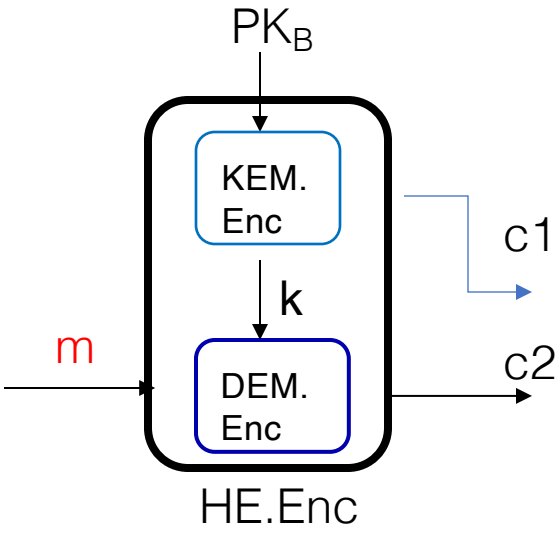
- Kyber is integrated into libraries and systems by industry.
  - Cloudflare integrated Kyber into CIRC;
  - Amazon supports hybrid modes involving Kyber AWS Key Management Service

Hybrid Encryption: KEM + DEM



- Existing KEMs reply on computational assumptions
- Can we have KEM **without computational assumptions**?

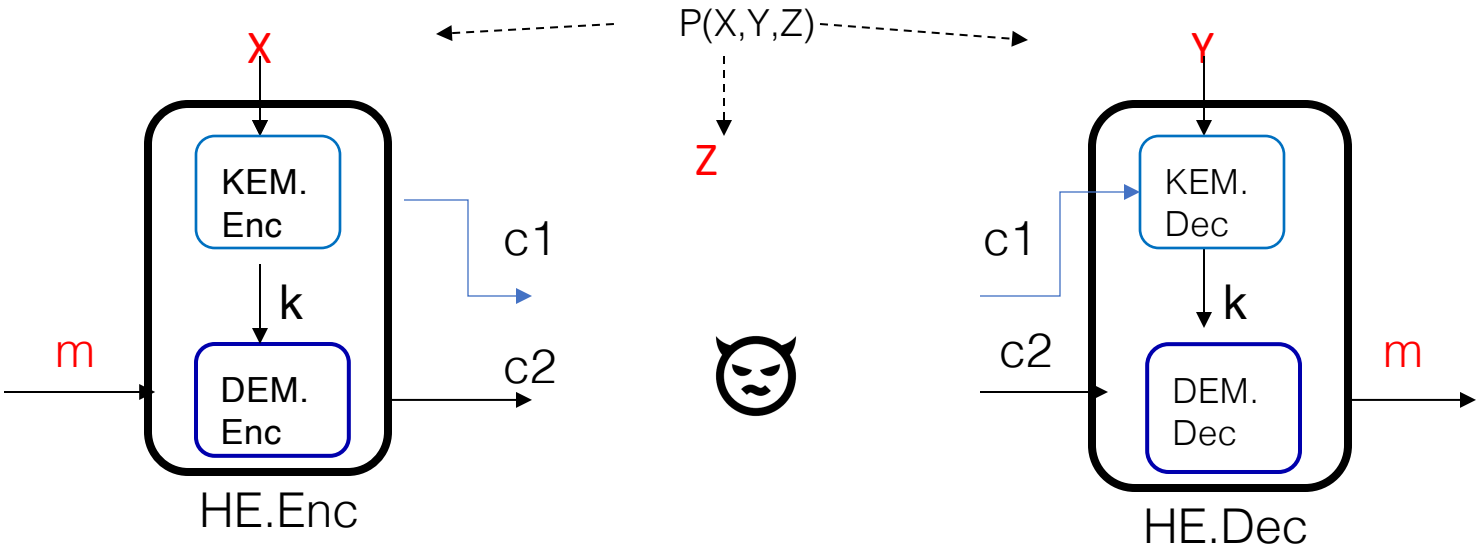
HE without Computational Assumption



Motivations:

- Computational assumptions remain vulnerable to advances in computing
- Expanding the crypto toolbox

HE in Correlated Randomness Model

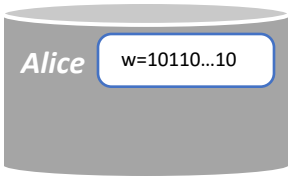


- KEM relies on correlated randomness
  - Information theoretic → iKEM
  - Computationally bounded → cKEM

Correlated Randomness Model:
Where correlated randomness comes from?

- Biometrics

1. Registrations



Server

2. Authentication

new scan

w'=01110…10

New scan code is correlated with the stored code.

Correlated Randomness Model

Where correlated randomness comes from?

- Biometrics

1. Registrations

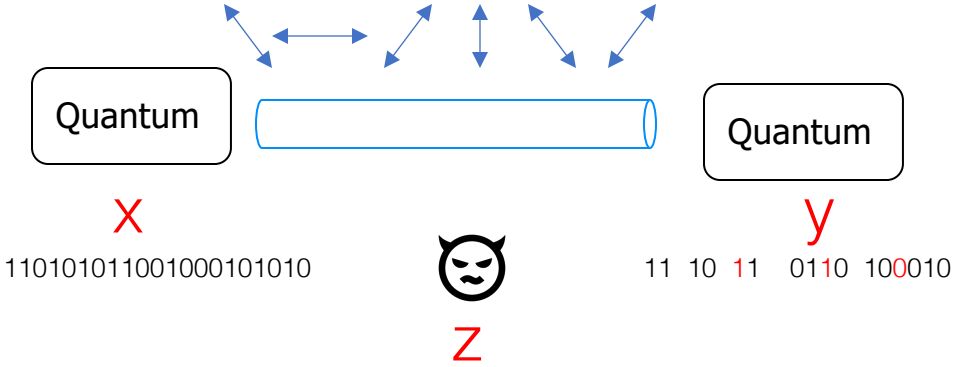
2. Authentication

new scan

w'=01110…10

New scan code is correlated with the stored code.

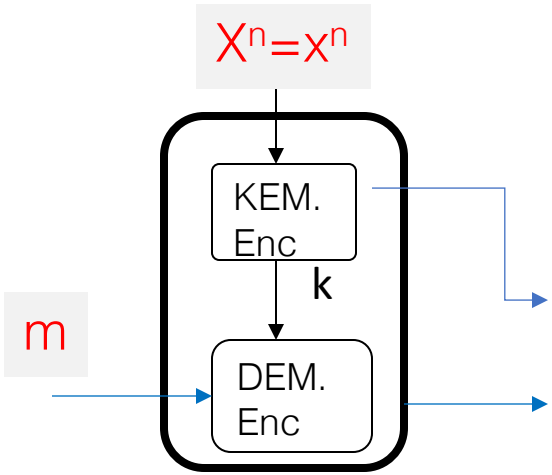
- Transmission over quantum channel



Adversaries - Security

Information theoretic

- Unbounded computation
- KEM &DEM are information theoretic
  - Long keys



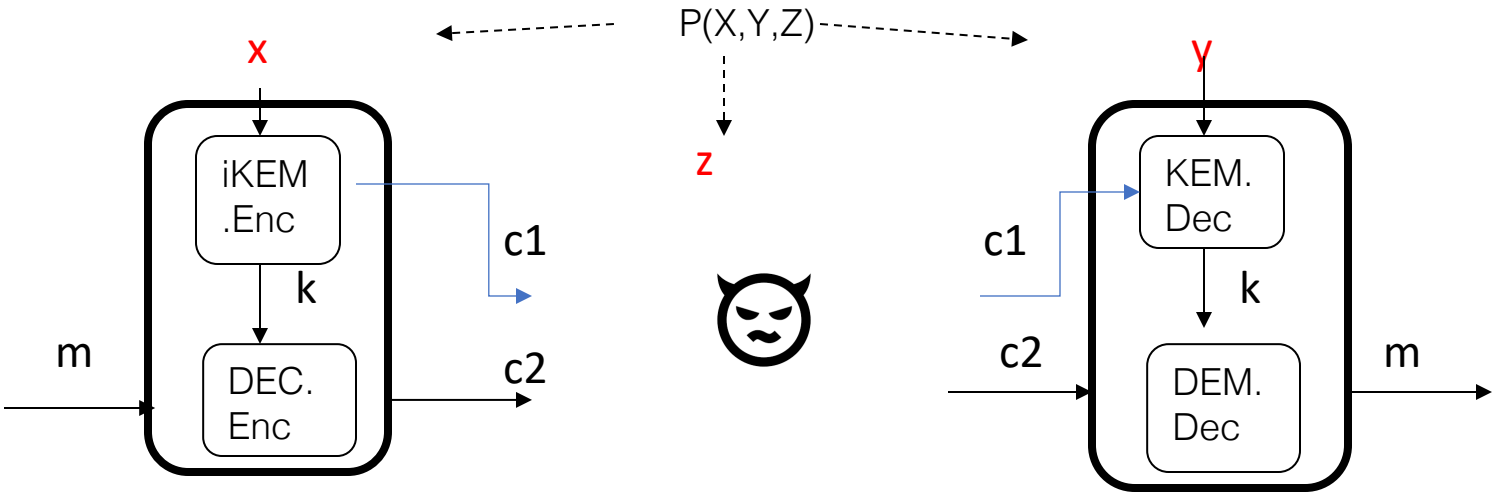
Computational Security

- Bounded computation
  - Access to quantum computer
- (iKEM or cKEM)+ DEM

→ Q-resistant security

  - Infeasible computation
    - Search a large key space
  - cKEM will use hard problems

HE in Correlated Randomness model



HE.Enc

$(k, c_1) \leftarrow$ iKEM.Enc(1^λ, x)
$c_2 \leftarrow$ DEM.Enc(1^λ, k, m)
$(c_1, c_2) =$ HE.Enc(1^λ, x, m)

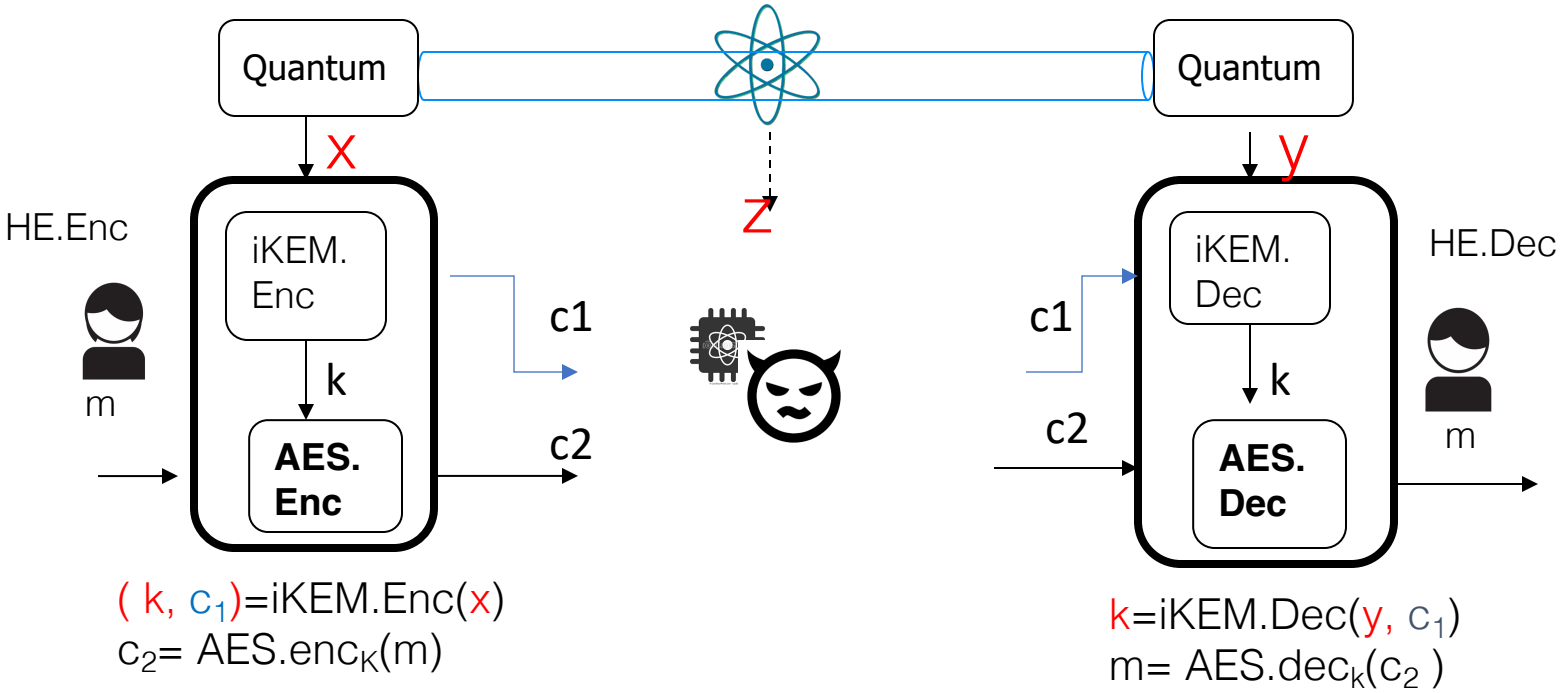
HE.Dec

$K \leftarrow$ iKEM.Dec(1^λ, c_1, y)
$m \leftarrow$ DEM.Dec(1^λ, k, c_2)

Composition Theorem:
IND-q-CEA iKEM + IND-OT DEM⇒IND-q-CPA HE

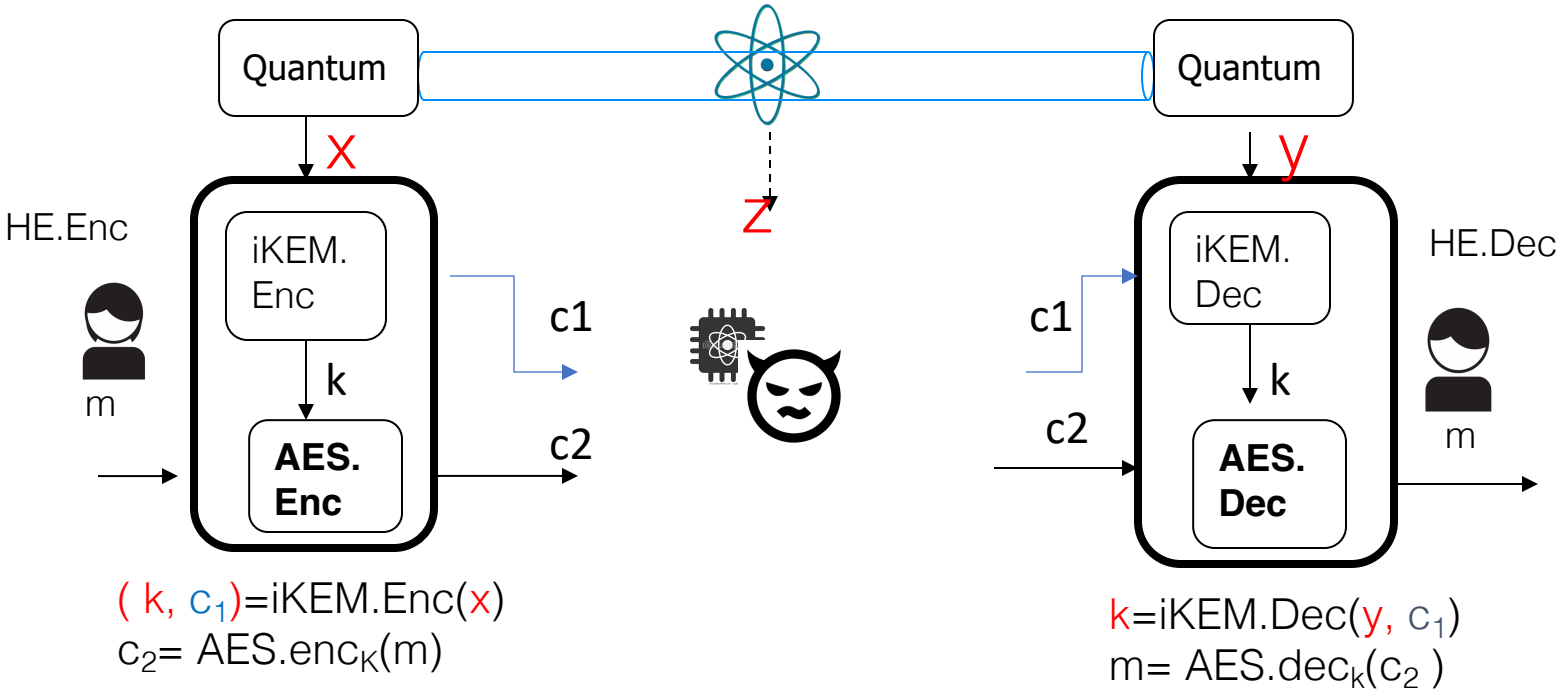
Sharifian & Safavi-Naini, Information-theoretic Key Encapsulation and its Applications to Secure Communication, International Symposium on Information Theory(ISIT), 202

Quantum-enabled Quantum-resistant HE



- KEM relies on correlated randomness
  - Information theoretic → iKEM
- Computational DEM
  - AES

Quantum-enabled Quantum-resistant HE



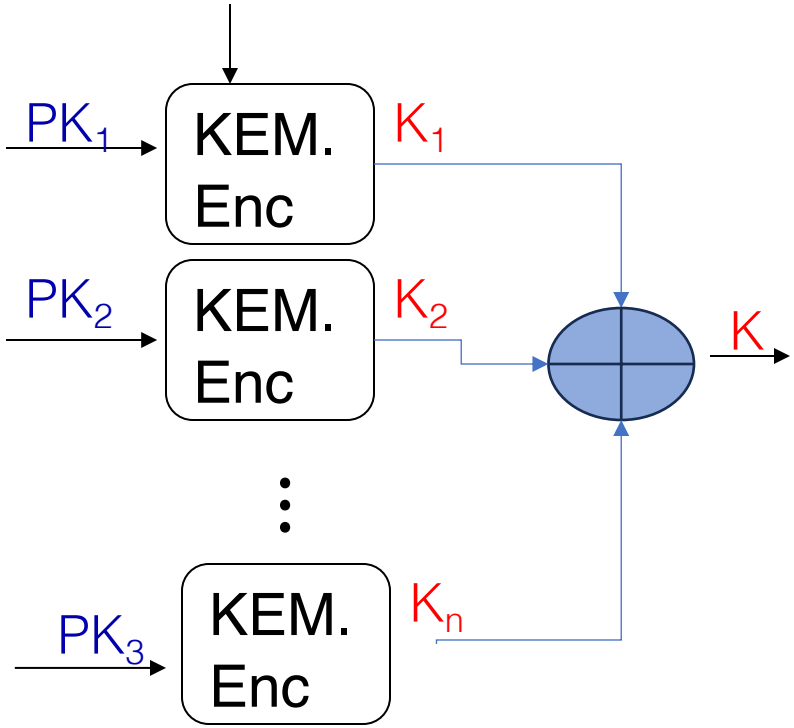
- KEM relies on correlated randomness
  - Information theoretic → iKEM
- Computational DEM
  - AES

Efficient Q-resistant hybrid encryption

k

KEM Combiners

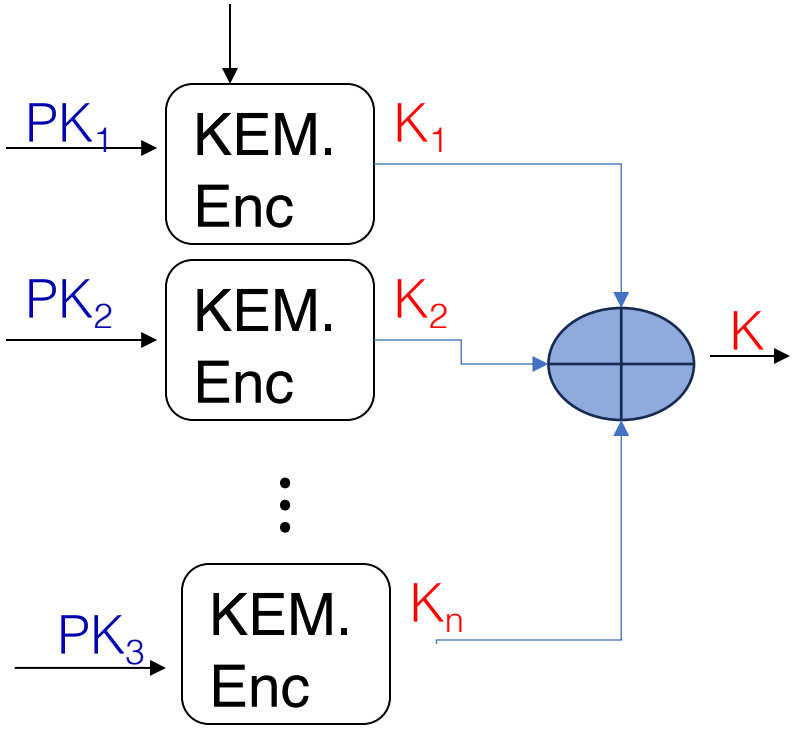
- Cryptographic combiners

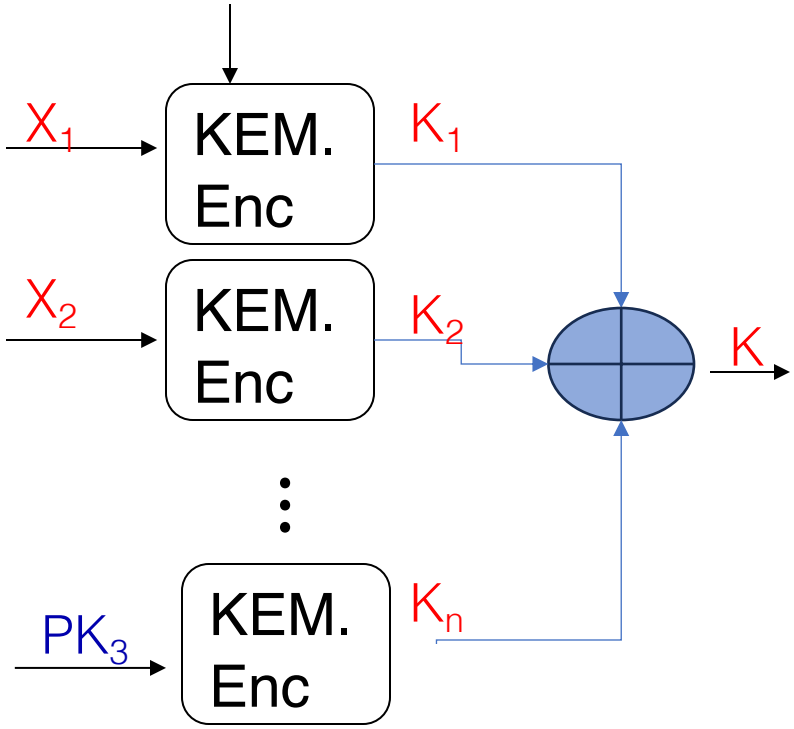


k

KEM Combiners

- Cryptographic combiners





Concluding remarks

- Quantum–resistant confidentiality
  - Proved security
  - No public key (hard problem)
  - Adversary with Access to quantum computer
  - Infeasible computation
    - Search a large key space

- Future work: quantum adversary

- Acknowledgement: Somnath Panja, Shaoquan Jiang, Setareh Sharifian, Nikita Tripathi, Ali Poostindouz