A Generic Construction of Tightly Secure Password-based Authenticated Key Exchange

eprint: 2023/1334

Jiaxin Pan

UNIKASSEL VERSITÄT

Runzhi Zeng

NTNU

Norwegian University of Science and Technology

Authenticated Key Exchange

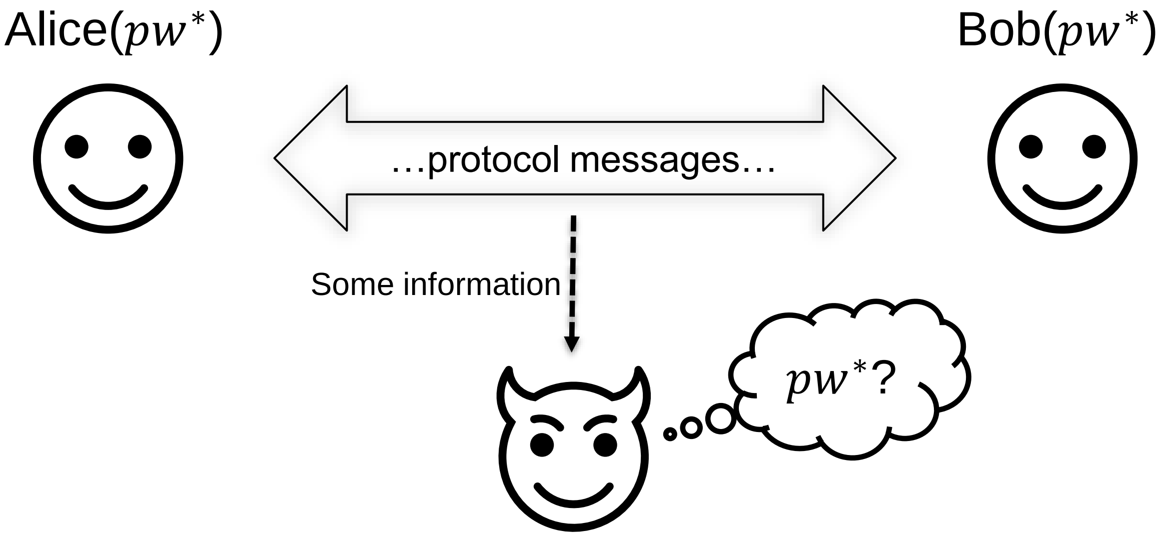
NTNU

Password-based AKE (PAKE)

-  is **password**
  - Authenticated by pre-shared password
  - Low entropy (Human memorable)

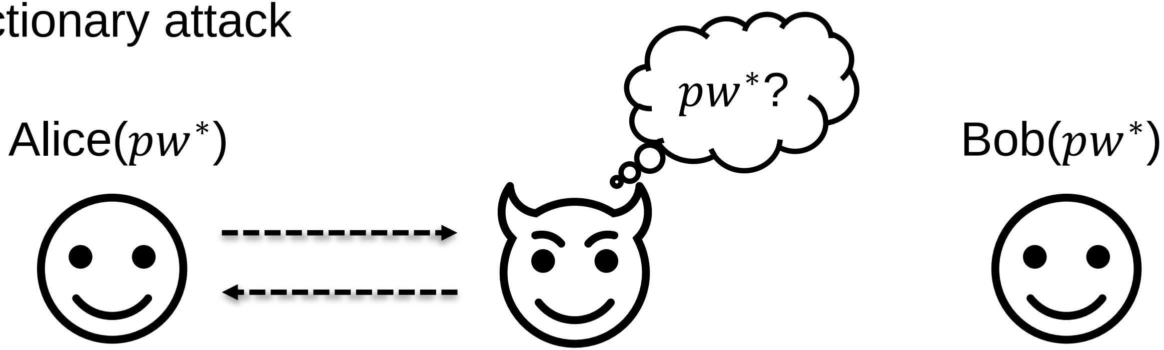
PAKE Security

- **Offline** dictionary attack



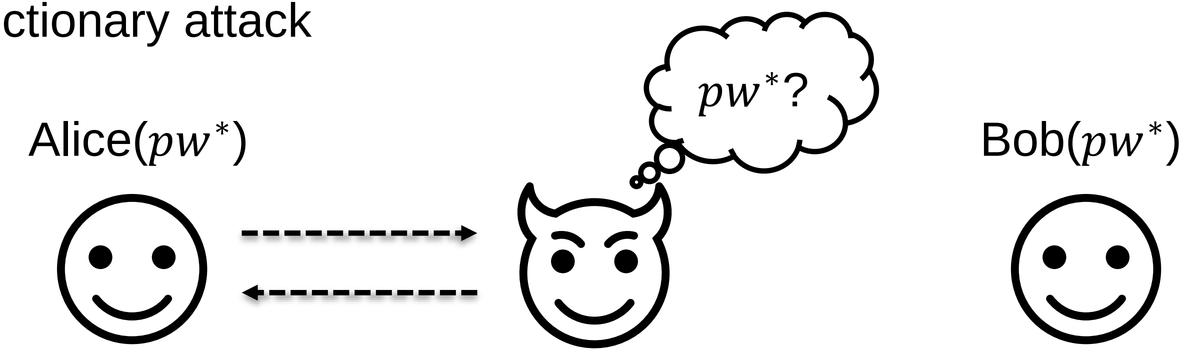
PAKE Security

- **Online** dictionary attack



PAKE Security

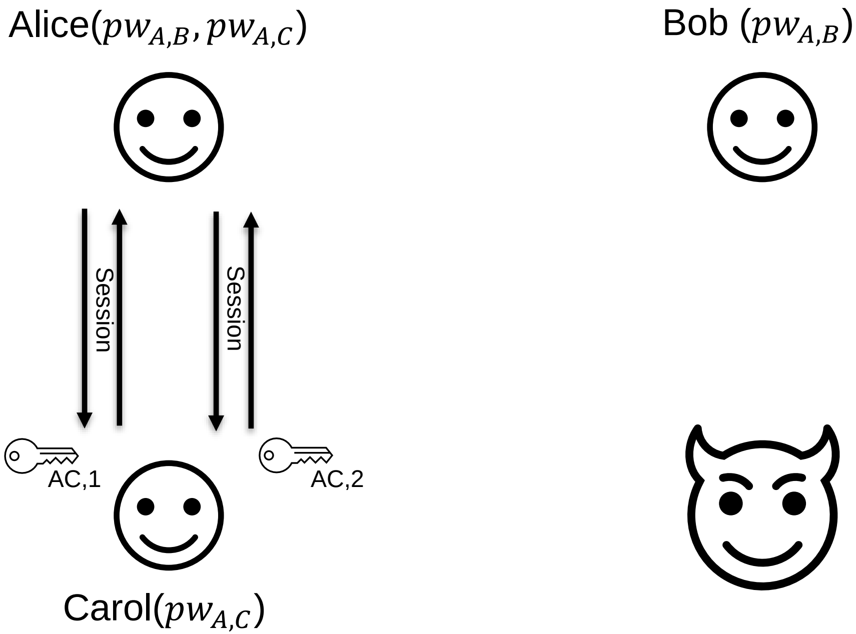
- **Online** dictionary attack



- A secure PAKE protocol...
  - Authenticity from password
  - Resist offline attack
  - The **best** attack (that A can perform)**: Online attack**

PAKE Security – BPR model [BPR00]

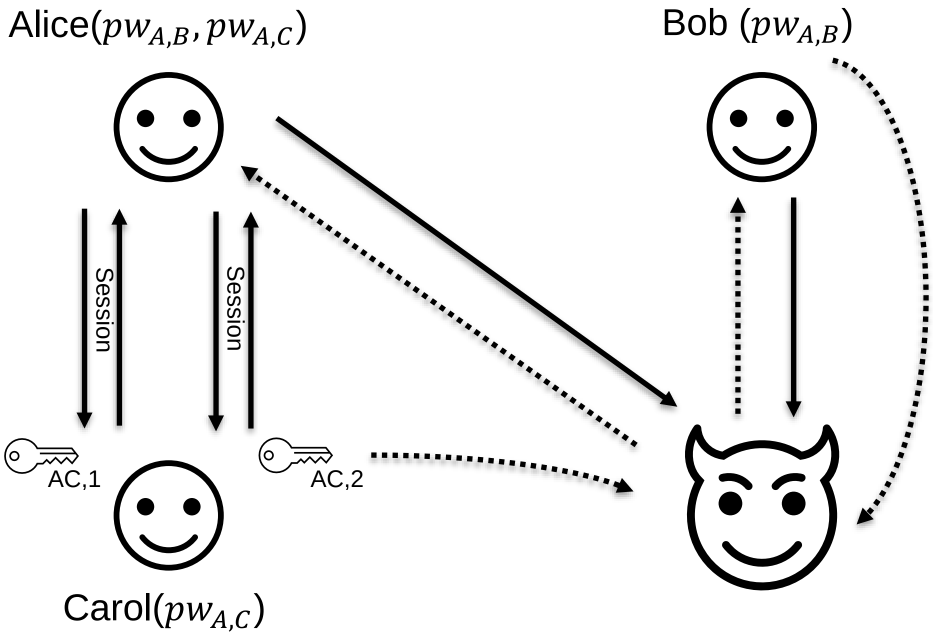
- Multiple user
- Multiple sessions



PAKE Security – BPR model [BPR00]

- Multiple user
- Multiple sessions

- Adversary Capabilities
  - Control the network
  - Reveal established session keys
  - Adaptively corrupt passwords

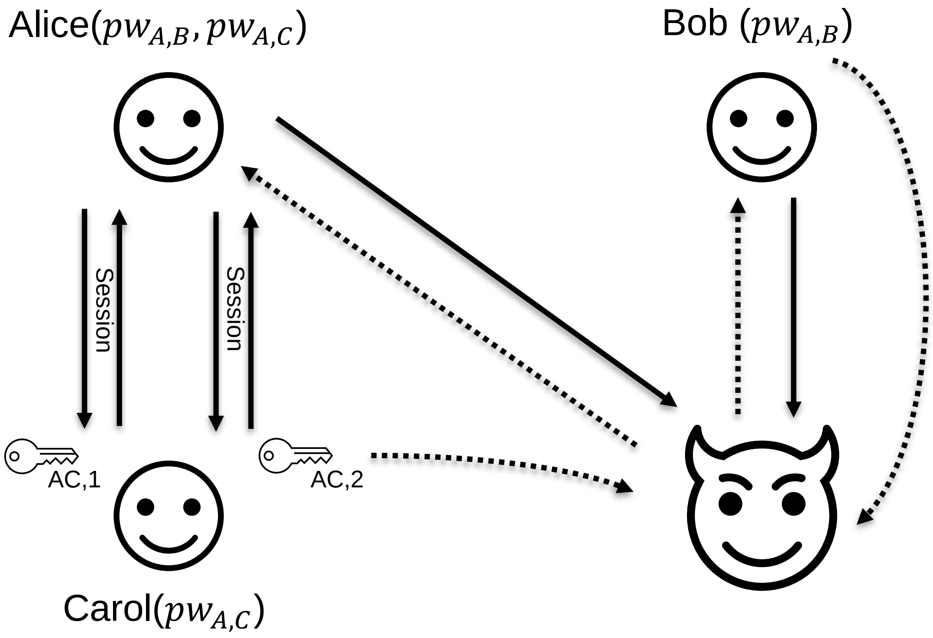


PAKE Security – BPR model [BPR00]

- Multiple user
- Multiple sessions

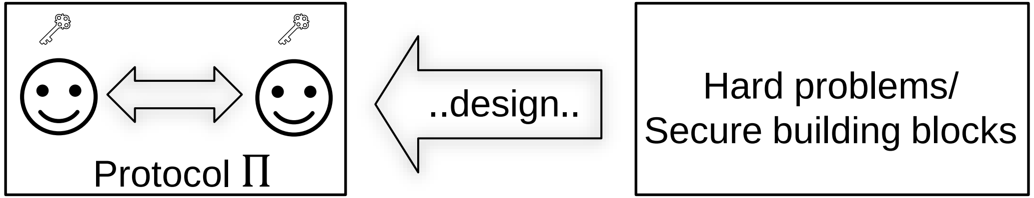
- Adversary Capabilities
  - Control the network
  - Reveal established session keys
  - Adaptively corrupt passwords

- Security Goals
  - Key Indistinguishability
  - Authentication
  - Resist offline attack
  - Best attack: Online dictionary attack



Tightness of Security Reduction

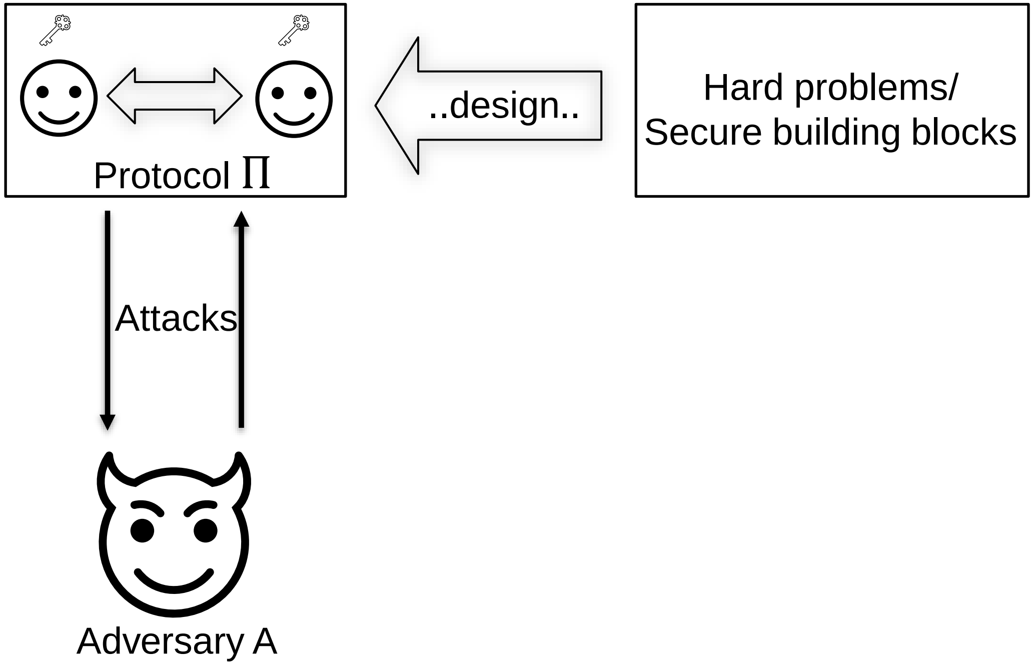
- Security Proof via Reduction



NTNU

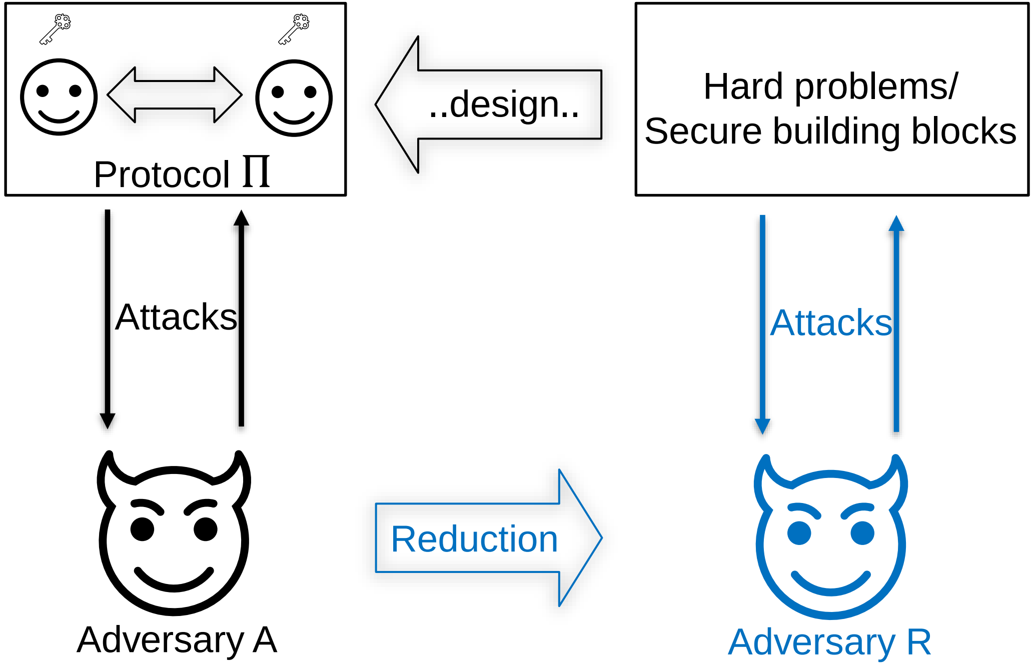
Tightness of Security Reduction

- Security Proof via Reduction
  - A breaks Π



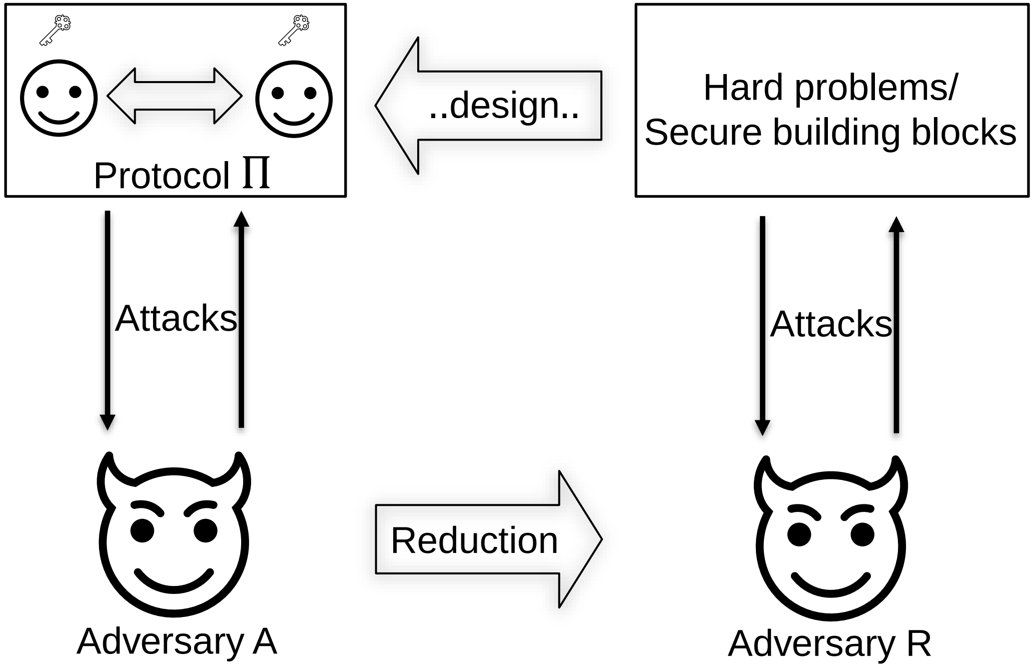
Tightness of Security Reduction

- Security Proof via Reduction
  - A breaks Π
    $\Longrightarrow$ R solves problems



Tightness of Security Reduction

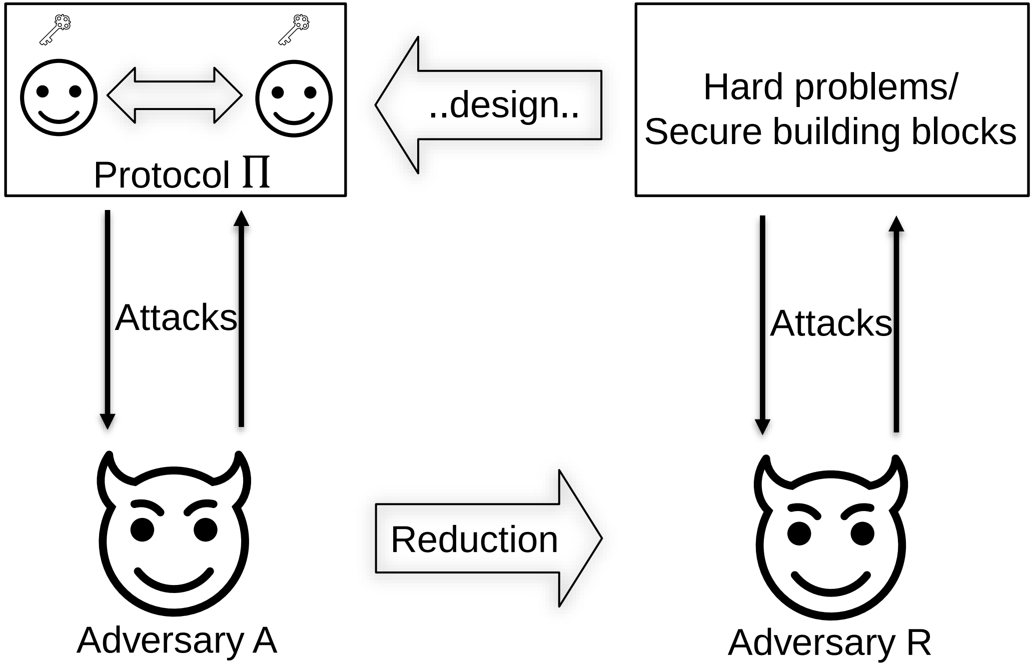
- Security Proof via Reduction
  - A breaks Π
    $\Longrightarrow$ R solves problems
- Tightness of Reduction
  - $\mathbf{Adv}(\mathrm{R}) \leq L \cdot \mathbf{Adv}(\mathrm{A})$
  - L: Security loss



Tightness of Security Reduction

- Security Proof via Reduction
  - A breaks Π
    $\Longrightarrow$ R solves problems

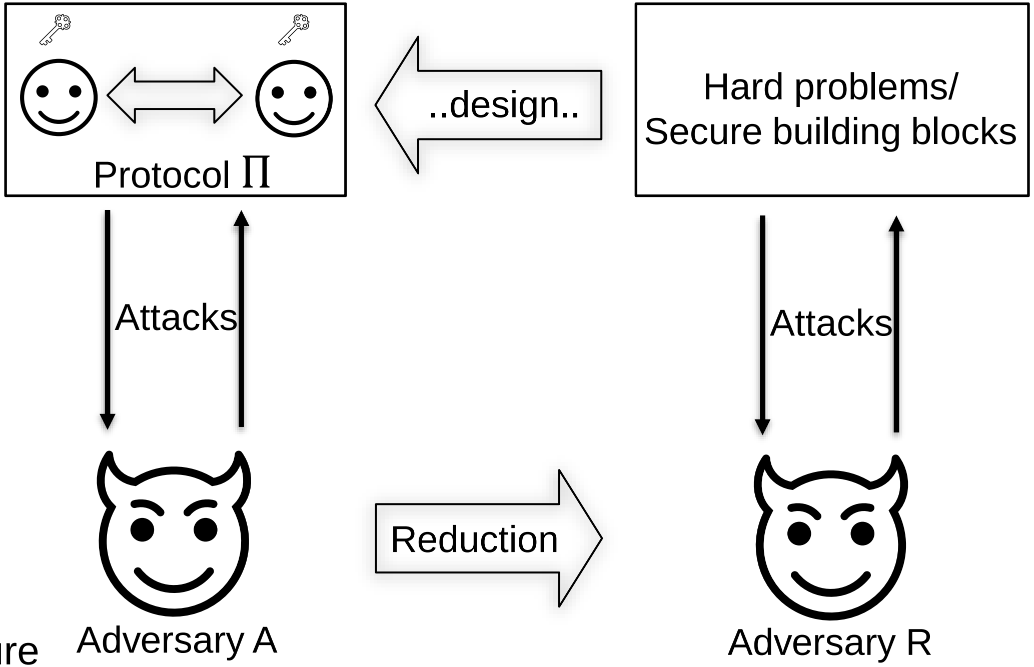
- Tightness of Reduction
  - $\mathbf{Adv}(\mathrm{R}) \leq L \cdot \mathbf{Adv}(\mathrm{A})$
  - L: Security loss
  - L smaller $\Longrightarrow$ tighter



NTNU

Tightness of Security Reduction

- Security Proof via Reduction
  - A breaks Π
    $\Longrightarrow$ R solves problems
- Tightness of Reduction
  - $\mathbf{Adv}(\mathrm{R}) \leq L \cdot \mathbf{Adv}(\mathrm{A})$
  - L: Security loss
  - L smaller $\Longrightarrow$ tighter
- Relevance: Parameter selection
  - L is large $\Longrightarrow$ inefficient or insecure



Post-Quantum PAKE

- Obstacles: Algebraic structure, efficiency…

- HPS-based constructions [KV09, ZY17]
- Bit-by-bit approach + Isogeny [AEK+22]
- Encrypted-Key-Exchange(EKE)-based constructions [BM92, BCP+23, LLHG23]

Post-Quantum PAKE

- Obstacles: Algebraic structure, efficiency…

- HPS-based constructions [KV09, ZY17]
- Bit-by-bit approach + Isogeny [AEK+22]
- **Encrypted-Key-Exchange(EKE)-based constructions** [BM92, BCP+23, LLHG23]
  - Based on KE protocol...
  - Ideal cipher model (ICM) and Random oracle model (ROM)...

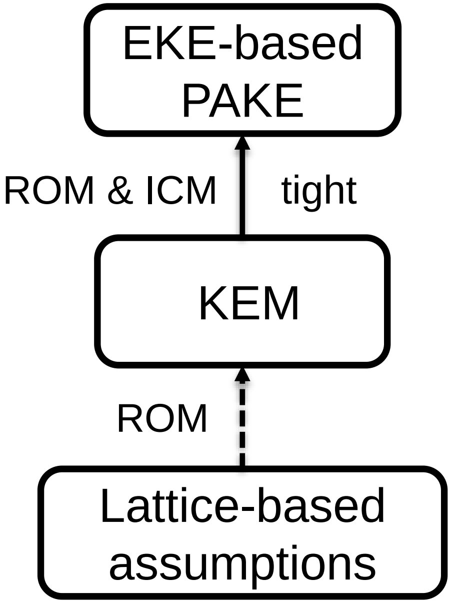
Post-Quantum PAKE

- Obstacles: Algebraic structure, efficiency…

- HPS-based constructions [KV09, ZY17]
- Bit-by-bit approach + Isogeny [AEK+22]
- **Encrypted-Key-Exchange(EKE)-based constructions** [BM92, BCP+23, LLHG23]
  - Based on KE protocol... (PQ KE is well studied)
  - ICM and ROM...
  - The only known tight construction is based on DH

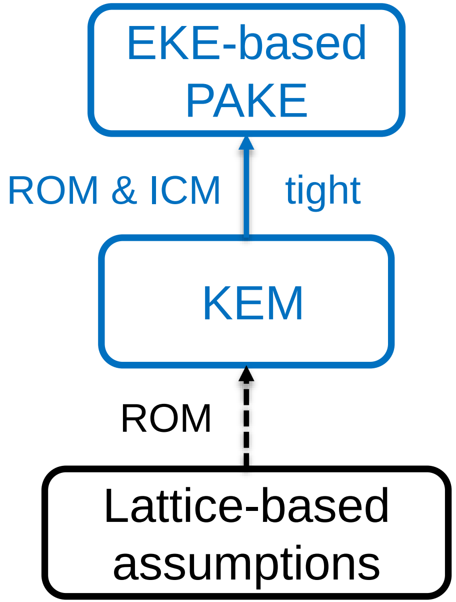
- **Can we have a <u>tightly-secure</u> <u>post-quantum</u> EKE-based PAKE protocol?**

Our Contributions



Our Contributions

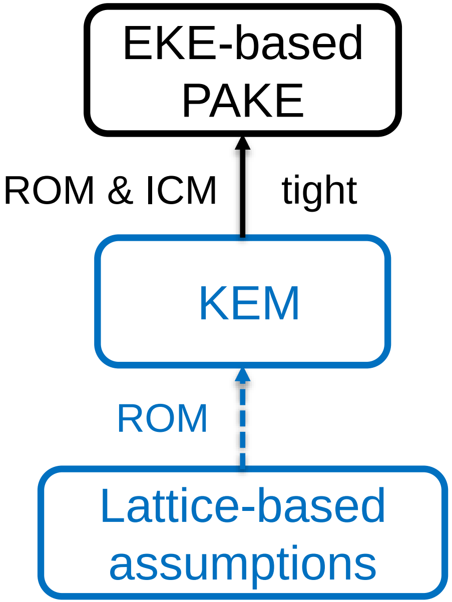
1. EKE-based PAKE with tight reduction from KEM
   – Muti-user-challenge KEM with
      • pk uniformity,
      • pseudorandom ciphertexts,
      • and PCA security
   – In the ROM and ICM



Our Contributions

1. EKE-based PAKE with tight reduction from KEM
   - Muti-user-challenge KEM with
     - pk uniformity,
     - pseudorandom ciphertexts,
     - and PCA security
   - In the ROM and ICM

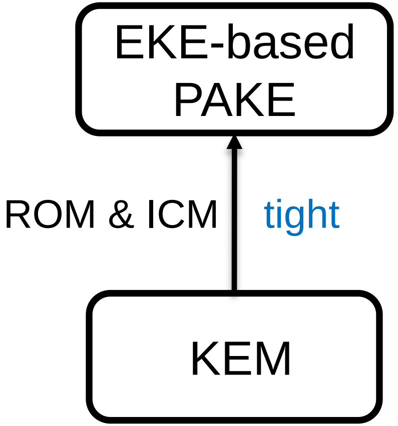
2. Lattice-based Instantiations
   - LWE, MLWE
   - Better concrete security bounds



Our Contributions

Table: Security Loss from **KEMs**

Scheme	Underlying KEM	Security Loss
LLHG23	twin-DH KEM	$\Theta(1)$
BCP+23	Single-user, single-challenge KEM	$O(q \cdot (q + S))$
Our work	Multi-user, multi-challenge KEM	$\Theta(1)$

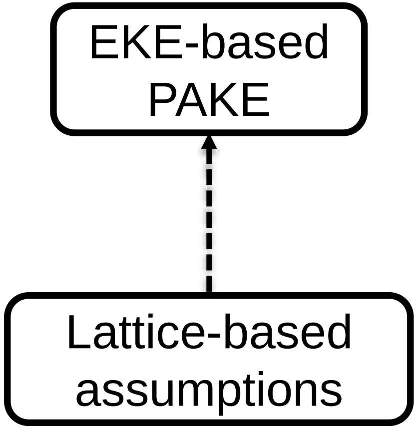


- S: Number of session;
- q: Number of queries to RO or IC;
- $\boldsymbol{S \ll q}$

Our Contributions

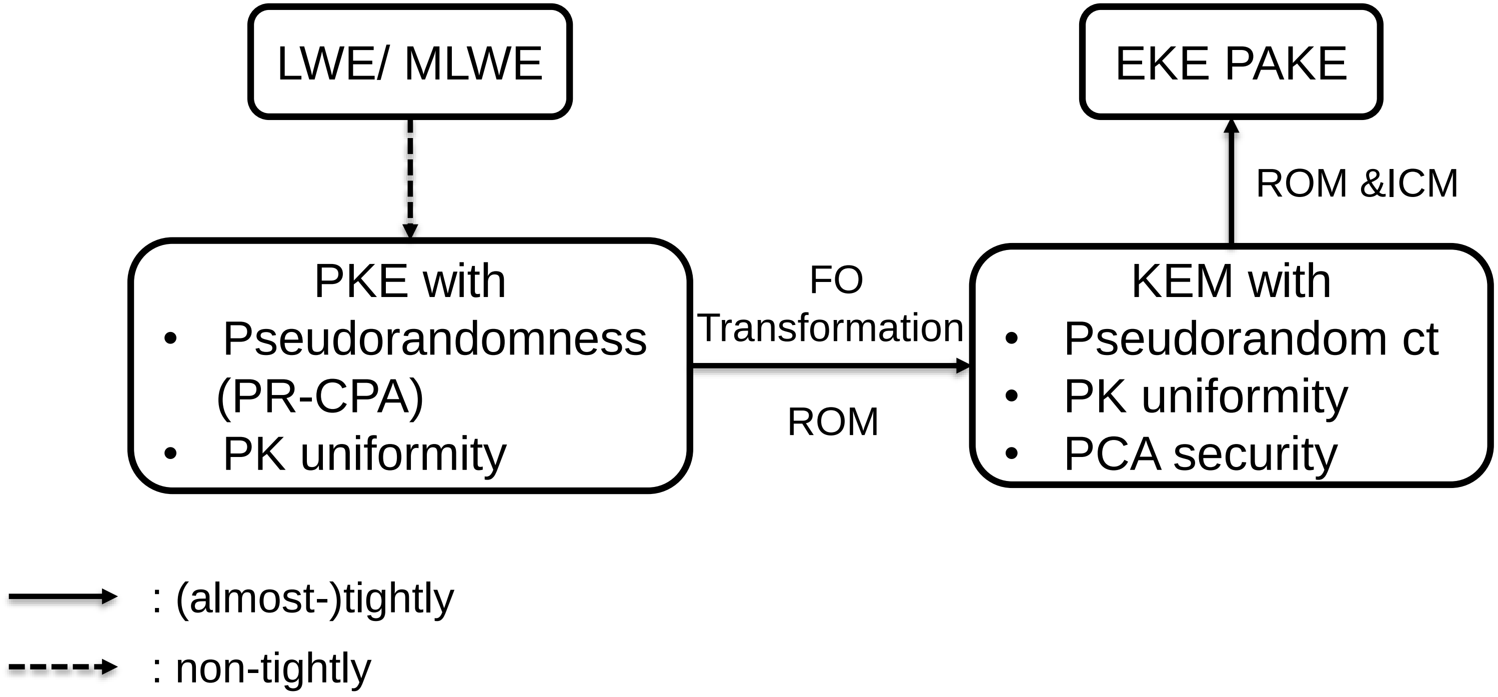
Table: Security Loss from **Assumptions**

Scheme	Assumption	Security Loss
LLHG23	twin DH	$\Theta(1)$
BCP+23	LWE	$O(\boldsymbol{q} \cdot (q + S))$
	MLWE (Kyber)	$O(\boldsymbol{q} \cdot (q + S))$
Our work	LWE	$O(q + S)$
	MLWE(Kyber)	$O(\boldsymbol{S} \cdot (q + S))$

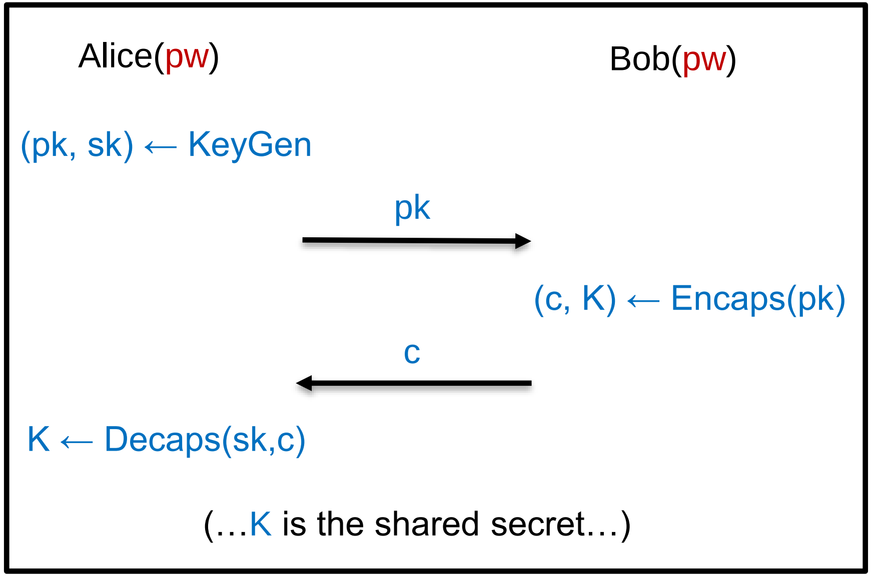


- S: Number of session;
- q: Number of queries to RO or IC;
- $\boldsymbol{S} \ll \boldsymbol{q}$

Technical Outline

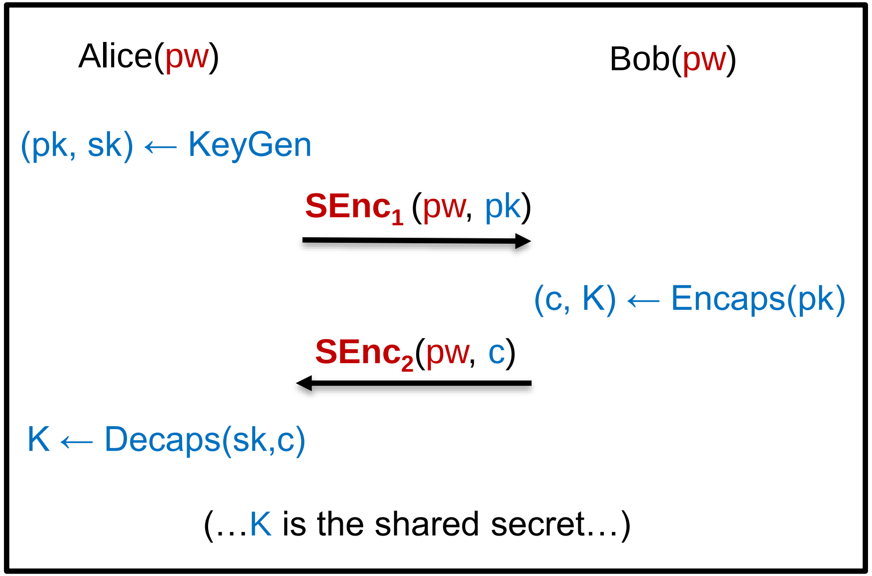


EKE Construction – PAKE from KEM



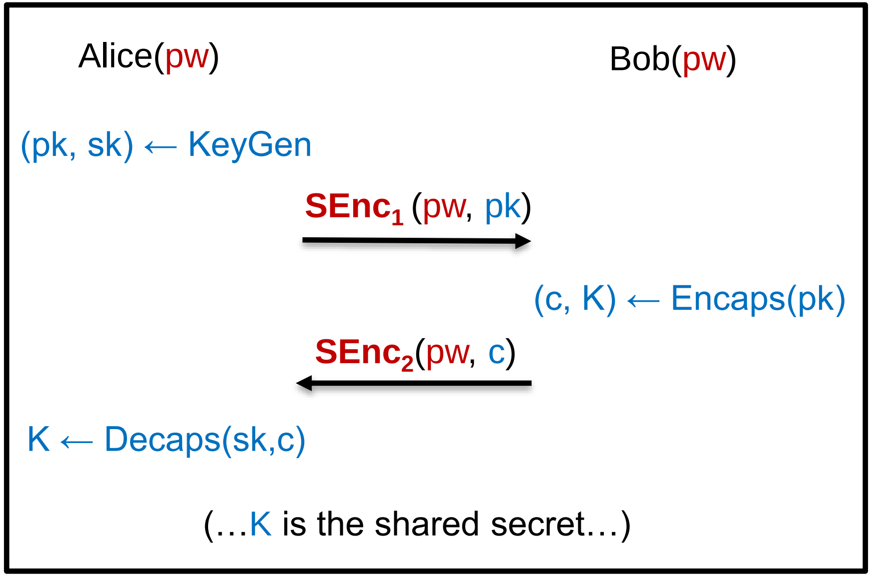
- KEM-based EKE [BCP+23]
  - Based on KEM-based key exchange

EKE Construction – PAKE from KEM



- KEM-based EKE [BCP+23]
  - Based on KEM-based key exchange
  - Encrypted by password (pw as symmetric key)

EKE Construction – PAKE from KEM

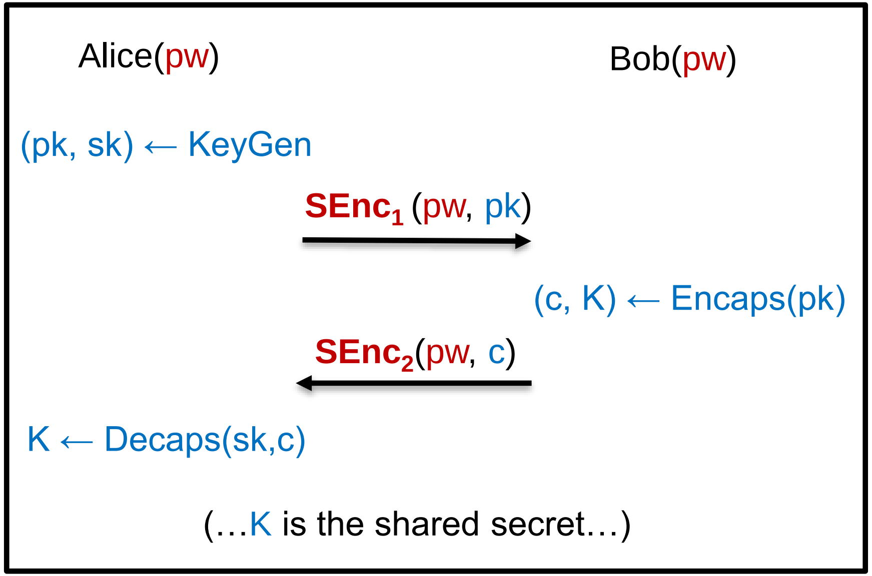


- KEM-based EKE [BCP+23]
  - Based on KEM-based key exchange
  - Encrypted by password
    (pw as symmetric key)

- To prove PAKE security...
  - What security properties should **KEM** and **SEnc** have?

NTNU

EKE Construction – PAKE from KEM



1. SEnc_1 and SEnc_2 are modelled as **ideal ciphers**

NTNU

EKE Construction – PAKE from KEM

Alice(pw) Bob(pw)

(pk, sk) ← KeyGen

$\mathbf{SEnc_1}$ (pw, pk) →

(c, K) ← Encaps(pk)

$\mathbf{SEnc_2}$(pw, c) ←

K ← Decaps(sk,c)

(…K is the shared secret…)

1. $SEnc_1$ and $SEnc_2$ are modelled as **ideal ciphers**
   - Embed challenges
   - **Against offline dictionary attacks**

NTNU

EKE Construction – PAKE from KEM

Alice(pw) Bob(pw)

(pk, sk) ← KeyGen

SEnc_1 (pw, pk) →

(c, K) ← Encaps(pk)

SEnc_2(pw, c) ←

K ← Decaps(sk,c)

(…K is the shared secret…)

1. SEnc_1 and SEnc_2 are modelled as **ideal ciphers**

2. KEM is required to have:

EKE Construction – PAKE from KEM

Alice(pw) Bob(pw)

(pk, sk) ← KeyGen

$SEnc_1$ (pw, pk) →

(c, K) ← Encaps(pk)

← **$SEnc_2$**(pw, c)

K ← Decaps(sk,c)

(…K is the shared secret…)

1. $SEnc_1$ and $SEnc_2$ are modelled as **ideal ciphers**

2. KEM is required to have:
   - **PK uniformity**

   (…since pk is output of ideal cipher; Against offline attacks…)

EKE Construction – PAKE from KEM

Alice(pw) Bob(pw)

(pk, sk) ← KeyGen

$\mathbf{SEnc_1}$ (pw, pk) →

(c, K) ← Encaps(pk)

$\mathbf{SEnc_2}$(pw, c) ←

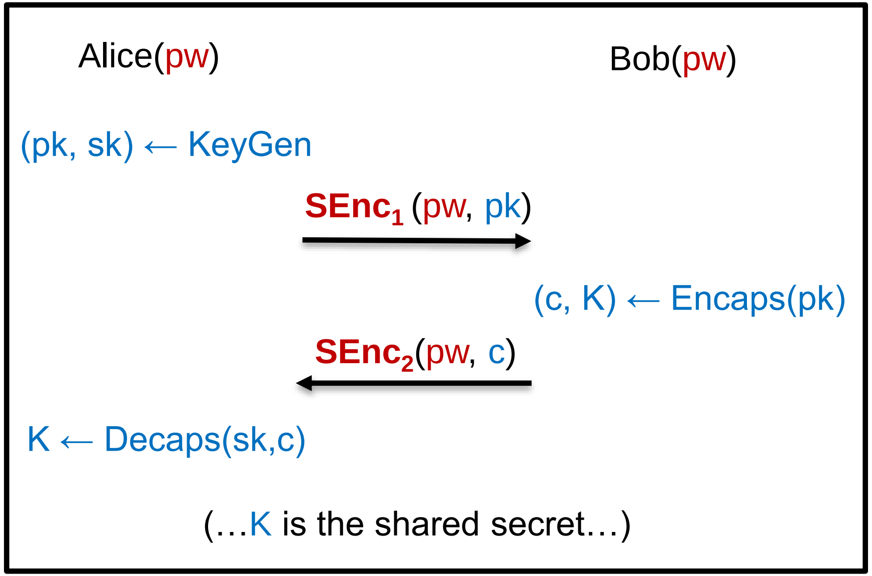
K ← Decaps(sk,c)

(…K is the shared secret…)

1. $SEnc_1$ and $SEnc_2$ are modelled as **ideal ciphers**

2. KEM is required to have:
   - PK uniformity
   - **Pseudorandom ciphertext**

EKE Construction – PAKE from KEM

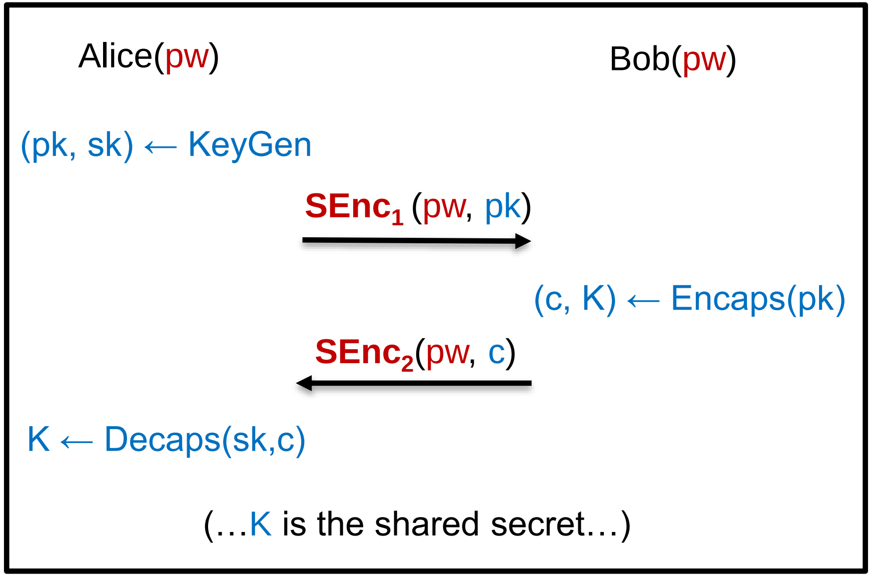


1. SEnc_1 and SEnc_2 are modelled as **ideal ciphers**

2. KEM is required to have:
   - PK uniformity
   - Pseudorandom ciphertext
   - **PCA security** (for tight reduction)

NTNU

EKE Construction – PAKE from KEM



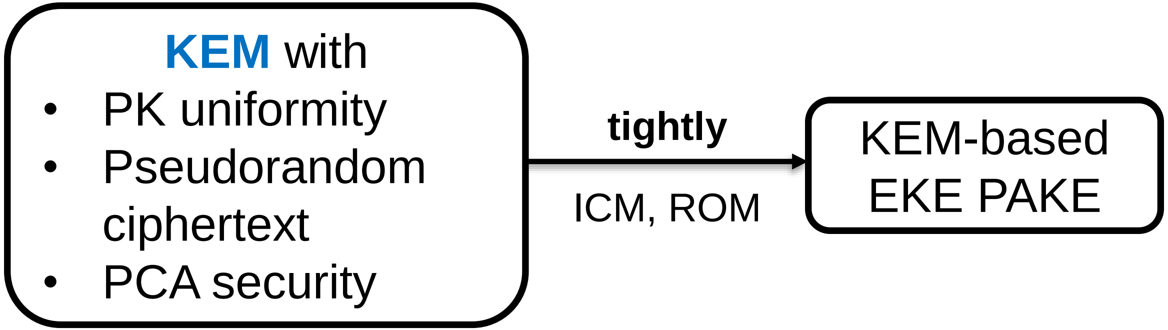
1. $SEnc_1$ and $SEnc_2$ are modelled as **ideal ciphers**

2. KEM is required to have:
   - PK uniformity
   - Pseudorandom ciphertext
   - PCA security

(Multi-user & multi-challenge settings)

NTNU

EKE Construction – PAKE from KEM



Instantiation from LWE/MLWE

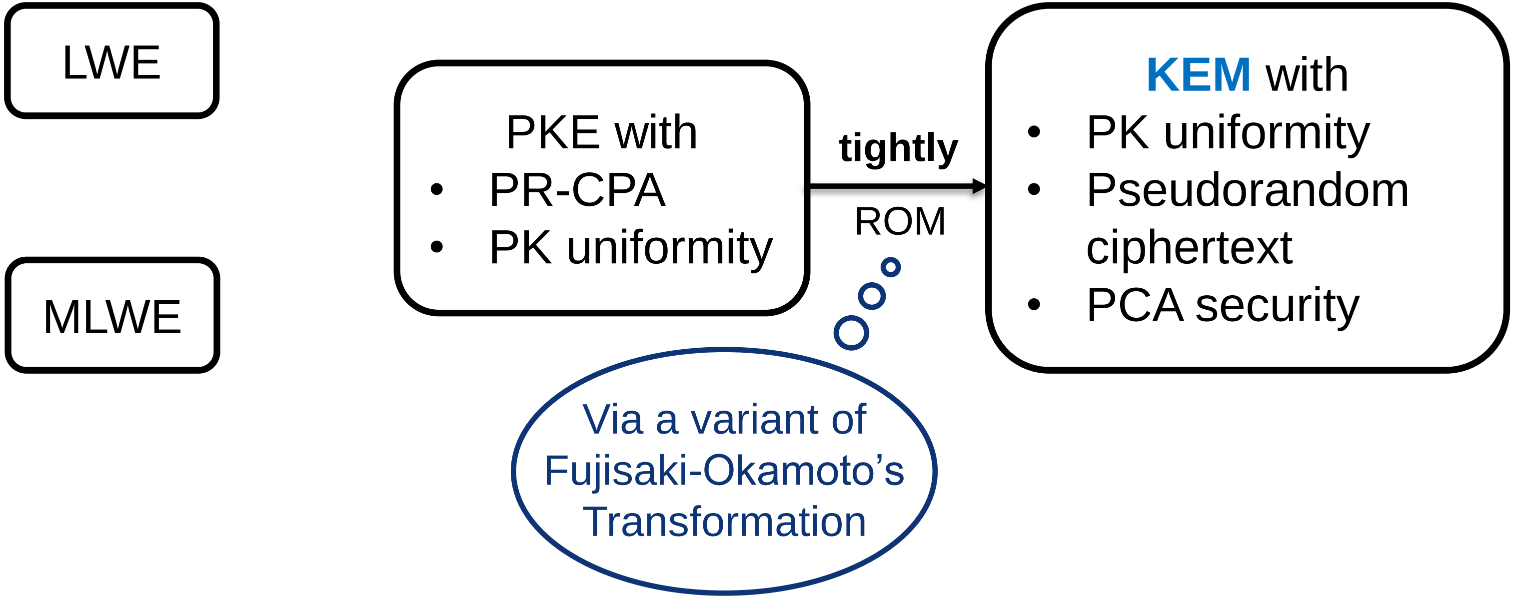
LWE

MLWE

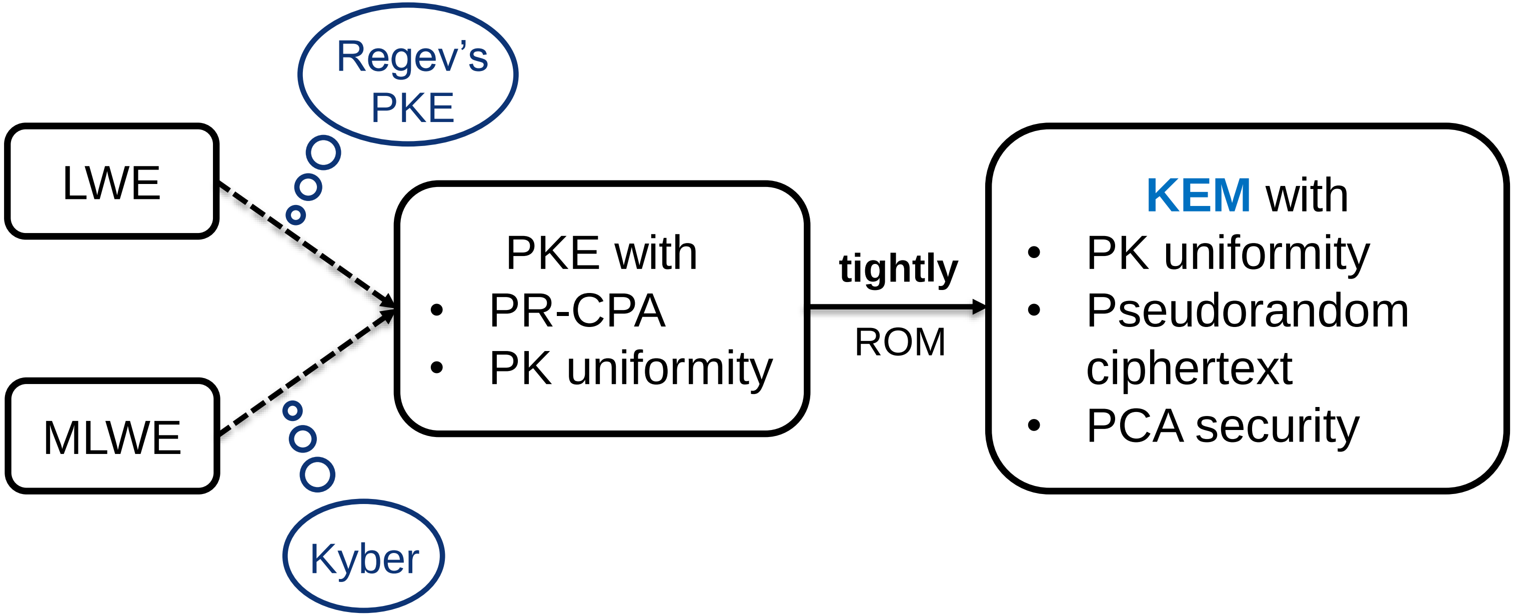
KEM with

- PK uniformity
- Pseudorandom ciphertext
- PCA security

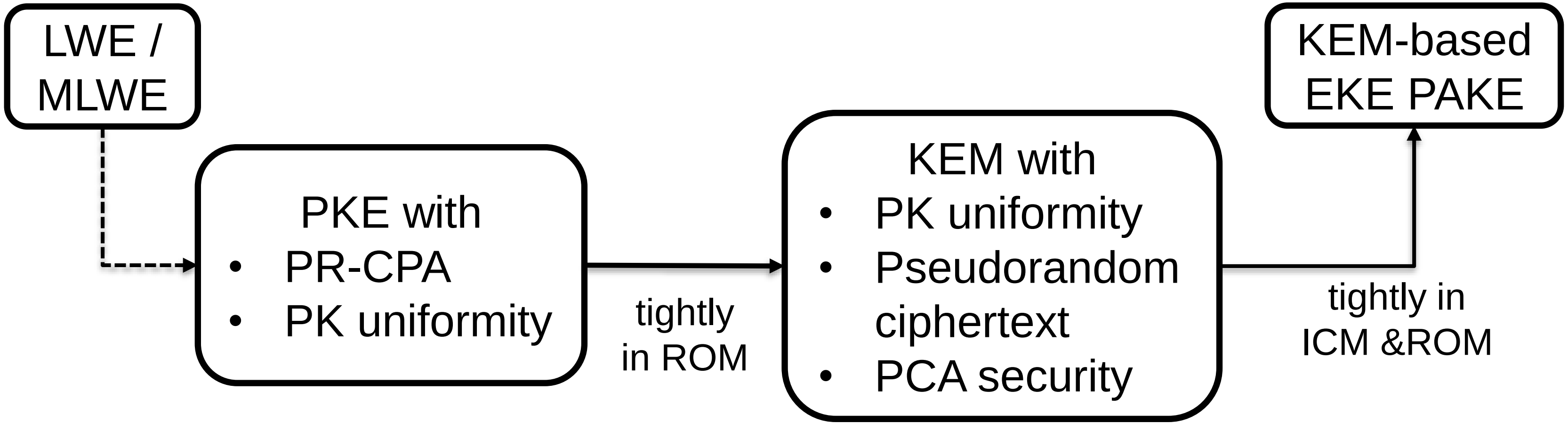
Instantiation from LWE/MLWE



Instantiation from LWE/MLWE

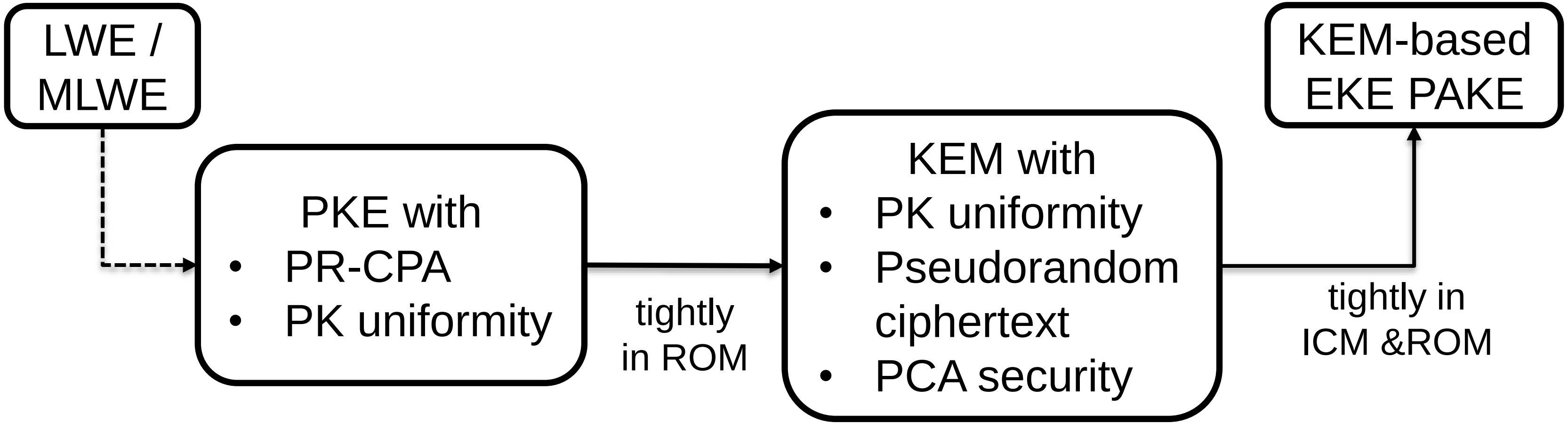


Summary and Open Problems



eprint: 2023/1334

Summary and Open Problems



Tight construction?
QICM & QROM?

eprint: 2023/1334