Tighter Security for Generic Authenticated Key Exchange in the QROM

Jiaxin Pan

Benedikt Wagner

Runzhi Zeng

UNIKASSEL VERSITÄT

CISPA HELMHOLTZ CENTER FOR INFORMATION SECURITY

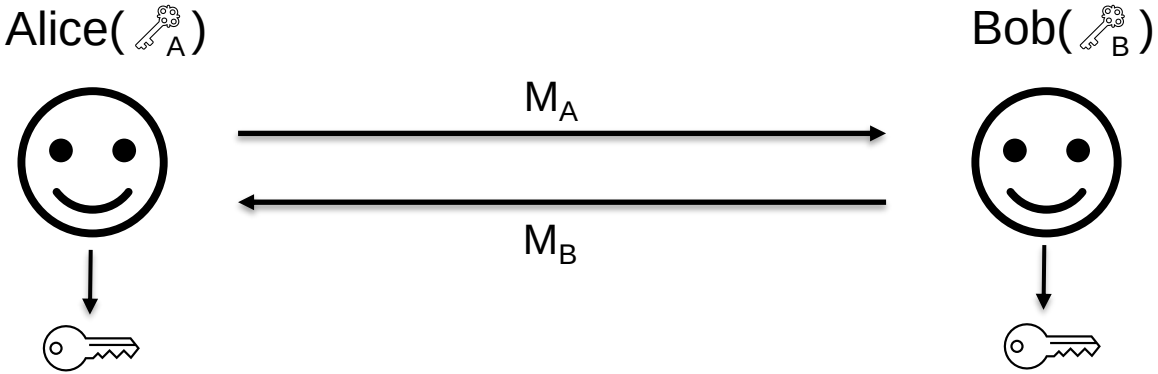
NTNU

Norwegian University of Science and Technology

eprint: 2023/1380

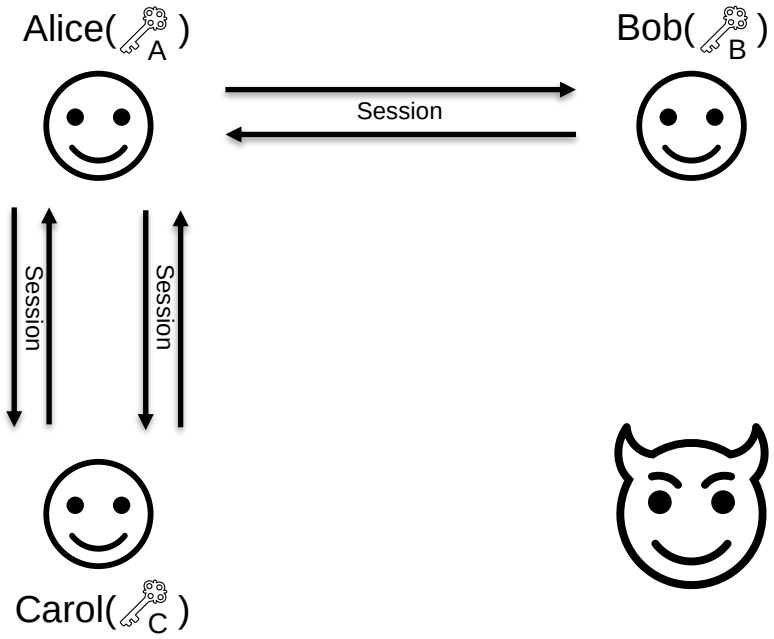
Authenticated Key Exchange

Two-message AKE



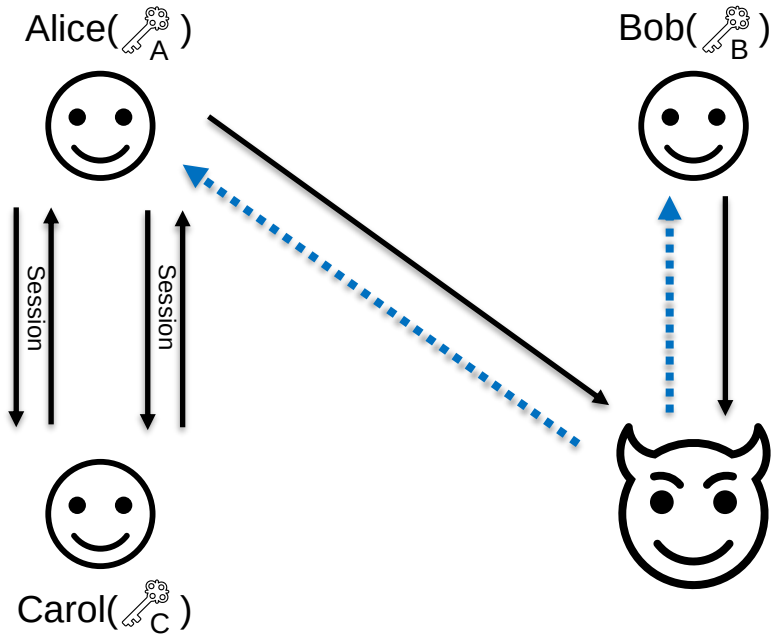
Security of AKE

- Multi-user and Multi-session Settings



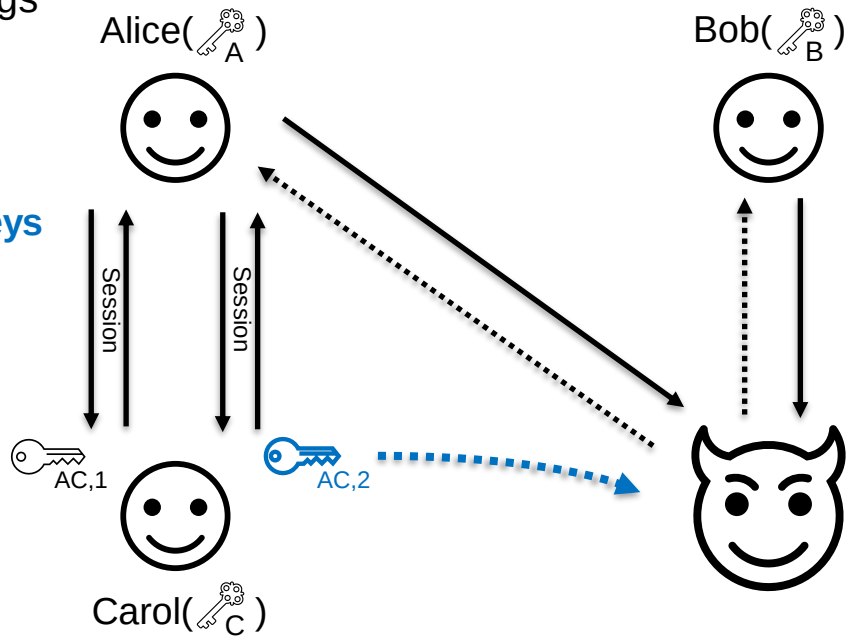
Security of AKE

- Multi-user and Multi-session Settings
- Adversary Capabilities
  - **Control the network**



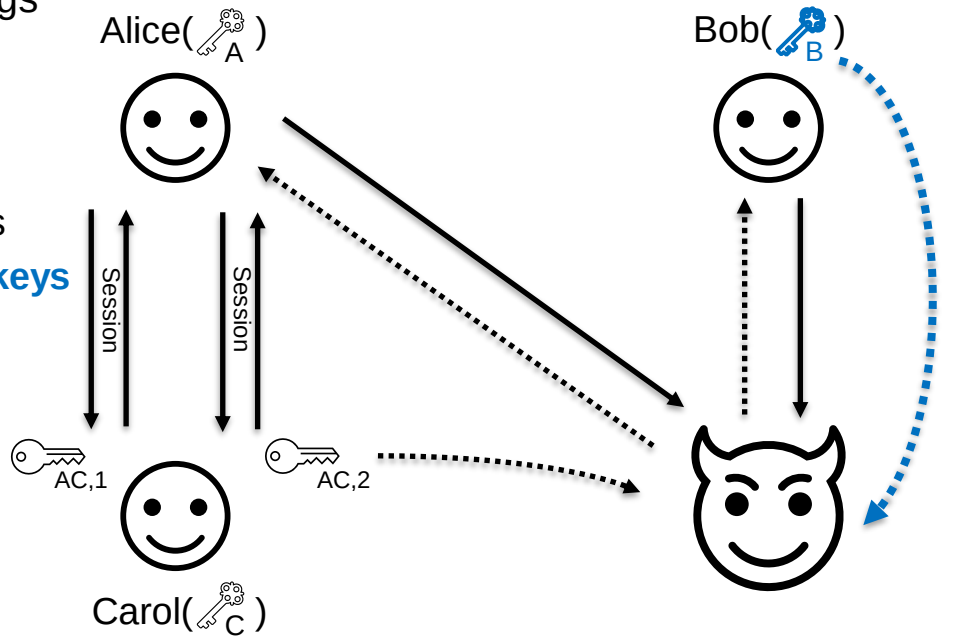
Security of AKE

- Multi-user and Multi-session Settings
- Adversary Capabilities
  - Control the network
  - **Reveal established session keys**



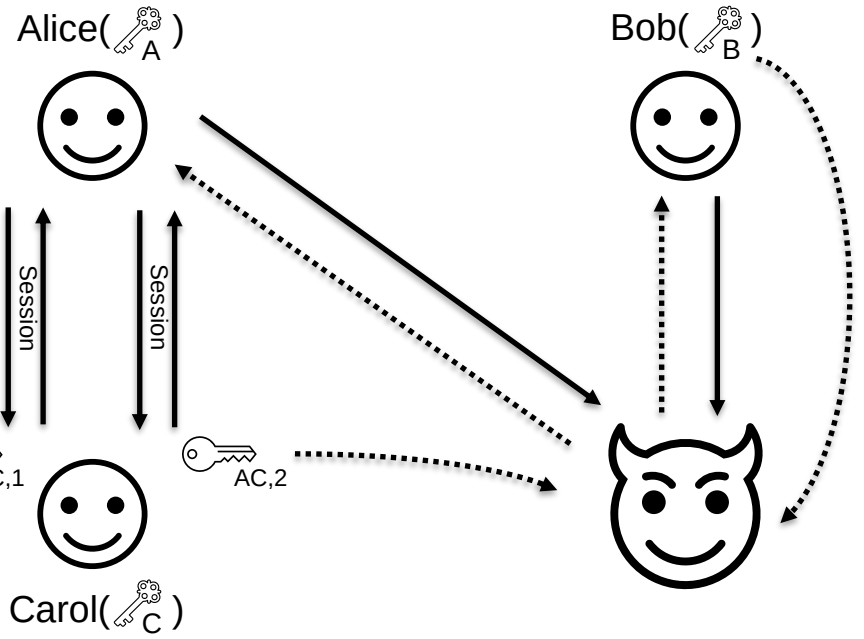
Security of AKE

- Multi-user and Multi-session Settings
- Adversary Capabilities
  - Control the network
  - Reveal established session keys
  - **Adaptively corrupt long-term keys**



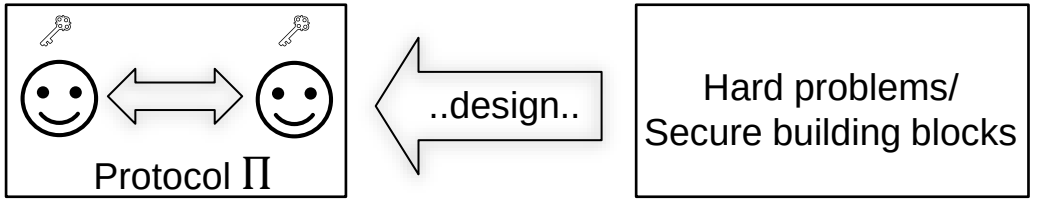
Security of AKE

- Multi-user and Multi-session Settings
- Adversary Capabilities
  - Control the network
  - Reveal established session keys
  - Adaptively corrupt long-term keys
- Security Goals
  - Key Indistinguishability
  - Authentication



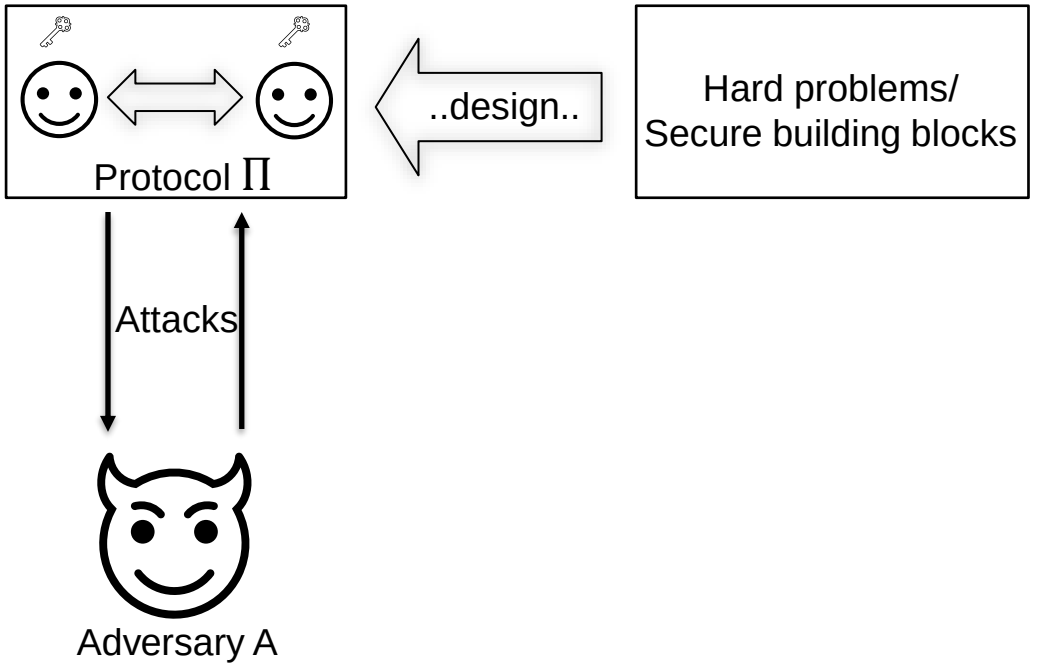
Tightness of Security Reduction

- Security Proof via Reduction



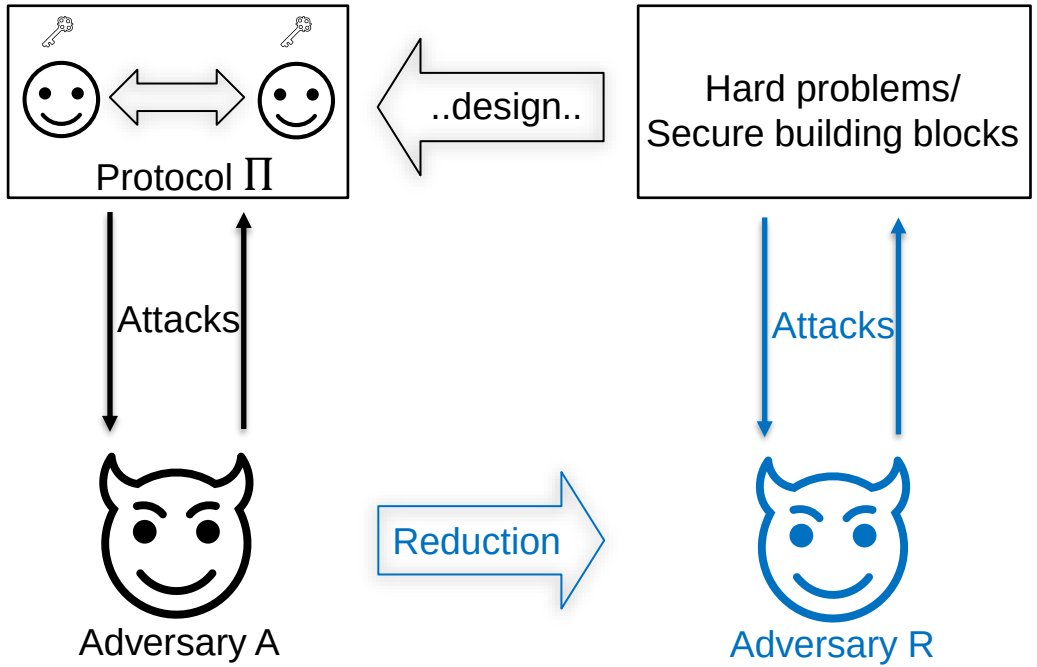
Tightness of Security Reduction

- Security Proof via Reduction
  - A breaks Π



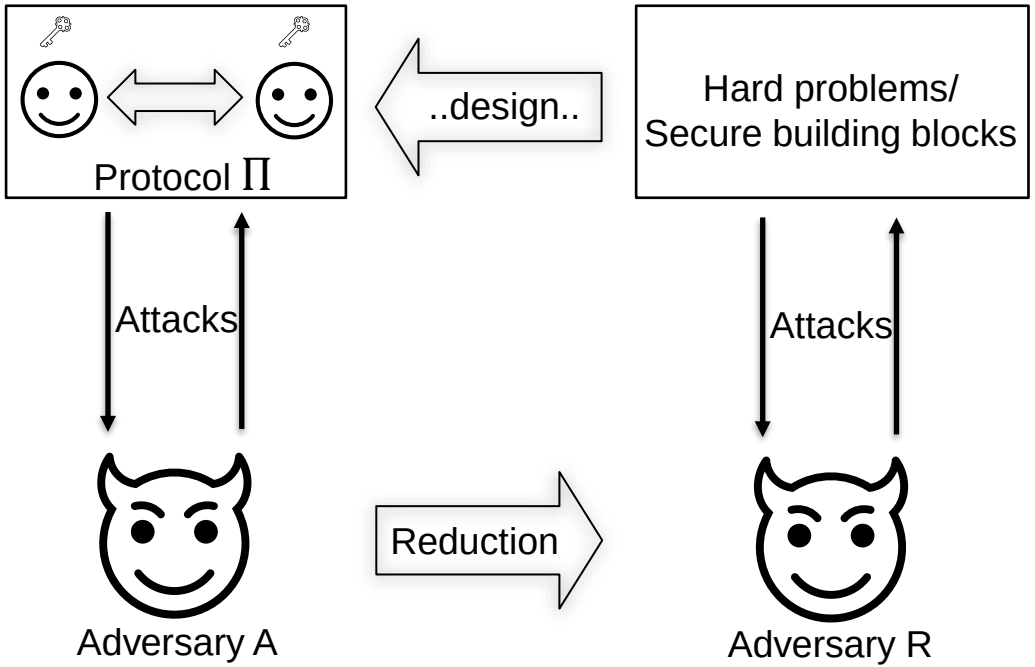
Tightness of Security Reduction

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



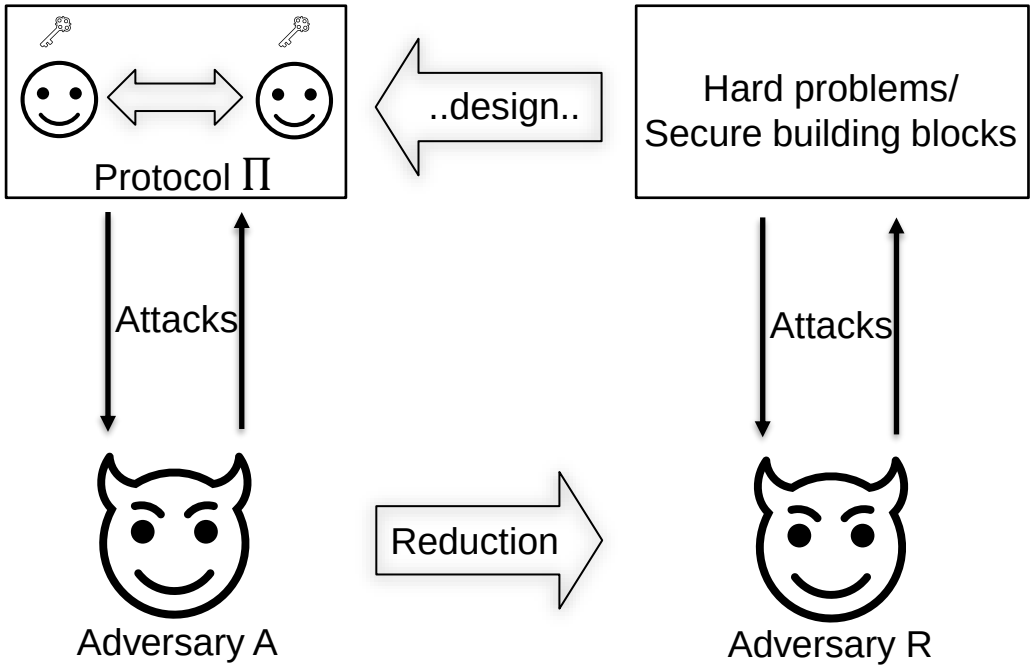
Tightness of Security Reduction

- 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



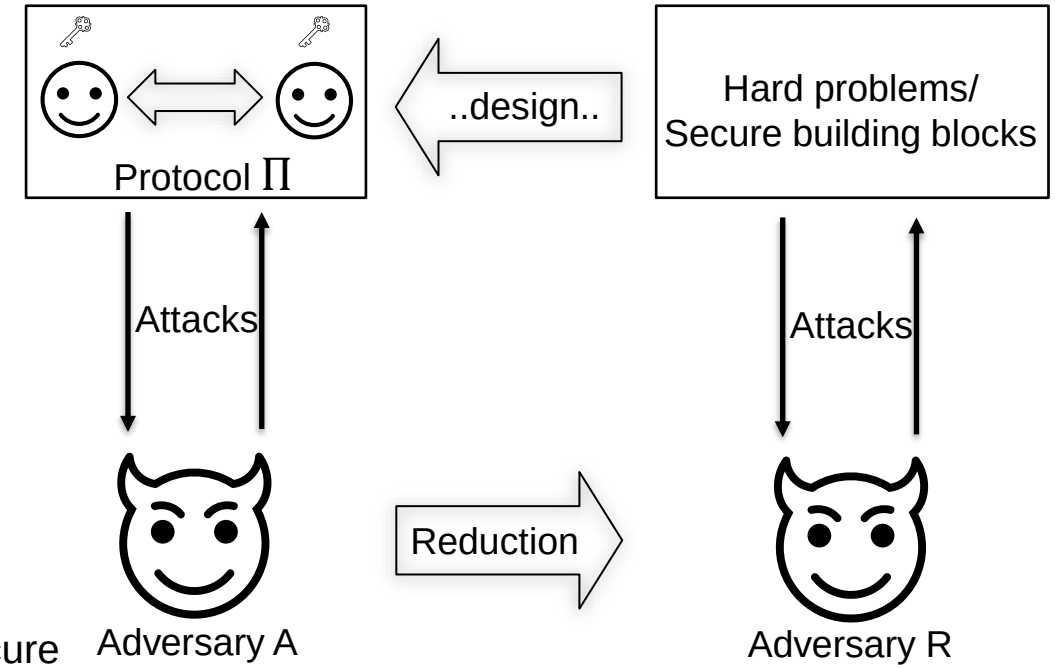
Tightness of Security Reduction

- 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

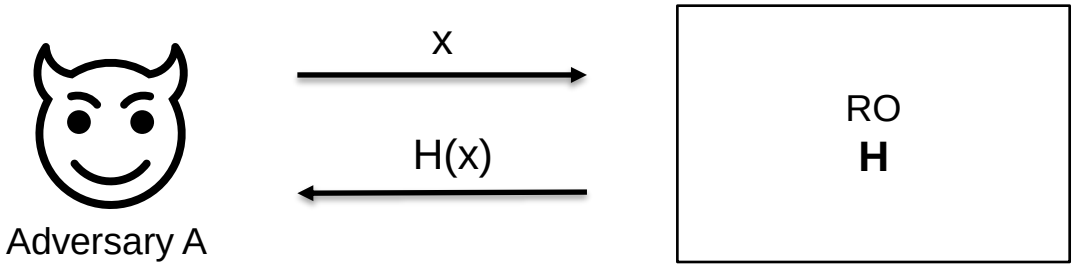


Tightness of Security Reduction

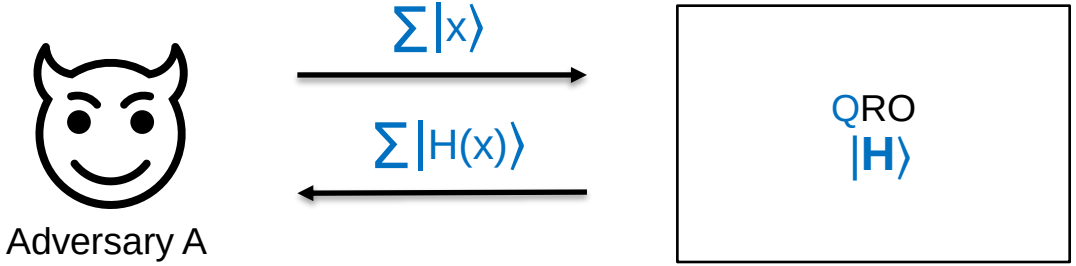
- Security Proof via Reduction
  - A breaks Π
    $\Longrightarrow$ R solves problems
- Tightness of Reduction
  - $\mathbf{Adv}(\mathrm{R}) \leq L \cdot \mathbf{Adv}(\mathrm{A})$
  - L: Security loss
  - L smaller $\Longrightarrow$ tighter
- Relevance: Parameter selection
  - L is large $\Longrightarrow$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



Quantum Random Oracle Model



Quantum Random Oracle Model



AKE in the (Q)ROM

Scheme	Construction	Assumption	Security Loss	Model
JKRS21	KEM	DDH	$\Theta(1)$	ROM
PWZ23	KEM	LWE	$\Theta(\lambda)$	ROM
HKSU20	PKE/KEM	LWE	$\Theta(N \cdot \boldsymbol{S} \cdot \sqrt{\boldsymbol{\epsilon^{-1}}})$	QROM
XAYLJ20	2KEM	Isogeny	$\Theta(N \cdot \boldsymbol{S} \cdot \sqrt{\boldsymbol{\epsilon^{-1}}})$	QROM

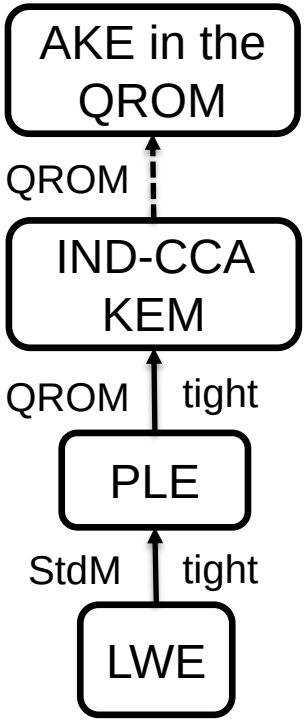
λ: Security parameter
N: Number of user;
$\boldsymbol{S}$**: Number of session**;
$\sqrt{\boldsymbol{\epsilon^{-1}}}$**: Square-root security loss**;

AKE in the (Q)ROM

Scheme	Construction	Assumption	Security Loss	Model
JKRS21	KEM	DDH	$\Theta(1)$	ROM
PWZ23	KEM	LWE	$\Theta(\lambda)$	ROM
HKSU20	PKE/KEM	LWE	$\Theta(N \cdot \boldsymbol{S} \cdot \sqrt{\epsilon^{-1}})$	QROM
XAYLJ20	2KEM	Isogeny	$\Theta(N \cdot \boldsymbol{S} \cdot \sqrt{\epsilon^{-1}})$	QROM
Our Goal	KEM	Post-Quantum	Tight, or tighter?	QROM

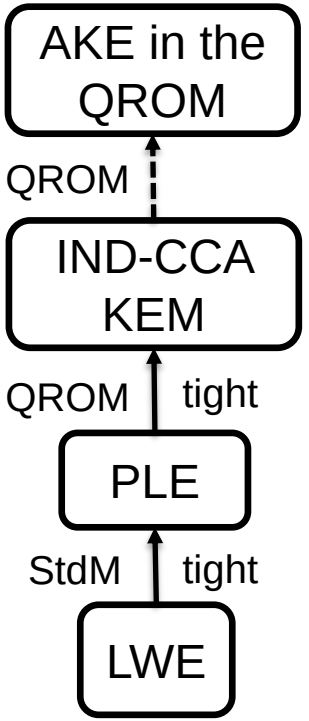
λ: Security parameter
N: Number of user;
$\boldsymbol{S}$**: Number of session**;
$\sqrt{\epsilon^{-1}}$**: Square-root security loss**;

Our Contributions



Our Contributions

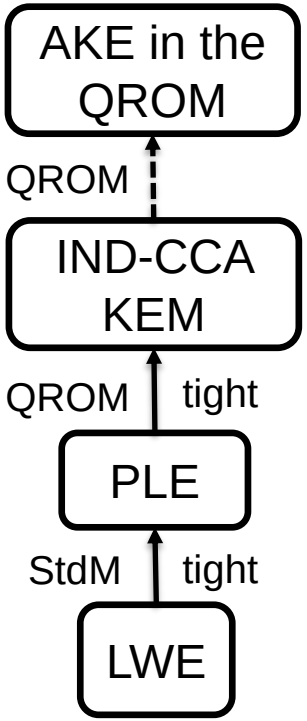
- LWE-based AKE with **Tighter** Security in the QROM
  - **Session-tight** and **without square-root loss**
  - Via multi-user-challenge(MUC)-IND-CCA secure KEM



Our Contributions

- LWE-based AKE with **Tighter** Security in the QROM
  - **Session-tight** and **without square-root loss**
  - Via multi-user-challenge(MUC)-IND-CCA secure KEM

- Parameter-lossy Encryption (PLE)
  - Used to construct **tightly MUC-IND-CCA secure KEM**
  - (Almost-)Tight construction from LWE

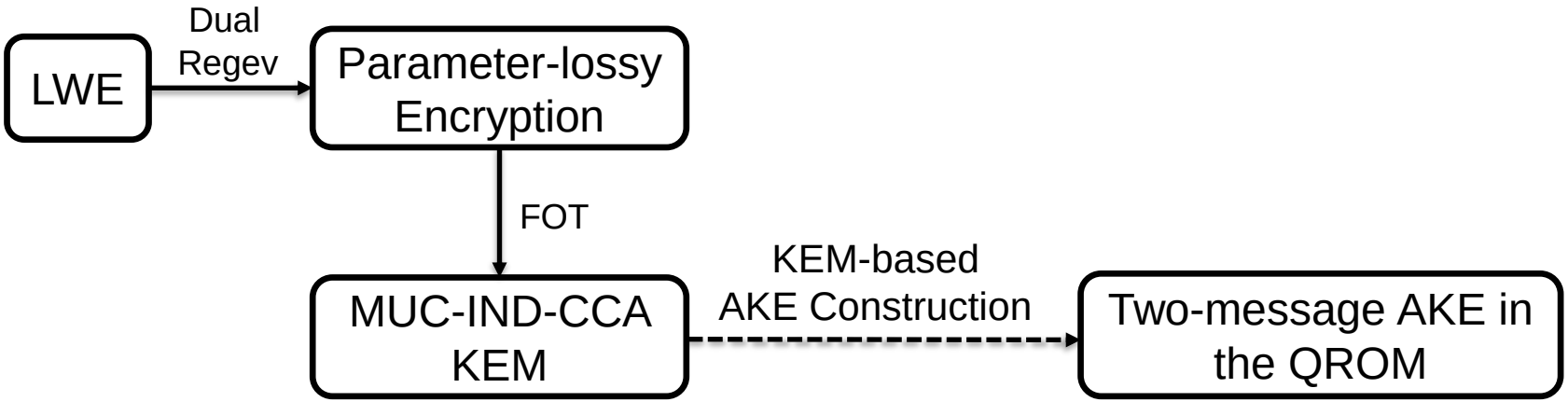


Our Contributions

Schemes	Construction	Assumptions	Security Loss	Model
JKRS21	KEM	DDH	$\Theta(1)$	ROM
PWZ23	KEM	LWE	$\Theta(\lambda)$	ROM
HKSU20	PKE/KEM	LWE	$\Theta(N \cdot \boldsymbol{S} \cdot \sqrt{\boldsymbol{\epsilon}^{-1}})$	QROM
XAYLJ20	2KEM	Isogeny	$\Theta(N \cdot \boldsymbol{S} \cdot \sqrt{\boldsymbol{\epsilon}^{-1}})$	QROM
Our work	KEM	LWE	$\Theta(N \cdot \lambda)$	QROM

Session-tight and **without square-root loss**

Technical Outline

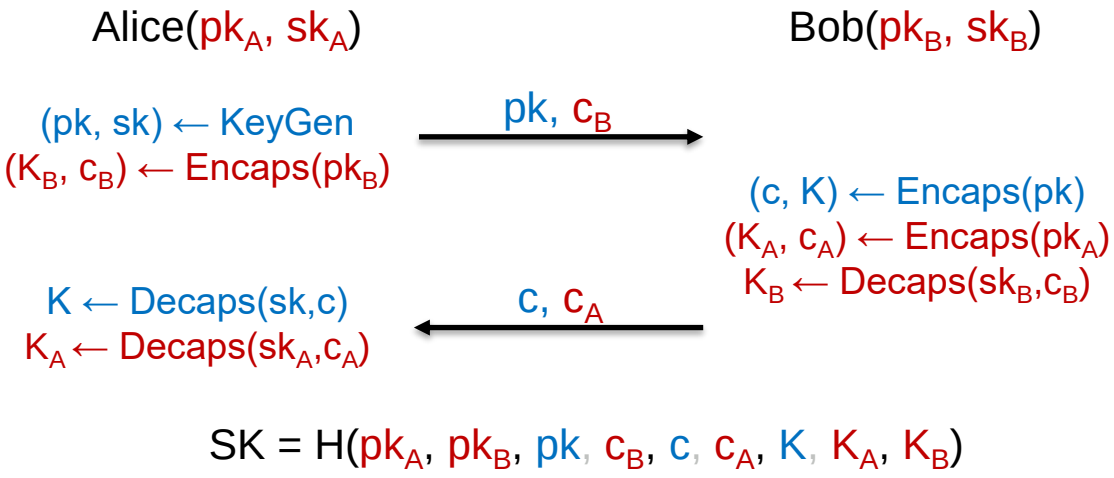


: (almost-)tightly

: non-tightly

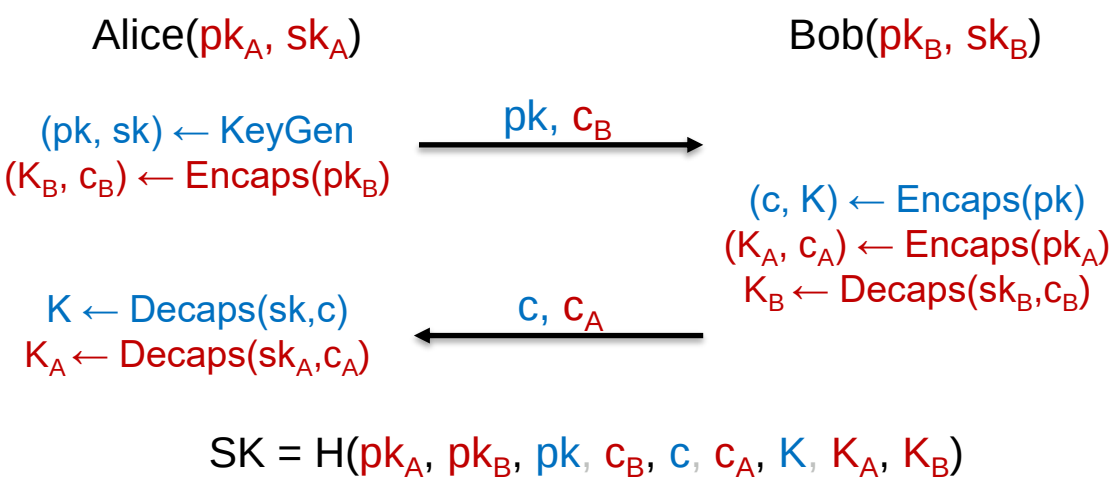
AKE from KEM

- Construction [JKRS21, PWZ23]: Static KEM + Ephemeral KEM



AKE from KEM

- Construction [JKRS21, PWZ23]: Static KEM + Ephemeral KEM



- Ephemeral KEM should have MUC-IND-CCA security
- Static KEM should have MUC-IND-CCA security with strong corruptions [JKRS21, PWZ23]

AKE from KEM

- Construction [JKRS21, PWZ23]: Static KEM + Ephemeral KEM (in the QROM)

- To have tight security in the QROM:
  - Ephemeral KEM should have MUC-IND-CCA security in the QROM
  - Static KEM should have MUC-IND-CCA security with strong corruptions in the QROM

AKE from KEM

- Construction [JKRS21, PWZ23]: Static KEM + Ephemeral KEM (in the QROM)

- To have tight security in the QROM:
  - Ephemeral KEM should have MUC-IND-CCA security in the QROM
  - Static KEM should have MUC-IND-CCA security with strong corruptions in the QROM

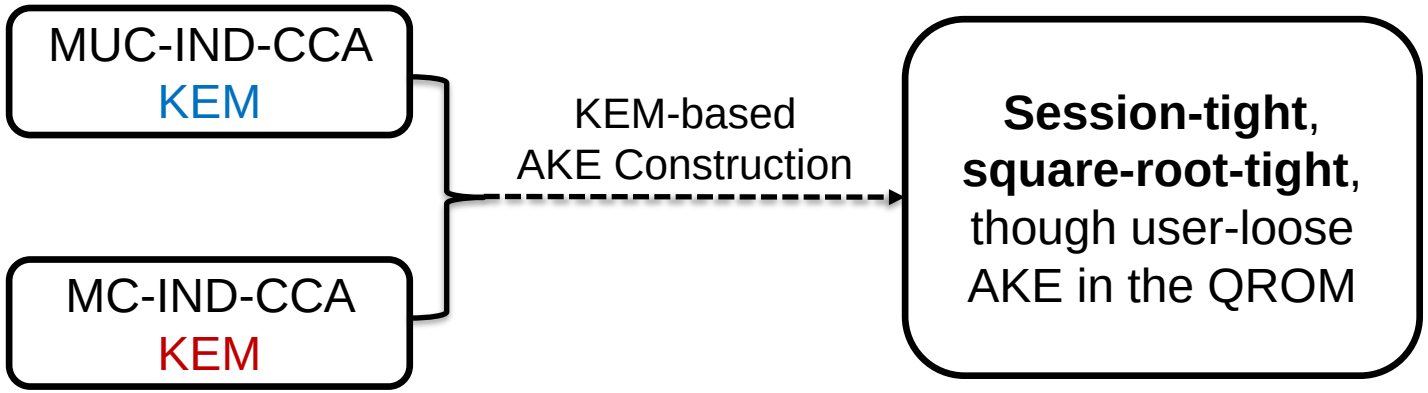
- Both are unknown how to construct from LWE...
  - Cannot use the re-randomization technique
  - Unknown how to construct such Static KEM from LWE in the QROM

AKE from KEM

- Construction [JKRS21, PWZ23]: Static KEM + Ephemeral KEM (in the QROM)
- To have tight security in the QROM:
  - Ephemeral KEM should have MUC-IND-CCA security in the QROM
  - Static KEM should have MUC-IND-CCA security with strong corruptions in the QROM
- Both are unknown how to construct from LWE...
  - Cannot use the re-randomization technique
  - Unknown how to construct such Static KEM from LWE in the QROM
- If we have ***MC-IND-CCA*** Static KEM + ***MUC-IND-CCA*** Ephemeral KEM...

AKE from KEM, tighter

- *MC-IND-CCA* Static KEM + *MUC-IND-CCA* Ephemeral KEM



MUC-IND-CCA KEM & Parameter-lossy Encryption

MUC-IND-CCA KEM

MC-IND-CCA KEM

- Unknown how to construct from LWE (not “re-randomizable”)

MUC-IND-CCA KEM & Parameter-lossy Encryption

MUC-IND-CCA KEM

MC-IND-CCA KEM

- Unknown how to construct from LWE (not “re-randomizable”)

Parameter-lossy Encryption

- Parameter-lossy Encryption
  - A multi-user version of lossy encryption [BHY09]
  - Lossy public keys & **lossy parameter**

MUC-IND-CCA KEM & Parameter-lossy Encryption

- Lossy Encryption

1. Key indistinguishability:

   real $pk \approx_c$ lossy lpk

2. Lossiness: (Informally) Ciphertexts have statistical indistinguishability under lossy key lpk...

3. $\Longrightarrow$ MC-IND-CPA PKE

MUC-IND-CCA KEM & Parameter-lossy Encryption

- Lossy Encryption

1. Key indistinguishability:

   real $pk \approx_c$ lossy lpk

2. Lossiness: (Informally) Ciphertexts have statistical indistinguishability under lossy key lpk...

3. $\Longrightarrow$ MC-IND-CPA PKE

- Parameter-lossy Encryption

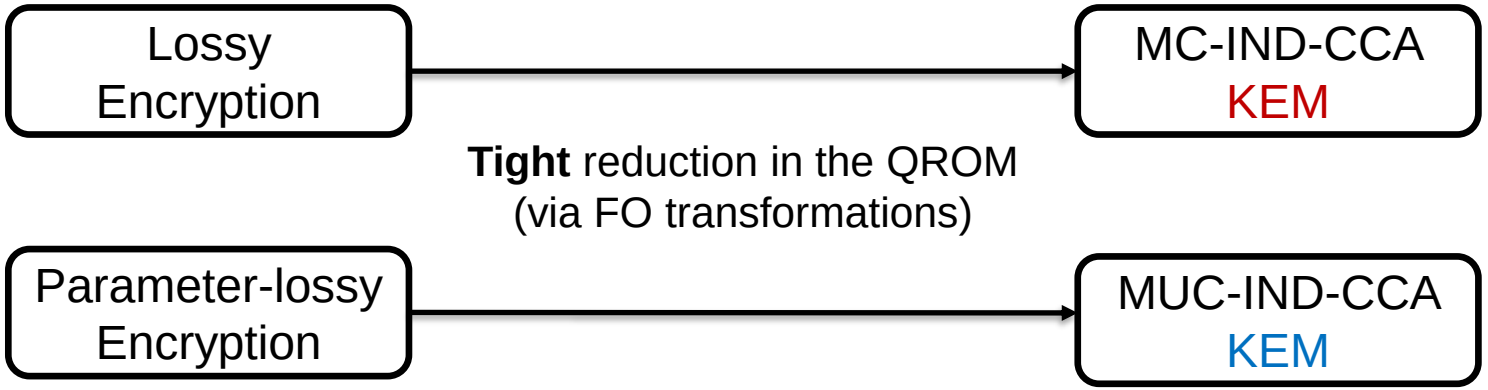
1. Parameter-key indistinguishability:

   real $(\boldsymbol{par}, pk_1, \ldots, pk_\mu) \approx_c$ lossy $(\boldsymbol{lpar}, lpk_1, \ldots, lpk_\mu)$

2. Lossiness: Statistical indistinguishability under lossy parameter $\boldsymbol{lpar}$ and lossy key lpk...

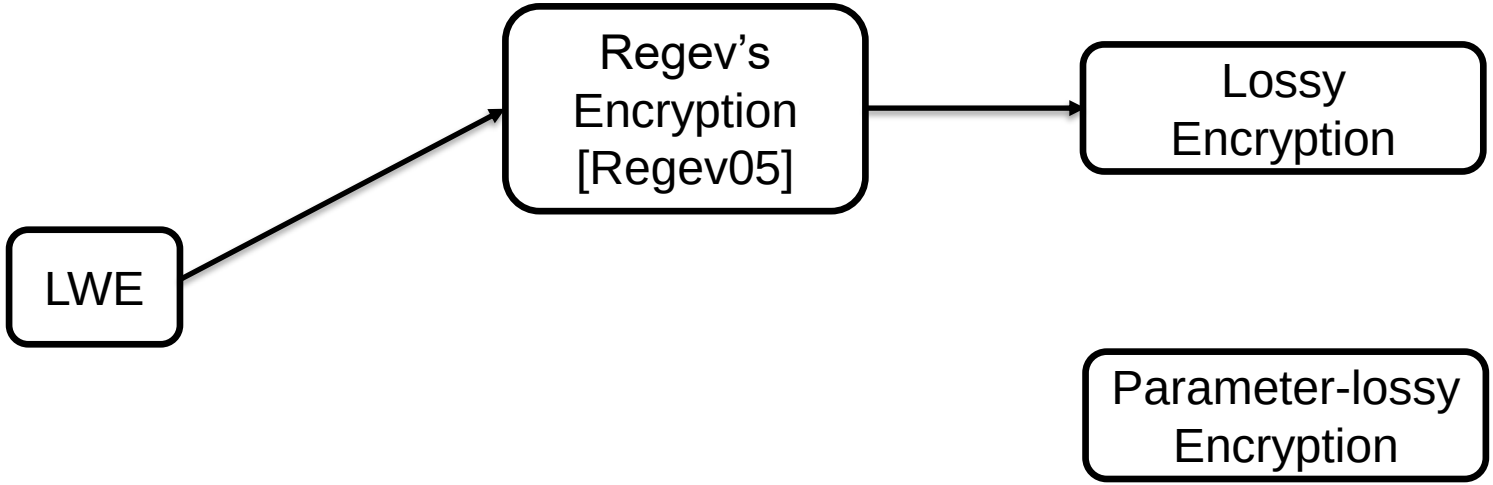
3. $\Longrightarrow$ M**U**C-IND-CPA PKE

MUC-IND-CCA KEM & Parameter-lossy Encryption

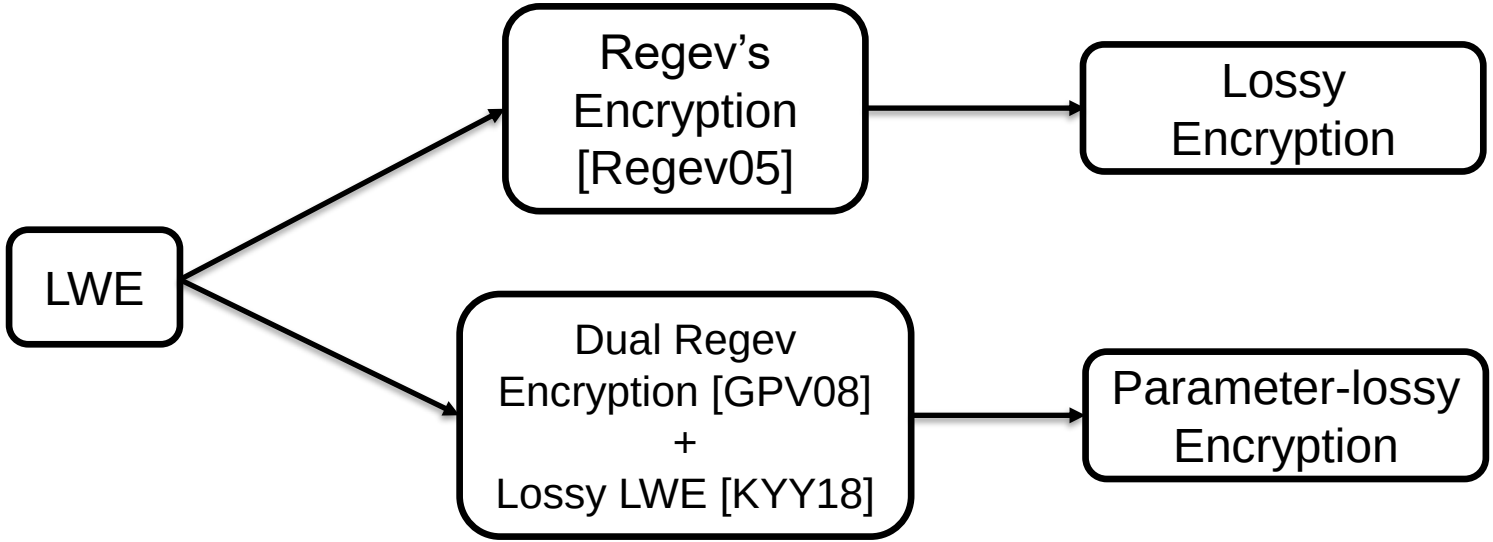


Parameter-lossy Encryption from LWE

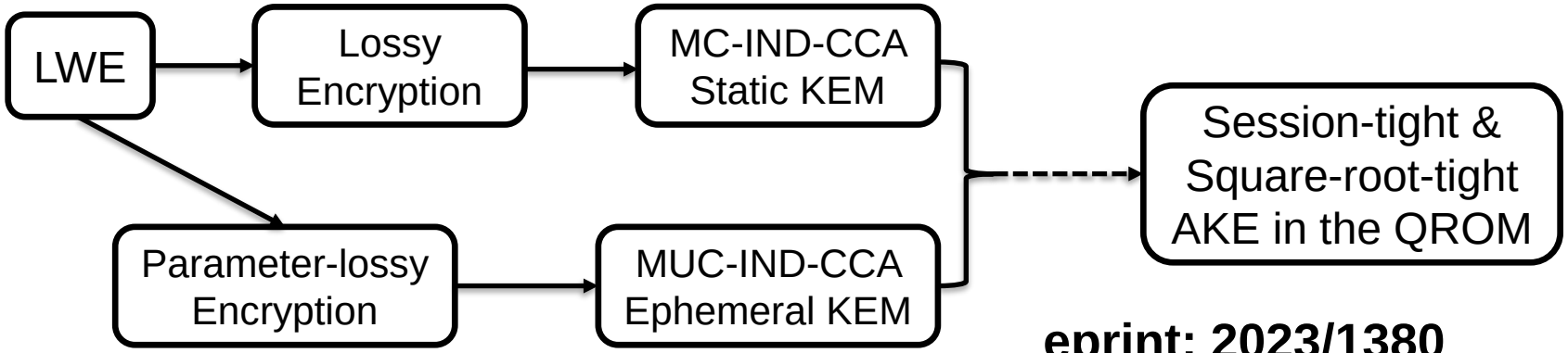
Parameter-lossy Encryption from LWE



Parameter-lossy Encryption from LWE

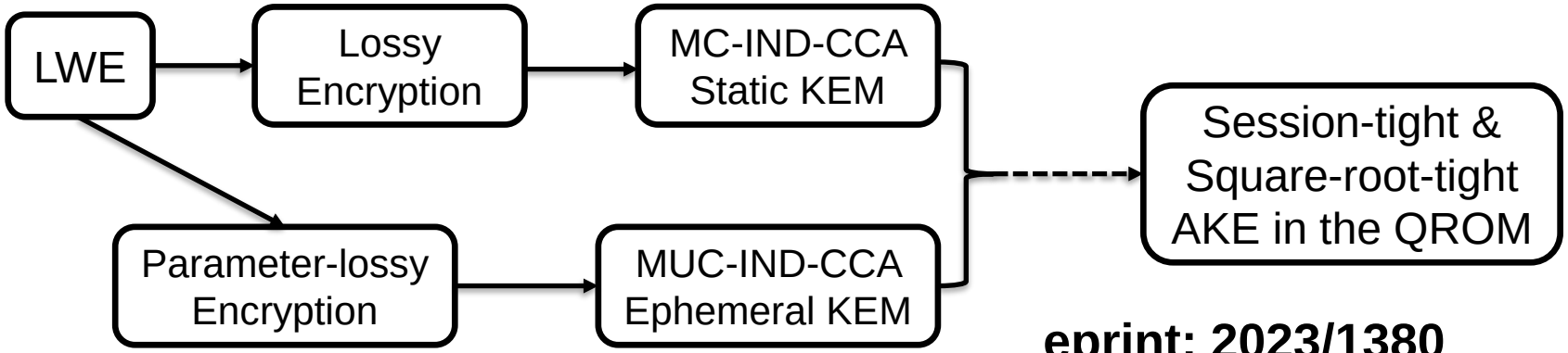


Summary and Open Problems



eprint: 2023/1380

Summary and Open Problems



eprint: 2023/1380

Also user-tight in the QROM?

References

KYY18 Shuichi Katsumata, Shota Yamada, Takashi Yamakawa: *Tighter security proofs for GPV-IBE in the quantum random oracle model.* ASIACRYPT 2018

XAYLJ20 Haiyang Xue, Man Ho Au, Rupeng Yang, Bei Liang, Haodong Jiang: *Compact authenticated key exchange in the quantum random oracle model.* eprint 2018/1282

HKSU20 Kathrin Hövelmanns, Eike Kiltz, Sven Schäge, Dominique Unruh: *Generic authenticated key exchange in the quantum random oracle model.* PKC 2020

JKRS21 Tibor Jager, Eike Kiltz, Doreen Riepel, Sven Schäge: *Tightly-secure authenticated key exchange, revisited*. EUROCRYPT 2021

PWZ23 Jiaxin Pan, Benedikt Wagner, Runzhi Zeng: *Lattice-based authenticated key exchange with tight security*. CRYPTO 2023