Lattice-based Authenticated Key Exchange with Tight Security

Jiaxin Pan[1], Benedikt Wagner[2], Runzhi Zeng[1]

[1] Norwegian University of Science and Technology
[2] CISPA Helmholtz Center for Information Security

Norwegian University of Science and Technology

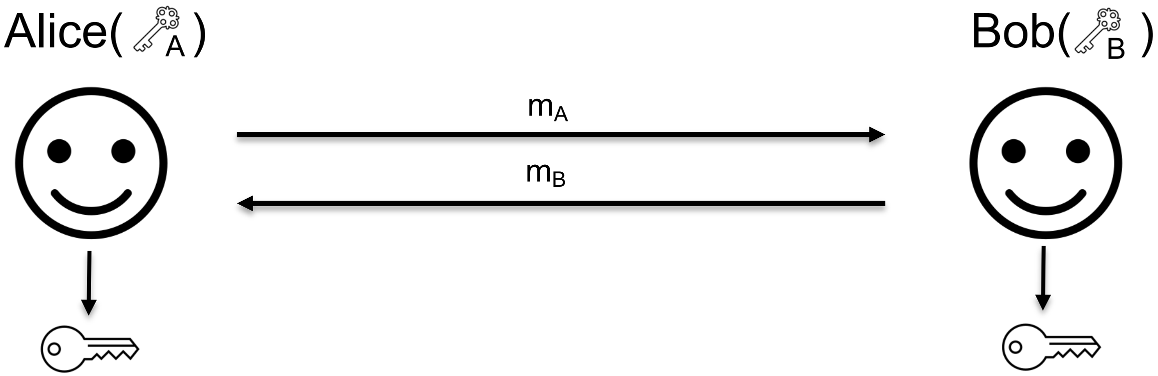
NTNU

AKE

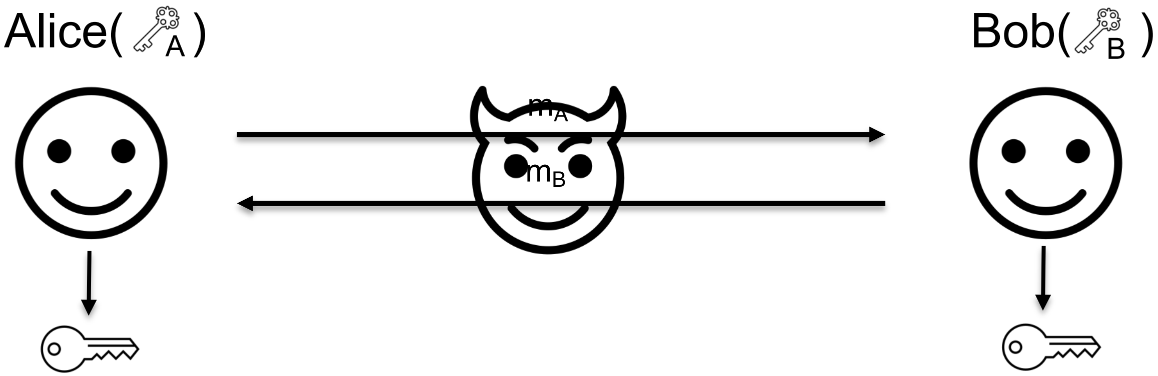
AKE

NTNU

Two-message AKE



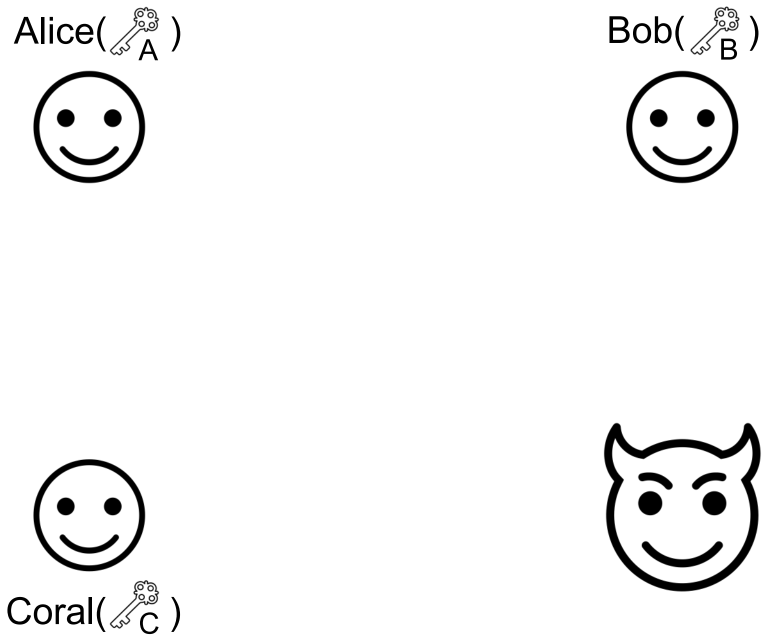
Security of AKE



NTNU

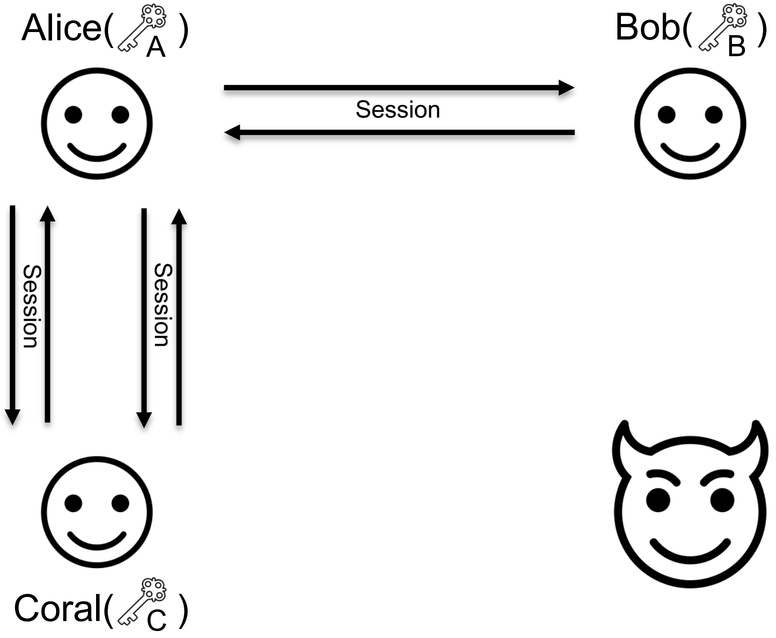
Security of AKE

- Multi-user and Multi-session Settings



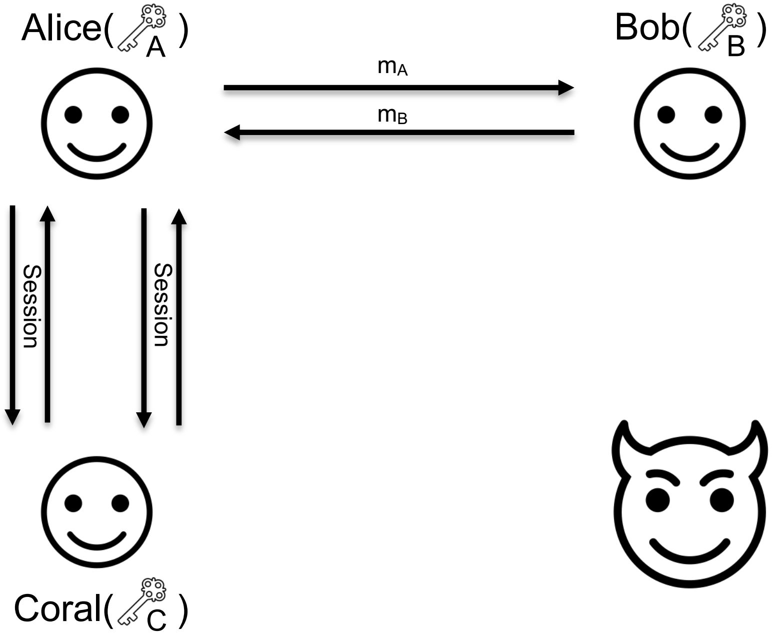
Security of AKE

- Multi-user and Multi-session Settings



Security of AKE

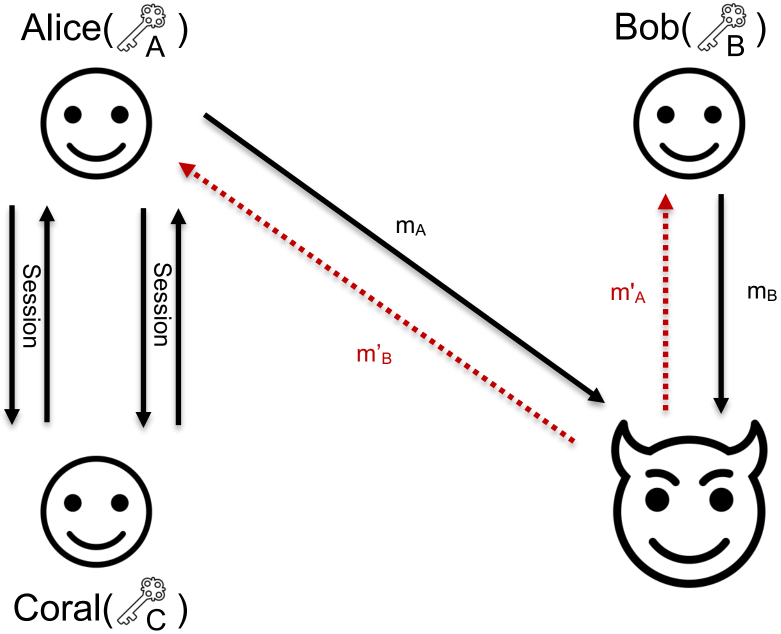
- Multi-user and Multi-session Settings
- Adversary Capabilities
  – Control the network



NTNU

Security of AKE

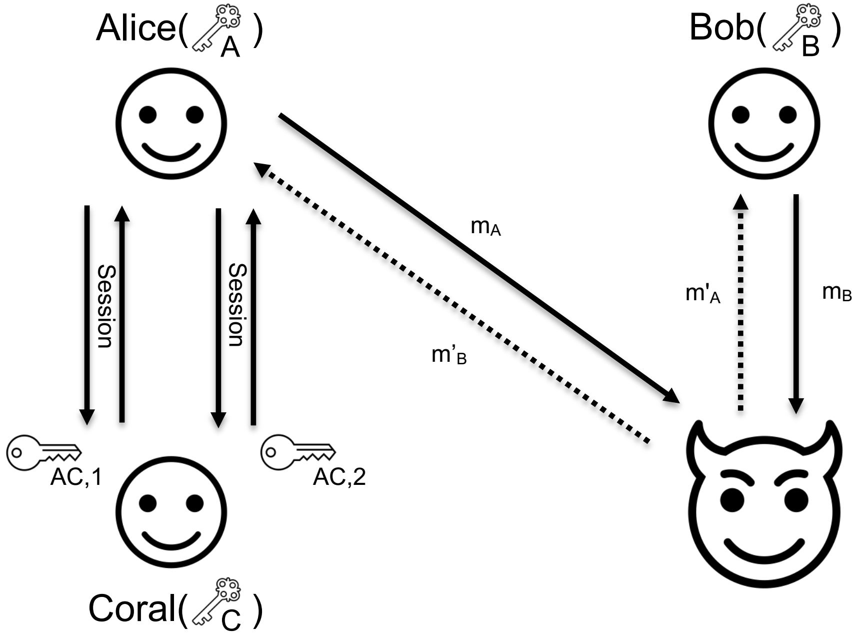
- Multi-user and Multi-session Settings
- Adversary Capabilities
  - Control the network



NTNU

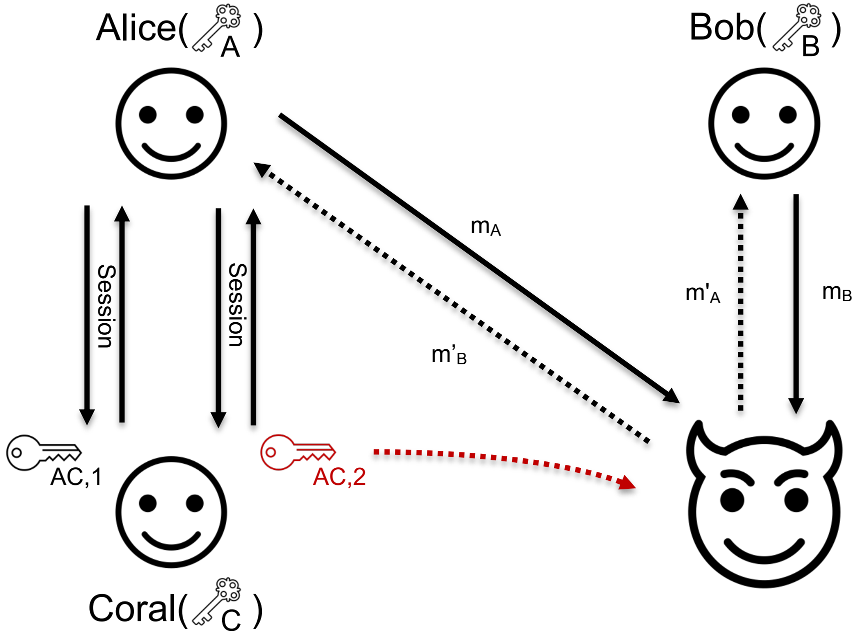
Security of AKE

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



Security of AKE

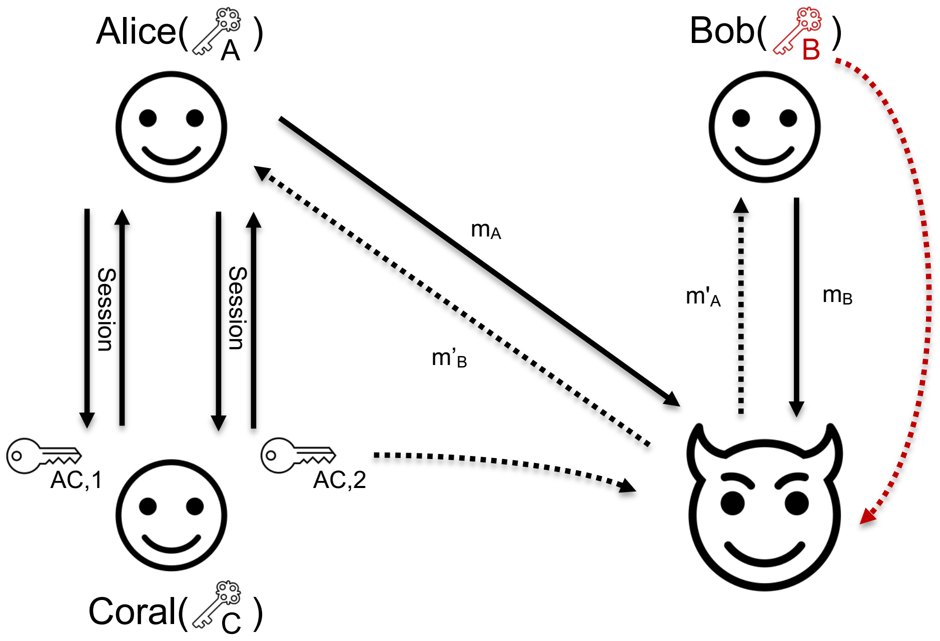
- Multi-user and Multi-session Settings
- Adversary Capabilities
  - Control the network
  - Reveal established session keys



NTNU

Security of AKE

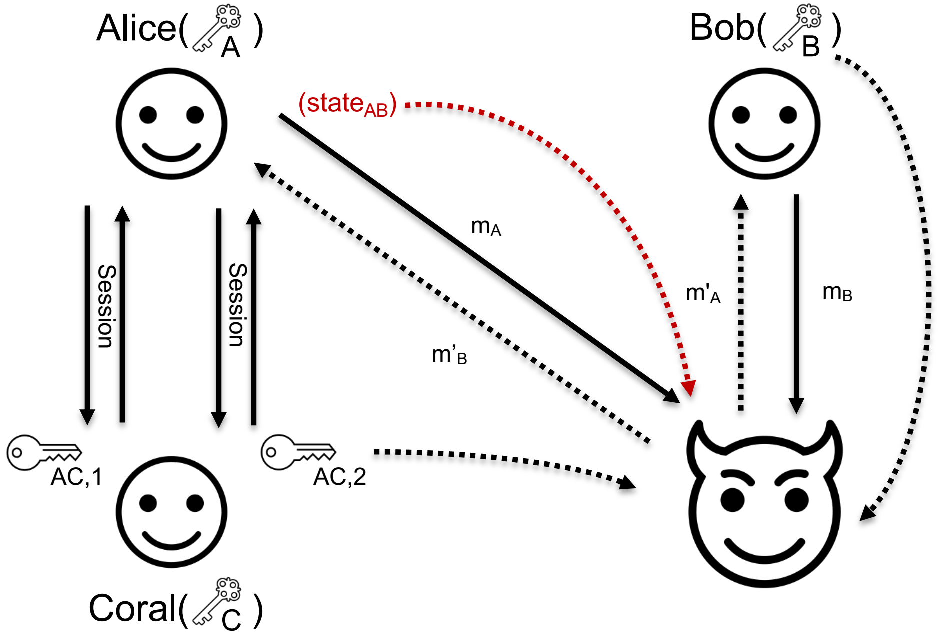
- Multi-user and Multi-session Settings
- Adversary Capabilities
  - Control the network
  - Reveal established session keys
  - Adaptively corrupt long-term keys



NTNU

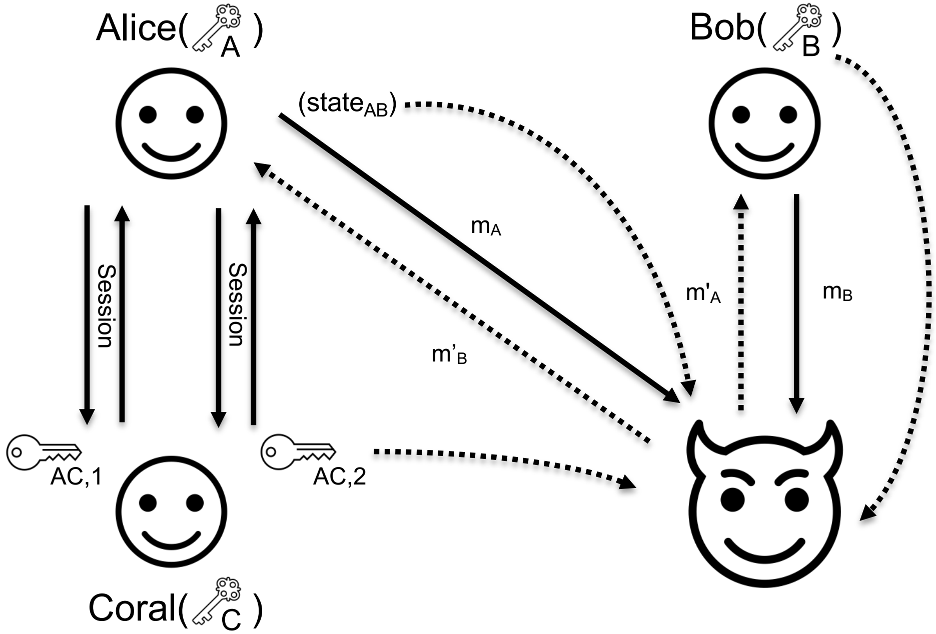
Security of AKE

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



Security of AKE

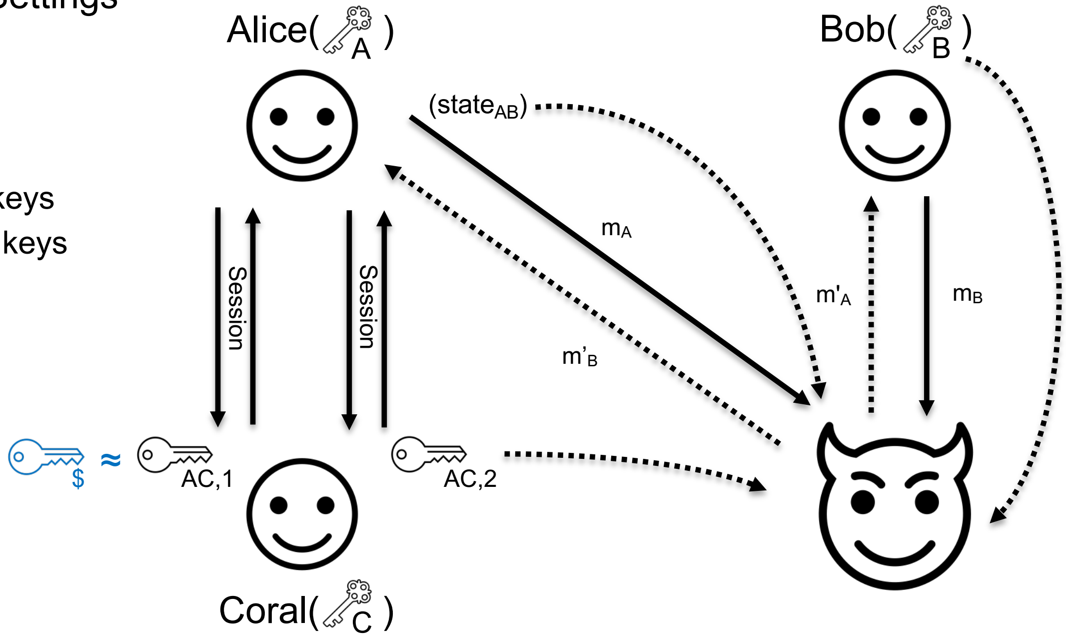
- Multi-user and Multi-session Settings
- Adversary Capabilities
  - Control the network
  - Reveal established session keys
  - Adaptively corrupt long-term keys
  - Reveal secret state
- Security Goals



NTNU

Security of AKE

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



NTNU

Tight Security

- Security Proof via Reduction

NTNU

Tight Security

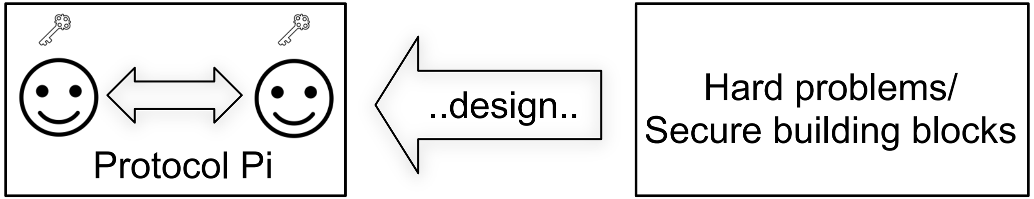
- Security Proof via Reduction

Hard problems/
Secure building blocks

NTNU

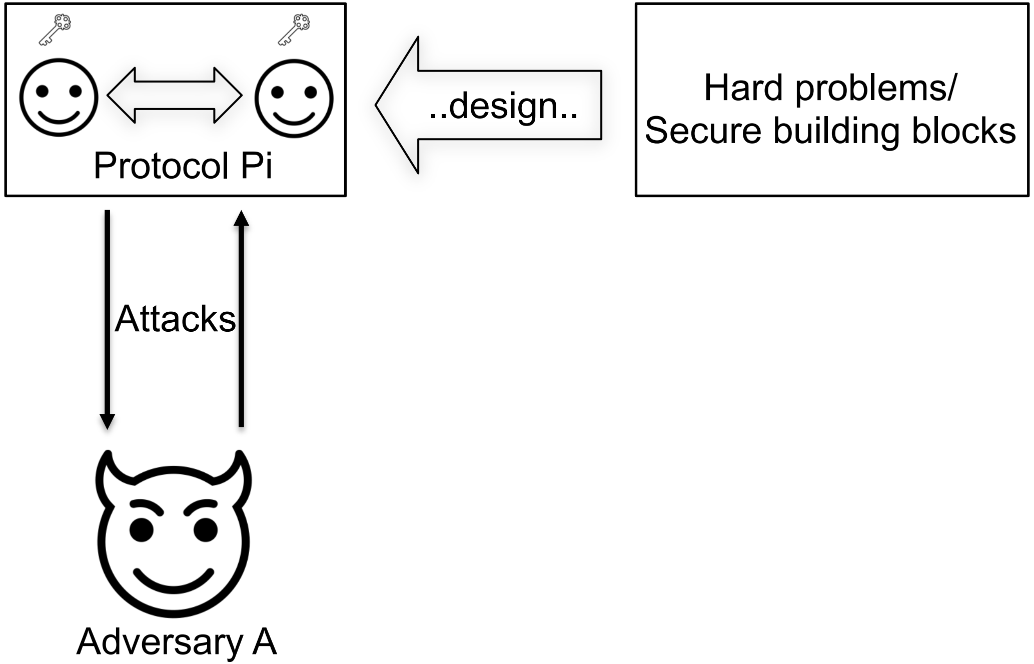
Tight Security

- Security Proof via Reduction



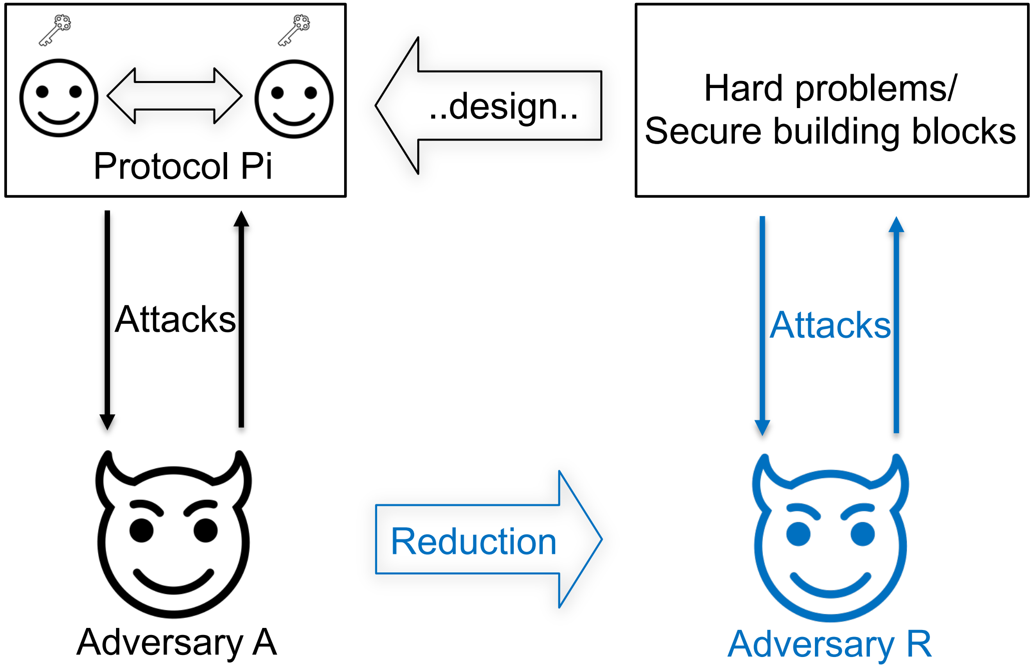
Tight Security

- Security Proof via Reduction
  - A breaks Pi



Tight Security

- Security Proof via Reduction
  - A breaks Pi
  - => R solves problems
    (or breaks building blocks)

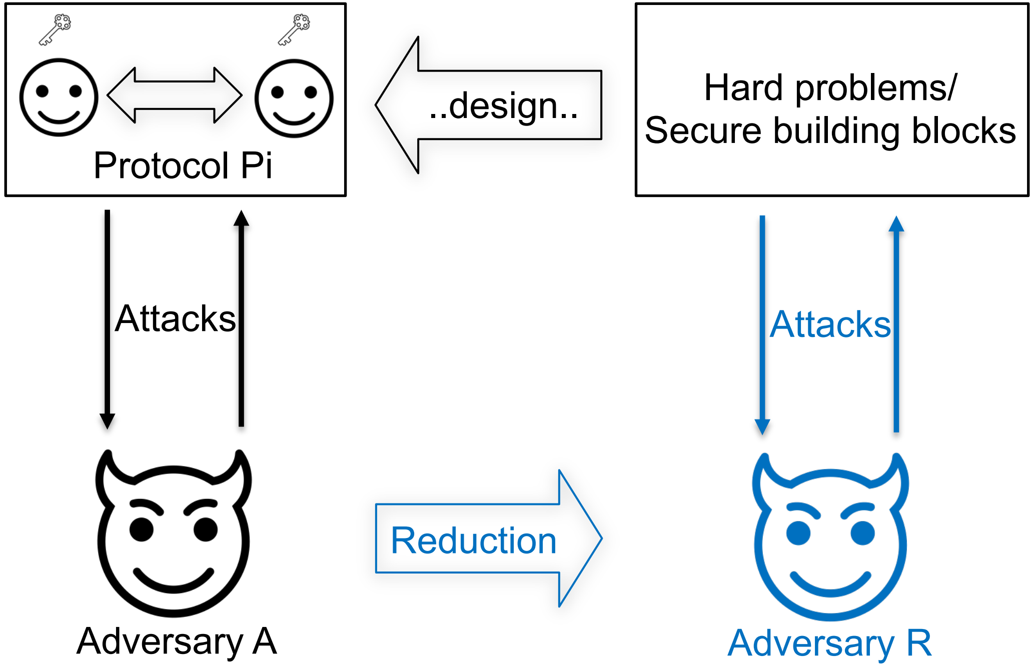


NTNU

Tight Security

- Security Proof via Reduction
  - A breaks Pi
  - => R solves problems
    (or breaks building blocks)

- Such reduction is tight if
  - $\mathbf{T}(R) \approx \mathbf{T}(A)$ (running time)
  - $\mathbf{Adv}(R) \approx \mathbf{Adv}(A)$ (winning advantage)



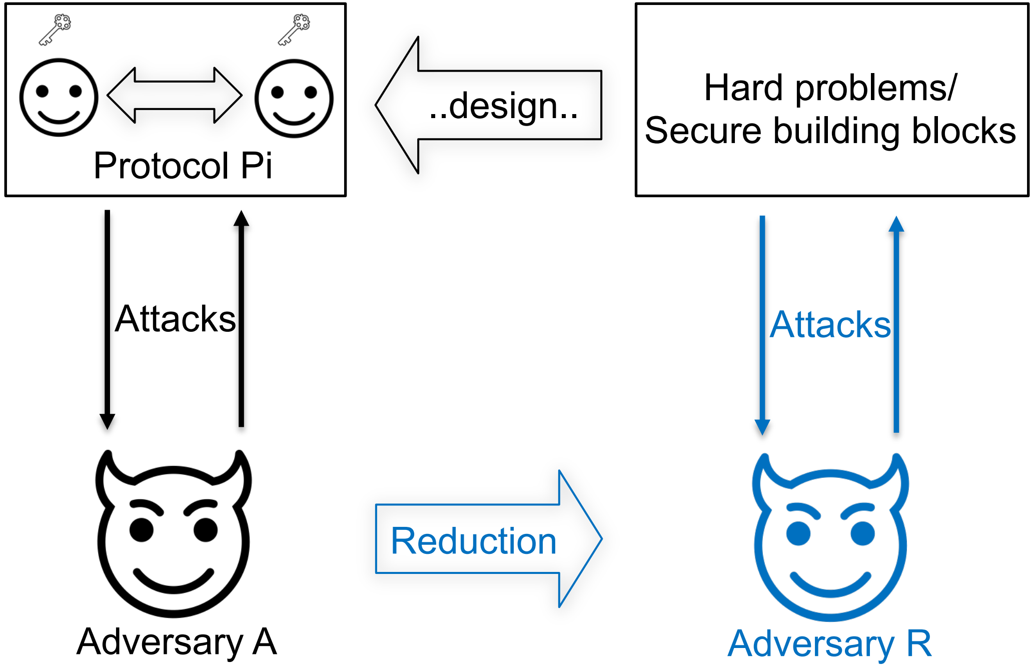
NTNU

Tight Security

- Security Proof via Reduction
  - A breaks Pi
  - => R solves problems
    (or breaks building blocks)

- Such reduction is tight if
  - $\mathbf{T}(R) \approx \mathbf{T}(A)$ (running time)
  - $\mathbf{Adv}(R) \approx \mathbf{Adv}(A)$ (winning advantage)

- Relevance: Parameter selection



NTNU

State-of-art tightly-secure AKE

Schemes	Construction	Assumptions	Model
BHJK15	KEM + SIGN	DDH	StdM
GJ18	KE + SIGN	DDH + CDH	ROM
JKRS21	KEM	DDH	ROM
HJK+21	KEM + SIGN	DDH	StdM

NTNU

Our Goal

Schemes	Construction	Assumptions	Model
BHJK15	KEM + SIGN	DDH	StdM
GJ18	KE + SIGN	DDH + CDH	ROM
JKRS21	KEM	DDH	ROM
HJK+21	KEM + SIGN	DDH	StdM
-	**KEM?**	**PostQuantum?**	-

NTNU

Our Contributions

1. LWE-based AKE with Tight Security in the ROM

Our Contributions

1. LWE-based AKE with Tight Security in the ROM
   - First tightly-secure AKE from a post-quantum assumption
   - Via a new KEM notion: OW-ChCCA security

NTNU

Our Contributions

1. LWE-based AKE with Tight Security in the ROM
   - First tightly-secure AKE from a post-quantum assumption
   - Via a new KEM notion: OW-ChCCA security

2. PKE with Tight Bi-SO Security on LWE in the ROM
   - Bilateral Selective-Opening Security [LYHW21]
   - First tight construction from a post-quantum assumption

NTNU

Our Contributions

1. **LWE-based AKE with Tight Security in the ROM**
   - First tightly-secure AKE from a post-quantum assumption
   - Via a new KEM notion: OW-ChCCA security

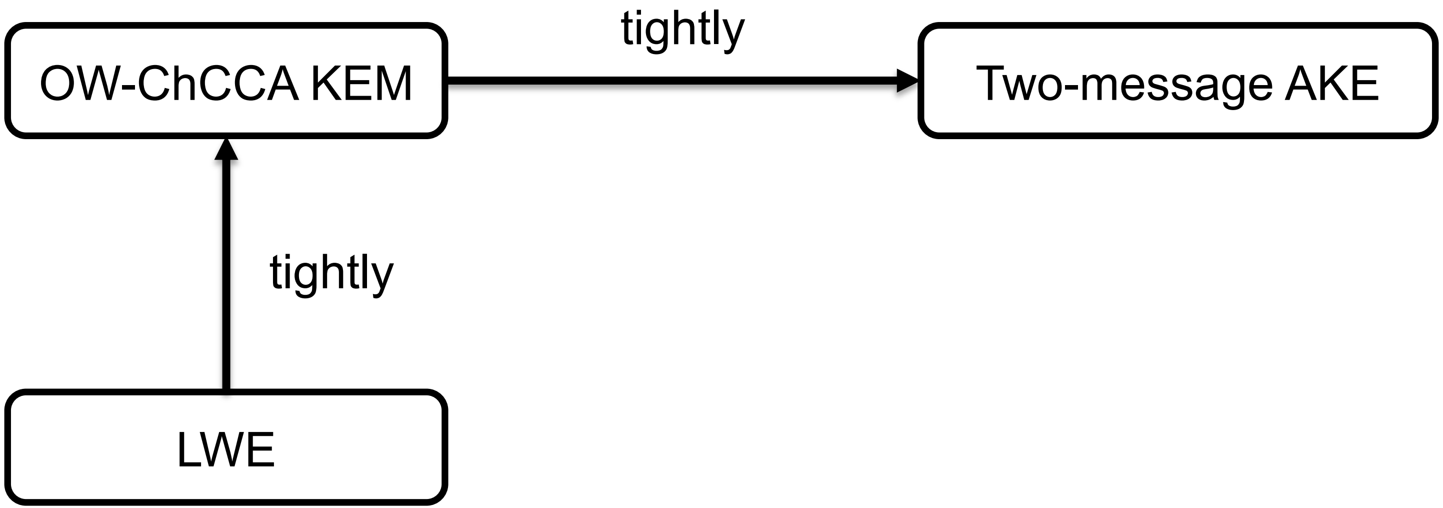
2. PKE with Tight Bi-SO Security on LWE in the ROM
   - Bilateral Selective-Opening Security [LYHW21]
   - First tight construction from a post-quantum assumption

Our Contributions

Schemes	Construction	Assumptions	Model
BHJK15	KEM + SIGN	DDH	StdM
GJ18	KE + SIGN	DDH + CDH	ROM
JKRS21	KEM	DDH	ROM
HJK+21	KEM + SIGN	DDH	StdM
Our work	**KEM**	**LWE**	**ROM**

NTNU

Outline of Technical Parts



AKE from KEM

- Construction [FSXY12,JKRS21]: Static KEM + Ephemeral KEM

Alice(pk_A, sk_A)		Bob(pk_B, sk_B)
$(pk, sk) \leftarrow \text{KeyGen}$	
$(K_B, c_B) \leftarrow \text{Encaps}(pk_B)$	pk, c_B →
	$(c, K) \leftarrow \text{Encaps}(pk)$
← c, c_A	$(K_A, c_A) \leftarrow \text{Encaps}(pk_A)$
	$K_B \leftarrow \text{Decaps}(sk_B, c_B)$
$K \leftarrow \text{Decaps}(sk, c)$	
$K_A \leftarrow \text{Decaps}(sk_A, c_A)$	

$$SK = H(pk_A, pk_B, pk, c_B, c, c_A, K, K_A, K_B)$$

NTNU

AKE from KEM

- Strategy: AKE adversaries → Security requirements of KEM
- Both are in multi-user and multi-challenge settings

AKE from KEM, tightly

AKE adversaries

Security requirements of KEM

Control the network → CCA security

NTNU

AKE from KEM, tightly

AKE adversaries

- Control the network
- Reveal session keys
- Reveal secret states

Security requirements of KEM

- CCA security

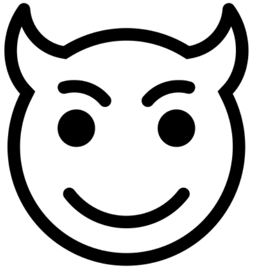
NTNU

AKE from KEM, tightly

- Proof by reduction

Alice(pk_A, sk_A)

Adversary
Impersonate Bob (pk^*_B)



$(pk, sk) \leftarrow$ KeyGen
$(K^*_B, c^*_B) \leftarrow$ Challenge

pk, c^*_B →

← c, c_A

$K \leftarrow$ Decaps(sk, c)
$K_A \leftarrow$ Decaps(sk_A, c_A)

$SK = H(pk_A, pk_B, pk, c_B, c, c_A, K, K_A, K^*_B)$

NTNU

AKE from KEM, tightly

- **Tight reduction ≈ cannot guess challenge session**

Alice(pk_A, sk_A)

(pk, sk) ← KeyGen

(K^*_B, c^*_B) ← Challenge

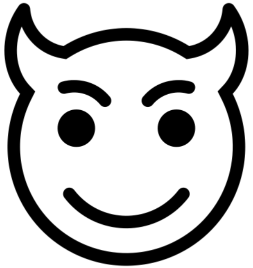
K ← Decaps(sk,c)

K_A ← Decaps(sk_A,c_A)

pk, c^*_B →

← c, c_A

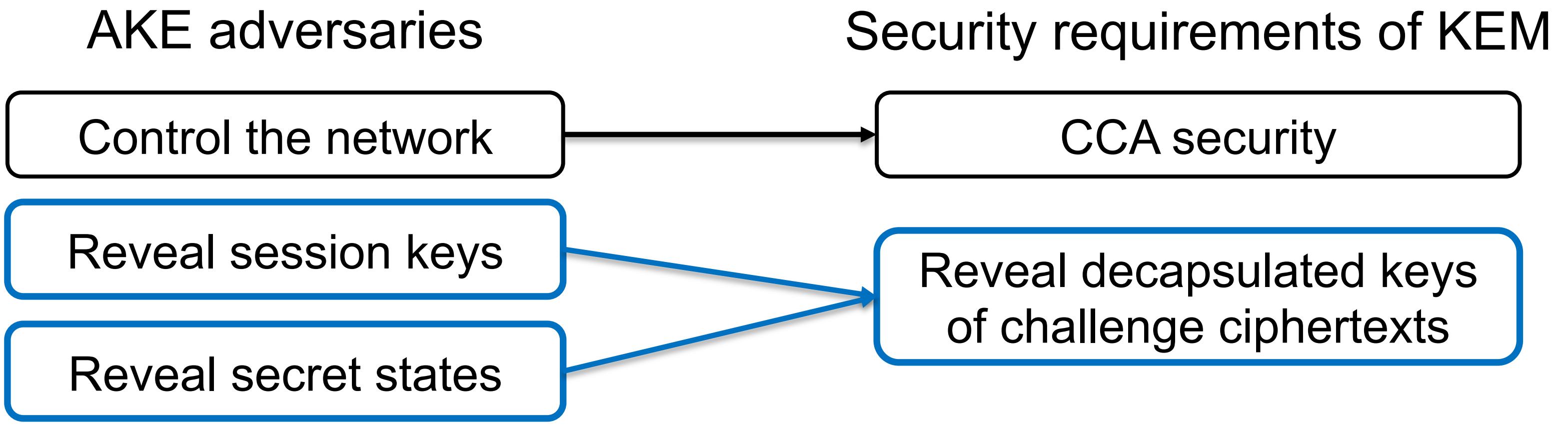
Adversary
Impersonate Bob (pk^*_B)



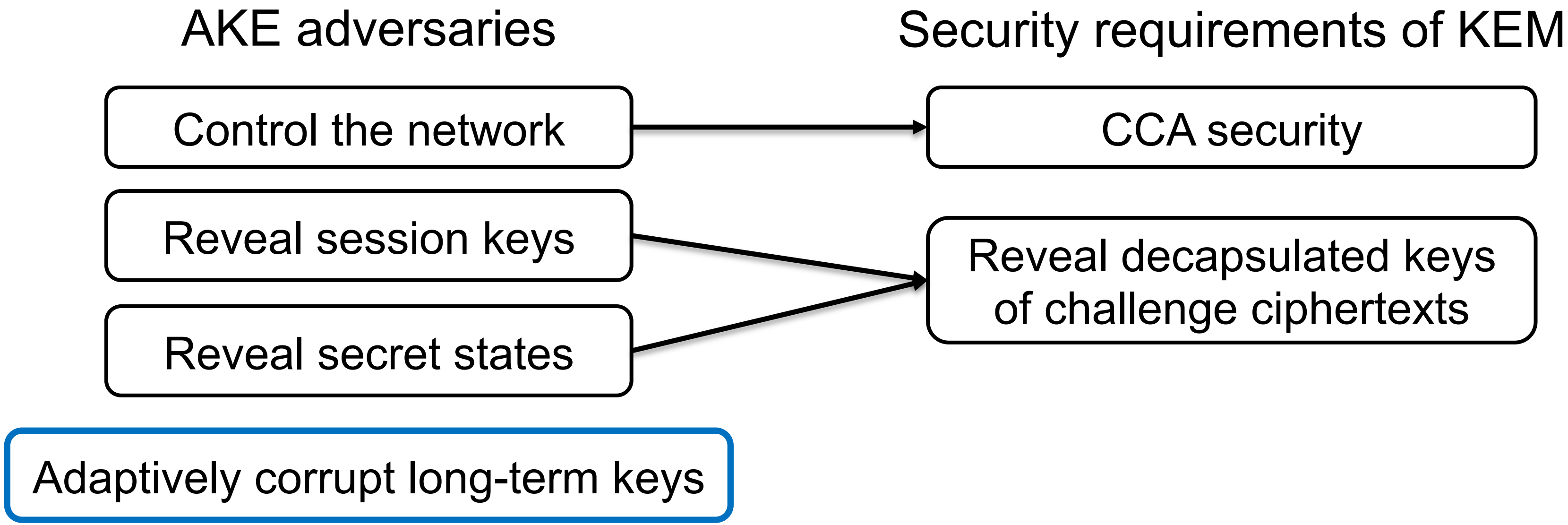
SK = H(pk_A, pk_B, pk, c_B, c, c_A, K, K_A, K^*_B)

NTNU

AKE from KEM, tightly



AKE from KEM, tightly



AKE from KEM, tightly

- Tight reduction ≈ cannot guess challenge session

Alice(pk_A, sk_A)

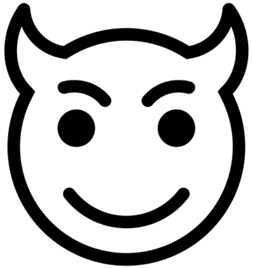
Adversary

$(pk, sk) \leftarrow$ KeyGen

$(K^*_B, c^*_B) \leftarrow$ Challenge

pk, c^*_B →

← c, c_A



$K \leftarrow$ Decaps(sk, c)

$K_A \leftarrow$ Decaps(sk_A, c_A)

Corrupt Bob(pk^*_B, sk^*_B)

$SK = H(pk_A, pk_B, pk, c_B, c, c_A, K, K_A, K^*_B)$

AKE from KEM, tightly

AKE adversaries

Control the network

Reveal session keys

Reveal secret states

Adaptively corrupt long-term keys

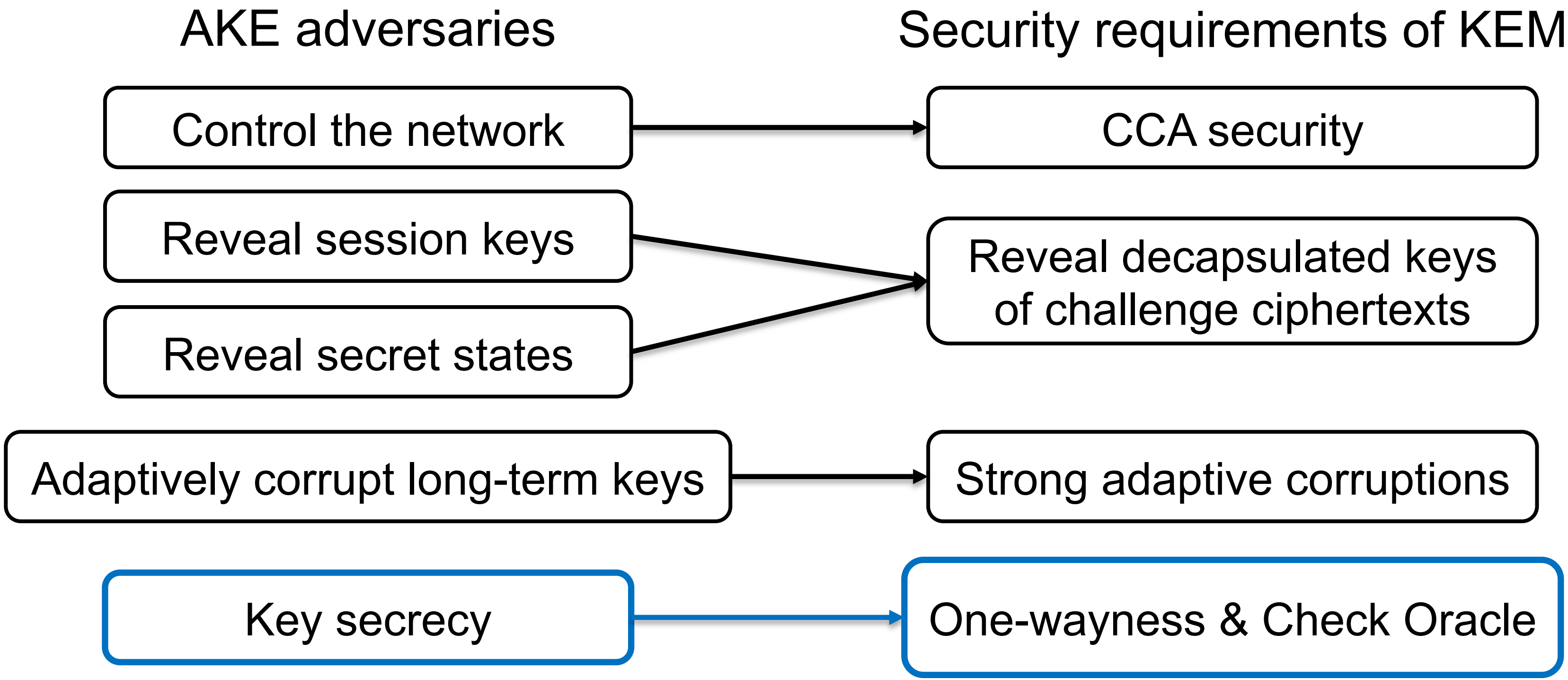
Security requirements of KEM

CCA security

Reveal decapsulated keys of challenge ciphertexts

Strong adaptive corruptions (allowed to corrupt users that generated challenge ciphertexts)

AKE from KEM, tightly



OW-ChCCA KEM

Security requirements of KEM

- CCA security
- Reveal decapsulated keys of challenge ciphertexts
- Strong adaptive corruptions
- One-wayness & Check Oracle

OW-ChCCA KEM

Security requirements of KEM

- CCA security
- Reveal decapsulated keys of challenge ciphertexts
- Strong adaptive corruptions
- One-wayness & Check Oracle

⇒

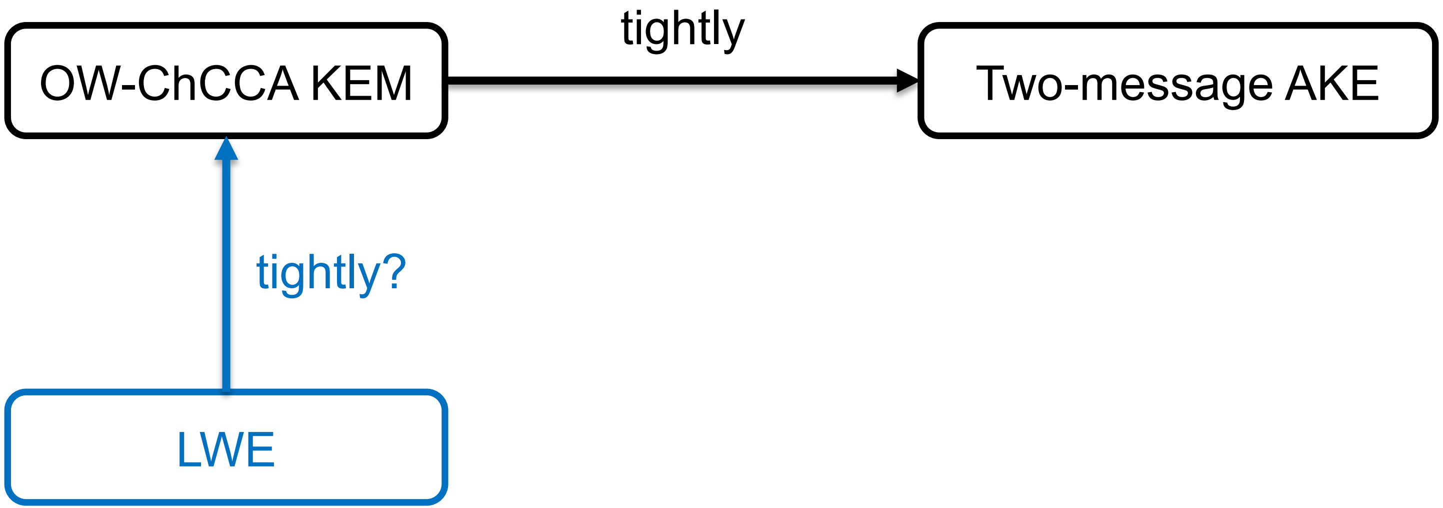
OW-ChCCA KEM

- Decapsulation Oracle
- Reveal Oracle
- Corruption Oracle
- Check Oracle
- One-wayness (for uncorrupted ciphertext)

OW-ChCCA KEM

NTNU

OW-ChCCA KEM from LWE, tightly



OW-ChCCA KEM from LWE, tightly

OW-ChCCA KEM

Corruption Oracle

Reveal Oracle

Decapsulation Oracle

Check Oracle

One-wayness

NTNU

OW-ChCCA KEM from LWE, tightly

OW-ChCCA KEM

- Corruption Oracle
- Reveal Oracle
- Decapsulation Oracle
- Check Oracle
- One-wayness

Challenge

multi-user
multi-challenge

OW-ChCCA KEM from LWE, tightly

OW-ChCCA KEM

- Corruption Oracle
- Reveal Oracle
- Decapsulation Oracle
- Check Oracle
- One-wayness

(Corruption Oracle and Reveal Oracle: even for challenge ciphertexts)

Challenge

multi-user
multi-challenge

OW-ChCCA KEM from LWE, tightly

OW-ChCCA KEM

- Corruption Oracle
- Reveal Oracle
- Decapsulation Oracle
- Check Oracle
- One-wayness

even for challenge ciphertexts

Challenge

- multi-user multi-challenge
- Strong Corruption & Reveal

NTNU

OW-ChCCA KEM from LWE, tightly

OW-ChCCA KEM

- Corruption Oracle
- Reveal Oracle
- Decapsulation Oracle
- Check Oracle
- One-wayness

Decapsulation Oracle and Check Oracle: Consistence with Corruption & Reveal

Challenge

- multi-user multi-challenge
- Strong Corruption & Reveal

OW-ChCCA KEM from LWE, tightly

OW-ChCCA KEM

- Corruption Oracle
- Reveal Oracle
- Decapsulation Oracle
- Check Oracle
- One-wayness

Challenge

- multi-user multi-challenge
- Strong Corruption & Reveal
- Decapsulation & Check consistent with Corruption & Reveal

OW-ChCCA KEM from LWE, tightly

Challenge

multi-user
multi-challenge

Strong Corruption
& Reveal

Decapsulation & Check
consistent with
Corruption & Reveal

OW-ChCCA KEM from LWE, tightly

Challenge

multi-user
multi-challenge

Strong Corruption
& Reveal

Decapsulation & Check
consistent with
Corruption & Reveal

Solutions

Dual Regev + lossy LWE
[GPV08, LSSS17, KYY18]

Double encryption
[NY90, BHJK15]

OW-ChCCA KEM from LWE, tightly

Challenge	Solutions
multi-user multi-challenge	Dual Regev + lossy LWE [GPV08, LSSS17, KYY18]
Strong Corruption & Reveal	Double encryption [NY90, BHJK15]
Decapsulation & Check consistent with Corruption & Reveal	RO reprogramming

NTNU

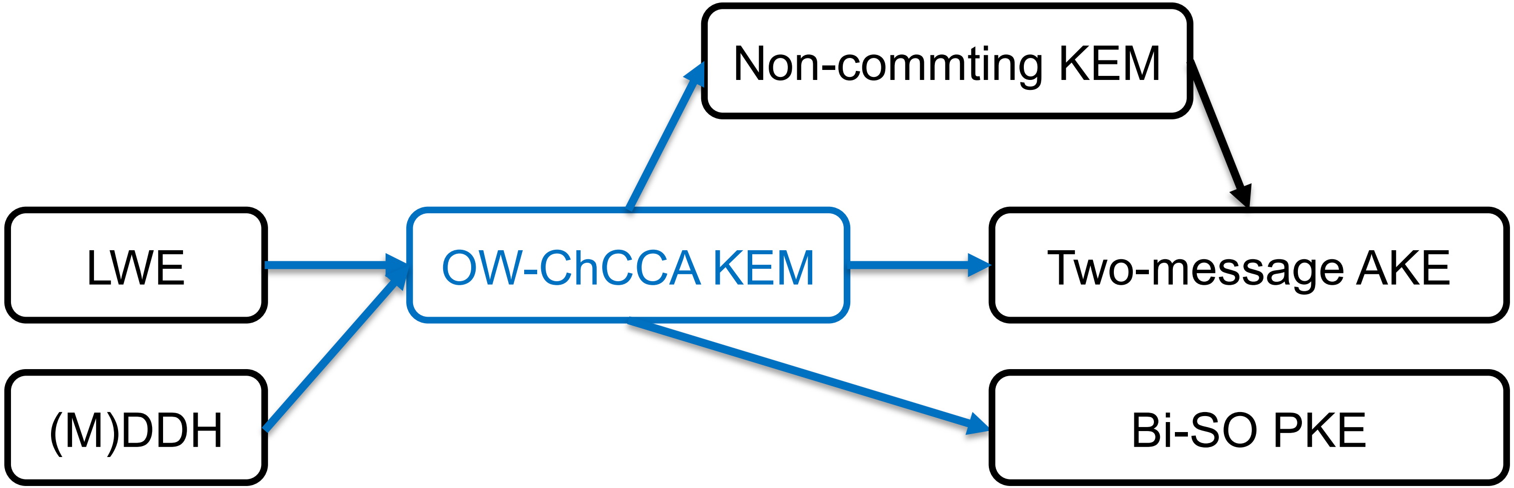
Summary and Open Problems

LWE

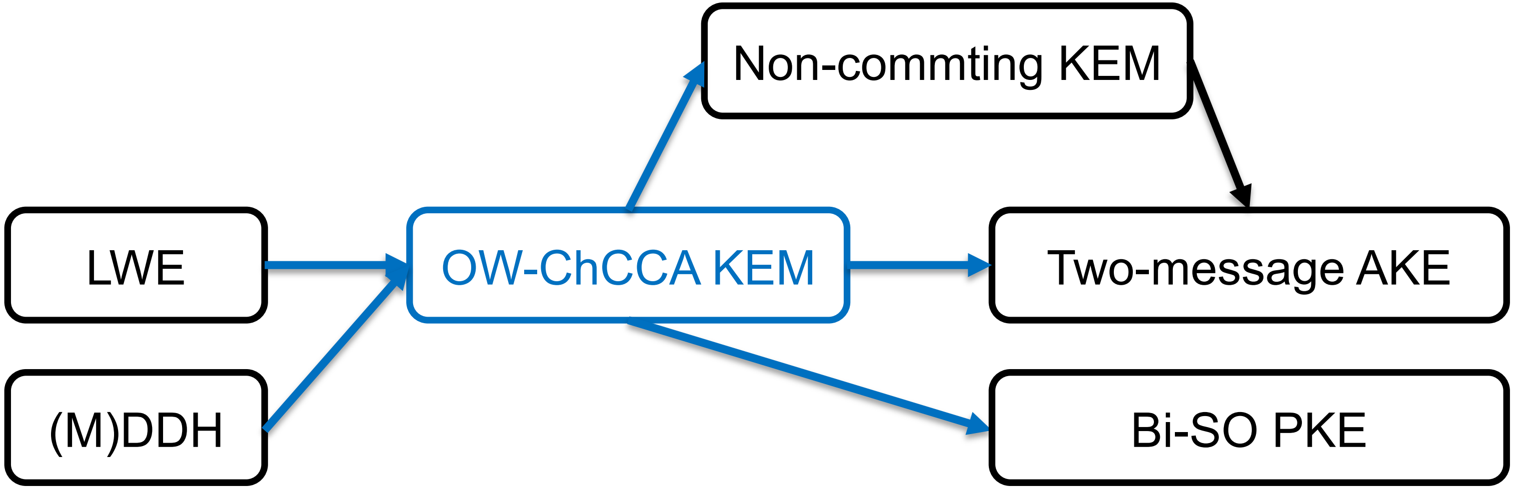
Two-message AKE

Summary and Open Problems

Summary and Open Problems



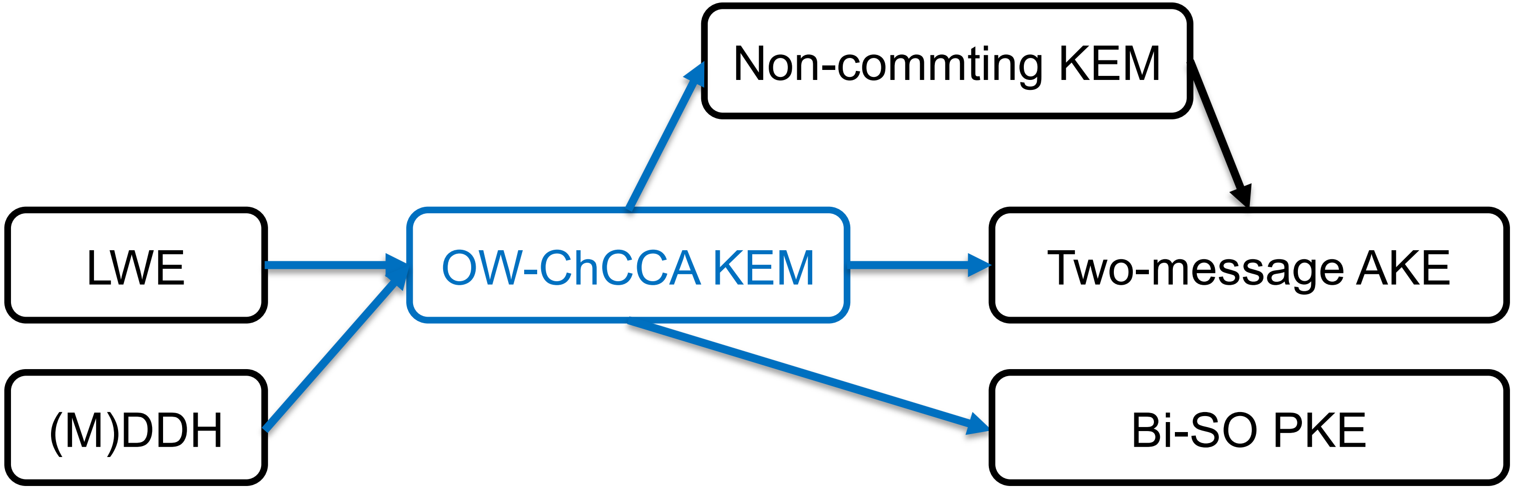
Summary and Open Problems



eprint: 2023/823

NTNU

Summary and Open Problems



QROM?

eprint: 2023/823

References

FSXY12 Atsushi Fujioka, Koutarou Suzuki, Keita Xagawa, Kazuki Yoneyama: *Strongly secure authenticated key exchange from factoring, codes, and lattices.* PKC 2012

BHJ+15 Christoph Bader, Dennis Hofheinz, Tibor Jager, Eike Kiltz, Yong Li: *Tightly-secure authenticated key exchange.* TCC 2015

LSSS17 Benoît Libert, Amin Sakzad, Damien Stehlé, Ron Steinfeld: *All-but-many lossy trapdoor functions and selective opening chosen-ciphertext security from LWE.* CRYPTO 2017

GJ18 Kristian Gjøsteen and Tibor Jager: *Practical and tightly-secure digital signatures and authenticated key exchange*. CRYPTO 2018

References

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

LYHW21 Junzuo Lai, Rupeng Yang, Zhengan Huang, Jian Weng: *Simulation-based bi-selective opening security for public key encryption.* ASIACRYPT 2021

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

HJK+21 Shuai Han, Tibor Jager, Eike Kiltz, Shengli Liu, Jiaxin Pan, Doreen Riepel, Sven Schäge: *Authenticated key exchange and signatures with tight security in the standard model.* CRYPTO 2021