Mo-meng Liu, Juliane Krämer, Yu-pu Hu, Johannes Buchmann. Quantum security analysis of a lattice-based oblivious transfer protocol. *Frontiers of Information Technology & Electronic Engineering*, 2017, **18**(9):1348-1369. http://dx.doi.org/10.1631/FITEE.1700039

Quantum security analysis of a lattice-based oblivious transfer protocol

Key words: Oblivious transfer; Post-quantum; Lattice-based; Learning with errors; Universally composable

Contact: Mo-meng Liu
E-mail: liumomeng@gmail.com

ORCID: http://orcid.org/0000-0002-8545-5551

Problems

- OTs built upon traditional number theoretic problems (discrete logarithm & factoring) cannot be secure against quantum attacks.

- OTs built upon post-quantum cryptography lack of quantum security proofs.

Motivation & Positive Results

Quantum security analysis of [PVW08]:

- **[PVW08] A Framework for Efficient and Composable Oblivious Transfer**
  Chris Peikert , Vinod Vaikuntanathan, Brent Waters. CRYPTO'08

Positive Results:

- **[Unr10] Universally Composable Quantum Multi-Party Computation**
  Dominique Unruh. CRYPTO10

- **[HSS11] Classical Cryptographic Protocols in A Quantum World**
  Sean Hallren, Adam Smith, Fang Song. CRYPTO11

- **[Son14] A Note on Quanutm Security for Post-Quantum Cryptography**
  Fang Song. PQC2014

Lattice-based OT in [PVW08]

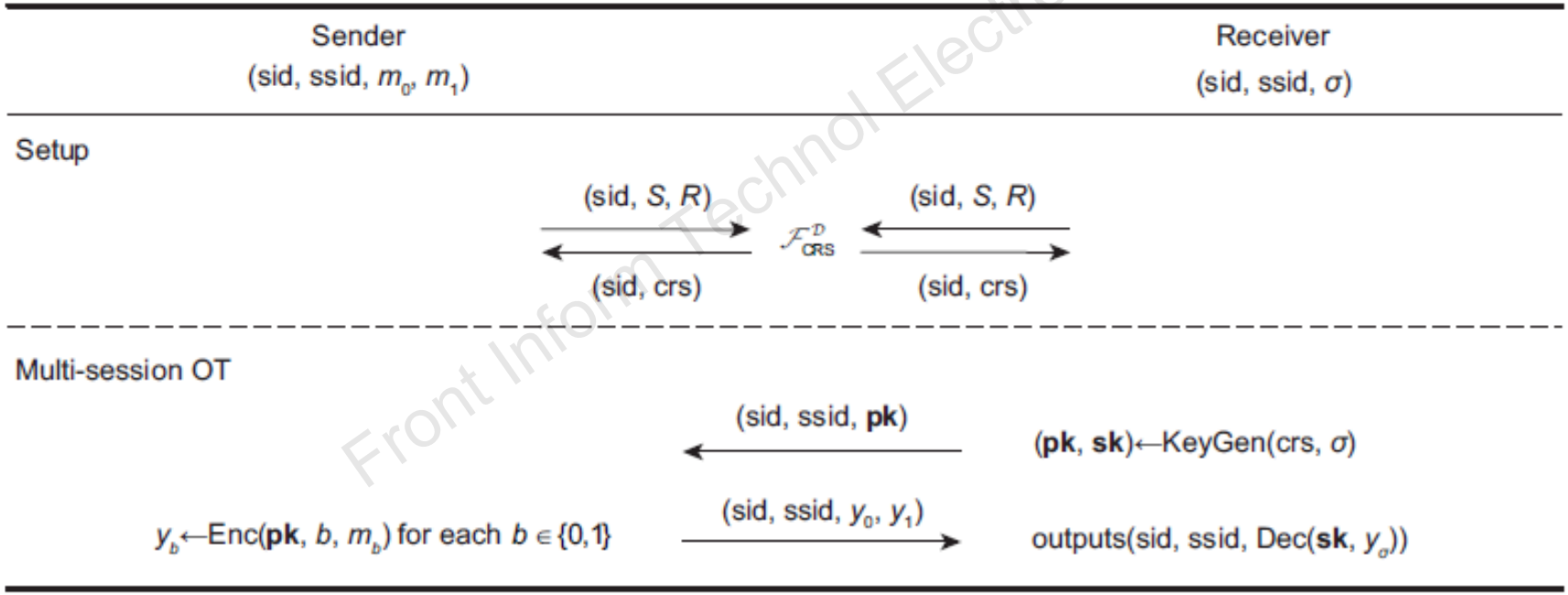
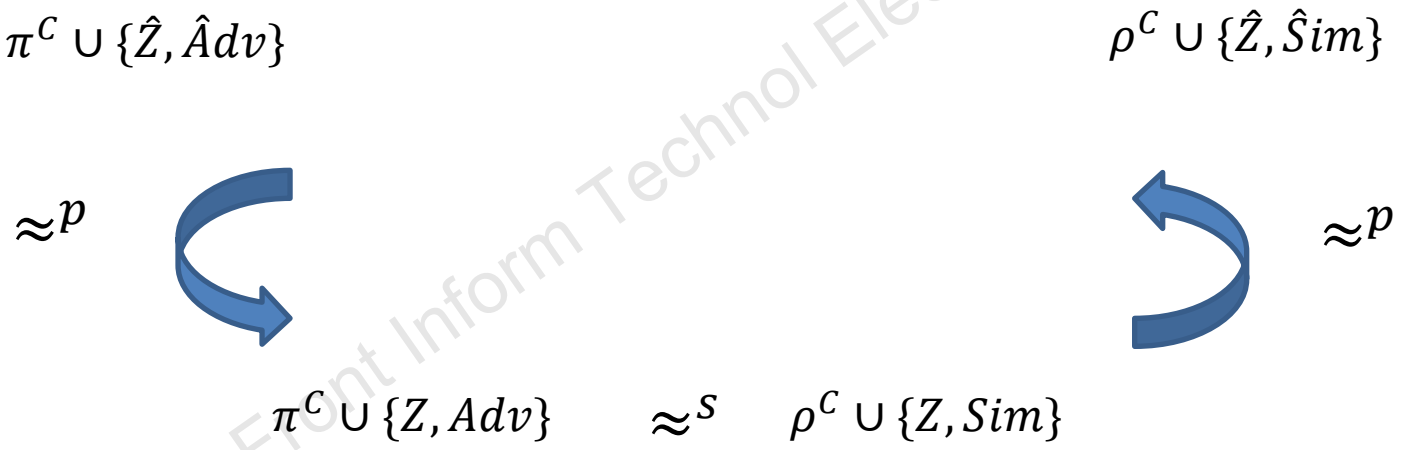


Fig. 1 Protocol $\mathrm{dm}^{\mathrm{mode}}$ for oblivious transfer

[Unr10]: Statistically Quantum Lifting Theorem

Theorem 13 (Quantum lifting theorem). *Let π and ρ be classical protocols. Assume that π statistically classical-UC-emulates ρ. Then π statistically quantum-UC-emulates ρ.*



$\widehat{M}$:QIM
M:ITM

[Unr10]: Computationally Quantum Lifting Theorem

A directly computational analogue of Quantum Lifting Theorem 

QPPT machines: $\mathrm{N} \cup \{M\} \approx^{p} \mathrm{N} \cup \{\widehat{M}\}$, then M is QPPT, denoted as M'

Computationally Quantum Lifting Theorem (QPPT)

$\pi^{C} \cup \{\hat{Z}, \hat{A}dv\}$ $\qquad$ $\rho^{C} \cup \{\hat{Z}, \hat{S}im\}$

$\approx^{p}$ $\qquad$ $\approx^{p}$

$\pi^{C} \cup \{Z', Adv'\}$ $\quad \approx^{c} \quad$ $\rho^{C} \cup \{Z', Sim'\}$

$\widehat{M}$:QIM
M:ITM
M':QPPT

Quantum Analysis on [PVW08]

In different corruption case: Statistical & Computational

Statistical: Use Statistically-QLT directly

Messy mode:
(1)Adv+R: statistical security for S

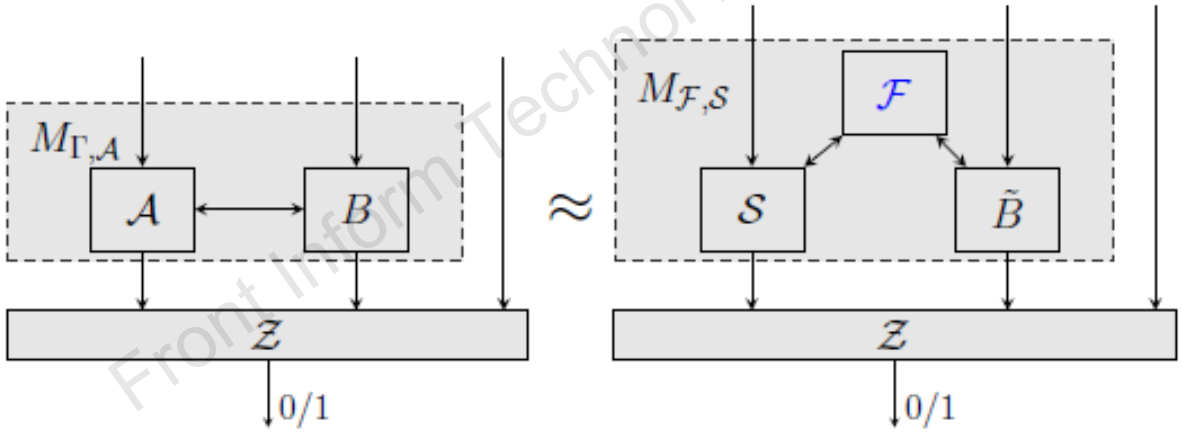
Computational: Prove (computational)QPPT classical UC security?

$$\pi^C \cup \{Z', Adv'\} \quad \approx^C \quad \rho^C \cup \{Z', Sim'\}$$

Lattice- based OT is quantum UC secure.

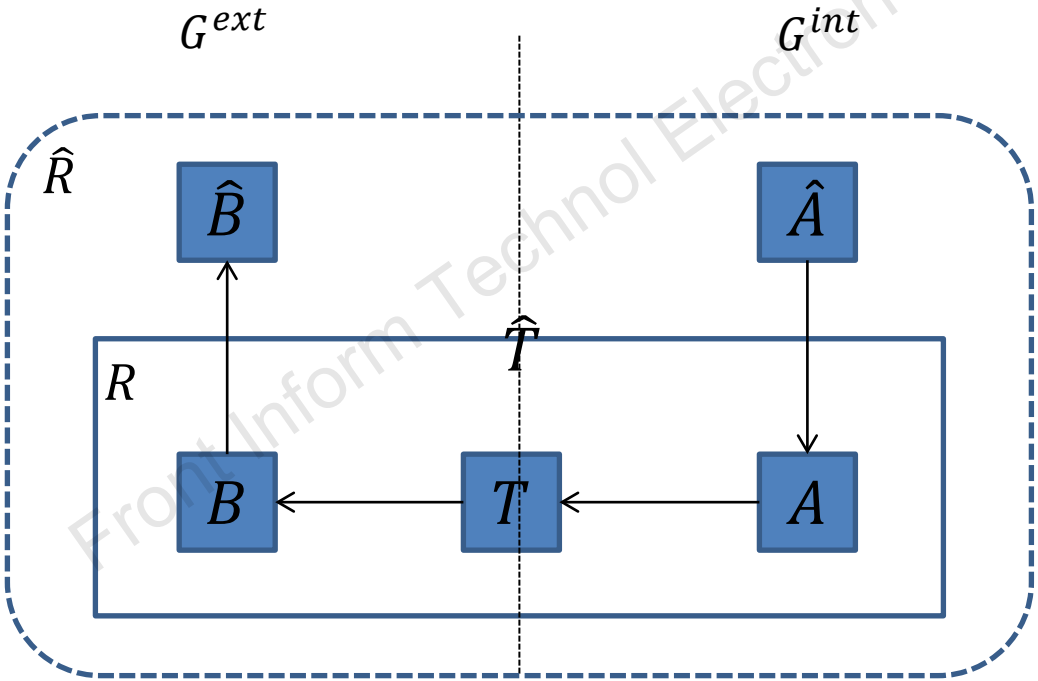
A Support from [HSS11]

Definition 4.4 (SHA). Two machines M_0 and M_ℓ are related by a (t, ε)-SHA of length ℓ if there is a sequence of intermediate machines $M_1, M_2, \ldots, M_{\ell-1}$ such that each adjacent pair M_{i-1}, M_i of machines, $i = 1, \ldots, \ell$, is $(t, \frac{\varepsilon}{\ell})$-simply related.



Quantum Security Analysis Framework [Son14]

- Game-preserving reduction:



Quantum Security Analysis Framework [Son14]

Game-preserving reduction: (Class-respectful reduction)

R is β-$(\hat{A}, \hat{B})$-respectful ($\hat{A}, \hat{B} \in Q$)

1.$(\beta, \hat{A})$-extendable

2. $(\hat{A}, \hat{B})$-closed

(1) R is black-box

(2) R is straight line

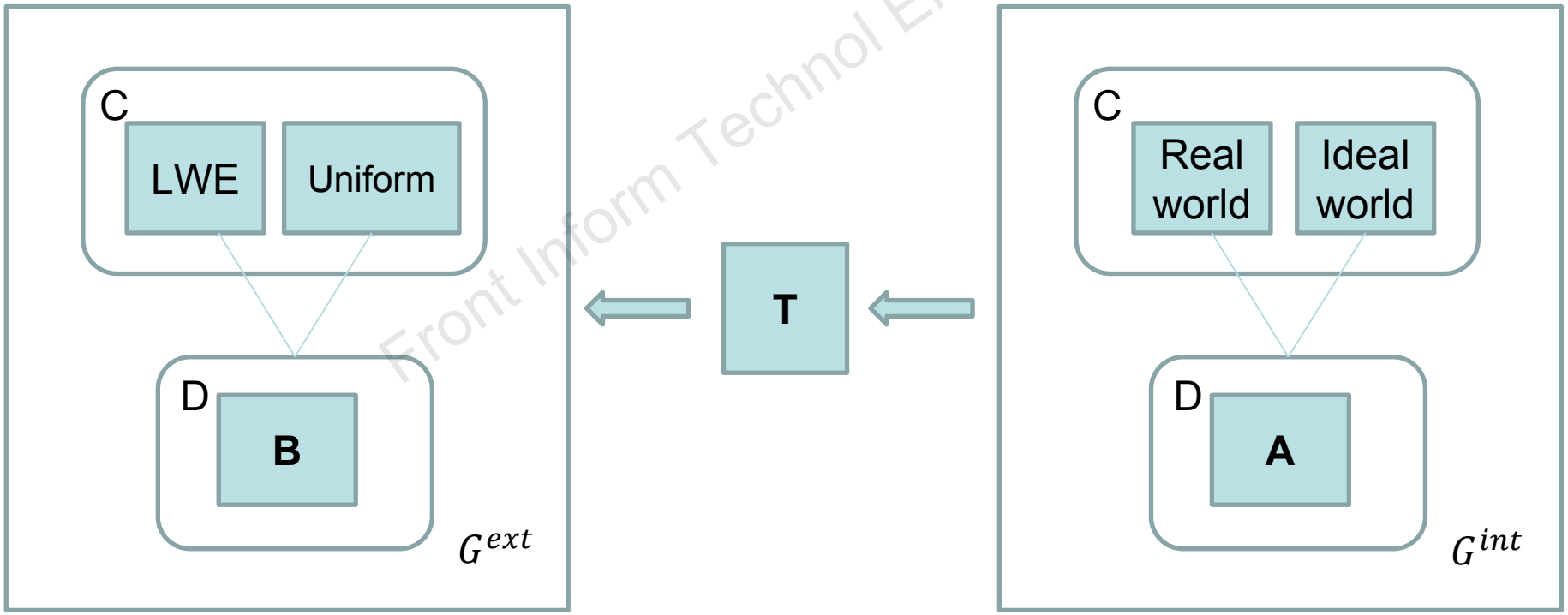
(3) R is $\hat{A}$-compatible

(4) R is value-dominating

Quantum Security Analysis Framework [Son14]

1.Define G^{int} : i.e. Distinguish (real world & ideal world)

2. Define G^{ext} : solve decisional LWE problem. i.e. Distinguish (A, b) & (A, b=As+e)



Conclusion & Future work

- Apply three tools [Unr10,HSS11,Son14] to the lattice-based OT protocol [PVW08] to show a comprehensive quantum security analysis of this OT protocol.
- Explore the post-quantum OT protocols with quantum security proofs.