UNIVERSITY OF TARTU 1632
erc
AIR FORCE OFFICE OF SCIENTIFIC RESEARCH
EXCITE Estonian Centre of Excellence in ICT Research
European Union Regional Development Fund
Investing in your future

Post-Quantum Verification of Fujisaki-Okamoto

Dominique Unruh

University of Tartu

[eprint]

Post-Quantum Encryption

- Quantum computers:
  Break existing public key crypto
- NIST competition:
  Search for next gen PK standard
- Classic McEliece, Crystals-Kyber, NTRU, Saber
- Typical construction:
  Fujisako-Okamoto in ROM

Formal verification

Standard approach:
Human writes proof, human reads proof

- Error-prone (especially with quantum)
- Experts must check every step

Formal verification:

Human writes proof, computer reads proof

- Experts only verify spec

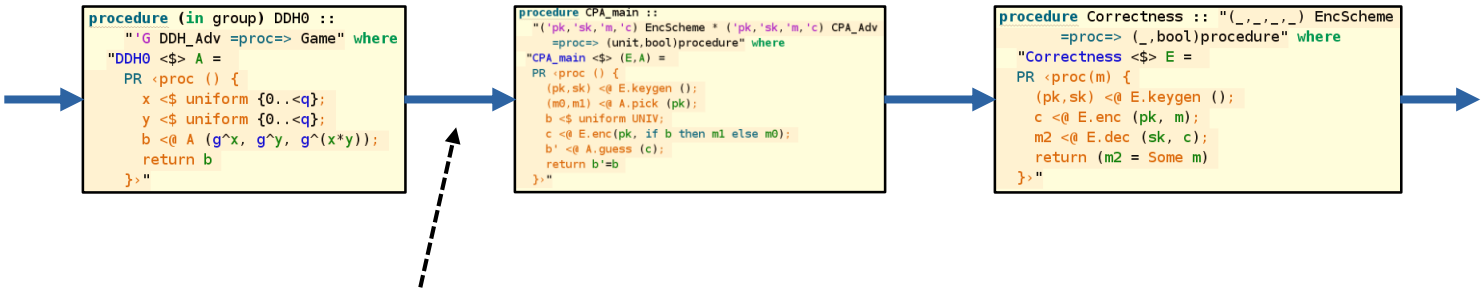
Approaches for formal verification

Many tools:

EasyCrypt, CryptHOL, FCF,
CryptoVerif, Verypto, …

Not quantum sound!

Game-based proofs



How to prove relationship?

EasyCrypt: probabilistic relational Hoare logic (pRHL)

qRHL

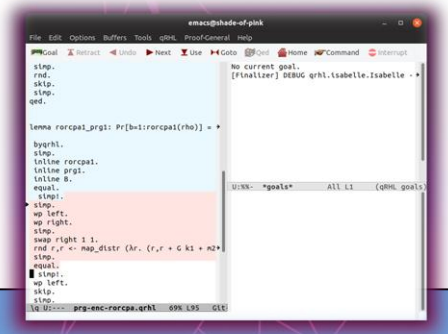
qRHL: Quantum relational Hoare logic

- Similar to pRHL from EasyCrypt
- But for quantum programs

$$\{|\Psi\rangle\}\ U \sim V\ \{|\Phi\rangle\}$$

qrhl-tool: Theorem prover for qRHL

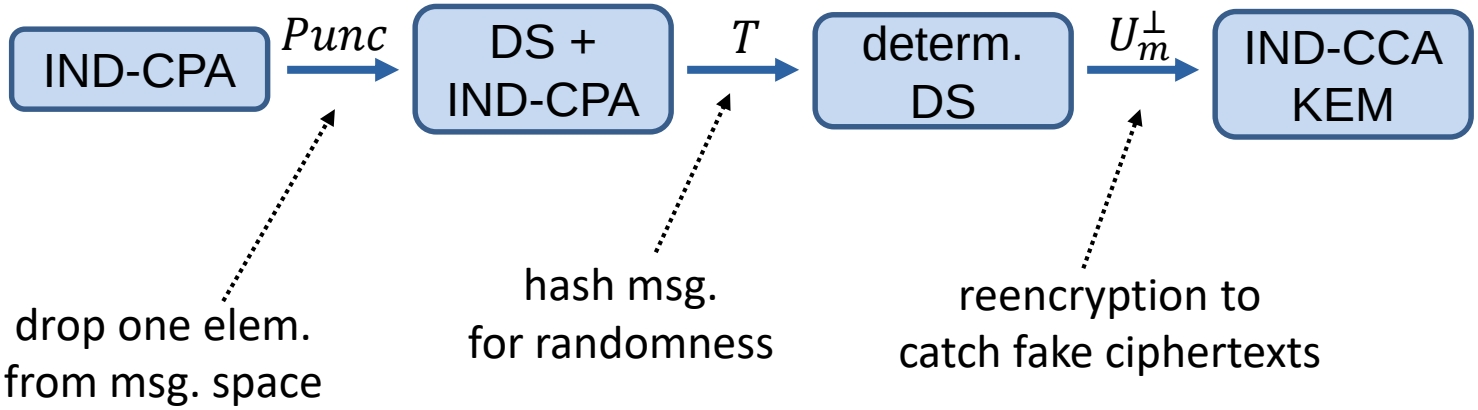
- Designed for quantum crypto proofs
  - Only toy examples!



HKSU

Hövelmanns, Kiltz, Schäge, and Unruh (PKC 2020)

- KEM via Fujisaki-Okamoto variant
- Supports decryption errors



Our contribution

- Formalized HKSU proof
- First nontrivial post-quantum proof
- Involves QROM! (Not “essentially classical”)
- Shows viability of qRHL approach
- Added O2H theorem to qrhl-tool
- Need for local variables

qRHL judgments

$$\{X =_q Y\} \quad quantum\ game_1 \sim quantum\ game_2 \quad \{X =_q Y\}$$

Pre/postconditions can talk about quantum states

Demo

```
game0FO.qrhl
game1FO.qrhl
lemma_game0FO_game1FO.qrhl
```

(available at https://tinyurl.com/hksu-ac2020)

Lessons learned

- Largest part like a classical formalization
  - Except for dragging along quantum-equality
- Few proof steps need quantum-specific reasoning
  - O2H theorem
  - Rewriting quantum circuits

Tedious! Need automation

Open questions / future work

- Verification of NIST candidates “as is”
- Better quantum automation
- Fully quantum protocols
  (e.g., QKD)

Postdoc/phd at University of Tartu:

Verification of Quantum Cryptography

European Research Council
Established by the European Commission

http://tinyurl.com/postdoc-vqc

- Quantum crypto?
- Quantum logic?
- Thm proving?

TARTU ÜLIKOOL · UNIVERSITAS TARTUENSIS · 1632