Quantum Security for Post-Quantum Cryptography

-- “Quantum-Friendly” Reductions

Fang Song
IQC, University of Waterloo

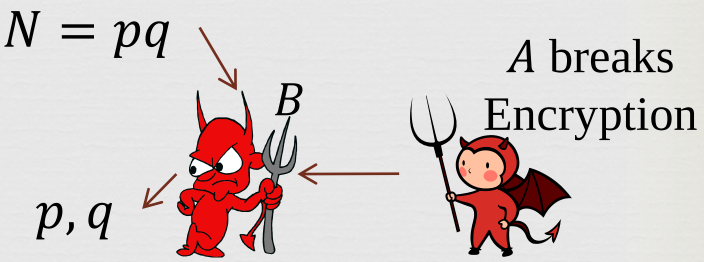
How do quantum attacks change classical cryptography?

- Crypto-systems based on the hardness of factoring and discrete-log are broken
  - Factoring and discrete-log are easy on a quantum computer [Shor'97]
- Relax…, there are "hard" problems for quantum computers
  - Lattices, code-based, multivariate equations,
  - Super-singular elliptic curve isogenies
  - …

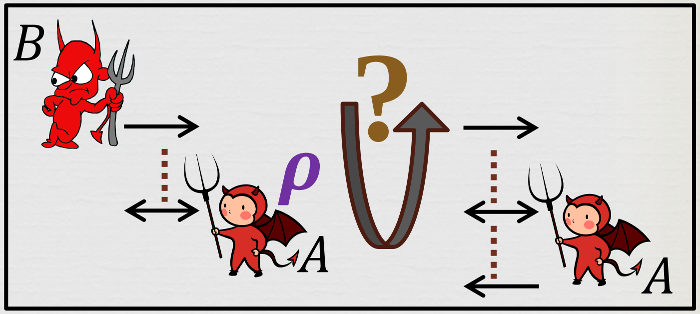
❖ Unfortunately, this is not the end of the story…

What do We Mean by "Secure"?

- Provable-security: need a proof, a.k.a. security ***reduction***.
  - Assume attacker A breaks scheme Π,
  - Construct B from A that solves a hard problem L.

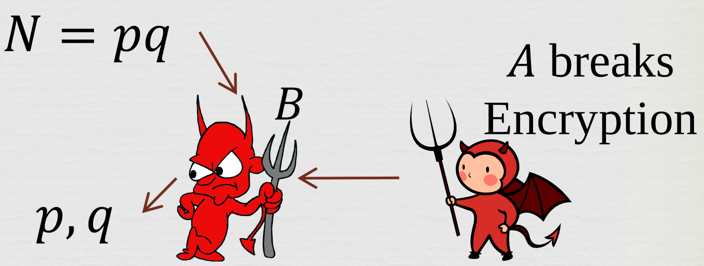


- Reductions may fail against quantum attackers (Even if L is "quantum-hard")
  - Many PQC only prove against classical attackers
- Ex.1 Quantum Rewinding
  - B runs and rewinds A till he's happy;
  - Difficulty with quantum aux. state.
    - No-cloning!
    - Information gain → disturbance on ρ.
  - So far, only can do quantum rewinding in special cases [Wat09,Unr12].



What do We Mean by “Secure”?

- Provable-security: need a proof, a.k.a. security ***reduction***.
  - Assume attacker A breaks scheme Π,
  - Construct B from A that solves a hard problem L.



- Reductions may fail against quantum attackers (Even if L is “quantum-hard”)
  - Many PQC only prove against classical attackers
- Ex.2 Quantum Random Oracle
  - Classical proofs often treat hash function H as a random oracle.
    - Evaluate H →Query H on x
  - What if a quantum adversary makes superposition queries $\sum|x\rangle$?
    - Many classical tricks do not (immediately) work.
    - FYI: a line of beautiful works [Zhandry’12’13,Unruh’Crypto14…]

What I Did in This Work

Q: What classical security reductions can go through against quantum attacks?

Main Result: Characterize "Quantum-Friendly" reductions.

- Case 1: Class-Respectful Reductions
  - Common case: adversary has quantum inner working, classical interaction with outside world.
  - Formalize sufficient conditions, simple to check.
  - Application: (quantum-safe) one-way functions → Signatures
    - An efficient variant: XMSS [BHH11] (Motivation of this work)
    - Not surprising; just making routine work rigorous and easier
- Case 2: Class-Translatable Reductions
  - Unify a few previous works, e.g., Full-Domain Hash in QRO

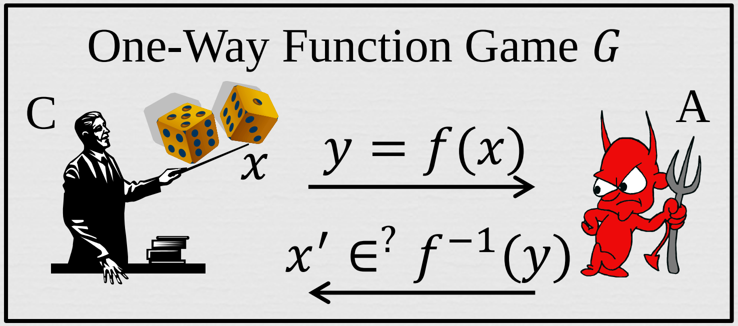
Side: Spell out Provable Quantum Security

- Before "how", be clear "what" to do to establish quantum security

Review: Provable Classical Security

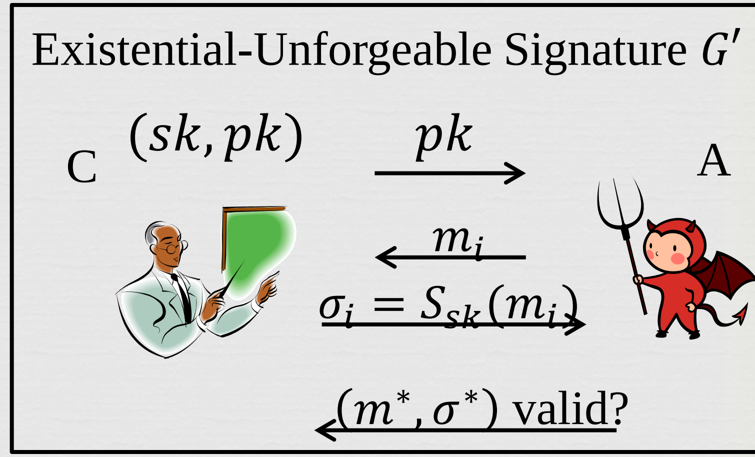
Use ***Games*** to formalize the following:

- Computational Assumption



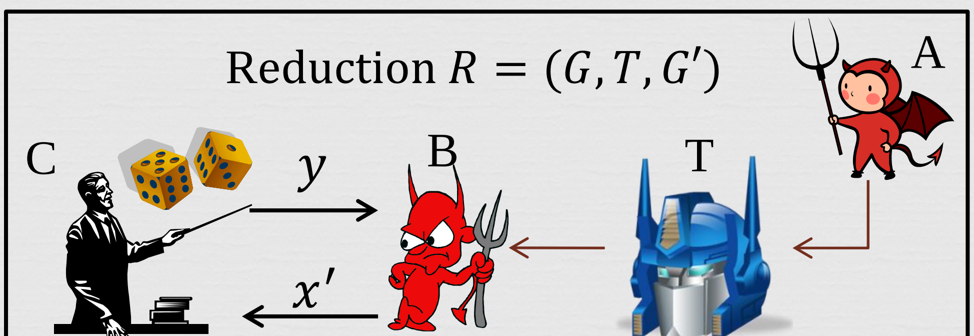
Assume $w(A, G) \coloneqq \Pr[A\ wins] < \delta$

- Security Requirement



Want $w(A, G') \coloneqq \Pr[A\ wins] < \epsilon$

- Security Reduction



Want $w(A, G') > \epsilon \Rightarrow w(B, G) > \delta$

Usually consider poly-time adversaries

Provable Quantum Security

Every component needs a "quantum" inspection

Classical

Quantum
(consider quantum poly-time adversaries $\boldsymbol{Q}$ only)

G

Formalize $\hat{G}$

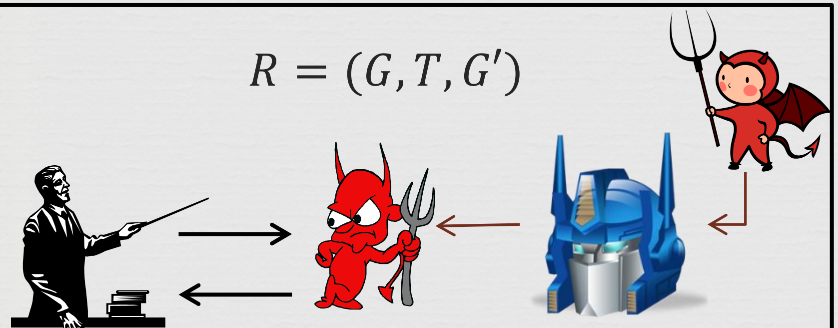
$< \delta$

- Case 1: Game-Preserving $\hat{G} = G$ & $\hat{G}' = G'$
  - Classical games capture what quantum attackers can do, except for inner (quantum) computation power.
- Case 2: Game-Updating $\hat{G} \neq G$ and/or $\hat{G}' \neq G'$
  - E.g., quantum RO, quantum-accessible signatures,…

etting
queries?

Want $\forall \hat{A} \in Q, w(\hat{A}, \hat{G}') < \epsilon$

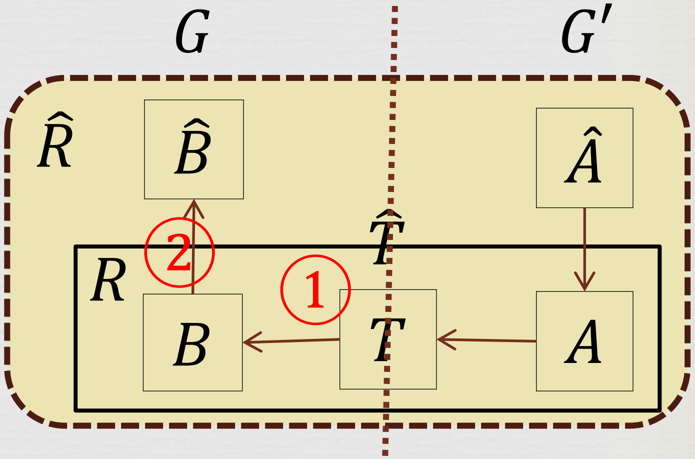
$R = (G, T, G')$



Does there exist $\hat{R} = (\hat{G}, \hat{T}, \hat{G}')$, s.t.
$\forall \hat{A}$, let $\hat{B} := \hat{T}(\hat{A})$,
$w(\hat{A}, \hat{G}') > \epsilon \Rightarrow w(\hat{B}, \hat{G}) > \delta$

Lifting Game-Preserving Reductions

- Basic Idea:
  - Given quantum adversary $\hat{A}$ that wins game G', find an "equivalent" classical adversary A.
  - Apply classical reduction R and get B.



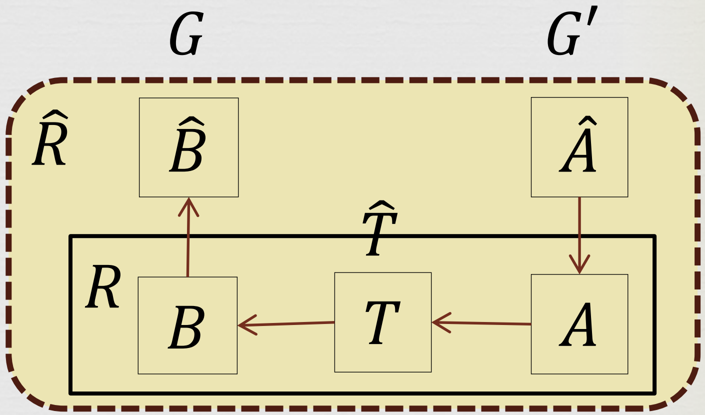
- Two conditions to make the basic idea work
  1. Does R/T work on A? A may not be poly-time.
  2. Is there a $\hat{B} \in Q$, s.t. $B =_G \hat{B}$? → Is $B \coloneqq T(A) \in E_G(Q)$?

- Definition. A and $\hat{A}$ are G-equivalent ($A =_G \hat{A}$), if $w(A, G) = w(\hat{A}, G)$.
- $E_G(Q) = \{\text{classical } A\text{: } \exists \hat{A} \in Q, s.t. A =_G \hat{A}\}$: collection of classical adversaries for which there exists a G-equivalent poly-time quantum adversary.

Lifting Game-Preserving Reductions (Cont'd)

- Definition. A classical reduction $R = (G, T, G')$ is Q-respectful if
  1. R is Q-extendable: $\forall A \in E_{G'}(Q)$,
     - R is well defined on A & $B := T(A)$,
     - $w(A, G') > \epsilon \Rightarrow w(B, G) > \delta$.
  2. R is Q-closed: $\forall A \in E_{G'}(Q)$, $B \in E_G(Q)$.

  $E_G(Q) = \{\text{classical } A : \exists \hat{A} \in Q, s.t. A =_G \hat{A}\}$



Theorem 1. If R is Q-respectful, then $\exists \widehat{R}$ for quantum adv's Q.

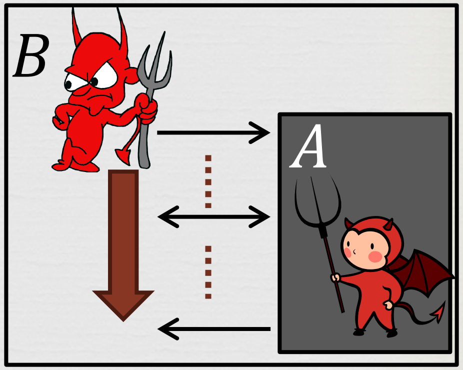
- Extendibility usually holds and easy to verify.
- Closedness could be subtle
  - E.g. R involves rewinding [Unr10].
  - But sometimes it is straightforward.

A Useful Condition for Closedness

Claim. If for any $A \in E_{G'}(Q)$, R is

- Black-box: B uses A as a black-box.
- Straight-line: When B runs A, it never goes back.
- Value-dominating: $w(A_1, G') = w(A_2, G') \Rightarrow w(B_1, G) = w(B_2, G)$.

Then R is Q-closed. ($\hat{B} = B^{\hat{A}}$)

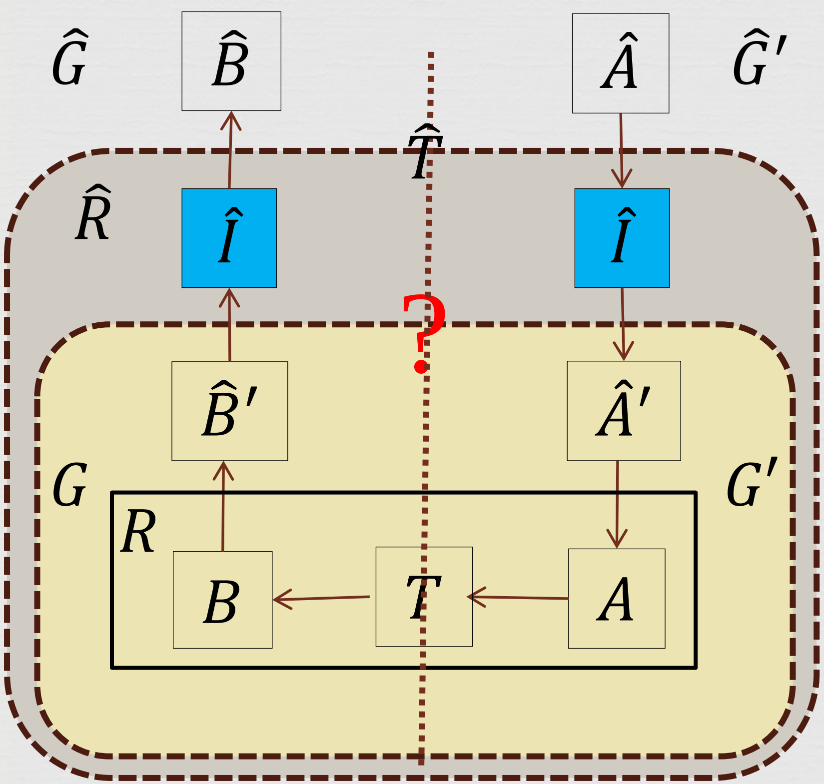


Application: Quantum-safe OWFs ⇒ Quantum-secure Signatures

- Made common belief and some previous claim rigorous (e.g. [IM'PQCrypto11]).
- Same holds for XMSS [BDH11]: more efficient OTS + (different) Hash tree.
  - More features not checked yet: e.g. forward security…
- [Zhandry'Crypto13] showed that (with very nice techniques)
  - Collision-Resistant Hash Function ⇒ QQ-secure Signatures.
  - QQ: adversary can ask for superposition signing queries $\sum |m\rangle$.

Lifting Game-Updating Reductions

Upshot: let an **interpreter** take you to the game-preserving land!



- Definition. A classical reduction $R = (G, T, G')$ is Q-translatable if $\exists \hat{I}$ s.t.,
  - $\hat{I}$ is a "good" interpreter.
    - $w(\hat{A}, \hat{G}') \approx w(\hat{A}', G')$
    - $w(\hat{B}, \hat{G}) \approx w(\hat{B}', G)$
  - R is $\hat{I}(Q)$-respectful.

- **Theorem 2**. If R is Q-translatable, then there exists $\hat{R} = (\hat{G}, \hat{T}, \hat{G}')$.

- Application: unify previous results
  - E.g., a more modular proof for Full-Domain Hash in Quantum RO.

Discussions

Takeaways

- To establish quantum security of a classical scheme, assumptions, security definitions, reductions all need to be re-examined.
- We've given characterizations for "quantum-friendly" reductions.
  - Simple cases: there is a tool to ease the routine wok.

Future Directions

- Apply and extend our characterization and tools
  - Many straightforward applications
  - More interesting cases: rewinding, QRO, generic interpreter …
- Reinvestigate fundamental objects
  - PesudoRandomFunctions ➔ Quantum-accessible PRPermutations?
  - May shed light on quantum unitary designs.
- Reduction has quantum access to adversary?
  - A different flavor of game-updating reductions.
  - E.g. Quantum Goldreich-Levin [AC'STACS02]

Thank you!