Feasibility and Completeness of Cryptographic Tasks in the Quantum World

Jonathan Katz*, Fang Song**, Hong-Sheng Zhou*, Vassilis Zikas*

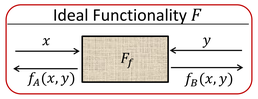
*Department of Computer Science, University of Maryland

**Department of Computer Science and Engineering, The Pennsylvania State University

Introduction

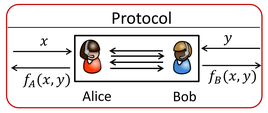
2-Party Secure Function Evaluation (SFE)

Two players want to jointly evaluate a function $f = (f_A, f_B)$, abstracted as an *ideal functionality* F_f



Goal: design a secure protocol to realize F

- Correctness: get correct outputs
- Privacy: Bob does not learn anything about x beyond $f_B(x,y)$; same for Alice



Natural question: *Which functionalities **can**/**cannot** be realized?*

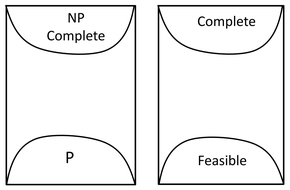
We work under the *universal-composable* security framework [DM00,Can01,Unr10]; in both computational and statistical settings.

adversaries have **bounded** computational power

adversaries are **unbounded**

Classical Landscape of "Cryptographic Complexity"

Analogous to Computational Complexity



Notation: $G \subseteq F$ means that we can realize G, given F as trusted setup.

DEF. Call F complete, if for any functionality G, $G \subseteq F$.

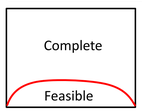
DEF. Call F feasible, if $F \subseteq$ authenticated channel.

Systematic study mainly on a sub-family [MPR09,MPR10,KMQ11]

$\mathcal{U} = \{F$: finite domain, deterministic$\}$

- Examples in $\mathcal{U}$:
  - Feasible: Identity function (feasible ones are usually trivial)
  - Complete: Oblivious Transfer (OT)
  - $\mathcal{U}$ also contains reactive functionalities, e.g., Commitment (COM)

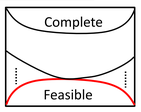
Computational landscape of $\mathcal{U}$



0/1 Law [MPR10]

Complicated (No 0/1 Law) [MPR09,KMQ11]

Statistical landscape of $\mathcal{U}$



Stepping into a Quantum World

How would the classical pictures change?

Negative Side: *adversaries* with quantum power

Known attacks

- *RSA* ← Quantum factoring alg. [Sho96]
- *Two-sender commitment* ← entanglement breaks binding [CSST11]

Possible changes:

- P1: some *feasible* F becomes *infeasible*
- P2: some *complete* F becomes no longer *complete*

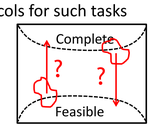
Positive Side: *honest players* with quantum power

- *Quantum Key Exchange* [BB84]
- Quantum *OT* protocol from *Commitment, i.e.* $OT \subseteq COM$ [BBCS92]

Classically, **provably** no statistical secure protocols for such tasks

Possible changes:

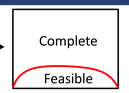
- P3: some *infeasible* (including complete) F becomes *feasible*
- P4: some *incomplete* (including feasible) F becomes *complete*



Our Results

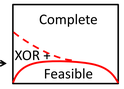
1. Quantum computational landscape *unchanged*

   Theorem (Quantum 0/1 Law) $\forall F \in \mathcal{U}$, F is either feasible or complete and they don't collapse.



2. Statistically: multiple classes collapse to three classes

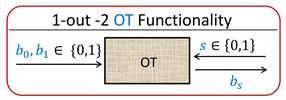
   Theorem $\forall F \in \mathcal{U}$, one of the two cases is true : 1) F is feasible; 2) F is complete or XOR-like

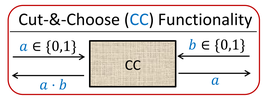


Technical Contribution: Generalize a framework for proving security of a class of quantum protocols

Our Approach

Key Lemma: There is a quantum protocol Π statistically realize **OT** from **CC**





- Alice chooses to observe Bob's bit
- Bob always sees Alice's bit

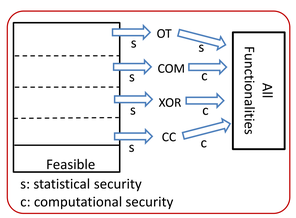
Proving Quantum *Computational* 0/1 Law

Classical characterization of $\mathcal{U}$ [MPR10]

Fact [MPR10] $\forall F \in \mathcal{U}$, F is either feasible or one of the following holds

1. $OT \subseteq_s F$
2. $COM \subseteq_s F$
3. $XOR \subseteq_s F$
4. $CC \subseteq_s F$

$\subseteq_s$ means the reduction achieves statistical security



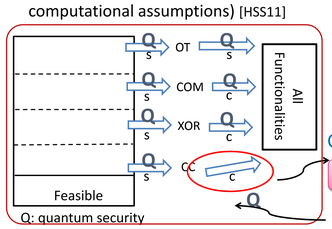
s: statistical security
c: computational security

Lifting Completeness to Quantum World

Claim 1 Classical completeness ➔ Quantum Completeness

Existing Tools

1. Quantum Lifting Lemma [Unruh10]: classical-statistical security ➔ quantum-statistical security
2. COM and XOR are quantum computationally compelte (with proper computational assumptions) [HSS11]



Question:

*Is **CC** complete quantumly?*

YES! by Key Lemma

Lifting Feasibility to Quantum World

Claim 2 Classical feasibility ≡ Quantum feasibility

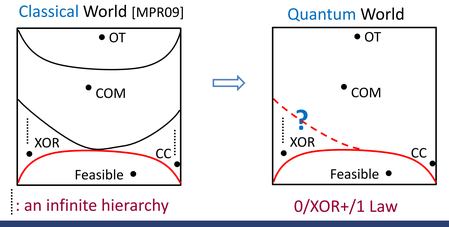
One Subtlety:

*Could **complete** functionalities collapse to being **feasible**?*

NO!

- commitment is not realizable even by quantum protocols if no extra trusted setup available (quantum analogue of [CF01])

Statistical Landscape

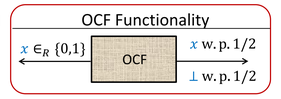


Constructing OT from CC

Construction in a Nutshell:

We follow the structure in [BBCS92]

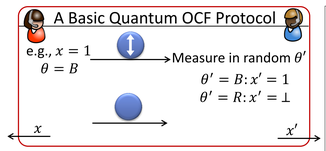
1. Weakly secure quantum protocol for *Oblivious Coin-Flipping* (OCF)
2. A checking subroutine that augments to standard security
3. Transforming OCF to OT



OCF is non-standard; mainly for presentation purpose

We realize the Checking subroutine (step 2) using **CC** ([BBCS92] uses COM)

1. Weakly secure quantum OCF protocol [BB84,BBCS92]



1. Alice picks at random one of two bases $\theta \in \{B, R\}$ to encode a random x

θ \ x	0	1
BLUE	⟷	↕
RED	⤢	⤡

2. Bob measures in a randomly chosen basis θ'.
3. Alice sends θ to Bob.

Correctness

- measure in wrong basis gives a random bit
- θ is randomly chosen

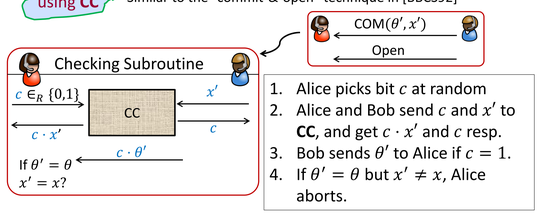
➔ w. p. ½, get $x' = x$; w. p. ½, get $x' = \perp$

2. Checking subroutine

Issue: dishonest Bob can measure after receiving θ, and always recover b!

Fix: Alice tests whether Bob did the measurement

using **CC** Similar to the "commit-&-open" technique in [BBCS92]



1. Alice picks bit c at random
2. Alice and Bob send c and x' to **CC**, and get $c \cdot x'$ and c resp.
3. Bob sends θ' to Alice if $c = 1$.
4. If $\theta' = \theta$ but $x' \neq x$, Alice aborts.

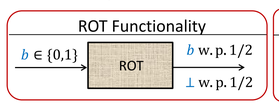
Claim. Alice catches any dishonest Bob w. p. $\geq 1/8$

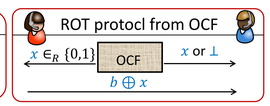
Proof. With probability ¼, $c = 1$ & $\theta' = \theta$, but in this case any Bob guesses right (it he didn't measure), i.e. $x' = x$ w.p. at most ½ because x is a random bit. Therefore w.p. at lest 1/8, Bob will get caught.

Warning: the order of sending x' and θ' matters

3. Converting OCF to OT

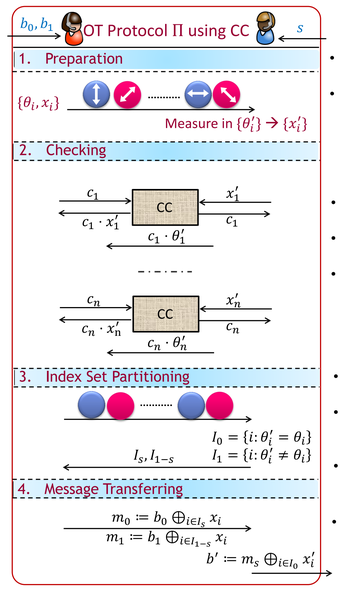
- Realize an equivalent variant: Rabin-OT (ROT) from **OCF**





- (Standard) transform from ROT to (1-out-2) OT [Cre87]

Full Protocol: OT from CC



- Alice picks $x_1, \ldots, x_n$ at random, and encodes them in random bases $\{\theta_i\}$
- Bob measures in random bases $\{\theta_i'\}$ and obtains $\{x_i'\}$
- Alice picks $c_1, \ldots, c_n$ at random, runs the checking subroutine.
- Alice aborts if inconsistency ever occurs
- Bob aborts if Alice checks too many positions, say $|\{i: c_i = 1\}| \geq 3n/5$
- Alice and Bob discard the positions that have been checked
- I_0 contains positions that Bob has correct measurement outcomes $x_i' = x_i$
- Bob send I_0, I_1 according to his chosen bit s
- Alice masks b_0, b_1; and Bob recovers b_s

A Peek on the Security Proof of OT Protocol Π

- Let $x = \{x_i = x_i' : i \in I_0\}, y = \{x_i : i \in I_1\}, z = \{x_i' : i \in I_1\}$,
- Checking step leaves (x, y) to Alice and (x, z) to Bob;
- **Guarantee**: y still appear random to Bob (i.e., *conditional min entropy* high)
- Mask b_s with x → Bob can recover b
- Mask b_{1-s} with y → Bob get nothing about b_{1-s} (this is a *one-time pad*!)
- Formal argument generalizes a quantum sampling framework in [BoumanFehr10] to a new setting (maybe of independent interest)

Open Questions

- Is XOR complete in the quantum statistical setting?
  - *Conjecture*: NO! and infinite hierarchy still exists
- What is the minimal computational assumption that suffices for 0/1 law in the quantum computational setting?
- Extending to larger class of functionalities
  - E.g., randomized, infinite domain

References

- [BB84] C.H. Bennett and G. Brassard. *Quantum cryptography: Public key distribution and coin tossing*. IEEE International Conference on Computers Systems and Signal Processing, pages 175–179, 1984.
- [BBCS92] Charles H. Bennett, Gilles Brassard, Claude Crepeau, and Marie-H'el`ene Skubiszewska. *Practical quantum oblivious transfer*. CRYPTO'91, pages 351–366, 1992.
- [BF10] Niek J. Bouman and Serge Fehr. *Sampling in a quantum population, and applications*. CRYPTO'10, pages 724–741, 2010.
- [Cre87] C. Crépeau. *Equivalence between two flavors of oblivious transfers.* Crypto'87, pages 350-354, 1987.
- [CF01] Ran Canetti and Marc Fischlin. *Universally composable commitments*. CRYPTO'01, pages 19–40, 2001.
- [CSST11] Claude Crepeau, Louis Salvail, Jean-Raymond Simard, and Alain Tapp. *Two provers in isolation*. ASIACRYPT'11, pages 407–430, 2011.
- [DM00] Yevgeniy Dodis and Silvio Micali. *Parallel reducibility for information-theoretically secure computation*. CRYPTO'00, pages 74–92, 2000.
- [HSS11] Sean Hallgren, Adam Smith, and Fang Song. *Classical cryptographic protocols in a quantum world*. CRYPTO'11, pages 411–428, 2011.
- [KMQ11] Daniel Kraschewski and Jorn M uller-Quade. *Completeness theorems with constructive proofs for finite-deterministic 2-party functions*. TCC'11, pages 364–381, 2011.
- [MPR09] Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek. *Complexity of multi-party computation problems: The case of 2-party symmetric secure function evaluation*. TCC '09, pages 256–273, 2009.
- [MPR10] Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek. *A zero-one law for cryptographic complexity with respect to computational UC security*. CRYPTO'10, pages 595–612, 2010.
- [Sho97] PeterW. Shor. *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*. SIAM J. Comput., 26(5):1484–1509, 1997.
- [Unr10] Dominique Unruh. *Universally composable quantum multi-party computation*. EUROCRYPT'10, pages 486–505, 2010.