A New Post-Quantum Proof Framework

Ritam Bhaumik, EPFL

(joint work with Benoît Cogliati, Jordan Ethan, and Ashwin Jha)

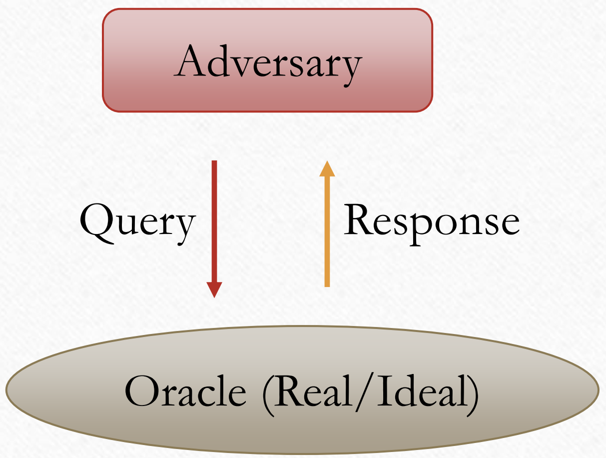
ASK 2023, Guangzhou
December 1, 2023

Clarification on 'Proofs'

- Proofs can mean many things in cryptography
  - Probabilistically Checkable Proofs
  - Proof of Work
  - Formal Verification
- Here we'll talk only about <u>reduction-based security proofs</u> for <u>indistinguishability games</u> involving <u>symmetric-key modes</u>

Proofs against Classical Adversaries

- **Step 1:** Write down all query-response pairs and call the resulting list the 'transcript'
- **Step 2:** Classify transcripts as bad and good
- **Step 3:** Compute probabilities of good transcripts in real and ideal worlds
- **Step 4:** Use some result from statistics to bound distinguishing advantage

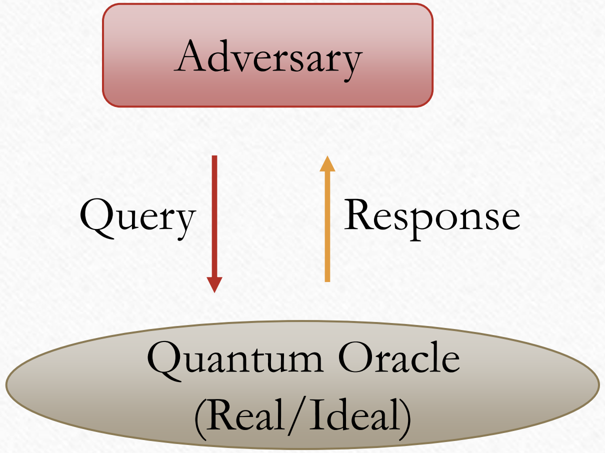


Proofs against Quantum Adversaries

- **Step 1:** Write down all query-response pairs and call the resulting list the 'transcript'

> Wait a minute, you can't do that!

~ Annoying Quantum People



Fundamental Obstacles

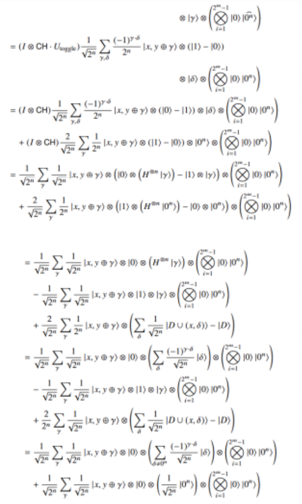
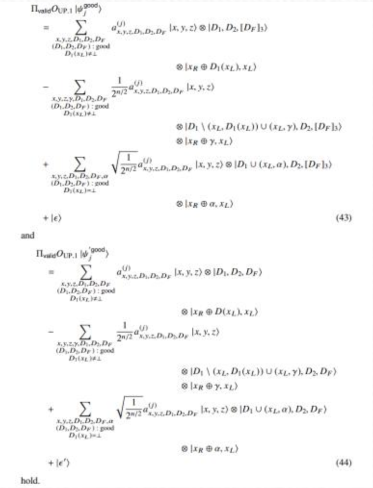
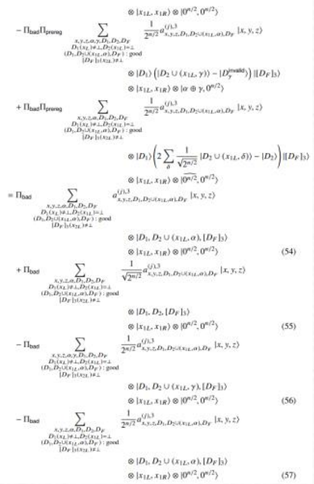
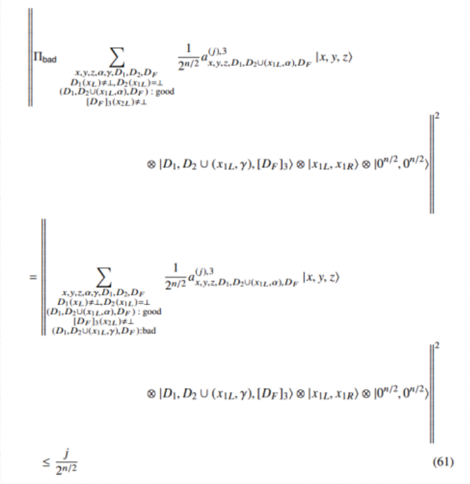
- Transcripts cannot be recorded
- Additional measurements not allowed
- ‘Uncomputing’ adds to complications

Enter ‘Compressed’ Oracles

- Proposed by Zhandry in 2019
- Achieves cool stuff like lazy sampling of a random function
- Can make it look like queries are being recorded in a database
- Indistinguishable from standard oracles

Hosoyamada-Iwata's Brave Approach

- Rewrite EVERYTHING in computational basis
- Wade through page after page of daunting computations

Drawbacks of HI approach

- Must keep track of numerous error terms
- Computations may become too tedious to verify to be convincing
- Bounds nowhere close to tight
- Overall loses the elegance of the compressed oracle approach

Chung et al. Framework

- Same goal: use classical reasoning on quantum games
- Uses computational basis to calculate some amplitude bounds
- Continues using Fourier basis otherwise
- Bounds probability of databases gaining certain ‘properties’
- Can be used for compact proofs of query lower-bounds

Combining the two

- Remain in the Fourier basis
- Create a two-world version of Chung et al.'s setup
- Retain HI's good database vs. bad database approach
- Adapt HI's central idea into Chung et al.'s framework:

Good databases evolve identically in either world.

Technical Details

Fourier Oracles

- Quantum Truth Table Representation

$$|f\rangle = \bigotimes_{x\in\mathcal{X}} |x\rangle\,|f(x)\rangle$$

- Standard Oracle

$$\mathsf{stO}\,|x\rangle\,|y\rangle \otimes \left|f\right\rangle = |x\rangle\,\left|y \oplus f(x)\right\rangle \otimes \left|f\right\rangle$$

- Fourier Oracle

$$\mathsf{stO}\,|x\rangle\,\left|\widehat{y}\right\rangle \otimes \left|\widehat{f}\,\right\rangle = |x\rangle\,\left|\widehat{y}\right\rangle \otimes \left|\widehat{f} + \widehat{\delta}_{xy}\right\rangle$$

Our Compressed Oracle

- Cell Compression Unitary

$$\mathsf{comp}_0 = |\bot\rangle\langle\widehat{0}| + |\widehat{0}\rangle\langle\bot| + \sum_{\widehat{y}\in\widehat{\mathcal{Y}}\setminus\{\widehat{0}\}} |\widehat{y}\rangle\langle\widehat{y}|$$

- Database Compression Unitary

$$\mathsf{comp} = \bigotimes_{\mathcal{X}} (I_m \otimes \mathsf{comp}_0)$$

- Compressed Oracle

$$\mathsf{cO} = (I_{m+n} \otimes \mathsf{comp}) \circ \mathsf{stO} \circ (I_{m+n} \otimes \mathsf{comp})$$

Transition Capacities

- A 'property' is any subset of databases, e. g., *has-a-collision*

Transition Capacity

A measure of the probability that a database in property P transitions into a database in property P' after a single query

- We borrow a useful transition capacity bound from Chung et al.
- This bound depends on the number of possible 'bad' responses

Two-Domain Systems

- Real and ideal domain to mimic distinguishing games
- Input domain mapped to the two domains via input-preparation maps

$$p_0 : \mathcal{I} \longrightarrow \widetilde{\mathcal{X}}_0, p_1 : \mathcal{I} \longrightarrow \widetilde{\mathcal{X}}_1$$

- Definitions of 'good' and 'bad' databases corresponding to each domain
- Domain-specific compressed oracles

$$\mathsf{cO}_0 \left|x\right\rangle \left|\widehat{y}\right\rangle \otimes \left|\widehat{d_0}\right\rangle = \left|x\right\rangle \left|\widehat{y}\right\rangle \otimes \mathsf{cO}_{p_0(x)\widehat{y}} \left|\widehat{d_0}\right\rangle$$

$$\mathsf{cO}_1 \left|x\right\rangle \left|\widehat{y}\right\rangle \otimes \left|\widehat{d_1}\right\rangle = \left|x\right\rangle \left|\widehat{y}\right\rangle \otimes \mathsf{cO}_{p_1(x)\widehat{y}} \left|\widehat{d_1}\right\rangle$$

Two-Domain Distance Bound

- Find a bijection between real and ideal good databases
- This should preserve 'evolution':

$$\langle d' | cO_{p_0(x)\hat{y}} | d \rangle = \langle h(d') | cO_{p_1(x)\hat{y}} | h(d) \rangle$$

- Trace distance between real and ideal final states bounded by

$$\left\llbracket \bot \overset{q}{\rightsquigarrow} \mathcal{B}_0 \right\rrbracket_0 + \left\llbracket \bot \overset{q}{\rightsquigarrow} \mathcal{B}_1 \right\rrbracket_1$$

- The big brackets denote cumulative transition capacities over q queries

Looking Ahead

- Our proof framework has a potential of developing into a go-to technique for doing post-quantum proofs for symmetric modes
- One limitation is that the compressed oracle can only replace PRFs, not SPRPs (where inverse calls are required as part of the mode's functionality)
- A concurrent publication has proposed a compressed permutation oracle to resolve this
- We are now working on integrating this permutation oracle into our proof framework
- If successful can greatly expand usability of framework
- Another possible future improvement: doing tighter security proofs

References

- Kai-Min Chung, Serge Fehr, Yu-Hsuan Huang, and Tai-Ning Liao, *On the compressed-oracle technique, and post-quantum security of proofs of sequential work*, EUROCRYPT 2021, Part II (Anne Canteaut and François-Xavier Standaert, eds.), LNCS, vol. 12697, Springer, Heidelberg, October 2021, pp. 598–629.
- Akinori Hosoyamada and Tetsu Iwata, *4-round Luby-Rackoff construction is a qPRP*, ASIACRYPT 2019, Part I (Steven D. Galbraith and Shiho Moriai, eds.), LNCS, vol. 11921, Springer, Heidelberg, December 2019, pp. 145–174.
- Mark Zhandry, *How to record quantum queries, and applications to quantum indifferentiability*, CRYPTO 2019, Part II (Alexandra Boldyreva and Daniele Micciancio, eds.), LNCS, vol. 11693, Springer, Heidelberg, August 2019, pp. 239–268.

Thank You!

https://eprint.iacr.org/2023/207

Judge a man by his questions, not by his answers.

~ Voltaire