On the Compressed-Oracle Technique, and Post-Quantum Security of Proofs of Sequential Work

Kai-Min Chung[1], Serge Fehr[2], Yu-Hsuan Huang[3], Tai-Ning Liao[4]

[1,3]Academia Sinica, Taiwan
[2]CWI Cryptology Group and Leiden University, The Netherlands
[4]National Taiwan University, Taiwan

Accpeted for publication at Eurocrypt 2021

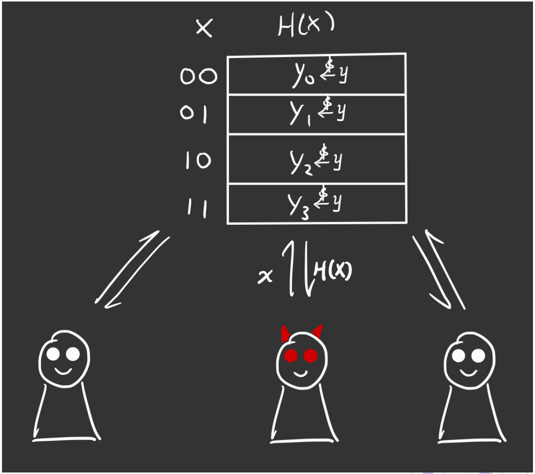
Overview

- (Quantum) Random Oracle Model
- Summary of Our Results
- Lazy Sampling Technique - Classical and Quantum
- Our Results in More Detail

Random Oracle Model:

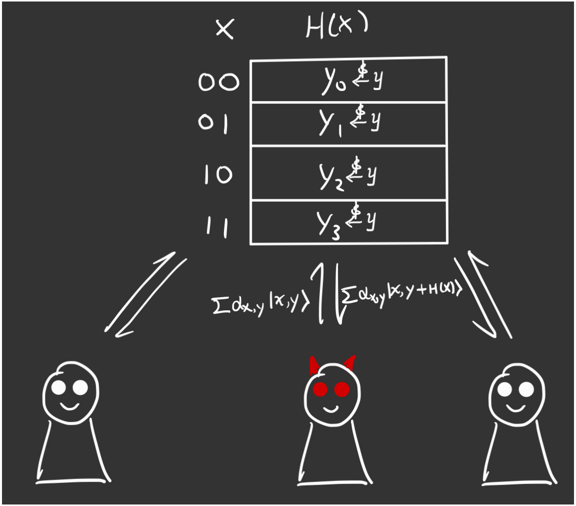
A way to analyze classical cryptographic schemes that use a hash function

$$\text{hash functions} \overset{\text{idealized}}{\approx} \begin{cases} \text{uniform sampled function,} \\ \text{everyone has access} \end{cases}$$

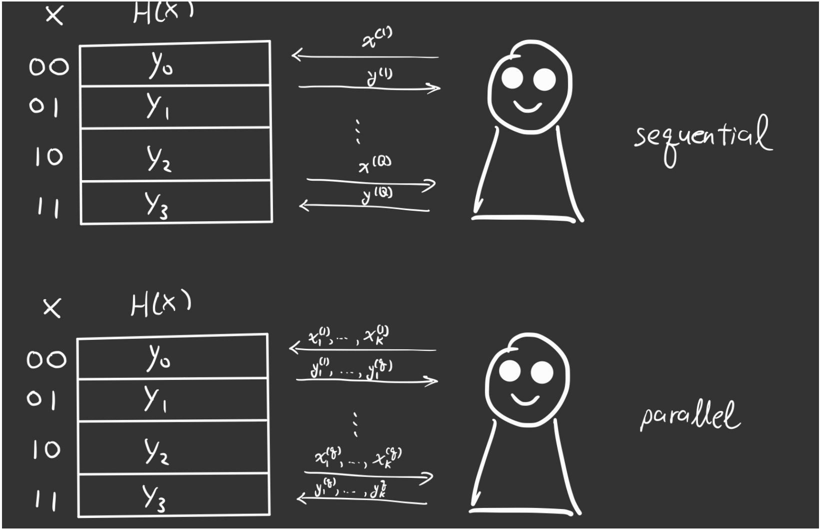


Quantum Random Oracle Model

$$\text{hash functions} \overset{\text{idealized}}{\approx} \begin{cases} \text{uniform sampled function,} \\ \text{everyone has quantum access} \end{cases}$$



(Q)ROM with Parallel Queries



A Typical Example Problem

0-preimage problem: finding x s.t. $H(x) = 0$,

- well-studied and understood classically and quantumly,
- e.g. running Grover's search in parallel is known to be optimal for parallel queries.

Another Example Problem

Hash-chain problem: finding $x_0, x_1, \ldots, x_q$ s.t. $x_{i+1} = H(x_i)$:

$$x_0 \stackrel{H}{\longmapsto} x_1 \stackrel{H}{\longmapsto} x_2 \stackrel{H}{\longmapsto} \cdots \stackrel{H}{\longmapsto} x_q$$

Another Example Problem

Hash-chain problem: finding $x_0, x_1, \ldots, x_q$ s.t. $x_{i+1} = H(x_i)$:

- easy with q sequential queries, but
- expected to be hard with $< q$ sequential queries,
- even if we can query k data points in parallel each round.

$$x_0 \xmapsto{H} x_1 \xmapsto{H} x_2 \xmapsto{H} \cdots \xmapsto{H} x_q$$

Another Example Problem

Hash-chain problem: finding $x_0, x_1, \ldots, x_q$ s.t. $x_{i+1} = H(x_i)$:

- easy with q sequential queries, but
- expected to be hard with $< q$ sequential queries,
- even if we can query k data points in parallel each round.

Easy to show classically (i.e. without quantum access).

- No quantum proof prior to our work.

$$x_0 \xmapsto{H} x_1 \xmapsto{H} x_2 \xmapsto{H} \cdots \xmapsto{H} x_q$$

Our Work

A framework for analyzing such problems in parallel QROM:

Our Work

A framework for analyzing such problems in parallel QROM:

Using our framework, one can

- prove **quantum** hardness using **classical** reasoning,
- by "lifting" the classical proof, if in suitable form,

Our Work

A framework for analyzing such problems in parallel QROM:

Using our framework, one can

- prove **quantum** hardness using **classical** reasoning,
- by "lifting" the classical proof, if in suitable form,
- Applied to various examples:
  - simplify existing proofs, e.g. 0-preimage,
  - obtain new bounds, e.g. collision, q-chain,
  - main application: first post-quantum security of proof of sequential work scheme by [Cohen and Pietrzak, 2018].

Our Work

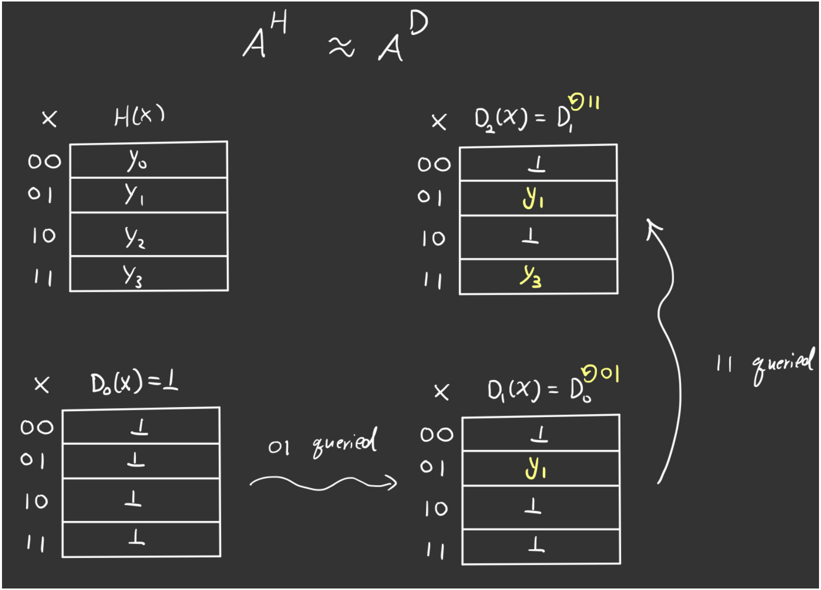
A framework for analyzing such problems in parallel QROM:

Using our framework, one can

- prove **quantum** hardness using **classical** reasoning,
- by “lifting” the classical proof, if in suitable form,
- Applied to various examples:
  - simplify existing proofs, e.g. 0-preimage,
  - obtain new bounds, e.g. collision, q-chain,
  - main application: first post-quantum security of proof of sequential work scheme by [Cohen and Pietrzak, 2018].

Independent and concurrent work: [Blocki et al., 2021].

Lazy Sampling



Lazy Sampling, Formally

Simulate RO H with a database D:

- formalized as a partial function $D : \mathcal{X} \to \mathcal{Y} \cup \{\perp\}$,
- initially $D_0(x) = \perp$ everywhere,
- each query $x \in \mathcal{X}$, if $D_i(x) = \perp$, update D_{i+1} at x to a random $y \in \mathcal{Y}$,
- after q queries, $D_q(x) \neq \perp$ for $\leq q$ values of x.

Lazy Sampling, Formally

Simulate RO H with a database D:

- formalized as a partial function $D : \mathcal{X} \to \mathcal{Y} \cup \{\perp\}$,
- initially $D_0(x) = \perp$ everywhere,
- each query $x \in \mathcal{X}$, if $D_i(x) = \perp$, update D_{i+1} at x to a random $y \in \mathcal{Y}$,
- after q queries, $D_q(x) \neq \perp$ for $\leq q$ values of x.

Important (example) observation:
if there's no $x \in \mathcal{X}$ s.t. $D_q(x) = 0$, then

- the adversary $\mathcal{A}$ is unlikely to output x s.t. $H(x) = 0$,
- best guess: some x s.t. $D_q(x) = \perp$,
- sucess probability $\leq 1/\#\mathcal{Y}$.

Lazy Sampling, Formally

Simulate RO H with a database D:

- formalized as a partial function $D : \mathcal{X} \to \mathcal{Y} \cup \{\perp\}$,
- initially $D_0(x) = \perp$ everywhere,
- each query $x \in \mathcal{X}$, if $D_i(x) = \perp$, update D_{i+1} at x to a random $y \in \mathcal{Y}$,
- after q queries, $D_q(x) \neq \perp$ for $\leq q$ values of x.

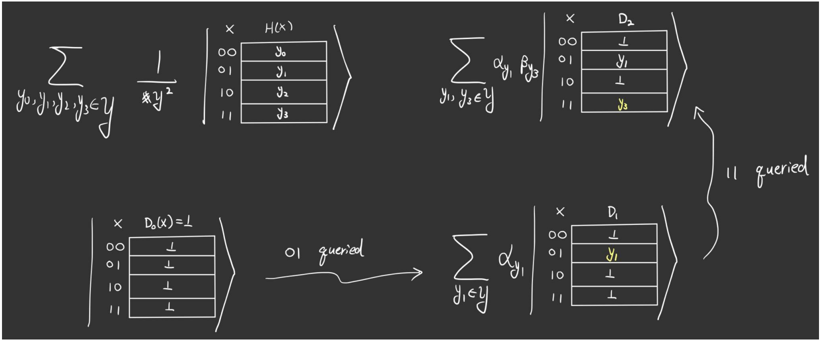
Important (example) observation:
if there's no $x \in \mathcal{X}$ s.t. $D_q(x) = 0$, then

- the adversary $\mathcal{A}$ is unlikely to output x s.t. $H(x) = 0$,
- best guess: some x s.t. $D_q(x) = \perp$,
- sucess probability $\leq 1/\#\mathcal{Y}$.

$$\Pr\left[\mathcal{A}^H \to x \text{ s.t. } H(x) = 0\right] \leq \Pr\left[\exists x \in \mathcal{X} \text{ s.t. } D_q(x) = 0\right] + 1/\#\mathcal{Y}$$

Quantum Lazy Sampling

(A way to understand Zhandry's "compressed oracle" [Zhandry, 2019])



Quantum Lazy Sampling

Similarly, QRO can be simulated quantumly s.t.[1]

- the state of database is a **superposition** $\sum \alpha_D |D\rangle$ of partial functions $D : \mathcal{X} \to \mathcal{Y} \cup \{\perp\}$ with $\leq q$ non-$\perp$ entries after q queries.

[1] This simulation is non-obvious, but is a way to understand the compressed oracle technique[Zhandry, 2019]

Quantum Lazy Sampling

Similarly, QRO can be simulated quantumly s.t.[1]

- the state of database is a **superposition** $\sum \alpha_D |D\rangle$ of partial functions $D : \mathcal{X} \to \mathcal{Y} \cup \{\perp\}$ with $\leq q$ non-$\perp$ entries after q queries.

Similar (example) property:
if there's no x s.t. $D_q(x) = 0$, where D_q now is obtained by **measuring** the database state, then

- the adversary $\mathcal{A}$ is unlikely to output x s.t. $H(x) = 0$,

[1] This simulation is non-obvious, but is a way to understand the compressed oracle technique[Zhandry, 2019]

Quantum Lazy Sampling

Similarly, QRO can be simulated quantumly s.t.[1]

- the state of database is a **superposition** $\sum \alpha_D |D\rangle$ of partial functions $D : \mathcal{X} \to \mathcal{Y} \cup \{\perp\}$ with $\leq q$ non-$\perp$ entries after q queries.

Similar (example) property:
if there's no x s.t. $D_q(x) = 0$, where D_q now is obtained by **measuring** the database state, then

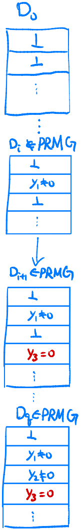
- the adversary $\mathcal{A}$ is unlikely to output x s.t. $H(x) = 0$,
- except with a small error bounded as follows.

$$\sqrt{\Pr\left[\mathcal{A}^H \to x \text{ s.t. } H(x) = 0\right]} \leq \sqrt{\Pr\left[\exists x \in \mathcal{X} \text{ s.t. } D_q(x) = 0\right]} + \sqrt{1/\#\mathcal{Y}}$$

[1] This simulation is non-obvious, but is a way to understand the compressed oracle technique[Zhandry, 2019]

Toy Example, and Its classical Analysis (for now)

How to bound $\Pr[D_q \in \mathsf{PRMG}]$, where $\mathsf{PRMG} := \{D \mid \exists x \text{ s.t. } D(x) = 0\}$?

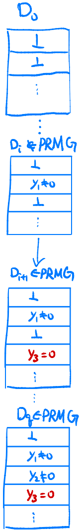


Toy Example, and Its classical Analysis (for now)

How to bound $\Pr[D_q \in \mathsf{PRMG}]$, where $\mathsf{PRMG} := \{D | \exists x \text{ s.t. } D(x) = 0\}$?

1. $\Pr[D_q \in \mathsf{PRMG}] \leq \sum_i \Pr[D_i \in \mathsf{PRMG} | D_{i-1} \notin \mathsf{PRMG}]$

$$\leq q \left[\neg\mathsf{PRMG} \xrightarrow{k} \mathsf{PRMG} \right]$$ ("transition capacity")



Toy Example, and Its classical Analysis (for now)

How to bound $\Pr[D_q \in \mathsf{PRMG}]$, where $\mathsf{PRMG} := \{D \mid \exists x \text{ s.t. } D(x) = 0\}$?

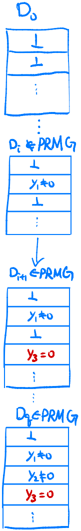
1. $\Pr[D_q \in \mathsf{PRMG}] \leq \sum_i \Pr[D_i \in \mathsf{PRMG} \mid D_{i-1} \notin \mathsf{PRMG}]$

   $$\leq q \left[\neg\mathsf{PRMG} \xrightarrow{k} \mathsf{PRMG} \right] \quad \text{(“transition capacity”)}$$

2. Observe

   $$D_{i-1} \notin \mathsf{PRMG} \text{ and } D_i \in \mathsf{PRMG}$$
   $$\Downarrow$$
   $$\exists j : D_i(x_j) = 0 \neq D_{i-1}(x_j).$$

   Thus, $\left[\neg\mathsf{PRMG} \xrightarrow{k} \mathsf{PRMG} \right] \leq k / \#\mathcal{Y}$,



Toy Example, and Its classical Analysis (for now)

How to bound $\Pr[D_q \in \mathrm{PRMG}]$, where $\mathrm{PRMG} := \{D \mid \exists x \text{ s.t. } D(x) = 0\}$?

1. $\Pr[D_q \in \mathrm{PRMG}] \leq \sum_i \Pr[D_i \in \mathrm{PRMG} \mid D_{i-1} \notin \mathrm{PRMG}]$

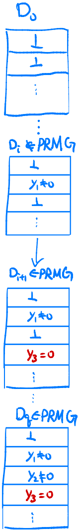
   $$\leq q \left[\neg\mathrm{PRMG} \xrightarrow{k} \mathrm{PRMG} \right] \quad \text{(“transition capacity”)}$$

2. Observe

   $$D_{i-1} \notin \mathrm{PRMG} \text{ and } D_i \in \mathrm{PRMG}$$
   $$\Downarrow$$
   $$\exists j : D_i(x_j) = 0 \neq D_{i-1}(x_j).$$

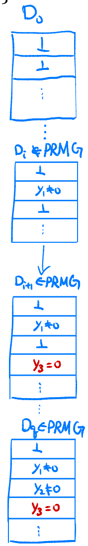
   Thus, $\left[\neg\mathrm{PRMG} \xrightarrow{k} \mathrm{PRMG} \right] \leq k/\#\mathcal{Y}$,

All together: $\Pr[D_q \in \mathrm{PRMG}] \leq q \cdot k/\#\mathcal{Y}$.



Toy Example, and Its classical Analysis (for now)

How to bound $\Pr[D_q \in \mathrm{PRMG}]$, where $\mathrm{PRMG} := \{D | \exists x \text{ s.t. } D(x) = 0\}$?



1. $\Pr[D_q \in \mathrm{PRMG}] \leq \sum_i \Pr[D_i \in \mathrm{PRMG} | D_{i-1} \notin \mathrm{PRMG}]$

$$\leq q \left[\neg\mathrm{PRMG} \xrightarrow{k} \mathrm{PRMG} \right] \quad \text{(“transition capacity”)}$$

2. Observe[2]

$$D_{i-1} \notin \mathrm{PRMG} \text{ and } D_i \in \mathrm{PRMG}$$

$$\Downarrow$$

$$\exists j : D_i(x_j) = 0 \neq D_{i-1}(x_j).$$

Thus, $\left[\neg\mathrm{PRMG} \xrightarrow{k} \mathrm{PRMG} \right] \leq k / \#\mathcal{Y}$,

All together: $\Pr[D_q \in \mathrm{PRMG}] \leq q \cdot k / \#\mathcal{Y}$.

[2]Terminology: “transition is (strongly) **recognizable** by **local properties** $\mathcal{L}_j = \{0\}$.”

High-level Recipe of The Proof

1. Decompose into sum of **transition capacities**:

$$\Pr[D_q \in \mathsf{P}] \leq \sum_i \left[\, \neg \mathsf{P}_{i-1} \xrightarrow{k} \mathsf{P}_i \,\right] \; (= q \cdot \left[\, \neg \mathsf{P} \xrightarrow{k} \mathsf{P} \,\right] \text{ for } \mathsf{P}_i = \mathsf{P}).$$

2. Bound the transition capacities by **local properties**

$$\left[\, \neg \mathsf{P}_{i-1} \xrightarrow{k} \mathsf{P}_i \,\right] \leq \sum_j \Pr[\mathsf{UNIF} \in \mathcal{L}_j],$$

that **recognize** the transition.

Our framework:
same recipe, different definition of transition capacity $[\![\cdot \to \cdot]\!]$, adjusted formulas:

1. $\sqrt{\Pr[D_q \in \mathsf{P}]} \leq \sum [\![\neg \mathsf{P}_{i-1} \xrightarrow{k} \mathsf{P}_i]\!]$,
2. $[\![\neg \mathsf{P}_{i-1} \xrightarrow{k} \mathsf{P}_i]\!] \leq \sqrt{10 \sum_j \Pr[\mathsf{UNIF} \in \mathcal{L}_j]}$ (same classical probabilities)

   (or $\leq e \sum_j \sqrt{10 \Pr[\mathsf{UNIF} \in \mathcal{L}_j]}$ in case of weak recognizability)

The 0-Preimage Example - Now Quantum

From classical analysis:

local properties $\mathcal{L}_j = \{0\}$ with $\Pr[\mathsf{UNIF} \in \mathcal{L}_j] = \frac{1}{\#\mathcal{Y}}$.

Our framework, Eq. 2:

$$[\![\neg\mathsf{PRMG} \xrightarrow{k} \mathsf{PRMG}]\!] \leq \sqrt{10 \sum_j \Pr[\mathsf{UNIF} \in \mathcal{L}_j]} \leq \sqrt{\frac{10k}{\#\mathcal{Y}}}.$$

Our framework, Eq. 1:

$$\sqrt{\Pr[D_q \in \mathsf{PRMG}]} \leq q \cdot [\![\neg\mathsf{PRMG} \xrightarrow{k} \mathsf{PRMG}]\!] \leq q\sqrt{\frac{10k}{\#\mathcal{Y}}}.$$

All together (reconfirming optimality of parallel Grover).

$$\Pr[D_q \in \mathsf{PRMG}] \leq \frac{10q^2k}{\#\mathcal{Y}}.$$

The 0-Preimage Example - Now Quantum

From classical analysis:

local properties $\mathcal{L}_j = \{0\}$ with $\Pr[\mathsf{UNIF} \in \mathcal{L}_j] = \frac{1}{\#\mathcal{Y}}$.

Our framework, Eq. 2:

$$[\![\neg\mathsf{PRMG} \xrightarrow{k} \mathsf{PRMG}]\!] \leq \sqrt{10 \sum_j \Pr[\mathsf{UNIF} \in \mathcal{L}_j]} \leq \sqrt{\frac{10k}{\#\mathcal{Y}}}.$$

Our framework, Eq. 1:

$$\sqrt{\Pr[D_q \in \mathsf{PRMG}]} \leq q \cdot [\![\neg\mathsf{PRMG} \xrightarrow{k} \mathsf{PRMG}]\!] \leq q\sqrt{\frac{10k}{\#\mathcal{Y}}}.$$

All together (reconfirming optimality of parallel Grover).

$$\Pr[D_q \in \mathsf{PRMG}] \leq \frac{10q^2k}{\#\mathcal{Y}}.$$

No need to understand definition of $[\![\cdot \to \cdot]\!]$. We can simply "lift" classical proof.

Additional Results

By the same recipe, we obtain several additional (new) results:

Q=kq	coarse-grained	fine-grained	algorithms
0-preimage	$O\left(\frac{Q^2}{\#\mathcal{Y}}\right)$	$O\left(\frac{kq^2}{\#\mathcal{Y}}\right)$	$\Omega\left(\frac{kq^2}{\#\mathcal{Y}}\right)$
collision	$O\left(\frac{Q^3}{\#\mathcal{Y}}\right)$	$O\left(\frac{k^2q^3}{\#\mathcal{Y}}\right)$	$\Omega\left(\frac{k^2q^3}{\#\mathcal{Y}}\right)$
q-chain	not applicable	$O\left(\frac{k^3q^3}{\#\mathcal{Y}}\right)$	?

[3]

[3] the red color bounds are our new results

A More Complex Application: PoSW

We proved the **post-quantum** security of non-interactive PoSW constructed by [Cohen and Pietrzak, 2018].

$$\mathrm{Adv} \leq O\left(k^2 q^2 \left(\frac{q+2}{2^{n+1}}\right)^t + \frac{k^3 q^3 n}{\#\mathcal{Y}} + \frac{tn}{\#\mathcal{Y}}\right)$$

- q query rounds with k query points per round,
- n, t security parameters.

A More Complex Application: PoSW

We proved the **post-quantum** security of non-interactive PoSW constructed by [Cohen and Pietrzak, 2018].

$$\mathrm{Adv} \le O\left(k^2 q^2 \left(\frac{q+2}{2^{n+1}}\right)^t + \frac{k^3 q^3 n}{\#\mathcal{Y}} + \frac{tn}{\#\mathcal{Y}}\right)$$

- q query rounds with k query points per round,
- n, t security parameters.

Technical challenge:

- PoSW scheme **intertwines several problems** (collision, q-chain, and more)
- Need tools to **decompose** complicated transition capacities.

Calculus for Capacities

We give basic rules to manipulate quantum transition capacities:

- $[\![P \xrightarrow{k} Q]\!] = [\![Q \xrightarrow{\mathrm{k}} P]\!]$,
- $\max\{[\![Q \xrightarrow{k} P]\!], [\![Q \xrightarrow{k} P']\!]\} \leq [\![Q \xrightarrow{\mathrm{k}} P \cup P']\!] \leq [\![Q \xrightarrow{\mathrm{k}} P]\!] + [\![Q \xrightarrow{\mathrm{k}} P]\!]$,
- $[\![P \cap Q \xrightarrow{k} P']\!] \leq \min\{[\![P \xrightarrow{k} P']\!], [\![Q \xrightarrow{\mathrm{k}} P']\!]\}$.

Calculus for Capacities

We give basic rules to manipulate quantum transition capacities:

- $[\![\mathsf{P} \xrightarrow{k} \mathsf{Q}]\!] = [\![\mathsf{Q} \xrightarrow{\mathsf{k}} \mathsf{P}]\!]$,
- $\max\{ [\![\mathsf{Q} \xrightarrow{k} \mathsf{P}]\!], [\![\mathsf{Q} \xrightarrow{k} \mathsf{P}']\!] \} \leq [\![\mathsf{Q} \xrightarrow{\mathsf{k}} \mathsf{P} \cup \mathsf{P}']\!] \leq [\![\mathsf{Q} \xrightarrow{\mathsf{k}} \mathsf{P}]\!] + [\![\mathsf{Q} \xrightarrow{\mathsf{k}} \mathsf{P}]\!]$,
- $[\![\mathsf{P} \cap \mathsf{Q} \xrightarrow{k} \mathsf{P}']\!] \leq \min\{ [\![\mathsf{P} \xrightarrow{k} \mathsf{P}']\!], [\![\mathsf{Q} \xrightarrow{\mathsf{k}} \mathsf{P}']\!] \}$.

But also more involved ones, e.g.

$$[\![\neg \mathsf{P}_0 \xrightarrow{k} \mathsf{P}_n]\!] \leq \sum_i \left([\![\neg \mathsf{P}_0 \xrightarrow{\bar{k}_i} \neg \mathsf{Q}]\!] + [\![\mathsf{Q} \backslash \mathsf{P}_{i-1} \xrightarrow{k_i} \mathsf{Q} \cap \mathsf{P}_i]\!], \right)$$

where $k = k_1 + \cdots + k_n$ and $\bar{k}_i = k_1 + \cdots + k_i$.

Calculus for Capacities

We give basic rules to manipulate quantum transition capacities:

- $[\![\mathsf{P} \xrightarrow{k} \mathsf{Q}]\!] = [\![\mathsf{Q} \xrightarrow{\mathsf{k}} \mathsf{P}]\!]$,
- $\max\{[\![\mathsf{Q} \xrightarrow{k} \mathsf{P}]\!], [\![\mathsf{Q} \xrightarrow{k} \mathsf{P}']\!]\} \leq [\![\mathsf{Q} \xrightarrow{\mathsf{k}} \mathsf{P} \cup \mathsf{P}']\!] \leq [\![\mathsf{Q} \xrightarrow{\mathsf{k}} \mathsf{P}]\!] + [\![\mathsf{Q} \xrightarrow{\mathsf{k}} \mathsf{P}]\!]$,
- $[\![\mathsf{P} \cap \mathsf{Q} \xrightarrow{k} \mathsf{P}']\!] \leq \min\{[\![\mathsf{P} \xrightarrow{k} \mathsf{P}']\!], [\![\mathsf{Q} \xrightarrow{\mathsf{k}} \mathsf{P}']\!]\}$.

But also more involved ones, e.g.

$$[\![\neg \mathsf{P}_0 \xrightarrow{k} \mathsf{P}_n]\!] \leq \sum_i \left([\![\neg \mathsf{P}_0 \xrightarrow{\bar{k}_i} \neg \mathsf{Q}]\!] + [\![\mathsf{Q} \backslash \mathsf{P}_{i-1} \xrightarrow{k_i} \mathsf{Q} \cap \mathsf{P}_i]\!], \right)$$

where $k = k_1 + \cdots + k_n$ and $\bar{k}_i = k_1 + \cdots + k_i$.

Allow to work with $[\![\cdot \to \cdot]\!]$ on an abstract level, without understanding the definition.

Recap

By means of

- abstracting away technical aspects of Zhandry's compressed oracle technique, and
- proving new technical results for parallel queries.

We offer a framework that, when applicable,

- proves query-complexity bounds in the parallel-query QROM,
- using **purely classical** means, by "lifting" corresponding classical proofs.

Applied to different example problems:

recover known results, find new results.

That's It

Thanks for your listening!

Arxiv. 2010.11658

Eprint. 2020/1305

References I

Blocki, J., Lee, S., and Zhou, S. (2021).
On the security of proofs of sequential work in a post-quantum world.
In 2nd Conference on Information-Theoretic Cryptography (ITC 2021). Schloss Dagstuhl-Leibniz-Zentrum für Informatik.

Cohen, B. and Pietrzak, K. (2018).
Simple proofs of sequential work.
In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pages 451–467. Springer.

References II

Zhandry, M. (2019).
How to record quantum queries, and applications to quantum indifferentiability.
In Boldyreva, A. and Micciancio, D., editors, Advances in Cryptology - CRYPTO 2019, volume 11693 of Lecture Notes in Computer Science, pages 239–268. Springer.