

Quantum pseudorandomness in Algorithmica, and its implications to cryptography and complexity

Luowen Qian

Boston University

Joint work with William Kretschmer (UT Austin),
Makrand Sinha (Simons Institute and UC Berkeley),
Avishay Tal (UC Berkeley)



Minimal Complexity Assumption for Cryptography

What is the minimal complexity assumption for cryptography?




Why do we need complexity assumptions for cryptography?

Why do we need complexity assumption for useful cryptographic task X under a realistic model until 1989?

For most X against polynomially bounded adversaries, we need one-way functions, thus at least $P \neq NP$ (very hard!)



The dawn of a new era for quantum cryptography:
The experimental prototype is working!



Transmitter
LA1
GM1
CAM1
FSM

THORLABS
Discovery

LASER RADIATION
DO NOT STARE INTO BEAM
CLASS 2 LASER PRODUCT

HWP
PBS
DM2
HWP
OWP



Why do we need complexity
assumption for useful
cryptographic task X under a
realistic model after 1989?

Information theoretic security is still unachievable

- Commitment, OT, ...
- Encryption of long messages
- Authentication of long messages
- ...

QKD is the exception!

For which cryptographic tasks do we still need $P \neq NP$?

(unknown)

Oracle separations (informal)



Theorem [Kretschmer, Q, Sinha, Tal'23]: It is possible to construct an oracle world where $P = NP$ (Algorithmica) but computationally secure quantum cryptography is still possible

- Quantum pseudorandomness
- (EFI) Commitments, OT, zero knowledge, MPC, undecodable black-holes [earlier talks today]

(this rules out relativizing proof techniques for proving quantum cryptography implies $P \neq NP$)

Pseudorandom States (PRS)

[Ji, Liu, Song'18; Morimae, Yamakawa'22]

A quantum algorithm G is an (single-copy secure [MY22]) n -qubit PRS generator if:

- Efficient generation

- Takes as input $k \in \{0, 1\}^\lambda$
- Runs in $\text{poly}(\lambda)$ time
- Outputs a pure state $|\psi_k\rangle\langle\psi_k|$ of $n(\lambda) > \lambda$ qubits

Just as classically, this guarantees non-triviality + “statistical fairness” in EFI

- Pseudorandomness:

- $|\psi_k\rangle$ is computationally indistinguishable from random, i.e., $\forall \text{QPT}_\lambda A$,
$$\left| \Pr_{k \leftarrow \{0,1\}^\lambda} [A(|\psi_k\rangle) = 1] - \Pr_{x \leftarrow \{0,1\}^{n(\lambda)}} [A(|x\rangle) = 1] \right| \leq \text{negl}(\lambda)$$

Many-copy security: [JLS18] indistinguishable from a Haar random state for any polynomial number of copies

How is separation possible?

- “QMA” adversary for breaking PRS
 - Merlin sends the pseudorandom seed/key k
 - Arthur checks that the input *state* is $|\psi_k\rangle$
- Issue: an instance of a QMA language must be a classical bitstring
 - NP (or even QMA) only considers solving classical problems (with a quantum computer)



Oracle separations (formal)

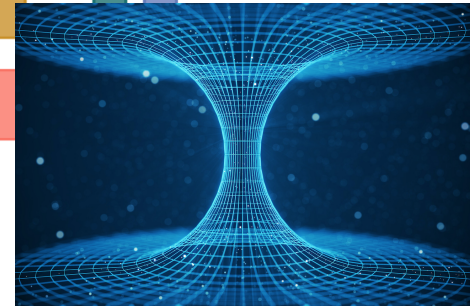
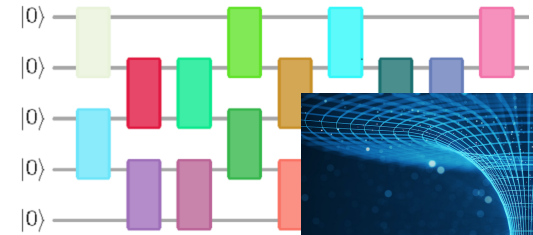
- In the black-box setting, post-quantum OWF \Rightarrow PRS \Rightarrow EFI & friends
- **Theorem** [Kretschmer, Q, Sinha, Tal'23]:
There is a classical oracle relative to which single-copy-secure PRS exists but $P = NP$ (Algorithmica), in fact $P = PH$
- **Theorem** [Kretschmer'21]:
There is a *quantum* oracle relative to which *many-copy-secure* PRS exists but $BQP = QMA$

Why isn't K21 conclusive?

1. Somewhat cheating: OWFs can never use a quantum oracle!
2. Quantum oracle separations rule out fewer proof techniques
[Aaronson'09]
3. Instantiations are unclear: K21 uses a Haar random oracle
(constructing pseudorandom unitaries is open [JLS18])
4. KQST23 gets $P = NP$ (Algorithmica) instead of $BQP = QMA$ in K21
(technically incomparable)

Quantum cryptography candidates without OWF

- Kawachi, Koshihara, Nishimura, Yamakami'05: hardness of quantum state distinguishability problem for a family of permutation states (implied by hardness of graph automorphism)
- (Quantum) *auxiliary input* EFI from complexity separations
 - Chailloux, Kerenidis, Rosgen'11: $\text{QMA} \neq \text{QIP}$
 - Brakerski, Canetti, Q'23: $\text{BQP} \neq \text{QCZK}$
- Folklore: random quantum circuits generate PRS?
- Bouland, Fefferman, Vazirani'20: wormholes generate PRS?
- **This work:** *first* nontrivial PRS construction separated from OWFs



Starting point: binary phase PRS

Input seed: $k \in \{0, 1\}^\lambda$ Boolean function $f_k: \{0, 1\}^n \rightarrow \{0, 1\}$

$$|0\rangle^{\otimes n} \xrightarrow{H^{\otimes n}} |+\rangle^{\otimes n} \xrightarrow{U_{f_k}} \sum_{x \in \{0, 1\}^n} (-1)^{f_k(x)} |x\rangle$$

- Proposed in [JLS18]; proven secure if $\{f_k\}$ is random oracle/PRF [Brakerski, Shmueli'19]
- Maybe still secure for some $\{f_k\}$ even if $P = NP$?
- If $P = NP$, then binary phase PRS is broken for all efficient $\{f_k\}$ [K21]

Hadamard/phase cocktail construction



t -Forrelation state for $f_1, \dots, f_t: U_{f_t}H \cdots U_{f_2}H U_{f_1}H |0\rangle^{\otimes n}$

- For a random oracle H , the 1-Forrelation state with $f_1 = H(k, \cdot)$ is PRS against BQP (restating binary phase PRS)
- 2-Forrelation state with $f_i = H(k, i, \cdot)$ is single-copy secure PRS against BQP^{PH} [KQST23]
- Under a t -Forrelation conjecture, the t -Forrelation state with $f_i = H(k, i, \cdot)$ is PRS against BQP^{PH} [KQST23]

Forrelation problem [Aaronson'09]

Given functions f and $g: \{0, 1\}^n \rightarrow \{0, 1\}$, distinguish whether

1. Fourier transform of f is correlated with g
2. f, g are uniformly random

- Forrelation is easy for BQP [Aaronson'09]
- Forrelation is hard on average against PH [Raz, Tal'18]
- OR ◦ Forrelation is hard on average against BQP^{PH} [Aaronson, Ingram, Kretschmer'22]



Hardness of shifted Forrelation

H is hard to find shifted Forrelation, if given quantum query access to h , it is hard to decide if h is sampled such that

1. $\exists k$ such that $H(k, 0, \cdot)$ is Forrelated with $H(k, 1, \cdot) \oplus h$
Fourier transform of $H(k, 0, x)$ is correlated with $H(k, 1, x) \oplus h(x)$
2. h is a random function

- Hardness implies single-copy security of 2-Forrelation state for H
- Random oracles satisfy this BQP^{PH} hardness by reduction to (a variant of) BQP^{PH} average-case hardness of $\text{OR} \circ \text{Forrelation}$ (we define and analyze a new discretely defined Forrelation distribution)

Implications for cryptography

- A new hardness property for a (classical) hash function (hardness of shifted Forrelation)
 - Useful for constructing quantum cryptography
 - Plausible as it holds for a random function
 - Weaker than $P \neq NP$ or even $P \neq PH$ (in the black-box setting)
- Instantiating 2-Forrelation state with cryptographic hash like SHA-3 is plausibly secure even if $P = PH$

We don't feel so good...



Does cryptography need complexity assumptions?

- K21+KQST23: at least appears independent of Impagliazzo's 5 worlds
 - MPC, encryption, authentication, ...
- Many-copy secure PRS implies $BQP \neq PP$ [K21]
- Any computational (even quantumly) falsifiable assumption implies a “unitary version of $P \neq PSPACE$ ” [Metger, Yuen'23; upcoming work]

Open:

- Does single-copy secure PRS imply (decisional) $P \neq PSPACE$?
- Can we prove quantum cryptography exists, or are there other barriers?

Cryptographer Workshops



Simons Auditorium

Lets summon a
~~demon~~

new cryptographic assumption

Omg this is
gonna be so fun

Cryptanalyst Workshops



WHO KEEPS
SUMMONING THEM

Ran Canetti Prize

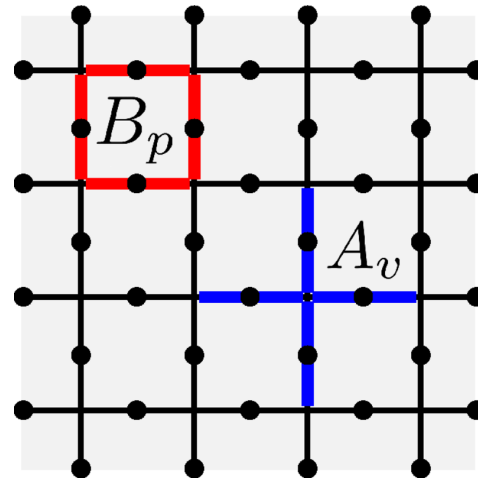
Give a simple candidate instantiation (not SHA-x) of 2-Forrelation state without one-way functions

Rewards:



(Meta-)complexity for quantum tasks

- There are natural computational tasks with quantum inputs/outputs not captured by our current complexity theory
 - Breaking quantum cryptography
 - Decoding results of a quantum experiment [Aharonov, Cotler, Qi'22]
 - Ground state preparation, tomography, quantum error correction, decoding black hole radiation...



(Meta-)complexity for quantum tasks

- There are natural computational tasks with quantum inputs/outputs not captured by our current complexity theory
- These separations motivate the study of (meta-)complexity for quantum tasks, as they cannot be reduced to studying solving classical (decisional) problems!
 - Many-copy secure PRS implies MCSP for quantum states is hard [K21]
 - Thus, MCSP for quantum states could be hard even if $BQP = QMA$
- We may need a framework to talk about the complexity of these computational tasks!

(Meta-)complexity for quantum tasks

“Computational complexity traditionally has tried to get ahead of new technologies, and modelled randomized, parallel, quantum computation and cryptography in the infancy of their development allowing complexity to help guide our understanding and development of these areas...

“Complexity theory also ought to reckon that practically we seem to be getting the best of $P = NP$ while avoiding losing cryptography simultaneously in Heuristica and Cryptomania among Russell's five worlds...perhaps it's time to rethink the models.”—Fortnow

<https://blog.computationalcomplexity.org/2023/04/my-week-at-simons.html> (retrieved Apr 25, 2023)

Past, present & future of quantum complexity

- Aaronson's lecture notes in Barbados (2016)
- Quantum search-to-decision reductions
[Irani, Rao, Natarajan, Nirkhe, Yuen'21]
- Quantum algorithmic measurements [ACQ22]
- $\text{stateQIP} = \text{statePSPACE}$ [Rosenthal, Yuen'22; MY23]
- Hopefully many more exciting new works coming soon 😊

Thank you! Questions?