# Quantum Cryptography in Algorithmica

**August 14, 2023**

William Kretschmer, Luowen Qian,
Makrand Sinha, Avishay Tal

arXiv:2212.00879

# Introduction

| | |
|---|---|
| **Algorithmica** | $\mathsf{P} = \mathsf{NP}$ |
| **Heuristica** | $\mathsf{P} \neq \mathsf{NP}$ but $\mathsf{DistNP} \subseteq \mathsf{AvgP}$ |
| **Pessiland** | $\mathsf{DistNP} \not\subseteq \mathsf{AvgP}$ but $\nexists$ OWFs |
| **Minicrypt** | $\exists$ OWFs but $\nexists$ PKE |
| **Cryptomania** | $\exists$ PKE |

| | |
|---|---|
| **Algorithmica** | $\mathsf{P} = \mathsf{NP}$ |
| **Heuristica** | $\mathsf{P} \neq \mathsf{NP}$ but $\mathsf{DistNP} \subseteq \mathsf{AvgP}$ |
| **Pessiland** | $\mathsf{DistNP} \not\subseteq \mathsf{AvgP}$ but $\nexists$ OWFs |
| **Minicrypt** | $\exists$ OWFs but $\nexists$ PKE |
| **Cryptomania** | $\exists$ PKE |

**Definition**

$f : \{0,1\}^n \to \{0,1\}^m$ is *one-way* if:

- $f$ efficiently computable
- For all poly-time $\mathcal{A}$:

$$\Pr_{x \sim \{0,1\}^n}[f(\mathcal{A}(f(x))) = f(x)] \leq \text{negl}(n)$$

## Definition

$f : \{0,1\}^n \to \{0,1\}^m$ is *one-way* if:

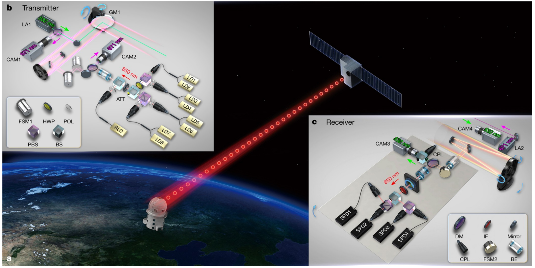
- $f$ efficiently computable
- For all poly-time $\mathcal{A}$:

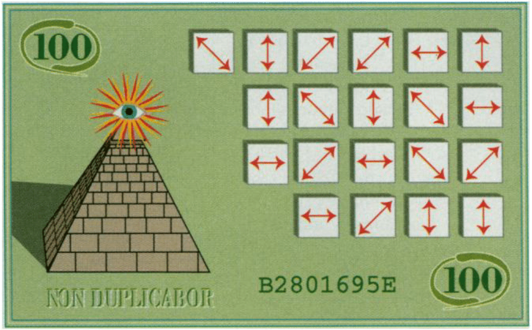
$$\Pr_{x \sim \{0,1\}^n}[f(\mathcal{A}(f(x))) = f(x)] \leq \text{negl}(n)$$

**Necessary** and **sufficient** for lots of classical cryptography

# Are OWFs **necessary** in a quantum world?

# Are OWFs **necessary** in a quantum world?



But most tasks still **require** computational assumptions, even quantumly:

But most tasks still **require** computational assumptions, even quantumly:

- Symmetric-key encryption

But most tasks still **require** computational assumptions, even quantumly:

- Symmetric-key encryption
- Commitment schemes

But most tasks still **require** computational assumptions, even quantumly:

- Symmetric-key encryption
- Commitment schemes
- Digital signatures

But most tasks still **require** computational assumptions, even quantumly:

- Symmetric-key encryption
- Commitment schemes
- Digital signatures
- Publicly-verifiable quantum money

But most tasks still **require** computational assumptions, even quantumly:

- Symmetric-key encryption
- Commitment schemes
- Digital signatures
- Publicly-verifiable quantum money
- Quantum copy-protected software

But most tasks still **require** computational assumptions, even quantumly:

- Symmetric-key encryption
- Commitment schemes
- Digital signatures
- Publicly-verifiable quantum money
- Quantum copy-protected software
- . . .

## Definition (Ji-Liu-Song 2018)

$\{|\varphi_k\rangle\}_{k\in\{0,1\}^\kappa}$ is *pseudorandom* if:

- Efficient generation of $|\varphi_k\rangle$ given $k \in \{0,1\}^\kappa$
- For all poly-time $\mathcal{A}$ and $T = \text{poly}(\kappa)$:

$$\Pr_{k\sim\{0,1\}^\kappa}\left[\mathcal{A}\left(|\varphi_k\rangle^{\otimes T}\right) = 1\right] - \Pr_{|\psi\rangle\leftarrow\mu_{\text{Haar}}}\left[\mathcal{A}\left(|\psi\rangle^{\otimes T}\right) = 1\right] \leq \text{negl}(\kappa)$$

## Definition (Morimae-Yamakawa 2022)

$\{|\varphi_k\rangle\}_{k\in\{0,1\}^\kappa}$ is *single-copy pseudorandom* if:

- $\kappa < n$, where $n = \#$ qubits
- Efficient generation of $|\varphi_k\rangle$ given $k \in \{0,1\}^\kappa$
- For all poly-time $\mathcal{A}$:

$$\Pr_{k\sim\{0,1\}^\kappa}[\mathcal{A}(|\varphi_k\rangle) = 1] - \Pr_{|\psi\rangle\leftarrow\mu_{\text{Haar}}}[\mathcal{A}(|\psi\rangle) = 1] \leq \text{negl}(\kappa)$$

- **Suffice** for commitments, signatures, multiparty computation, zero-knowledge... [Morimae-Yamakawa 2022, Ananth-Qian-Yuen 2022]
- **Implied** by OWFs [Ji-Liu-Song 2018]
- Plausibly **weaker assumption** than OWFs

- **Suffice** for commitments, signatures, multiparty computation, zero-knowledge... [Morimae-Yamakawa 2022, Ananth-Qian-Yuen 2022]
- **Implied** by OWFs [Ji-Liu-Song 2018]
- Plausibly **weaker assumption** than OWFs (?)

**Theorem [K. 2021]**

There is a **quantum oracle** $\mathcal{O}$ such that:

1. $\mathsf{BQP}^{\mathcal{O}} = \mathsf{QMA}^{\mathcal{O}}$, and
2. PRSs exist relative to $\mathcal{O}$

$\Rightarrow$ PRSs without OWFs!

**Theorem [K. 2021]**

There is a **quantum oracle** $\mathcal{O}$ such that:

1. $\mathsf{BQP}^{\mathcal{O}} = \mathsf{QMA}^{\mathcal{O}}$, and
2. PRSs exist relative to $\mathcal{O}$

$\Rightarrow$ PRSs without OWFs!

Limitations:

- "Cheating": OWFs can't depend on $\mathcal{O}$!

**Theorem [K. 2021]**

There is a **quantum oracle** $\mathcal{O}$ such that:

1. $\mathsf{BQP}^{\mathcal{O}} = \mathsf{QMA}^{\mathcal{O}}$, and
2. PRSs exist relative to $\mathcal{O}$

$\Rightarrow$ PRSs without OWFs!

Limitations:

- "Cheating": OWFs can't depend on $\mathcal{O}$!
- Quantum oracles are weak

## Theorem [**K.** 2021]

There is a **quantum oracle** $\mathcal{O}$ such that:

1. $\mathsf{BQP}^{\mathcal{O}} = \mathsf{QMA}^{\mathcal{O}}$, and
2. PRSs exist relative to $\mathcal{O}$

$\Rightarrow$ PRSs without OWFs!

Limitations:

- "Cheating": OWFs can't depend on $\mathcal{O}$!
- Quantum oracles are weak
- Not real-world instantiable

# This Work

**Theorem [This work]**

There exists a property of a cryptographic hash function that:

## Theorem [This work]

There exists a property of a cryptographic hash function that:

(1) **Suffices** for single-copy PRSs

**Theorem [This work]**

There exists a property of a cryptographic hash function that:

(1) **Suffices** for single-copy PRSs

(2) Holds for a **random oracle**

**Theorem [This work]**

There exists a property of a cryptographic hash function that:

(1) **Suffices** for single-copy PRSs

(2) Holds for a **random oracle**

(3) Is **independent** of P vs NP in the black box setting

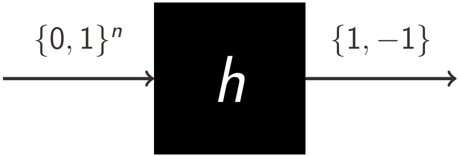
| | |
|---|---|
| **Algorithmica** | $\mathsf{P} = \mathsf{NP}$ **PRSs still possible!** |
| **Heuristica** | $\mathsf{P} \neq \mathsf{NP}$ but $\mathsf{DistNP} \subseteq \mathsf{AvgP}$ |
| **Pessiland** | $\mathsf{DistNP} \not\subseteq \mathsf{AvgP}$ but $\nexists$ OWFs |
| **Minicrypt** | $\exists$ OWFs but $\nexists$ PKE |
| **Cryptomania** | $\exists$ PKE |

$$H = \{(f_k, g_k)\}_{k \in \{0,1\}^\kappa}$$

$$f_k, g_k : \{0,1\}^n \to \{1, -1\}$$

$$H = \{(f_k, g_k)\}_{k \in \{0,1\}^\kappa}$$

$$f_k, g_k : \{0,1\}^n \to \{1,-1\}$$



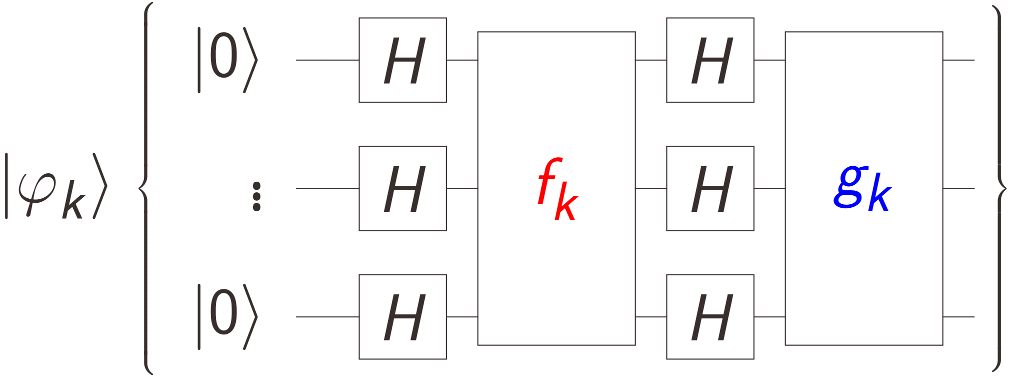

Given $h$, decide if:

(1) $h$ uniformly random

(2) $\exists k$: $h$ correlated with $\hat{f}_k \cdot g_k$

$$H = \{(f_k, g_k)\}_{k \in \{0,1\}^\kappa}$$

$$f_k, g_k : \{0,1\}^n \to \{1, -1\}$$



## Forrelation [Aaronson 2009]

Given $f, g : \{0,1\}^n \to \{1,-1\}$, decide if:

(1) $f$ and $g$ are both uniformly random, or

(2) $\hat{f}$ is correlated with $g$

## Forrelation [Aaronson 2009]

Given $f, g : \{0,1\}^n \to \{1,-1\}$, decide if:

(1) $f$ and $g$ are both uniformly random, or

(2) $\hat{f}$ is correlated with $g$

- Forrelation $\in$ BQP [Aaronson 2009]

## Forrelation [Aaronson 2009]

Given $f, g : \{0,1\}^n \to \{1,-1\}$, decide if:

(1) $f$ and $g$ are both uniformly random, or

(2) $\hat{f}$ is correlated with $g$

- Forrelation $\in$ BQP [Aaronson 2009]
- Forrelation $\notin$ PH [Raz-Tal 2018]

## Forrelation [Aaronson 2009]

Given $f, g : \{0,1\}^n \to \{1,-1\}$, decide if:

(1) $f$ and $g$ are both uniformly random, or

(2) $\hat{f}$ is correlated with $g$

- Forrelation $\in$ BQP [Aaronson 2009]
- Forrelation $\notin$ PH [Raz-Tal 2018]
- OR $\circ$ Forrelation $\notin$ $\text{BQP}^{\text{PH}}$ [Aaronson-Ingram-**K.** 2022]

H$_1$: $|\varphi_k\rangle$

H$_2$: $|\Phi_h\rangle := \frac{1}{\sqrt{2^n}} \sum_x h(x)|x\rangle$ for $h$ correlated w/ $\hat{f}_k \cdot g_k$

H$_3$: $|\Phi_h\rangle$ for $h$ uniform

H$_4$: $|\psi\rangle$ Haar-random

# Open Problems

# Multi-copy security? True under a conjecture about $t$-Forrelation

Multi-copy security? True under a conjecture about $t$-Forrelation

Oracle where P $=$ QMA but PRSs exist?

Multi-copy security? True under a conjecture about $t$-Forrelation

Oracle where $\mathsf{P} = \mathsf{QMA}$ but PRSs exist?

Do single-copy PRSs imply $\mathsf{P} \neq \mathsf{PSPACE}$?

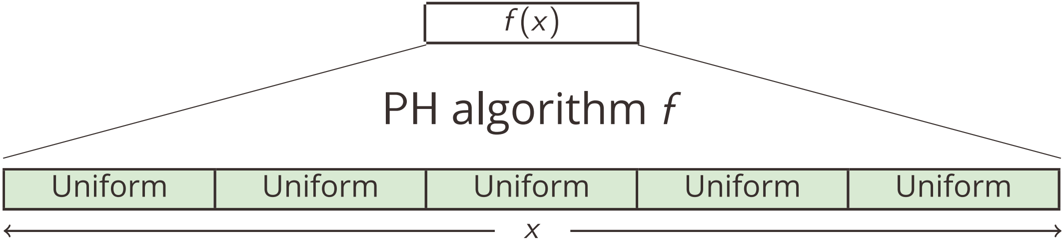
# William Kretschmer

https://www.cs.utexas.edu/~kretsch/

kretsch@cs.utexas.edu

The University of Texas at Austin
Computer Science

- Goal: OR $\circ$ Forrelation $\notin \mathsf{BQP}^{\mathsf{PH}}$
- Idea: PH can't be "sensitive" to a single Forrelated block



- Goal: OR $\circ$ Forrelation $\notin$ $\mathsf{BQP}^{\mathsf{PH}}$
- Idea: PH can't be "sensitive" to a single Forrelated block