Quantum-Computable One-Way Functions without One-Way Functions

William Kretschmer
UC Berkeley

Luowen Qian
NTT Research, Inc.

Avishay Tal
UC Berkeley

Looking for jobs!

Speaker

QIP 2025

(Post-Quantum) One-Way Functions (OWFs)

$$f: \{0,1\}^\lambda \to \{0,1\}^\lambda$$

- Easy to compute for P
  (deterministic efficient classical algorithms)
- Hard to invert for BQP (efficient quantum algorithms)

Quantum-Computable OWF (qOWF)

$$f : \{0,1\}^\lambda \to \{0,1\}^\lambda$$

- Easy to compute for BQP
  (pseudo-deterministic efficient quantum algorithms)
- Hard to invert for BQP

Compute $f(x)$ correctly with probability $1 - \varepsilon$
in time $\mathrm{poly}(\lambda, \log 1/\varepsilon)$

[Impagliazzo'95]

Cryptography today (Impagliazzo's 5 worlds)

🧠 **Algorithmica**: $\mathrm{P} = \mathrm{NP}$

❌

🔒 **Cryptomania**: OWFs +
- Public-key encryption
- Public-key signature
- Secure multiparty computations

Fact: 🧠 Algorithmica ⇒ none of 🔒 Cryptomania; attack is black-box

Resolution of "$\mathrm{P} \stackrel{?}{=} \mathrm{NP}$" is worth $\geq \$10^6$ (Clay),
realistically $\$10^{10} \sim 10^{12}$ 💰💰💰💰 (OpenAI o3-mini)

"Cryptographers seldom sleep well." –Silvio Micali

Quantum information helps cryptography

- Bennett-Brassard'84: QKD with unbounded security
- K'21: Relative to a quantum oracle, ∃pseudorandom unitaries yet $\mathrm{BQP} = \mathrm{QMA}$ (quantum analogue of $\mathrm{P} = \mathrm{NP}$)
  - No *quantum-sensitive* black-box attack of "$\mathrm{BQP} = \mathrm{QMA} \Rightarrow$ no quantum cryptography"
- K-Q-Sinha-T'23: Relative to a classical oracle, ∃weak pseudorandom states yet $\mathrm{P} = \mathrm{NP}$
  - No black-box attack of "$\mathrm{P} = \mathrm{NP} \Rightarrow$ no quantum cryptography"
- Lombardi-Ma-Wright'24: Relative to a classical oracle, ∃weak pseudorandom states secure against adversaries with non-adaptive-query access to arbitrarily powerful classical oracles
  - Quantum cryptography potentially evades all traditional complexity hardness?

Which quantum cryptography, so far?

[Ananth-Q-Yuen'22, Morimae-Yamakawa'22, …]

NP-resilient quantum cryptography:

- (Statistical) QKD
- Private-key encryption
- Secure multiparty computations

Cryptomania:

- Public-key encryption
- Public-key signature
- Secure multiparty computations

Classical communication?
(can broadcast bits; not qubits)

Only quantum-sensitive separation

Requires long-term quantum memory

Our contribution 🧠 Algorithmica 🤝 🔒“Cryptomania”

Relative to a classical oracle,

- ∃Quantum-computable cryptography:
  - Public-key encryption with semantic security
  - Public-key signatures with existential unforgeable security
  - Oblivious transfer and MPC with simulation security

  (without quantum communication/long-term quantum memory)
- $\mathrm{P} = \mathrm{NP}$

Quantum-sensitive or not, there is no black-box attack of
“$\mathrm{P} = \mathrm{NP} \Rightarrow$ no quantum-computable cryptography”

Today: Baby case of main theorem

Relative to a classical oracle,

- $\exists$Quantum-computable one-way functions (OWFs)
  - Still sufficient for constructing public-key signatures [Song'14]
- $\mathrm{P} = \mathrm{NP}$ (thus $\nexists$OWFs)

Quantum-Computable One-Way Functions
without One-Way Functions

Tool: Forrelation

∃oracle distributions $A \sim$ (Forrelated, Uniform) such that

- Distinguishing is easy for BQP^{A}
  [Aaronson'09]
- Computationally indistinguishable even against $\mathrm{PH}^{A} = \mathrm{NP}^{\mathrm{NP}^{\mathrm{NP}^{\cdots A}}}$
  [Raz-T'18]
  - ➢ Classically indistinguishable even if $\mathrm{P} = \mathrm{NP}$

Key idea: oracle encryption

[Aaronson-Ingram-K'22]

Use Forrelation as a "quantum-exclusive" encryption

0	0	1	1	0	1

⇓

Uniform	Uniform	Forrelated	Forrelated	Uniform	Forrelated

Classical eyes can't see different colors even if $\mathrm{P} = \mathrm{NP}$

Oracle construction

Random oracle R: $\{0,1\}^* \to \{0,1\}$

- $R(k,x)$ is a pseudorandom function (PRF) for $k,x \in \{0,1\}^\lambda$
- $\Rightarrow \exists \mathrm{OWF}^R$

Encode/encrypt R with Forrelation: $Forr[R]$

- R is now only accessible by quantum computers

Our oracle (informal): $\mathrm{PH}^{Forr[R]}$

✓ Collapses $\mathrm{P} = \mathrm{NP}$

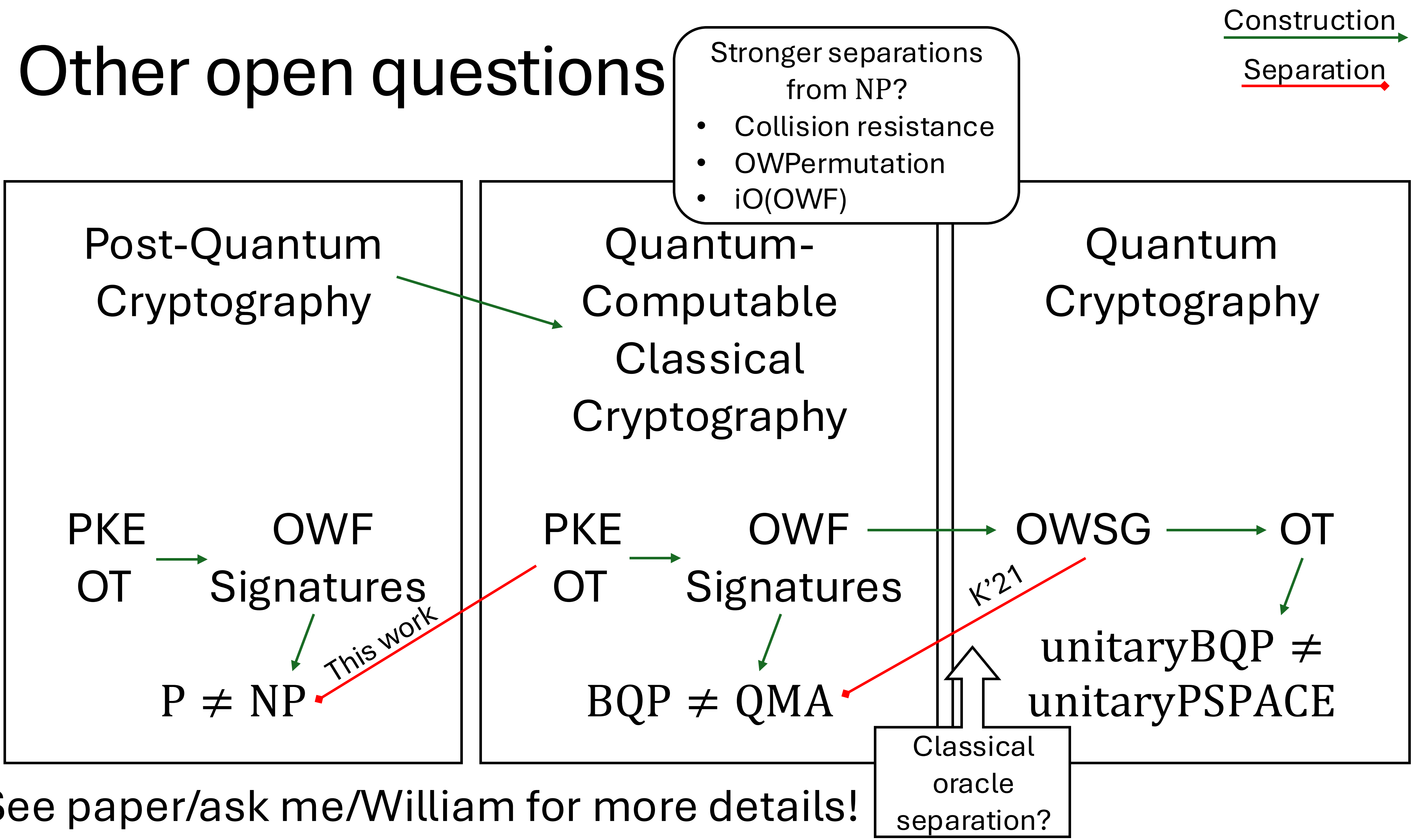
- Is R still a quantum-secure PRF? (See paper for technical details)

Concrete candidate assumptions?

- Possible approach: heuristically instantiate $Forr[R]$
  - ISSUE: Forrelated distribution is not known to be efficient
- Hope our new separation also inspires future research
- Fortunately (?), NP is efficient ⇒ we can efficiently find (or rule out) provably secure quantum cryptography instantiations too! (Algorithmica strikes again)

  Consider NP statement: $\exists C, \Pi$ s.t. Π proves that instantiation C is (in)secure

Other open questions



See paper/ask me/William for more details!