“One-Way Functions” without One-Way Functions

William Kretschmer
UC Berkeley

Luowen Qian
NTT Research, Inc.

Avishay Tal
UC Berkeley

Note: This talk may contain a slight amount of quantum cryptography despite the title.
Technical background on quantum computing is probably NOT necessary.

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

- Easy to compute for P
- Hard to invert for BQP

Why P?
($\mathrm{P} \subseteq \mathrm{BPP} \subseteq \mathrm{BQP}$)

Randomized-Computable OWF

- Easy to compute for BPP (pseudo-deterministic)
- Hard to invert for BQP

Why not consider this?

- Current standard assumptions $\Rightarrow$ OWF directly
- A randomized-computable $f(x; r)$ is distributionally one-way $\Rightarrow \exists$OWF

Quantum-Computable OWF (qOWF)

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

Why not consider this?

- Current standard assumptions $\Rightarrow$ OWF directly
- This work: qOWF $\nRightarrow$ OWF

Revisit later

Main theorem 1

Relative to a classical oracle,

- ∃Quantum-computable one-way functions
- $\mathrm{P} = \mathrm{NP}$ (thus ∄OWF)

Corollary: no relativizing or fully-black-box reductions can prove "∃qOWF ⇒ $\mathrm{P} \neq \mathrm{NP}$" [Reingold-Trevisan-Vadhan'04]

(unlike "∃randomized-computable OWF ⇒ ∃OWF ⇒ $\mathrm{P} \neq \mathrm{NP}$"!)

Main theorem 2

Relative to a classical oracle,

- ∃Quantum-computable cryptography:
  - Public-key encryption (PKE) with semantic security
  - Public-key signatures with existential unforgeable security
  - Oblivious transfer (OT) with simulation security

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

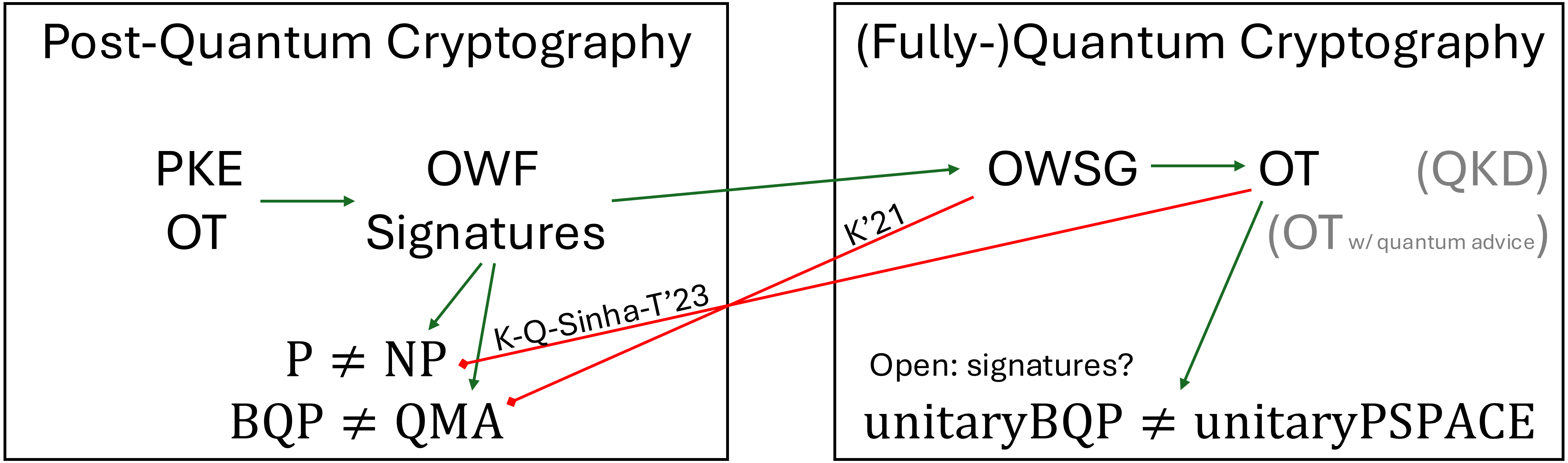
[Impagliazzo'95]

Interpretation: 🧠 Algorithmica 🤝 🔒 "Cryptomania"

Background: Quantum Cryptography without OWF

Construction

Separation



Do quantum cryptography require weaker assumptions *just* because challenges are quantum? (e.g. QKD)

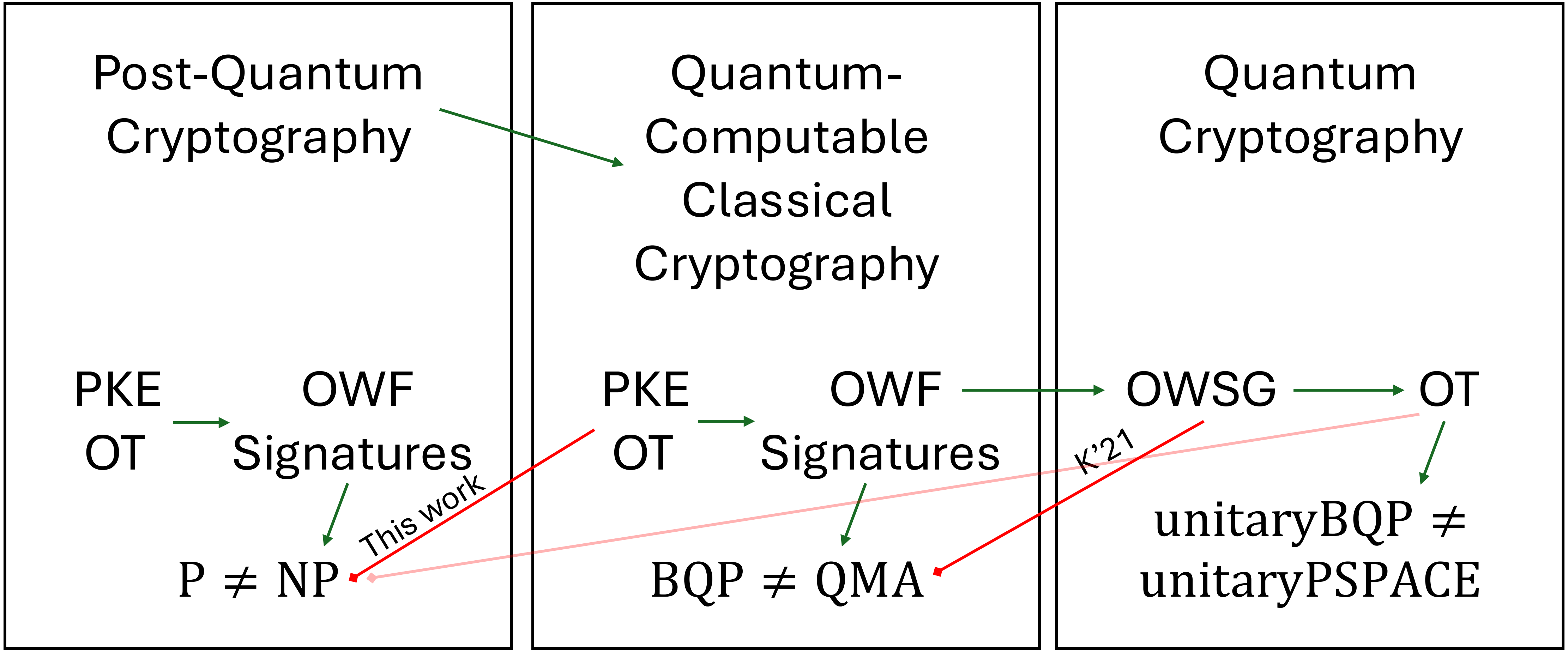
Our work: no, e.g. qOWF

QKD: Bennett-Brassard'84
OT⇒unitaryPSPACE: Bostanci-Efron-Metger-Poremba-Q-Yuen'23, Lombardi-Ma-Wright'24
OWSG⇒OT: Khurana-Tomer'24
OT w/ quantum advice: Morimae-Nehoran-Yamakawa'24 & Q'24

Our work: an intermediate category

Construction

Separation



Proof sketch for main theorem 1

Construct a classical oracle relative to which:

- $\exists$Quantum-computable one-way functions
- $\mathrm{P} = \mathrm{NP}$

Tool: Forrelation

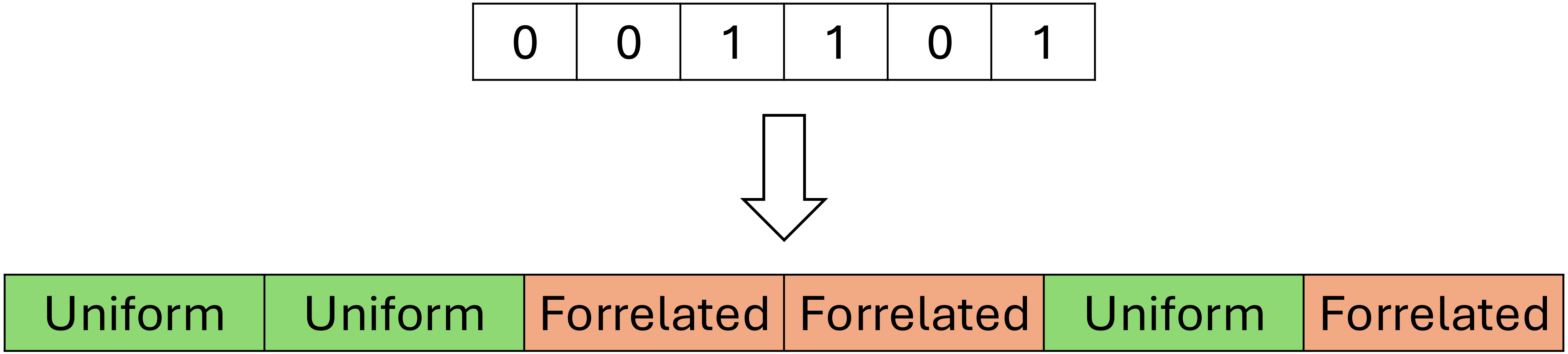
$\exists$oracle distributions $A \sim$ (Forrelated, Uniform) such that

- Distinguishing is easy for $\mathrm{BQP}^{\mathrm{A}}$
  [Aaronson'09]
- Computationally indistinguishable even against $\mathrm{PH}^{\mathrm{A}} = \mathrm{NP}^{\mathrm{NP}^{\mathrm{NP}^{\cdots\mathrm{A}}}}$
  [Raz-Tal'18]
  - ➢ Classically indistinguishable even if $\mathrm{P} = \mathrm{NP}$

Key idea: oracle encryption

[Aaronson-Ingram-Kretschmer'22]

Use Forrelation as a "quantum-exclusive" encryption



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?

Main technical lemma (informal)

- Sample $A(k,x) \leftarrow Forr[H^N]$
  - ➢ Each subfunction $A(k,\cdot) \leftarrow Forr[H]$

H = a small random function

- Sample $h \leftarrow H, k^* \leftarrow [N]$ u.a.r.

Then the following oracles are indistinguishable against $\mathrm{BQP}^{\mathrm{PH}}$:

$$\{A, h\} \approx \{A^{k^* \mapsto Forr[h]}, h\}$$

$h =$				
	0	1	0	1

$\Downarrow$

	Uniform	Forrelated	Uniform	Uniform
k^*	Forrelated	Uniform	Forrelated	Forrelated
	Forrelated	Uniform	Forrelated	Uniform
	Uniform	Uniform	Forrelated	Forrelated

vs.

Uniform	Forrelated	Uniform	Uniform
Uniform	**Forrelated**	**Uniform**	**Forrelated**
Forrelated	Uniform	Forrelated	Uniform
Uniform	Uniform	Forrelated	Forrelated

Proof sketch for main theorem 2

Construct a classical oracle relative to which:

- $\exists$Quantum-computable trapdoor one-way functions
  - Public key is pseudorandom (for OT)
- $\mathrm{P} = \mathrm{NP}$

Our oracle (informal): $\mathrm{PH}^{Forr[R, I^R]}$ (I^R inverts some region of R)

➢ Reduce security to main lemma under non-uniform H

Cryptographic protocols from qOWF

Recall: ∃OWF ⇒ Prove "$\exists x$: OWF$(x) = y$" in zero knowledge

✓ "$\exists x$: OWF$(x) = y$" is an NP statement

✓ ∃OWF ⇒ zero knowledge proof for NP

GMW compiler does this

Question: ∃qOWF ⇒ Prove "$\exists x$: qOWF$(x) = y$" in zero knowledge?

➢ Careful! "$\exists x$: qOWF$(x) = y$" is a QCMA statement

➢ ∃OWF ⇒ <u>classical</u> zero knowledge proof for QCMA? (open)

Resolution: use <u>post-quantum fully-black-box</u> reductions

e.g. Chatterjee-Liang-Pandey-Yamakawa

Concrete candidate assumptions?

- Possible approach: heuristically instantiate $Forr[R]$
  - ISSUE: Forrelated distribution is not known to be efficient

Founding Quantum Cryptography on Quantum Advantage

or, Towards Cryptography from #P-Hardness

Dakshita Khurana* Kabir Tomer†

Quantum Cryptography from Meta-Complexity

Taiga Hiroka[1] and Tomoyuki Morimae[1]

Efficient Quantum Pseudorandomness from Hamiltonian Phase States

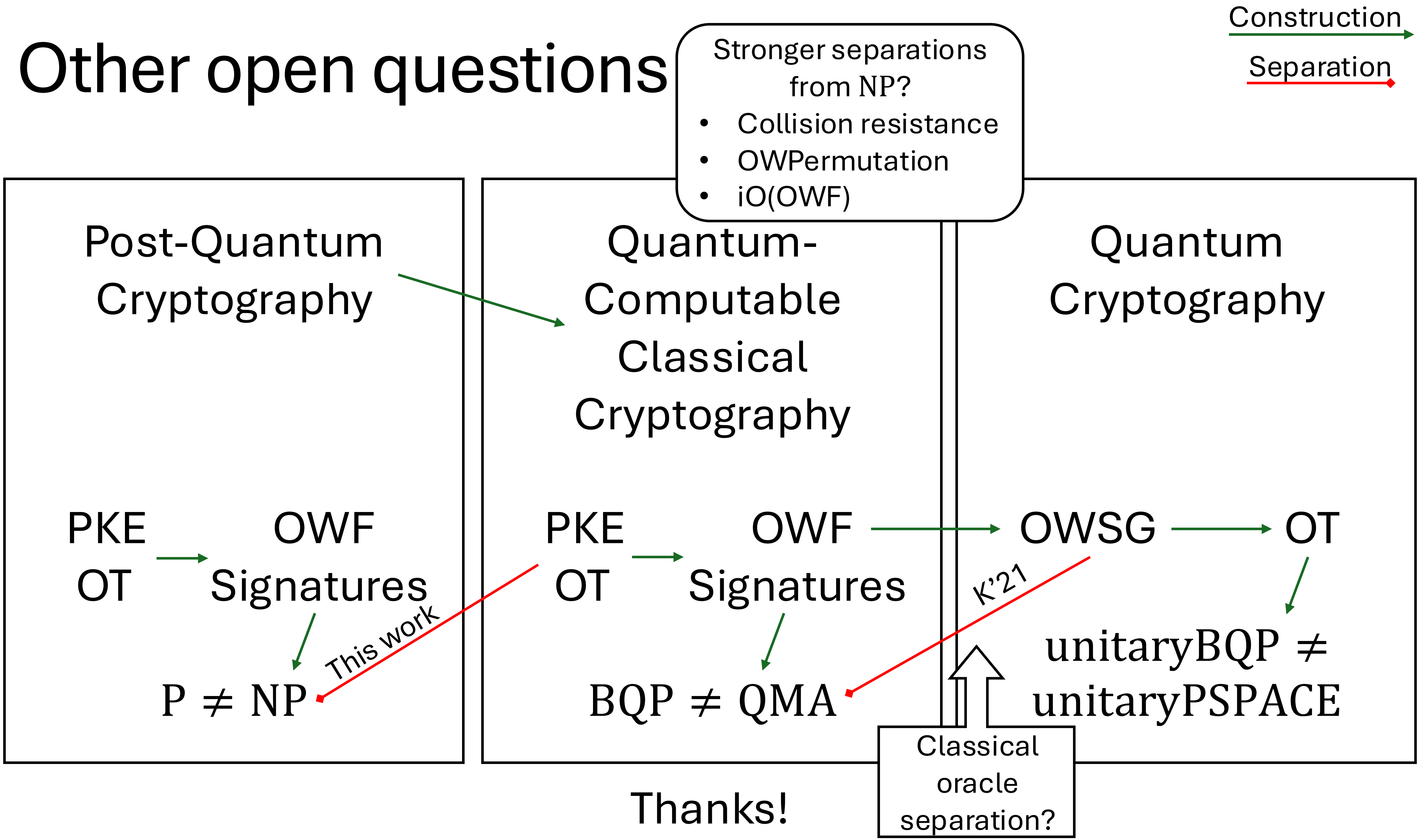
John Bostanci[1], Jonas Haferkamp[2], Dominik Hangleiter[3,4], and Alexander Poremba[5]

A Meta-Complexity Characterization of Quantum Cryptography

Bruno P. Cavalar* Eli Goldin† Matthew Gray‡ Peter Hall§

- Hope our new separation also inspires future research

Other open questions



Thanks!