The Complexity-Theoretic Foundations of Quantum Cryptography

Dakshita Khurana

NTT Research, UIUC

Based on joint work with Kabir Tomer (UIUC)

Holy Grail

- Build cryptography without making *any* unproven assumptions
- Obstacle: Secure (classical) cryptography can exist only if P!=NP
- Dream: Build cryptography while only making *minimal* unproven assumptions
- For classical crypto, the minimal assumption = existence of *one-way functions*

Do one-way functions exist?

Impagliazzo's Five Worlds

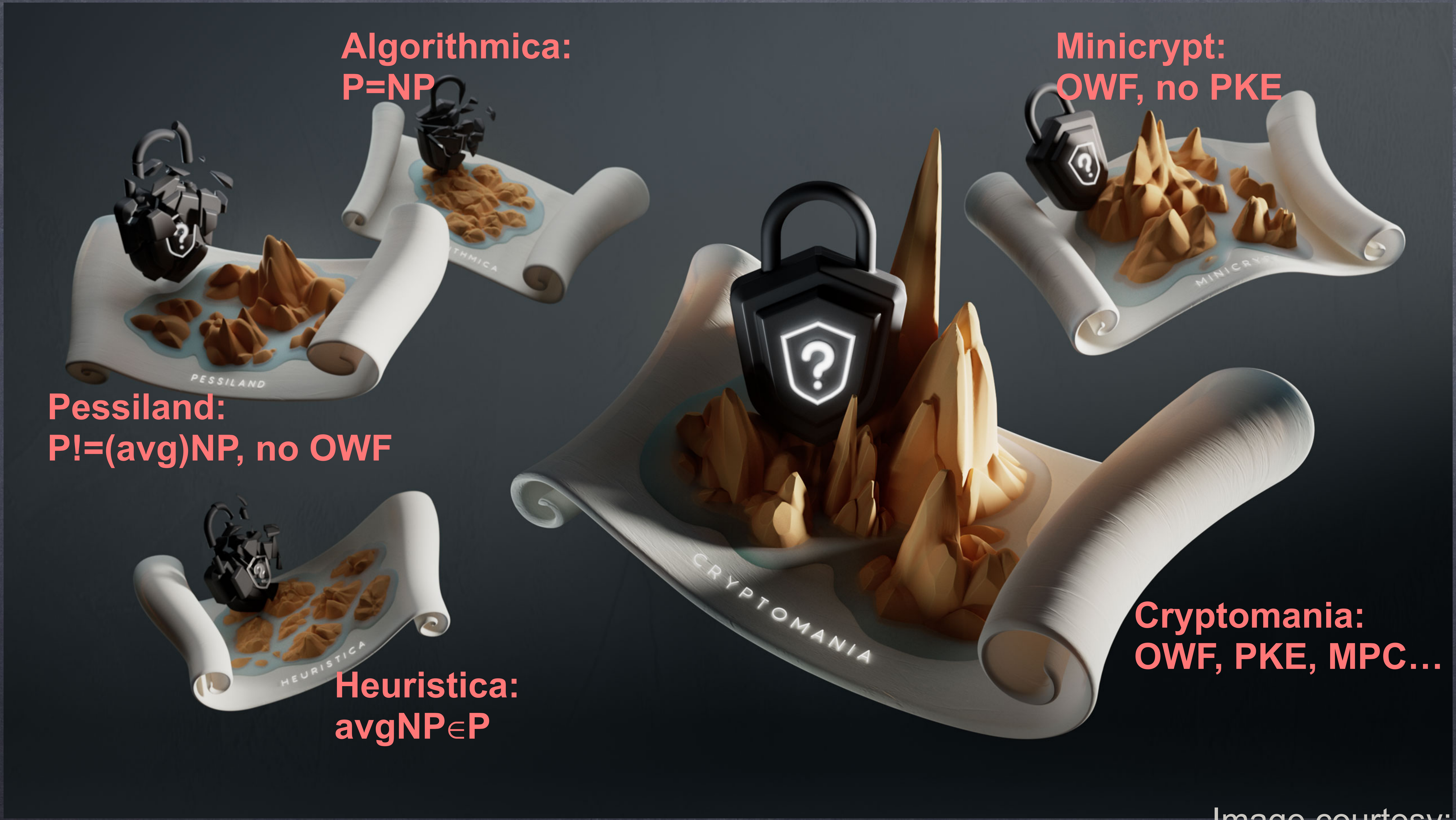


Image courtesy: Quanta magazine

Quantum Cryptography

- Cryptography without *any* unproven assumptions

- Cryptography is about (much) more than key distribution.

- For example, we care about commitments, MPC, signatures, PKE, ….

Quantum Commitments and MPC

- Just like QKD, commitments secure against computationally unbounded adversaries were believed to exist

  See e.g., [Bennett-Crepeau-Josza-Langlois'93]

- Quantum MPC believed to exist, based on commitments against unbounded adversaries

  First proposed in [Crepeau-Kilian'88], proven secure in [Mayers-Salvail'94, Yao'95]

- Years later: proof that ***commitments against unbounded adversaries are impossible!***

  In independent works [Mayers'97], [Lo-Chau'97]

What we know so far..

Secure Computation

Theorem

[Bartusek-Coladangelo-K-Ma’21, Grilo-Lin-Song-Vaikuntanathan’21, Ananth-Qian-Yuen’22]:

(One-way functions =>) **Commitments => secure computation with quantum participants**

(Provably impossible without quantum capabilities [Impagliazzo-Rudich’89])

What we know so far..

Public-Key Encryption with Quantum Public Keys

Theorem

[Barooti-Grilo-HugueninDumittan-Malavolta-Vu-Walter’24, Kitagawa-Morimae-Nishimaki-Yamakawa’24]:

One-way functions => public-key encryption with quantum public keys

(Provably impossible with classical keys [Impagliazzo-Rudich’89])

Quantum World(s)

Minicrypt:
OWF, QMPC, QPKE

Can commitments/quantum crypto be based on assumptions *weaker than* OWF?

A Promised Land

- Relative to a quantum oracle, commitments can exist even if BQP = QMA

  [Kretschmer'21]

- Relative to a classical oracle, commitments can exist even if P = NP

  [Kretschmer-Qian-Sinha-Tal'23]

- (Maybe?) relative to a classical oracle, commitments can exist even if all problems that can be classically described can be easily solved?

  [Lombardi-Ma-Wichs'24]

- Meaning — there's a strong possibility that quantum cryptography can be based on assumptions that *are* mathematically weaker than one-way functions/that maybe true even if P = NP

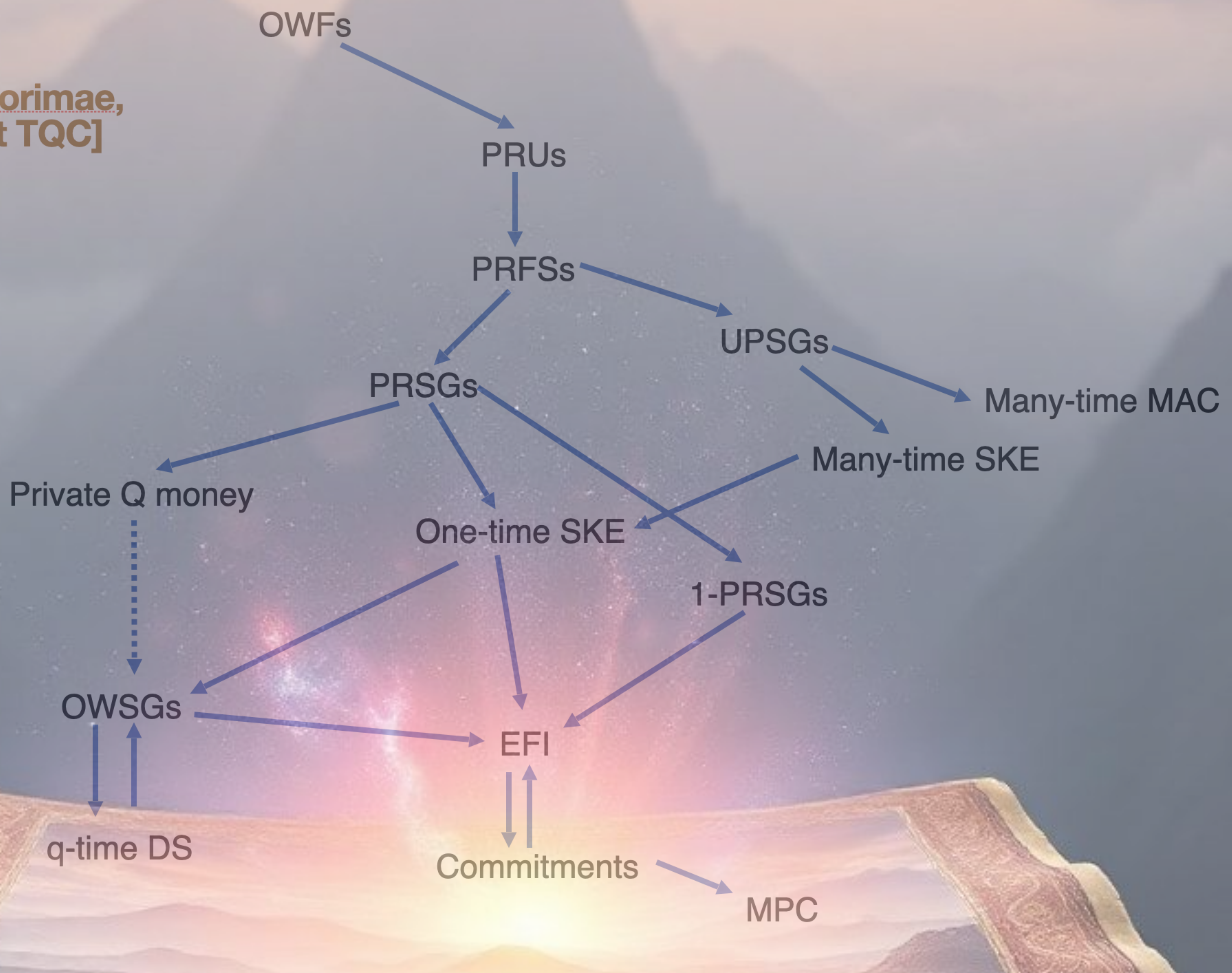
“Pseudorandom” states imply commitments

[Ananth-Qian-Yuen’22, Morimae-Yamakawa’22]

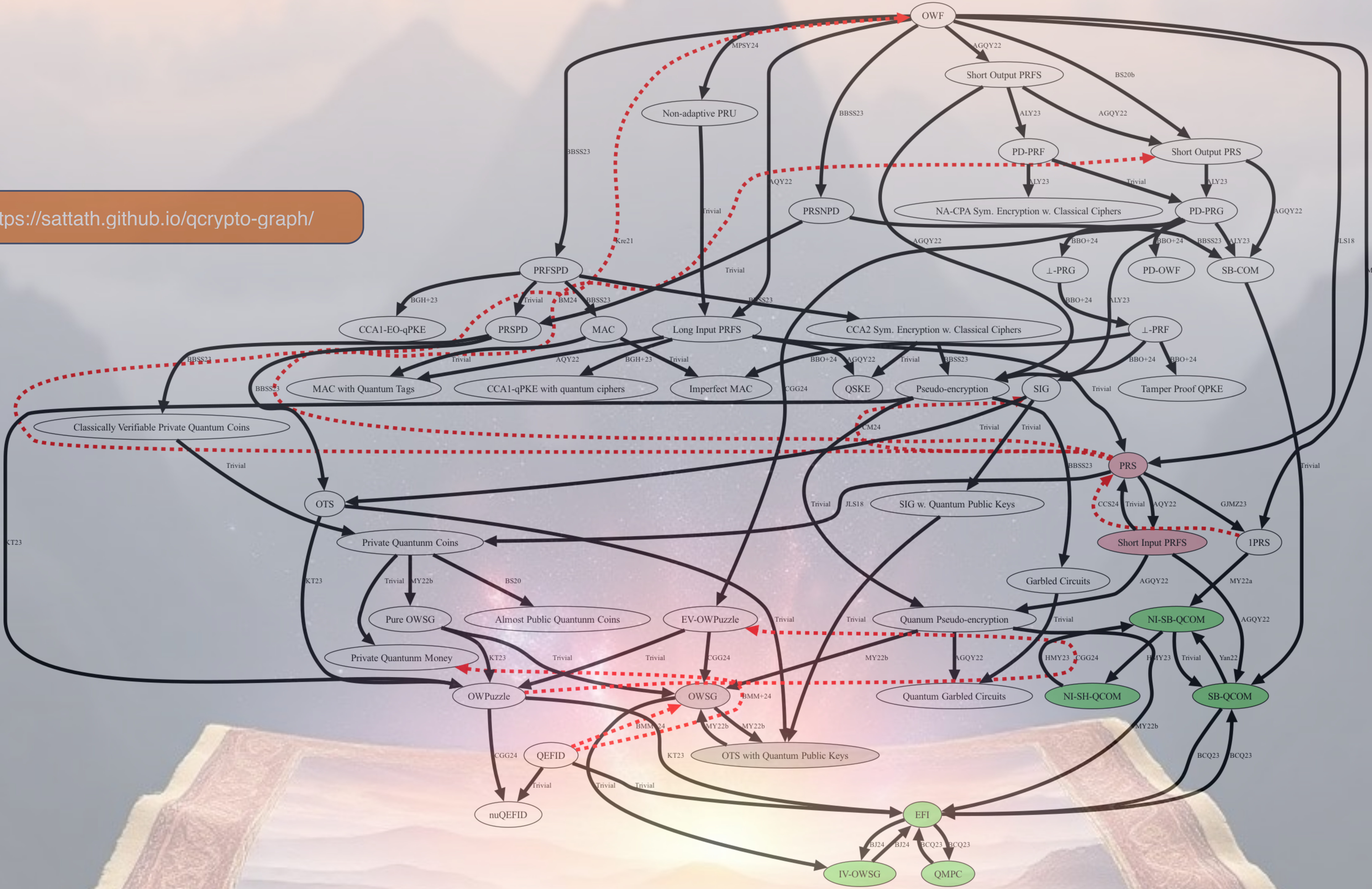
- Gen (s) —> $|\psi_s\rangle$, where |s| < $||\psi_s\rangle|$

  s.t. $|\psi_s\rangle$ is computationally indistinguishable from “random” state

[Tomoyuki Morimae, invited talk at TQC]



https://sattath.github.io/qcrypto-graph/



Some Questions

1. Is there a quantum analogue of one-way functions?

2. What hard problems should we base quantum cryptosystems on?

3. What connections does quantum cryptography have with complexity theory?

Some Questions

1. Is there a quantum analogue of one-way functions?
2. What hard problems should we base quantum cryptosystems on?
3. What connections does quantum cryptography have with complexity theory?

What Do Quantum One-way Assumptions Look Like?

Q One-way functions

Quantumly computable f
s.t. inverting f(x) is hard,
w.h.p over uniformly chosen x

What Do Quantum One-way Assumptions look like?

Q One-way functions

One-way states

(Quantum) efficient algorithm $x \rightarrow |\psi_x\rangle$
s.t. inverting $|\psi_x\rangle^{\otimes t}$ is hard

Digital signatures, encryption schemes, etc. where the hard task is to find a classical secret [Morimae-Yamakawa'22]

What Do Quantum One-way Assumptions Look Like?

Q One-way functions

One-way states

One-way puzzles

One-Way Puzzles [K-Tomer'24a]

Quantum process sampling hard-on-average problems along with solutions

$Samp$ → $(x, y) \quad s.t.\ \mathscr{R}(x, y) = 1$

(Efficient)

- Given *y*, computationally intractable to find x s.t. $\mathscr{R}(x, y) = 1$

One-Way Puzzles [K-Tomer'24a]

Quantum process sampling hard-on-average problems along with solutions

$Samp$ → $(x, y) \quad s.t. \ \mathscr{R}(x, y) = 1$

(Efficient)

Not necessarily an NP relation!

For a classical sampler, it is wlog for $\mathscr{R}$ to be an NP relation

- Given y, computationally intractable to find x s.t. $\mathscr{R}(x, y) = 1$

What Do "Quantum" One-way Assumptions Look Like?

Q One-way functions

One-way states

One-way puzzles

State puzzles

State Puzzles

[K-Tomer'24, Qian-Raizes-Zhandry'24]

Capture the hardness of synthesizing a quantum state given a public string

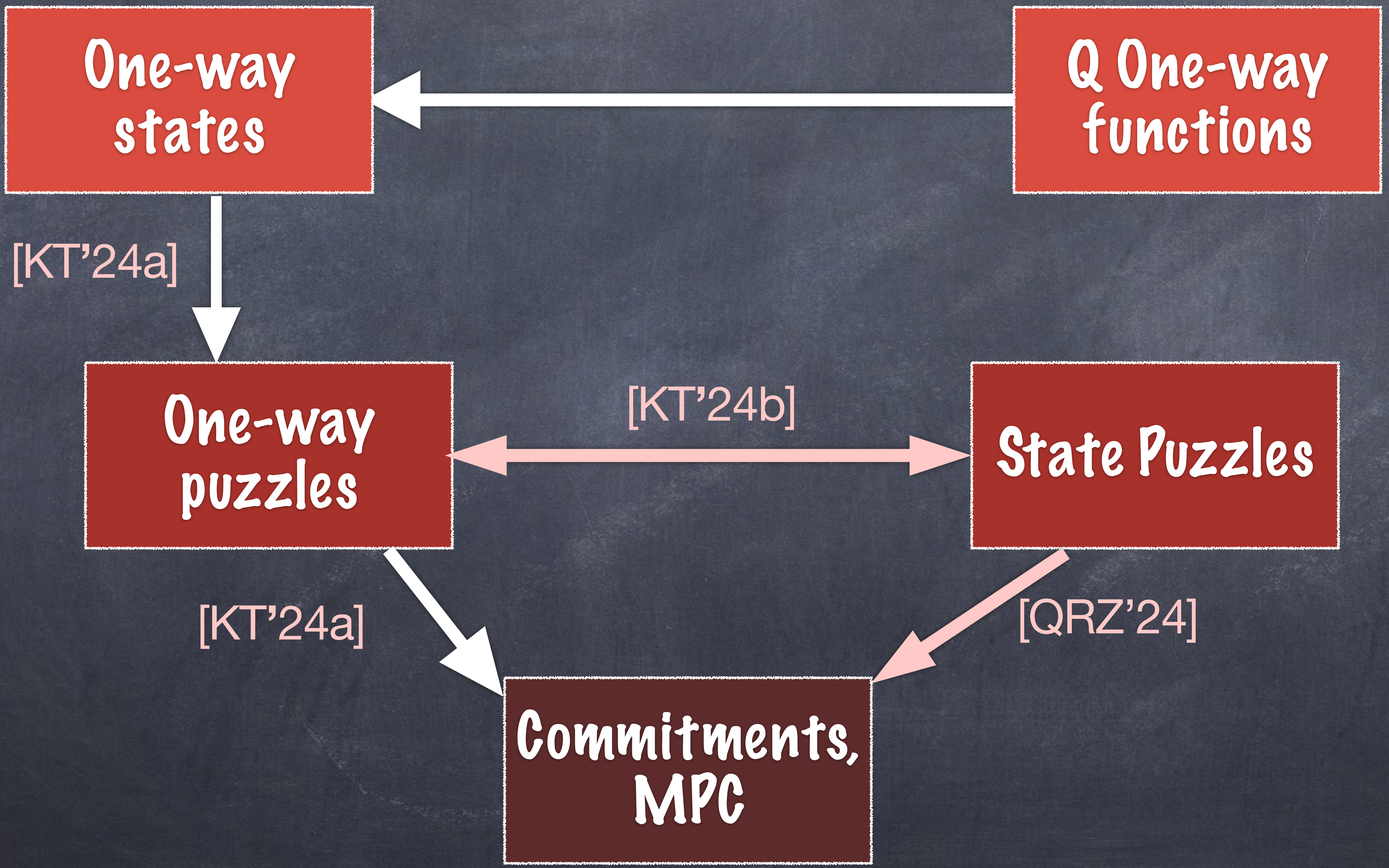
Samp (Efficient) → $s, |\psi_s\rangle$

- Computationally infeasible to invert, i.e.

  given *s* output a state that overlaps with $|\psi_s\rangle$

- Implied by quantum money "mini-schemes"

What Do "Quantum" One-way Assumptions Look Like?



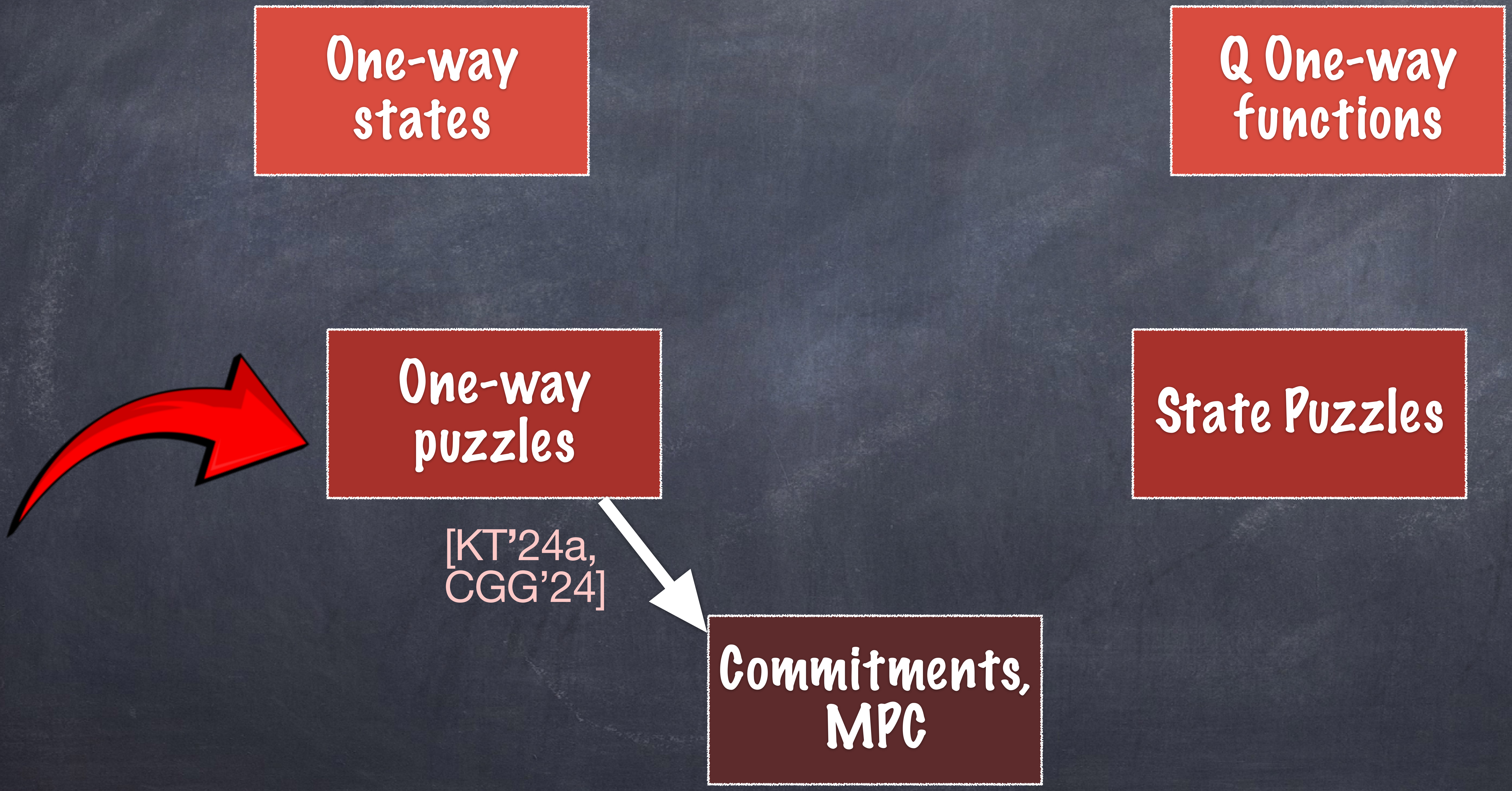
Distributional One-Way Puzzles [Chung-Goldin-Gray'24]

Hardness of distributional inversion

- Given *y*, computationally intractable to *sample* $x \sim X \mid y$

Distributional one-way puzzles $\Longleftrightarrow$ one-way puzzles [Chung-Goldin-Gray'24]

What Do "Quantum" One-way Assumptions Look Like?



Some Questions

1. Is there a quantum analogue of one-way functions?
2. What hard problems should we base quantum cryptosystems on?
3. What connections does quantum cryptography have with complexity theory?

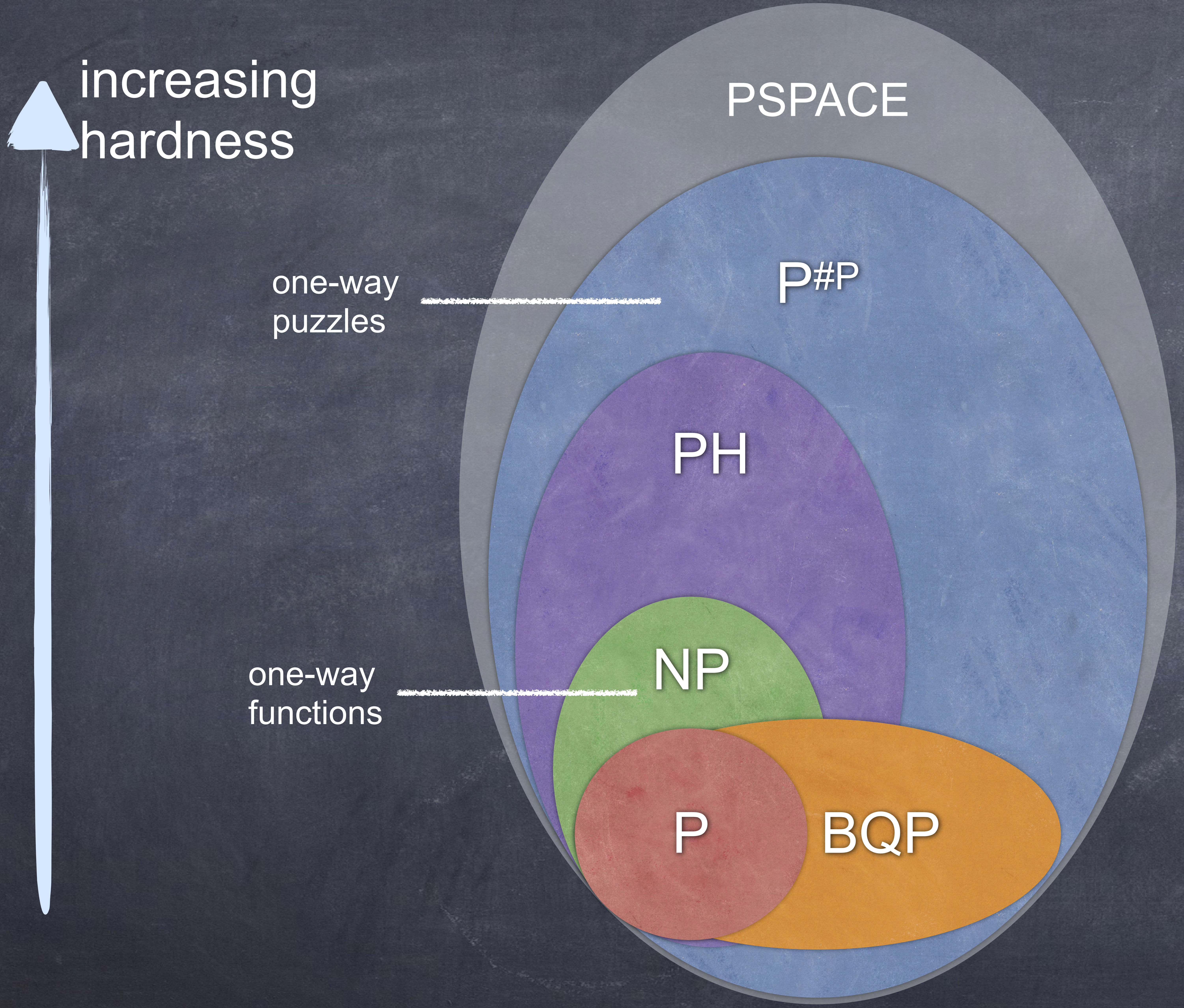
Goal: Build one-way puzzles from mathematical problems that are harder than problems in NP

One-Way Puzzles [K-Tomer'24a]

Quantum process sampling hard-on-average problems along with solutions

$Samp$ (Efficient) $\longrightarrow$ $(x, y) \quad s.t. \; \mathscr{R}(x, y) = 1$

- Given *y*, computationally intractable to find x s.t. $\mathscr{R}(x, y) = 1$


increasing
hardness
PSPACE
P#P
one-way
puzzles
PH
NP
one-way
functions
P
BQP

One-way puzzles from #P-hardness

Theorem [K-Tomer'24b (arXiv: 2409.15248)]

Assume certain conjectures from the quantum advantage literature,

Then one-way puzzles exist iff $P^{\#P} \neq BQP$.

Building puzzles

- Goal: Build one-way puzzles from the mildest possible assumption

- One-way puzzles are invertible by #P, so they exist only if $P^{\#P} \neq BQP$ [CGGHLP'24]
- Can we base one-way puzzles only on #P-hardness?

Dream: QCrypto from #P Hardness

- #P is a counting complexity class
- Captures the complexity of answering:

  how many satisfying assignments does this Boolean formula have?

#P Complete Problem

- The permanent of a matrix $perm(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i,\sigma_i}$

$$\operatorname{perm}\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = aei + bfg + cdh + ceg + bdi + afh.$$

- #P hard in the worst case. Also #P hard in the average case (great for crypto!)
- Quantum cryptography from the hardness of computing perm(A) for a given A?

A Bottleneck

- Goal: Puzzle sampler needs to *efficiently sample* (x, y) such that:

  BQP machines cannot find x given y

- Can we set $(x, y) = (perm(A), A)$?

- Unlikely that random matrices can be (quantumly) efficiently sampled together with their permanents.

BosonSampling, Random Circuit Sampling, IQP, etc..

[Aaronson-Arkhipov'11]

- Quantum circuits can efficiently sample from a distribution A such that *probabilities of outputs encode permanents of unitary matrices*

- Permanents hard to compute $\Longrightarrow$
  probabilities of outcomes are hard to compute

Use this to build puzzles?

- For a random a, it is hard to compute $\Pr_{a \leftarrow A}[a]$
- Can we set $(x, y) = \left(\Pr_{a \leftarrow A}[a], a \right)$?
- This, again, is hard to sample :(
- All that is easy to sample is $a \leftarrow A$

Let's use some indirection

- The following is a distributional one-way puzzle:
  - Sample $a \leftarrow A$. Say, a is n bits long.
  - Sample $i \leftarrow [0, n-1]$.
  - Output $(y, x) \leftarrow (a_1 a_2 \ldots a_{i-1}, a_i)$

Proof (oversimplified)

- Given *Adv* that on input $(a_1 a_2 \ldots a_{i-1})$ samples a_i perfectly
- We will build a machine R to approximate $\Pr_{a \leftarrow A}[a]$. Say $a = 0100...$
  - Run *Adv* on $puz = \perp$ many times to approximate p_0
  - Run *Adv* on $puz = 0$ many times to approximate $p_{1|0}$. Set $p_{01} = p_0 \cdot p_{1|0}$
  - Run *Adv* on $puz = 01$ many times to approximate $p_{010} = p_{01} \cdot p_{0|01}$
  - Run *Adv* on $puz = 010$ many times to approximate $p_{0100} = p_{010} \cdot p_{0|010}$

Proof (oversimplified)

- Given *Adv* that on input $(a_1 a_2 \ldots a_{i-1})$ samples a_i perfectly
- We built a machine B to approximate every $Pr[a]$ (upto small errors)
- When *Adv* is a distributional puzzle inverter, it only samples from a distribution that has (1/poly) statistical distance from the correct dist.
- So, B will only be able to *approximate* $Pr[a]$ on average.

On the Assumption

Assumption: Quantum computers can efficiently sample from a distribution A such that $\Pr_{a \leftarrow A}[a]$ *are hard to approximate (on average) & not always* < $\frac{1}{p(n).2^n}$

- Implied by conjectures in sampling-based quantum advantage
  - BosonSampling — Permanents of random matrices with $\mathcal{N}(0,1)$ Gaussian entries are #P-hard to approximate on average [Aaronson-Arkhipov'11]
  - Random Circuit Sampling — Output probabilities of Random Quantum Circuits are #P-hard to approximate on average [Boixo et.al.'18…..]
  - IQP [Bremner-Montanaro-Shepherd'14….]

On the Assumption

Hard Problem: For a quantumly efficiently sampleable distribution A, approximate $\Pr_{a \leftarrow A}[a]$ (on average)

- Does this imply one-way functions?
  - Proofs of sampling-based advantage *require* that this problem cannot be solved in BPP^{NP}.
  - If a BPP reduction could use a OWF inverter to solve this problem, then BPP^{NP} will solve this problem. This would counter quantum advantage conjectures.
  - More generally, this is conjectured to be #P-hard, so we don't even expect BQP or PH reductions.

Assumptions in Q Crypto

- One-way puzzles, state puzzles and commitments can be based on RCS/ BosonSampling/IQP conjectures
- What about other quantum cryptographic primitives, such as signatures, public-key encryption or pseudorandom states?

Some Questions

1. Is there a quantum analogue of one-way functions?

2. What hard problems should we base quantum cryptosystems on?

3. What connections does quantum cryptography have with complexity theory?

Quantum Complexity Theory

- Traditional complexity theory considers the problem of deciding languages with *classical* instances
- Quantum cryptographic tasks (e.g., breaking a quantum commitment) cannot be neatly framed as classical-instance problems
- New "complexity theory" studying unitary transformations [Bostanci-Efron-Metger-Poremba-Qian-Yuen'23, Lombardi-Ma-Wright'23, Chia-Chung-Huang-Shih'24…]

Quantum Worlds

Microcrypt:
OWPuzz exist

Commitments, MPC

Minicrypt:
OWF exist

QPKE, signatures,
Commitments, MPC

Additional Possible worlds

Microcrypt:
OWPuzz exist

EVcrypt:
OWSG exist

Efficiently verifiable
QPKE, Signatures

MiniQcrypt:
QOWF exist

Q Cryptography with
classical communication

Minicrypt:
OWF exist

Separating these worlds

- [Chen-Coladangelo-Sattath’24, Bostanci-Chen-Nehoran’24, Behera-Malavolta-Morimae-Mour-Yamakawa’24]:

  Unitary oracles separating OWSG and QOWF from one-way puzzles.

- [Kretschmer-Qian-Tal’24]:

  Classical oracles separating OWF from QOWF.

- [Goldin-Morimae-Mutreja-Yamakawa’24]:

  Unitary oracles separating QOWF from classical communication primitives.

Additional Possible worlds

Microcrypt:
OWPuzz exist

$P^{\#P}$!= BQP

EVcrypt:
OWSG exist

Efficiently verifiable QPKE, Signatures

MiniQcrypt:
QOWF exist

QCMA != BQP

Q Cryptography with classical communication

Minicrypt:
OWF exist

NP != BQP

Additional Possible worlds

Microcrypt:
OWPuzz exist

EVcrypt:
OWSG exist

Efficiently verifiable QPKE, Signatures

MiniQcrypt:
QOWF exist

Q Cryptography with classical communication

Minicrypt:
OWF exist

Open Problems

- Can we further weaken assumptions for commitments?
  (Can we efficiently implement every unitary if P = PSPACE?)
- What is the relationship between quantum advantage and quantum cryptography?
- When can we extract computational/cryptographic hardness from physical processes?

Thank you!