

Title: How Low Can We Go? Exploring Minimal Assumptions in Quantum Cryptography

Speakers: Dakshita Khurana

Collection/Series: Year of Quantum Across Canada

Subject: Quantum Information

Date: October 09, 2025 - 5:30 PM

URL: <https://pirsa.org/25100139>

Abstract:

In this talk, I will explore the fascinating landscape of minimal assumptions in quantum cryptography—how little we need to assume to build secure quantum protocols. We will cover key cryptographic primitives including quantum encryption, signatures, and money, and show how these primitives imply the existence of one-way puzzles, a quantum analogue of classical one-way functions. I will also highlight the utility of one-way puzzles and discuss concrete assumptions that enable their realization, revealing intriguing connections with quantum advantage.

Foundations of Quantum Cryptography




(Or: Why quantum cryptographers worry less than classical cryptographers)

Dakshita Khurana (UIUC, NTT Research)



Based on joint work with Kabir Tomer (UIUC)

Holy Grail

-  Goal: Build cryptography without making *any* unproven assumptions
-  Secure *classical* cryptography can exist only if $P \neq NP$
(actually, need one-way functions to exist)
-  **QKD** without any unproven computational assumptions [Bennett-Brassard'84]

Assumptions in Quantum Cryptography



Can we quantumly realize other cryptography without unproven assumptions?

Zero-Knowledge

Secure Computation

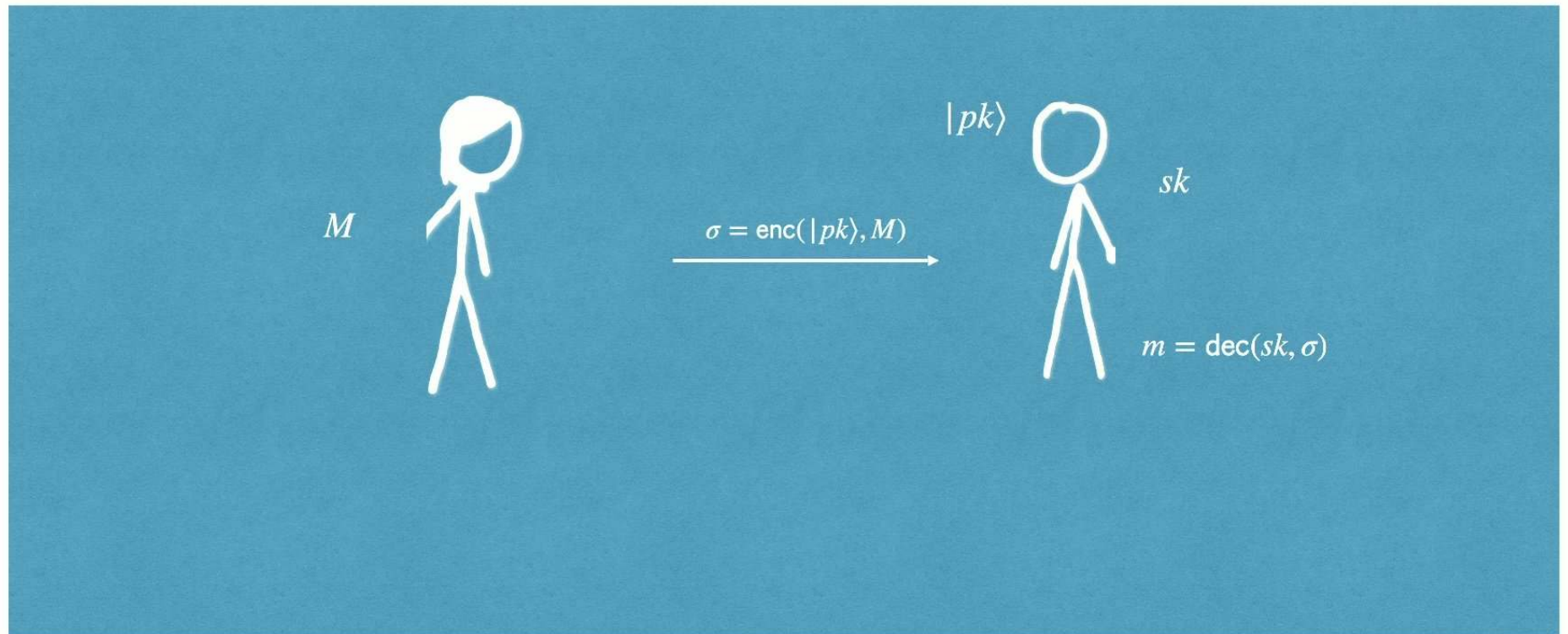
Signatures

Coin-tossing

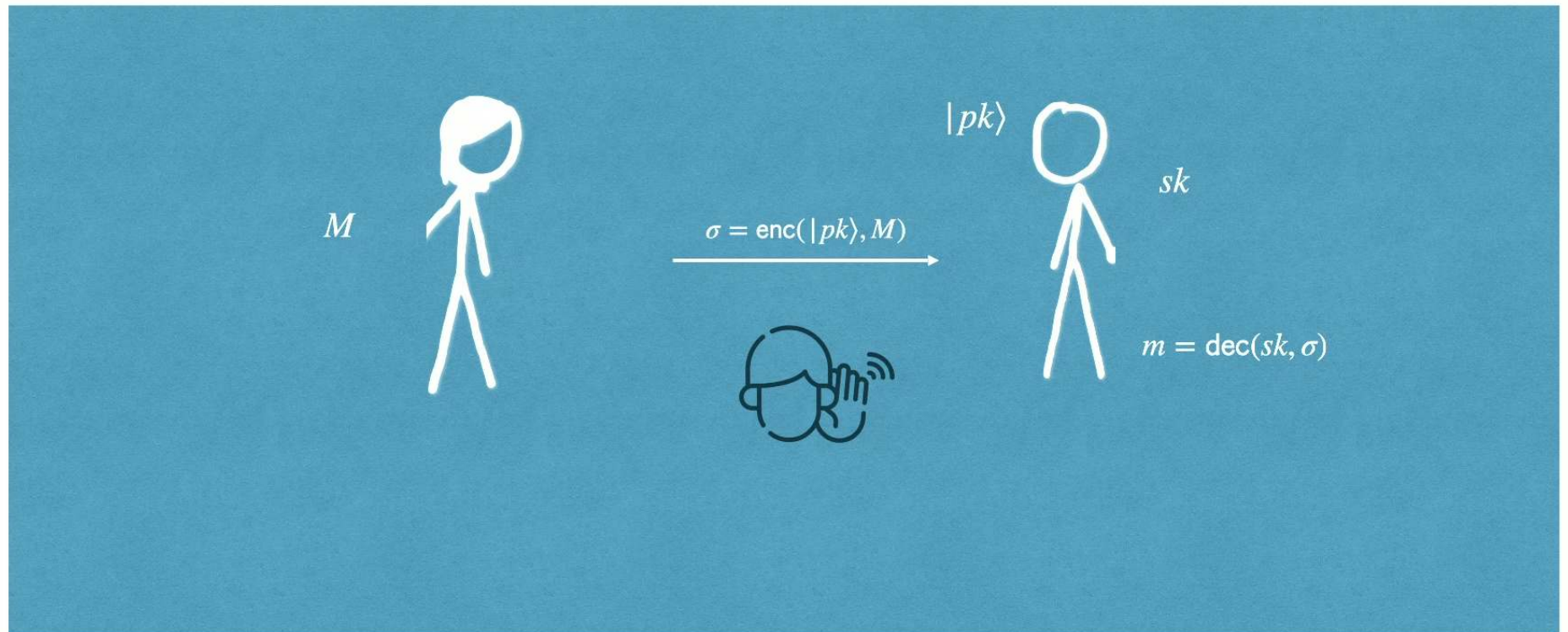
Commitments

Public-Key Encryption

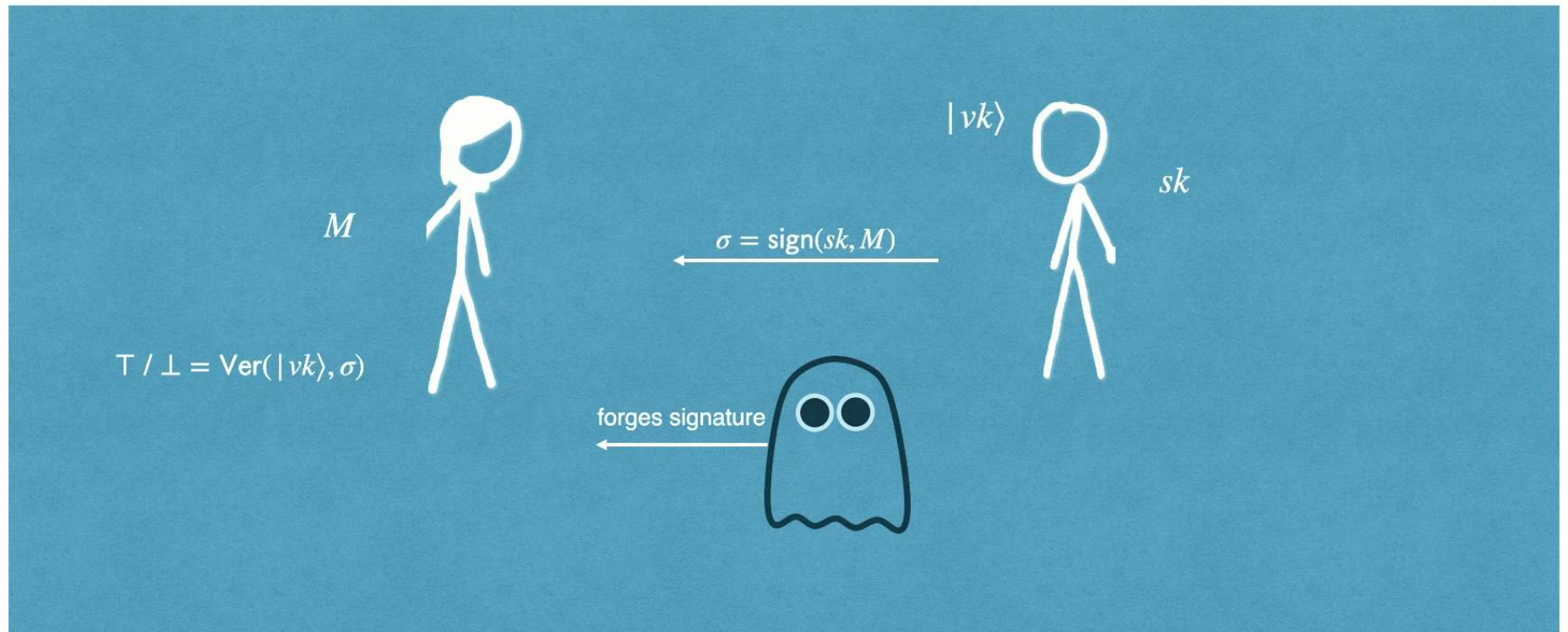
Public-key Encryption



Public-key Encryption



Signatures



Nature of Hardness

- At the very least, we want efficiently sampleable (pk, sk) such that:

Given $|pk\rangle^{\otimes poly(n)}$, it is computationally hard to output sk

(or)

Given pk , it is computationally hard to output $|sk\rangle$



Can we capture this hardness via simple cryptographic primitives?

State Puzzles

[K-Tomer'25, Qian-Raizes-Zhandry'25]

The hardness of synthesizing a secret quantum state given a public string

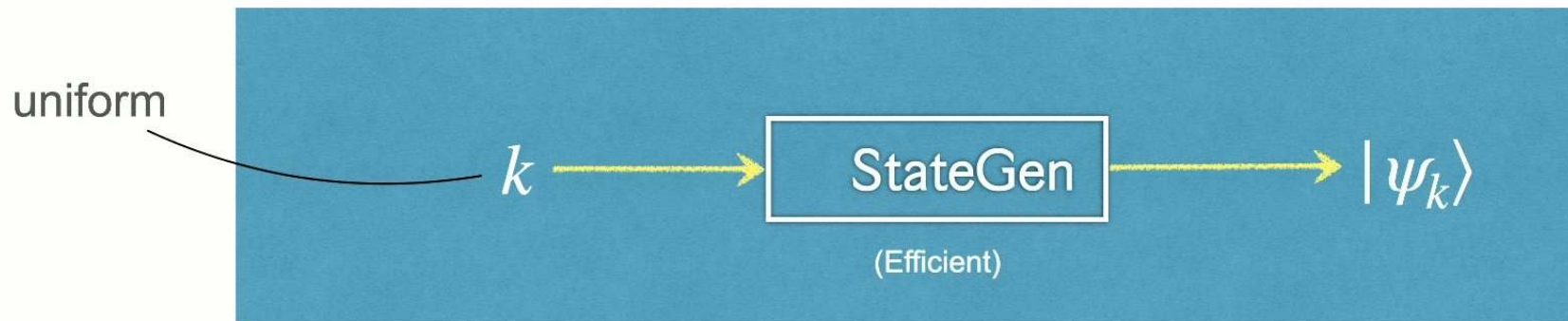


- No polynomial-time quantum circuit can, given s , output a state that overlaps noticeably with $|\psi_s\rangle$

One-way States

[Morimae-Yamakawa'22]

The hardness of guessing a classical secret key given a public state



- No polynomial-time quantum circuit can, given $|\psi_k\rangle^{\otimes poly(n)}$, guess a key k' such that $\langle \psi_{k'} | \psi_k \rangle \geq 1/poly(n)$

One-way Puzzles

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

Samp

(Efficient)



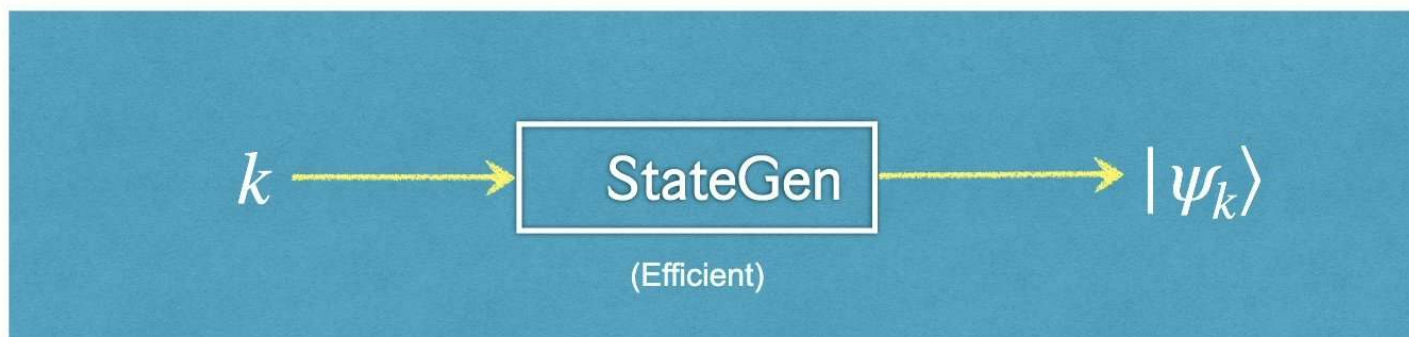
$(x, y) \text{ s.t. } \mathcal{R}(x, y) = 1$

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

Not necessarily an NP relation!

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

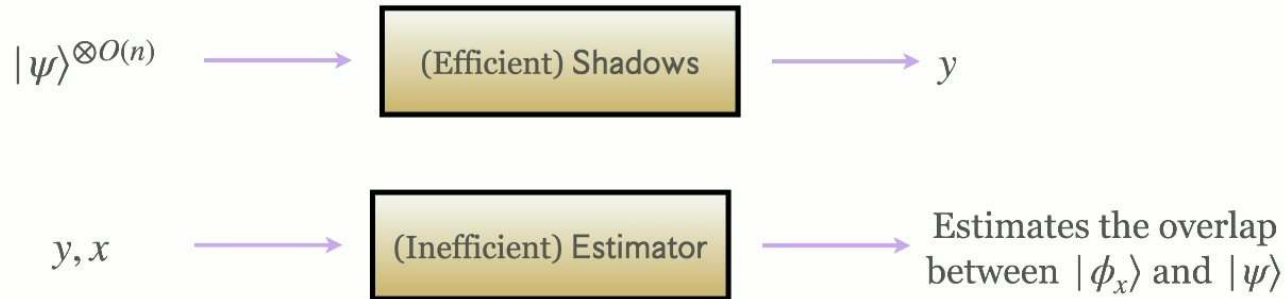
One-way States \implies One-way Puzzles



Convert quantum challenges to classical challenges while maintaining hardness of inversion

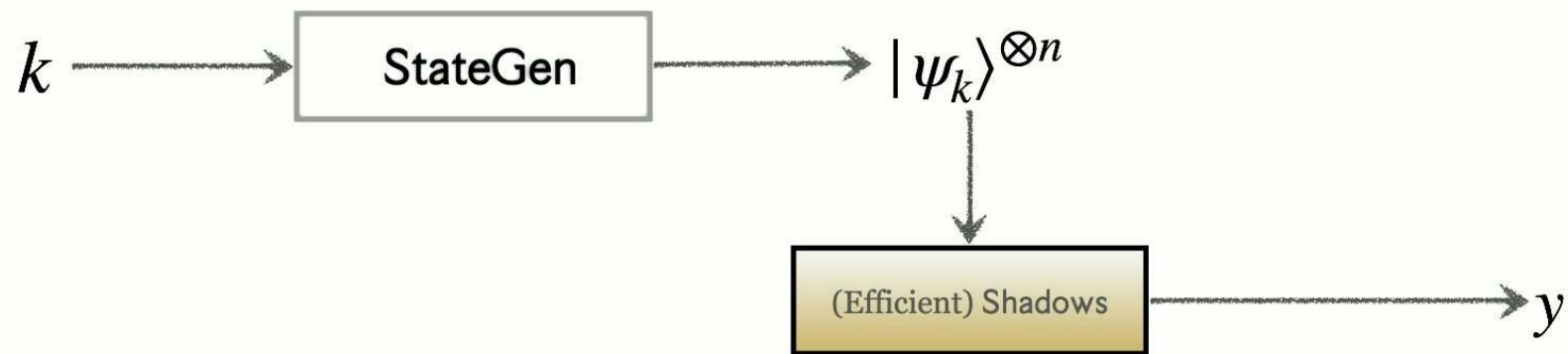
One-way States \implies One-way Puzzles

Efficient Shadow Tomography [HKP20]



Formally: With high probability over y , for small constant $\epsilon > 0$,
 $\forall x \in \{0,1\}^n$, $E(y, x)$ is ϵ -close to $|\langle \phi_x | \psi \rangle|^2$


One-way States \implies One-way Puzzles



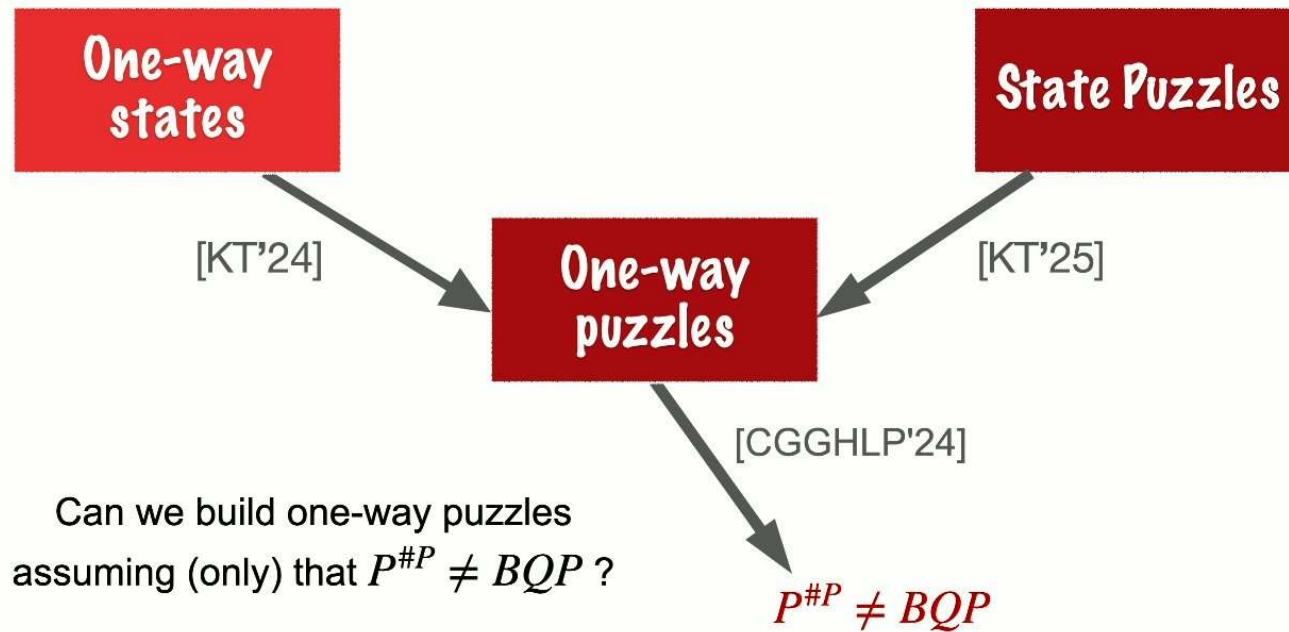
Puzzle sampler \longrightarrow (k, y) such that given y , it is hard to find k

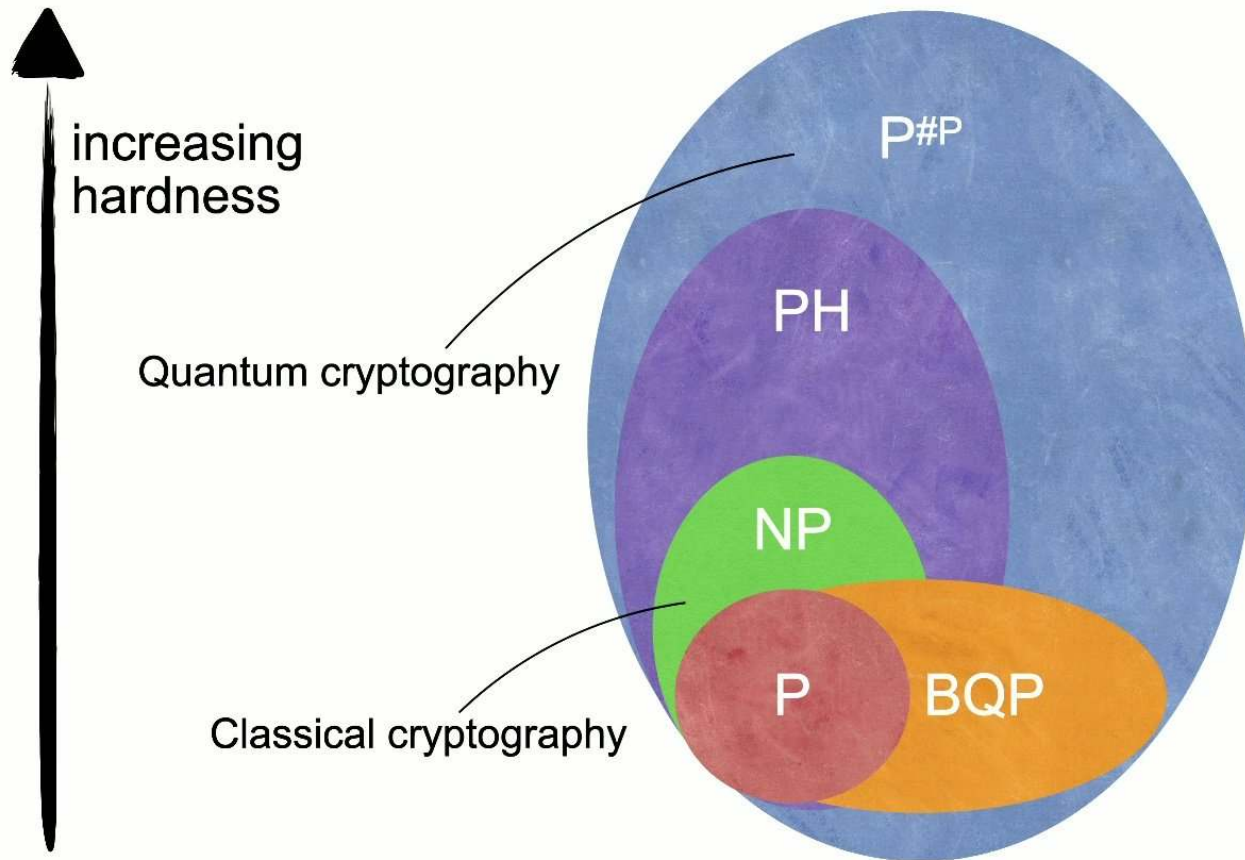
State Puzzles \implies One-way Puzzles

Capture the hardness of synthesizing a secret state $|\psi_s\rangle$ given a public string s

- [Grover-Rudolph'02]
It is possible to synthesize arbitrary states $|\psi_s\rangle$ given access to an oracle that exactly computes probabilities
- [K-Tomer'25]
Robust version — It is possible to **approx.** synthesize arbitrary states $|\psi_s\rangle$ given access to an oracle that **approx.** computes probabilities of a quantum process
- State puzzles exist \implies approximating probability outcomes of quantum processes is hard

One-way puzzles exist

So far,

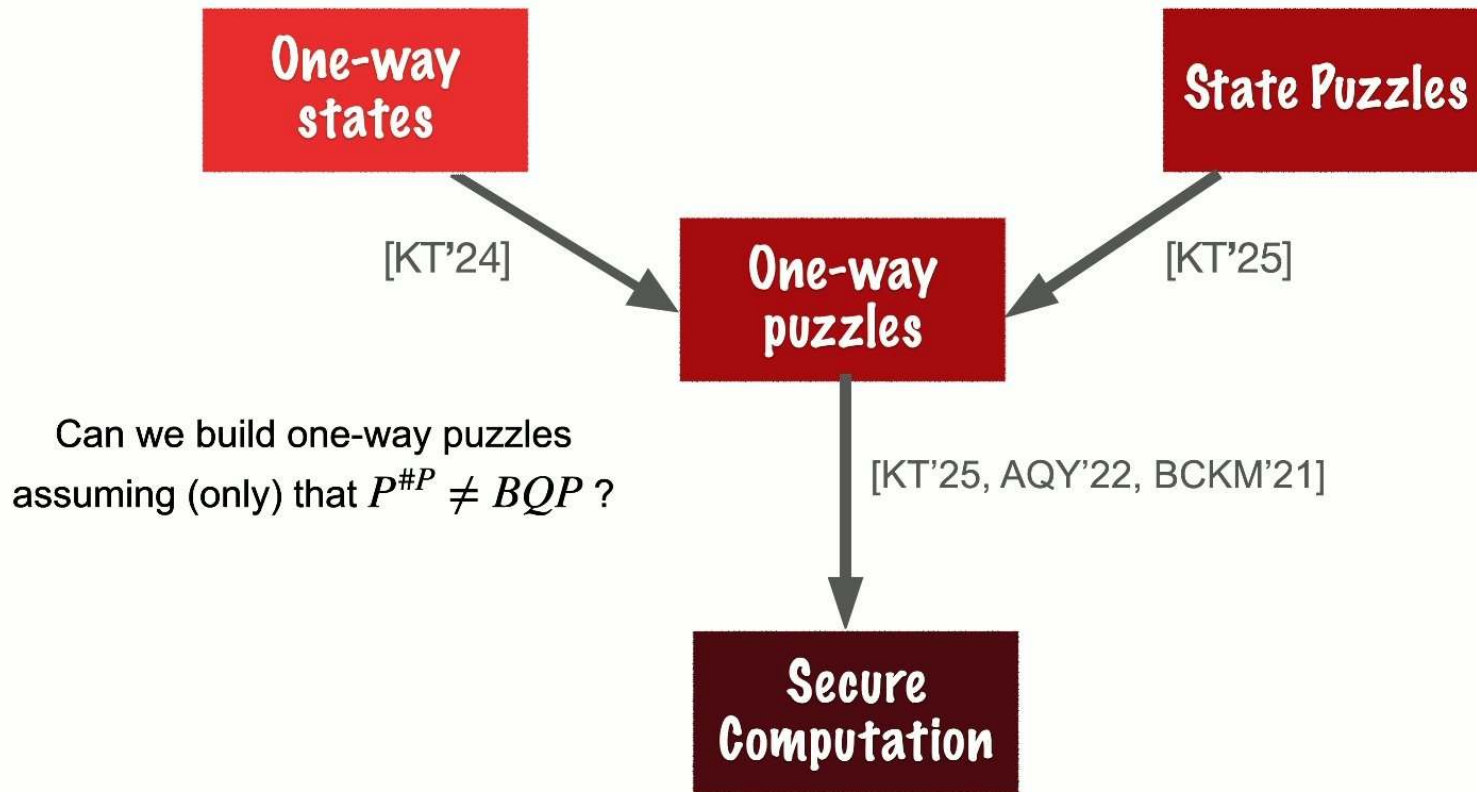




Dream: QCrypto from #P Hardness

- Dream: $P^{\#P} \neq BQP \implies$ quantum commitments exist.

Why care?



Secure Computation



On the Assumption

Assumption: There is a quantumly efficiently sampleable distribution A such that $\Pr_{a \leftarrow A} [a]$ are avg-case hard to approx. upto $\frac{1}{p(n).2^n}$ additive error in QPT.

- Literature in sampling-based quantum advantage conjectures this is **#P-hard**
 - 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....., Movassagh 23,...]
 - IQP [Bremner-Montanaro-Shepherd'14.....]

One-way puzzles and #P-hardness

Theorem [K-Tomer'25]

Assume certain conjectures from the quantum advantage literature,
Then one-way puzzles exist iff $P^{\#P} \neq BQP$.

Open Problems

- Obtain secure computation from even weaker assumptions (e.g. $P = PSPACE$?)
- Identify other cryptographically useful sources of hardness in a quantum world, and build signatures, encryption or quantum money.