Complexity $\cap$ Cryptography II:

Cryptography without One-Way Functions

Kabir Tomer (UIUC)
Based on joint work with Dakshita Khurana (UIUC)

Those who cannot prove… assume!

Those who cannot prove… assume!

- The limits of computation are poorly understood.

Those who cannot prove… assume!

- The limits of computation are poorly understood.

- It is hard to prove that a task cannot be performed by efficient adversaries.

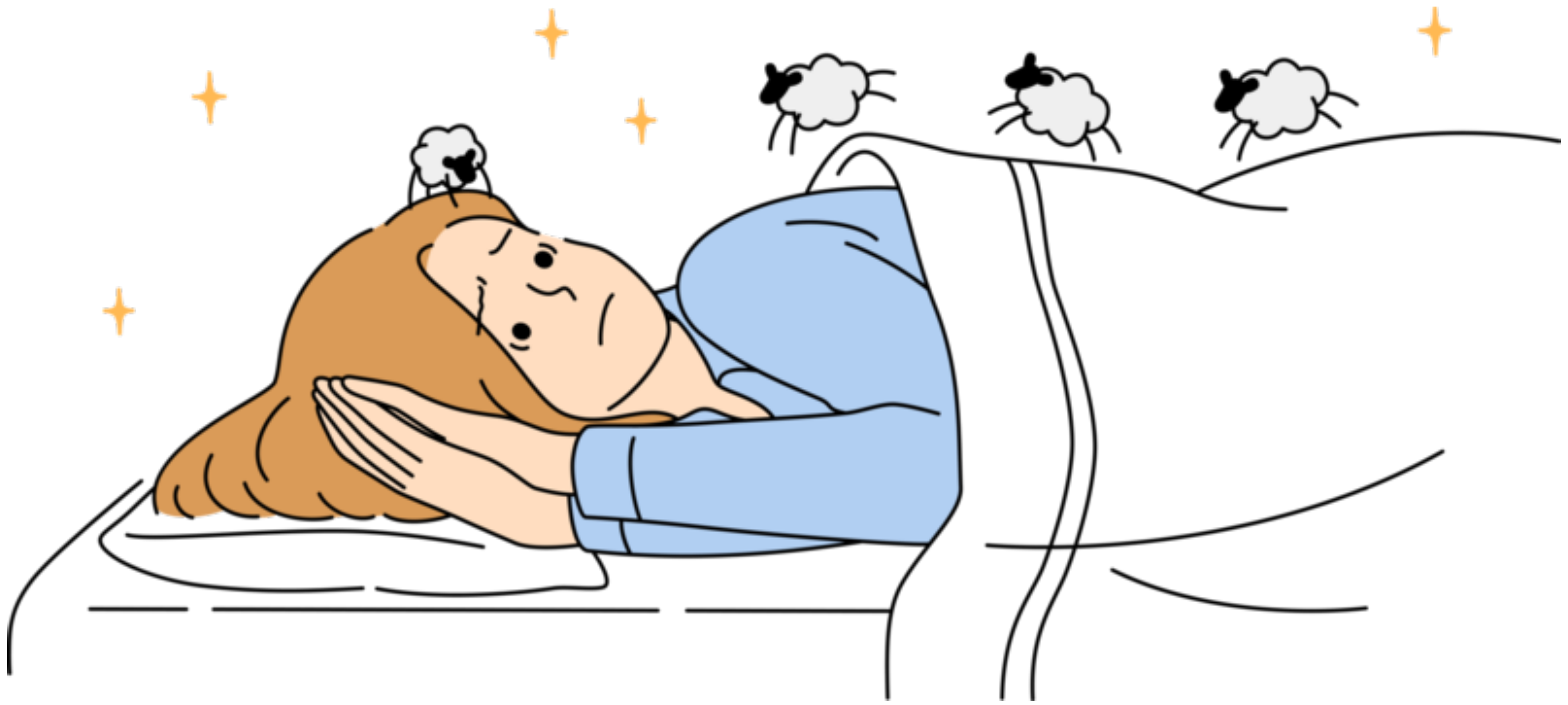
Those who cannot prove… assume!

- The limits of computation are poorly understood.
- It is hard to prove that a task cannot be performed by efficient adversaries.
- But cryptography is *all about* claiming that certain tasks cannot be performed by efficient adversaries.

Those who cannot prove… assume!

- The limits of computation are poorly understood.
- It is hard to prove that a task cannot be performed by efficient adversaries.
- But cryptography is *all about* claiming that certain tasks cannot be performed by efficient adversaries.
- So we must make assumptions.

What if our assumptions are false?



Cryptographers seldom sleep well([M]).

[M] Micali, Silvio, Personal Communication.

Goal: Make the mildest possible assumptions

Classical
Cryptography

$\downarrow$

$\boxed{\text{One-Way Functions}}$

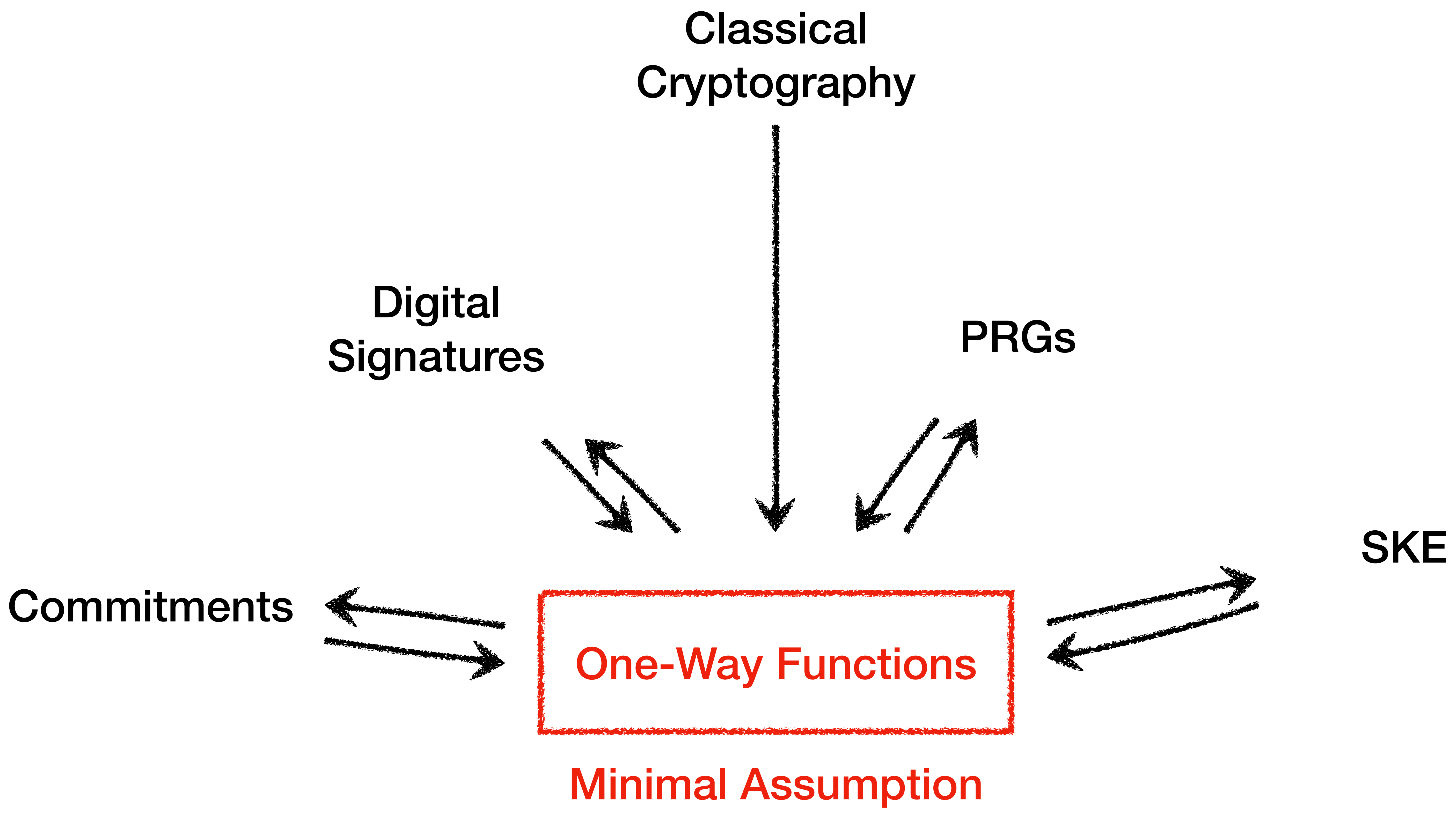
Goal: Make the mildest possible assumptions

Classical
Cryptography

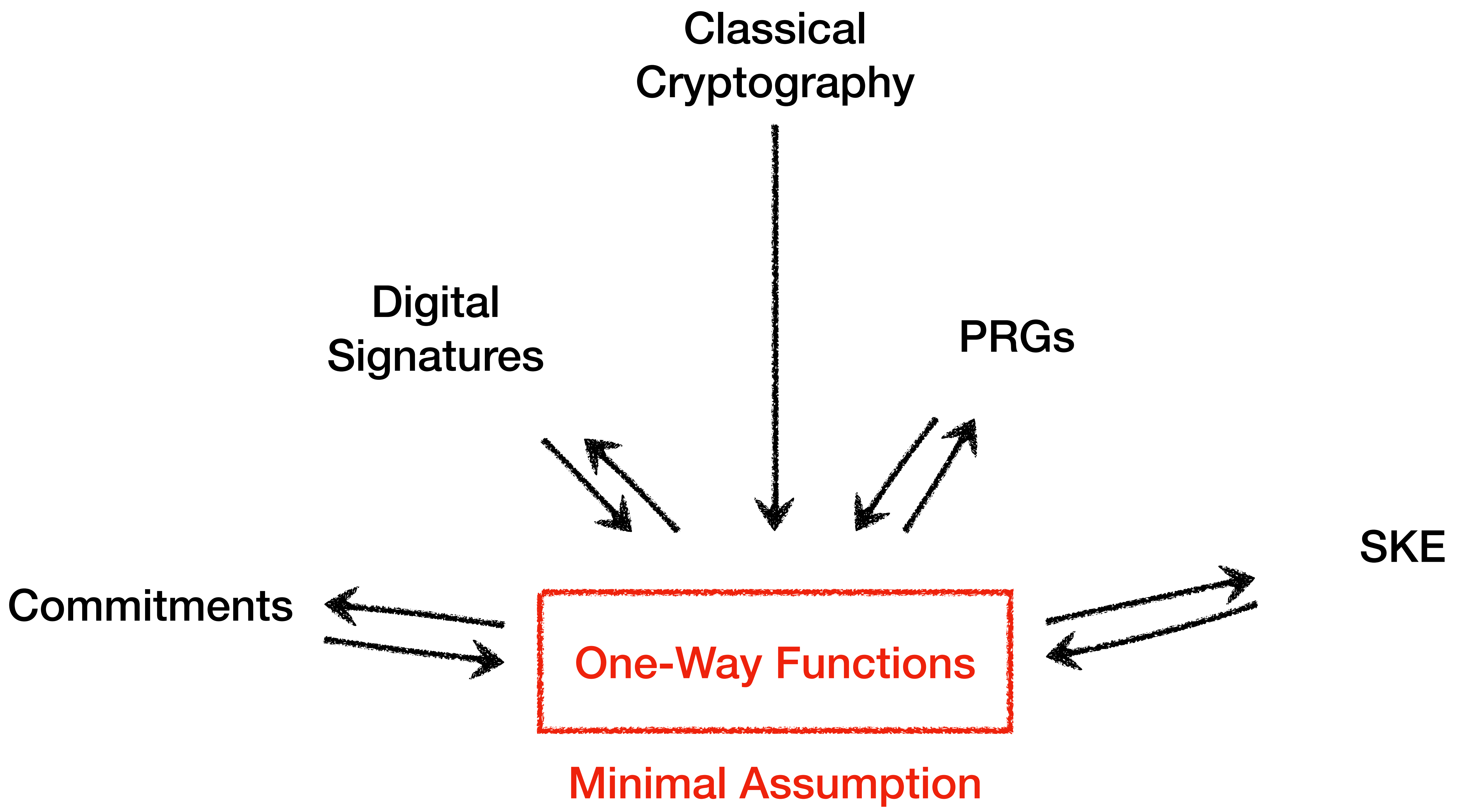
One-Way Functions

Minimal Assumption

Goal: Make the mildest possible assumptions



Goal: Make the mildest possible assumptions



Requires
$P \neq NP$

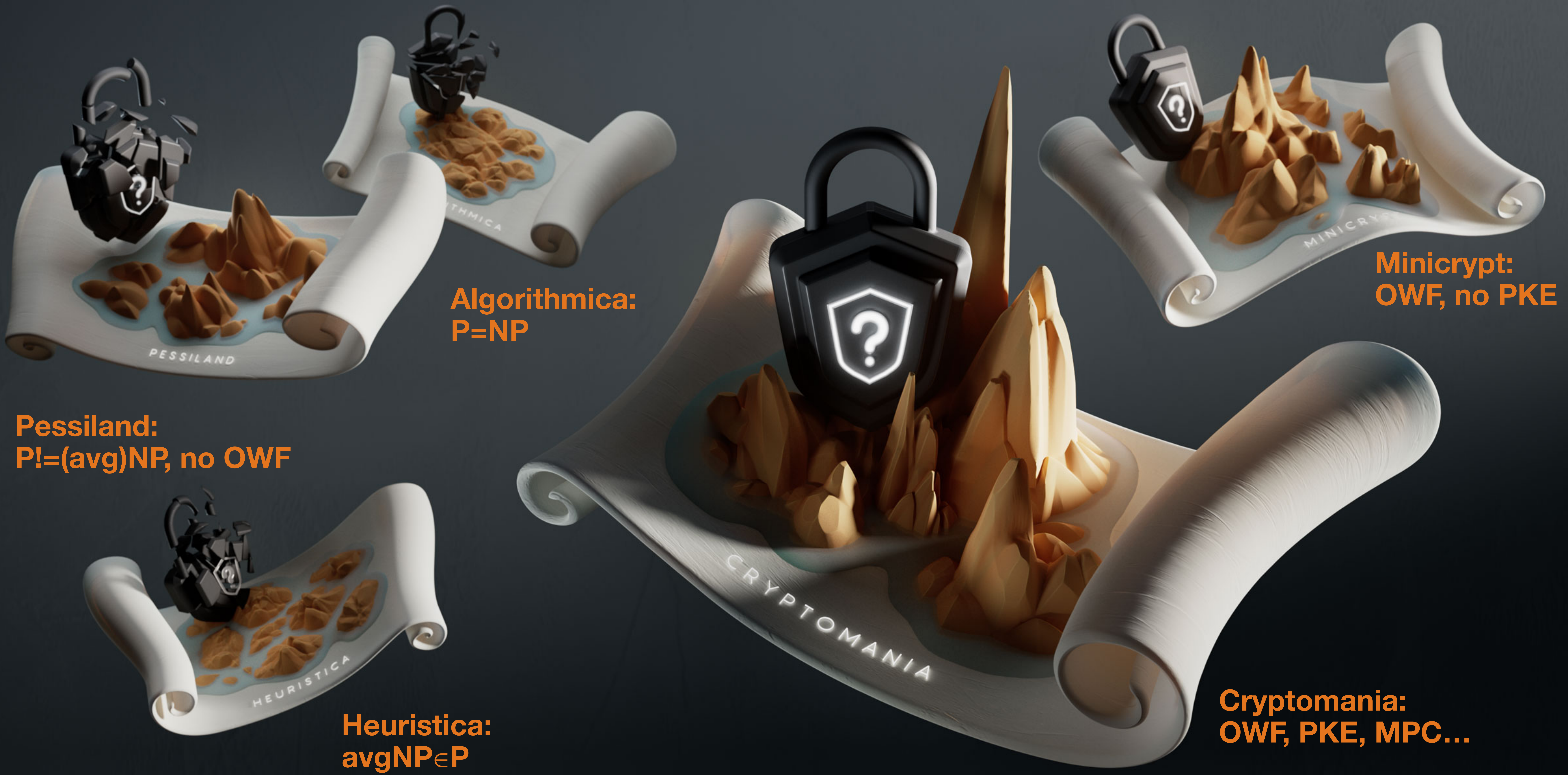


Image courtesy: Quanta magazine

A Quantum Dream: Crypto Without Assumptions

∃ Quantum Key Distribution ***unconditionally*** secure against ***unbounded*** adversaries

[Bennett-Brassard'84]

- What about other primitives?

Signatures

Secure Computation

Commitments

Zero-Knowledge

Coin-tossing

Public-Key Encryption

30 years ago…

- Commitments secure against unbounded adversaries were believed to exist

    See e.g., [Brassard-Crepeau-Josza-Langlois’93]

30 years ago…

- Commitments secure against unbounded adversaries were believed to exist

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

- Quantum MPC using commitments against unbounded adversaries

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

30 years ago…

- Commitments secure against unbounded adversaries were believed to exist

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

- Quantum MPC using commitments against unbounded adversaries

  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]

No escape from computational assumptions?

- Cannot achieve security against *unbounded* adversaries for most cryptographic primitives

No escape from computational assumptions?

- Cannot achieve security against *unbounded* adversaries for most cryptographic primitives

- Must consider computationally bounded adversaries ☹

No escape from computational assumptions?

- Cannot achieve security against *unbounded* adversaries for most cryptographic primitives
- Must consider computationally bounded adversaries ☹
- But we can weaken the assumptions required! ☺

Escaping Cryptomania

MPC and PKE from One-Way Functions

Escaping Cryptomania

MPC and PKE from One-Way Functions

One-Way Functions → Commitments → Secure MPC

[Bartusek-Coladangelo-Khurana-Ma'21, Grilo-Lin-Song-Vaikuntanathan'21, Ananth-Qian-Yuen'22]

Escaping Cryptomania

MPC and PKE from One-Way Functions

One-Way Functions → Commitments → Secure MPC

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

One-Way Functions → Public Key Encryption*

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

*with quantum public keys and ciphertexts

Escaping Cryptomania

MPC and PKE from One-Way Functions

One-Way Functions → Commitments → Secure MPC

[Bartusek-Coladangelo-Khurana-Ma'21, Grilo-Lin-Song-Vaikuntanathan'21, Ananth-Qian-Yuen'22]

One-Way Functions → Public Key Encryption*

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

Both impossible in the classical setting! [Impagliazzo-Rudich'89]

*with quantum public keys and ciphertexts

Can we base quantum cryptography on assumptions <u>even weaker</u> than one-way functions?

Escaping Minicrypt

Pseudorandom States

(efficient)

$$\boxed{\text{Gen}(k)} \longrightarrow |\psi_k\rangle$$

$$|\psi_k\rangle^{\otimes poly(n)} \approx_c |\phi\rangle^{\otimes poly(n)}$$

where $|\phi\rangle$ is a truly (Haar) random quantum state and k is a uniform string

Escaping Minicrypt

Pseudorandom States

(efficient)

$$\boxed{\text{Gen}(k)} \longrightarrow |\psi_k\rangle$$

$$|\psi_k\rangle^{\otimes poly(n)} \approx_c |\phi\rangle^{\otimes poly(n)}$$

where $|\phi\rangle$ is a truly (Haar) random quantum state and k is a uniform string

- Can be constructed from one-way functions [Ji-Liu-Song'16]

Escaping Minicrypt

Pseudorandom States

(efficient)

$$\boxed{\text{Gen}(k)} \longrightarrow |\psi_k\rangle$$

$$|\psi_k\rangle^{\otimes poly(n)} \approx_c |\phi\rangle^{\otimes poly(n)}$$

where $|\phi\rangle$ is a truly (Haar) random quantum state and k is a uniform string

- Can be constructed from one-way functions [Ji-Liu-Song’18]
- Relative to a quantum oracle, pseudorandom states can exist even if BQP = QMA [Kretschmer’21]

Pseudorandom states are useful! [AQY'22, MY'22]

Pseudorandom states are useful! [AQY'22, MY'22]

- Using pseudorandom states we can define distributions:
  - $\mathscr{D}_0$: Output a (Haar) random quantum state
  - $\mathscr{D}_1$: Output a pseudorandom quantum state

Pseudorandom states are useful! [AQY'22, MY'22]

- Using pseudorandom states we can define distributions:
  - $\mathscr{D}_0$: Output a (Haar) random quantum state
  - $\mathscr{D}_1$: Output a pseudorandom quantum state
- This gives a pair of distributions that are
  - **E**fficient to sample from
  - Statistically **F**ar
  - Computationally **I**ndistinguishable

Pseudorandom states are useful! [AQY'22, MY'22]

- Using pseudorandom states we can define distributions:
  - $\mathscr{D}_0$: Output a (Haar) random quantum state
  - $\mathscr{D}_1$: Output a pseudorandom quantum state
- This gives a pair of distributions that are
  - **E**fficient to sample from
  - Statistically **F**ar
  - Computationally **I**ndistinguishable
- AKA an **EFI** pair, known to be equivalent to (quantum) bit commitments [BCQ'22, Yan'22]

Cryptography even if $\mathsf{P} = \mathsf{NP}$ **!**

- Relative to a quantum oracle, commitments can exist even if $\mathsf{BQP} = \mathsf{QMA}$ [Kretschmer'21]

Cryptography even if $\mathsf{P} = \mathsf{NP}$!

- Relative to a quantum oracle, commitments can exist even if $\mathsf{BQP} = \mathsf{QMA}$ [Kretschmer'21]
- Relative to a classical oracle, commitments can exist even if $\mathsf{P} = \mathsf{NP}$ [KQST'23, KQT'24]

Cryptography even if $\mathsf{P} = \mathsf{NP}$ **!**

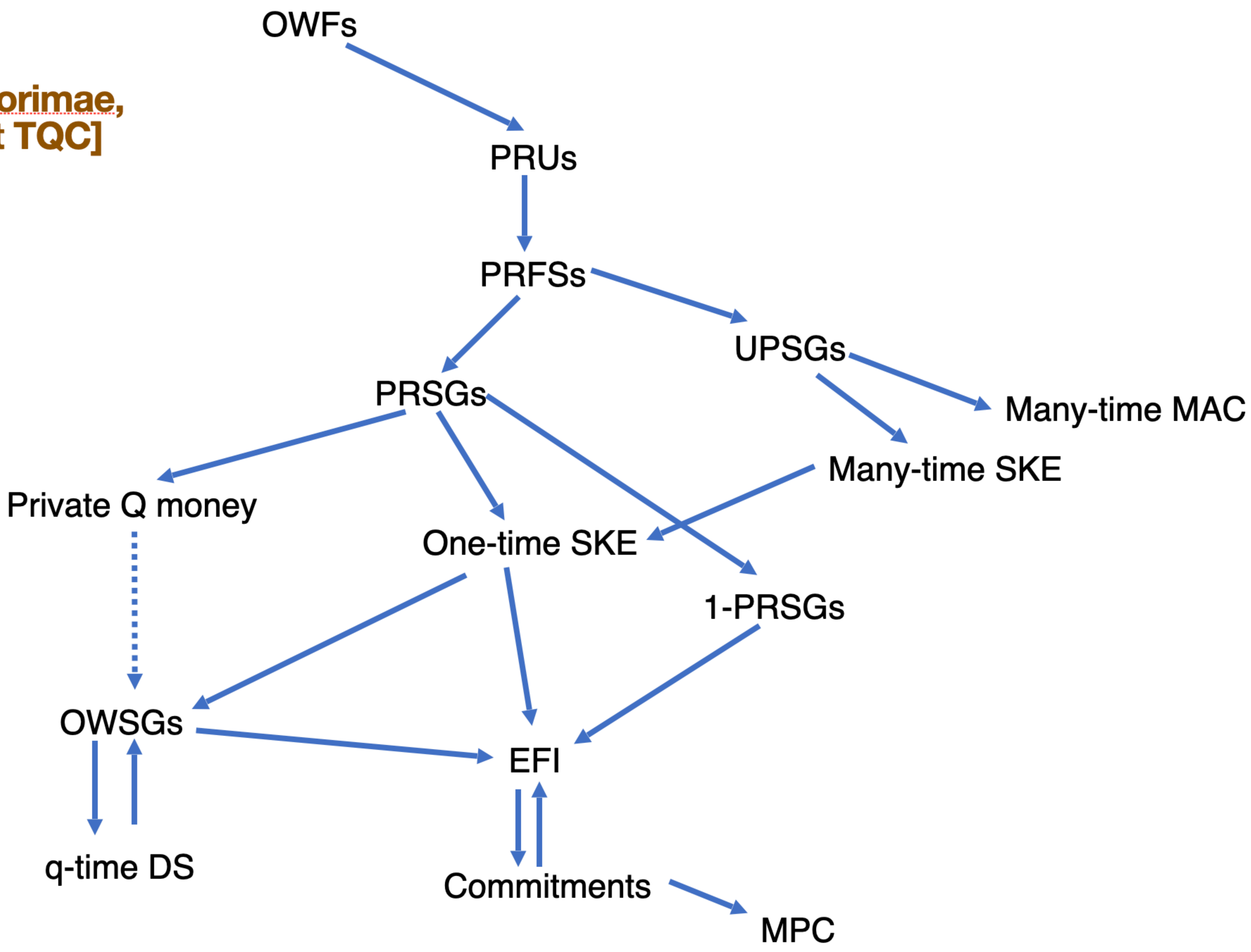
- Relative to a quantum oracle, commitments can exist even if $\mathsf{BQP} = \mathsf{QMA}$ [Kretschmer'21]
- Relative to a classical oracle, commitments can exist even if $\mathsf{P} = \mathsf{NP}$ [KQST'23, KQT'24]
- Conjectured that commitments can exist relative to *any* classical oracle! [LMW'24]

Cryptography even if $\mathsf{P} = \mathsf{NP}$!

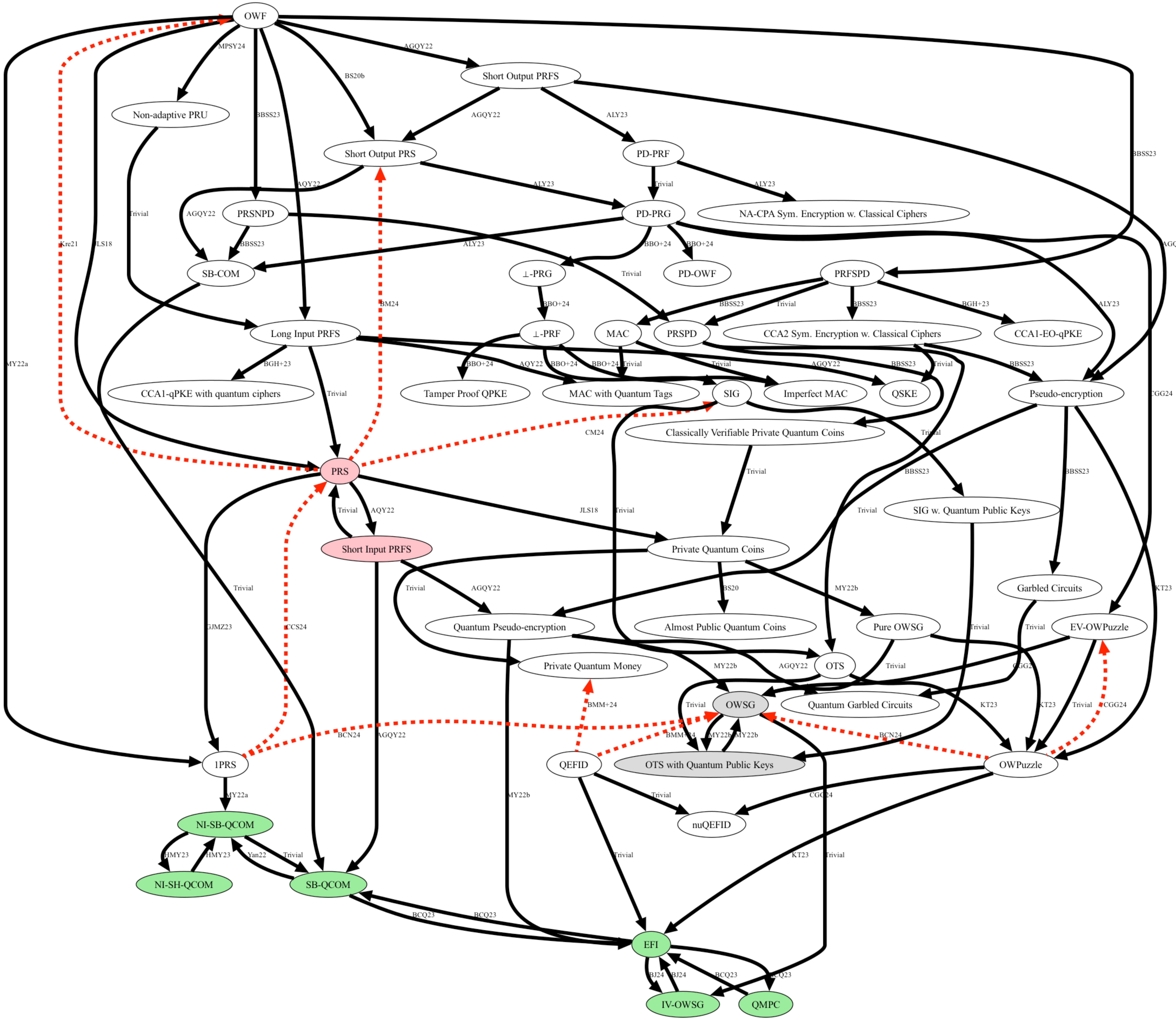
- Relative to a quantum oracle, commitments can exist even if $\mathsf{BQP} = \mathsf{QMA}$ [Kretschmer'21]
- Relative to a classical oracle, commitments can exist even if $\mathsf{P} = \mathsf{NP}$ [KQST'23, KQT'24]
- Conjectured that commitments can exist relative to *any* classical oracle! [LMW'24]

Recall that in the quantum world, commitments are sufficient for MPC!

[Tomoyuki Morimae, invited talk at TQC]



[https://sattath.github.io/microcrypt-zoo/]



How can we understand quantum cryptography without one-way functions?

What questions can we ask?

Understanding Microcrypt: Some Lenses

1. Is there a quantum “minimal” primitive/analogue of one-way functions?

2. Can we build cryptosystems from concrete mathematical problems that are harder than inverting one-way functions?

3. Classical cryptography cannot exist if P=NP. What connections does quantum cryptography have with (traditional) complexity theory?

Understanding Microcrypt: Some Lenses

1. Is there a quantum “minimal” primitive/analogue of one-way functions?

2. Can we build cryptosystems from concrete mathematical problems that are harder than inverting one-way functions?

3. Classical cryptography cannot exist if P=NP. What connections does quantum cryptography have with (traditional) complexity theory?

One-Wayness in a Quantum World

- Classically, one-way functions capture the hardness inherent in cryptographic search problems in natural way.
- Additional desirable properties: robustness, combiners, universal constructions, etc.
- Is there a quantum equivalent?

One-Wayness in a Quantum World

Quantum One-Way Function

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

Can exist even if $\mathsf{P} = \mathsf{NP}$
Cannot exist if $\mathsf{BQP} = \mathsf{QMA}$

One-Wayness in a Quantum World

Quantum One-Way Function

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]

One-Wayness in a Quantum World

Quantum One-Way Function

One-Way States

State Puzzles

(Quantum) efficient algorithm $\rightarrow (s, |\psi_s\rangle)$

s.t. hard to output $|\psi_s\rangle$ given s

$\uparrow$

Quantum Money,
Quantum Secret Key
Primitives

One-Wayness in a Quantum World

Quantum One-Way Function

One-Way States

State Puzzles

One-Way Puzzles

One-Way Puzzles [Khurana-T. 24]

Efficient quantum process sampling problems along with their solutions.

(efficient)

$$\boxed{\mathsf{Samp}(1^n)} \longrightarrow (x, y) \in \mathscr{R}$$

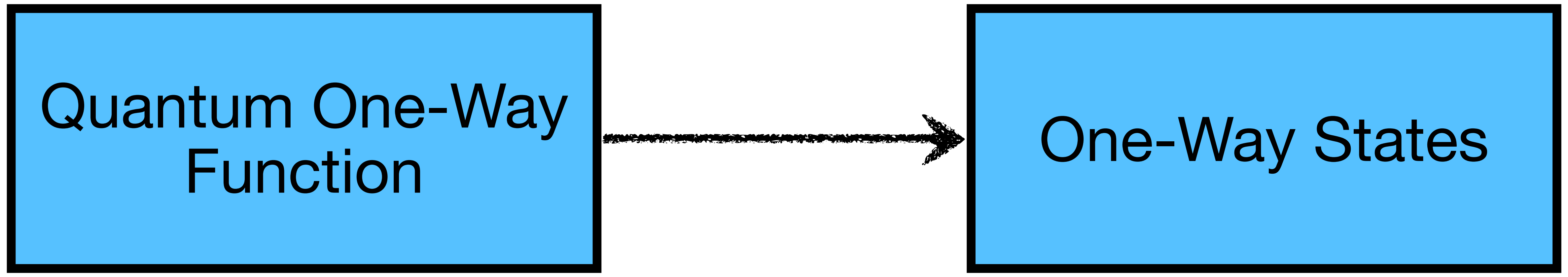
Given y, computationally infeasible to find x' s.t. $(x', y) \in \mathscr{R}$

Note that $\mathscr{R}$ does not need to be an NP relation (or even efficient)!

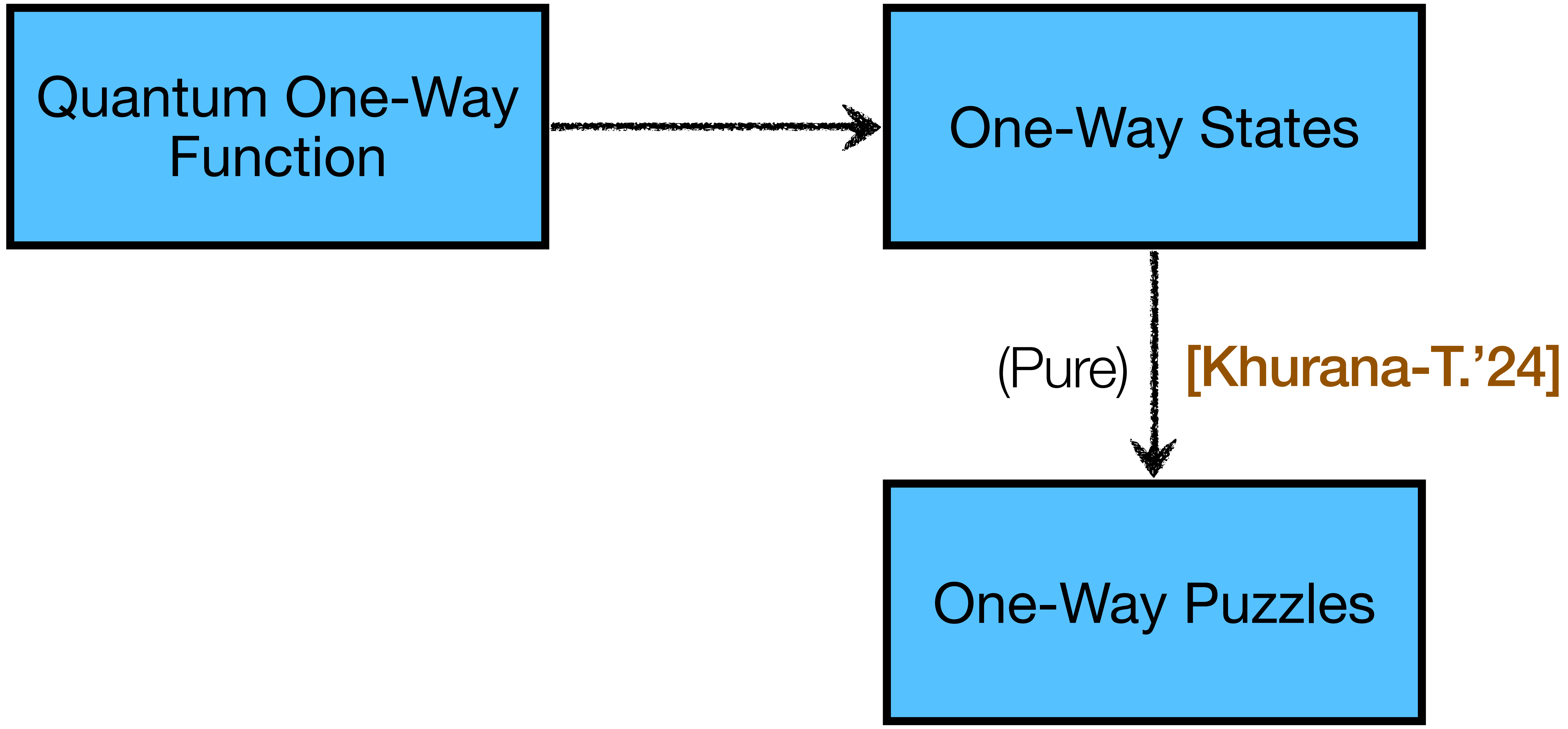
What can we do with one-wayness?

Quantum One-Way Function

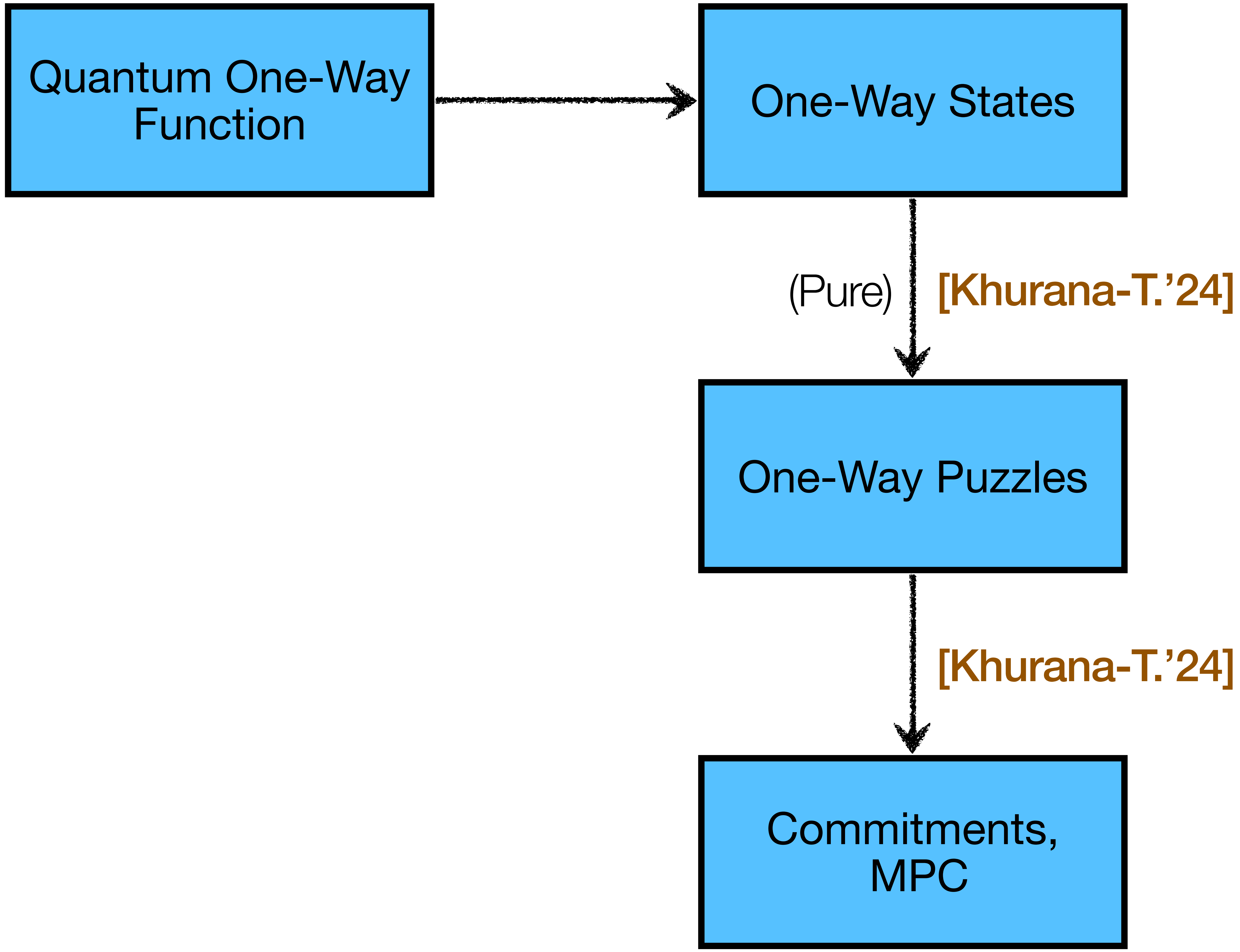
What can we do with one-wayness?



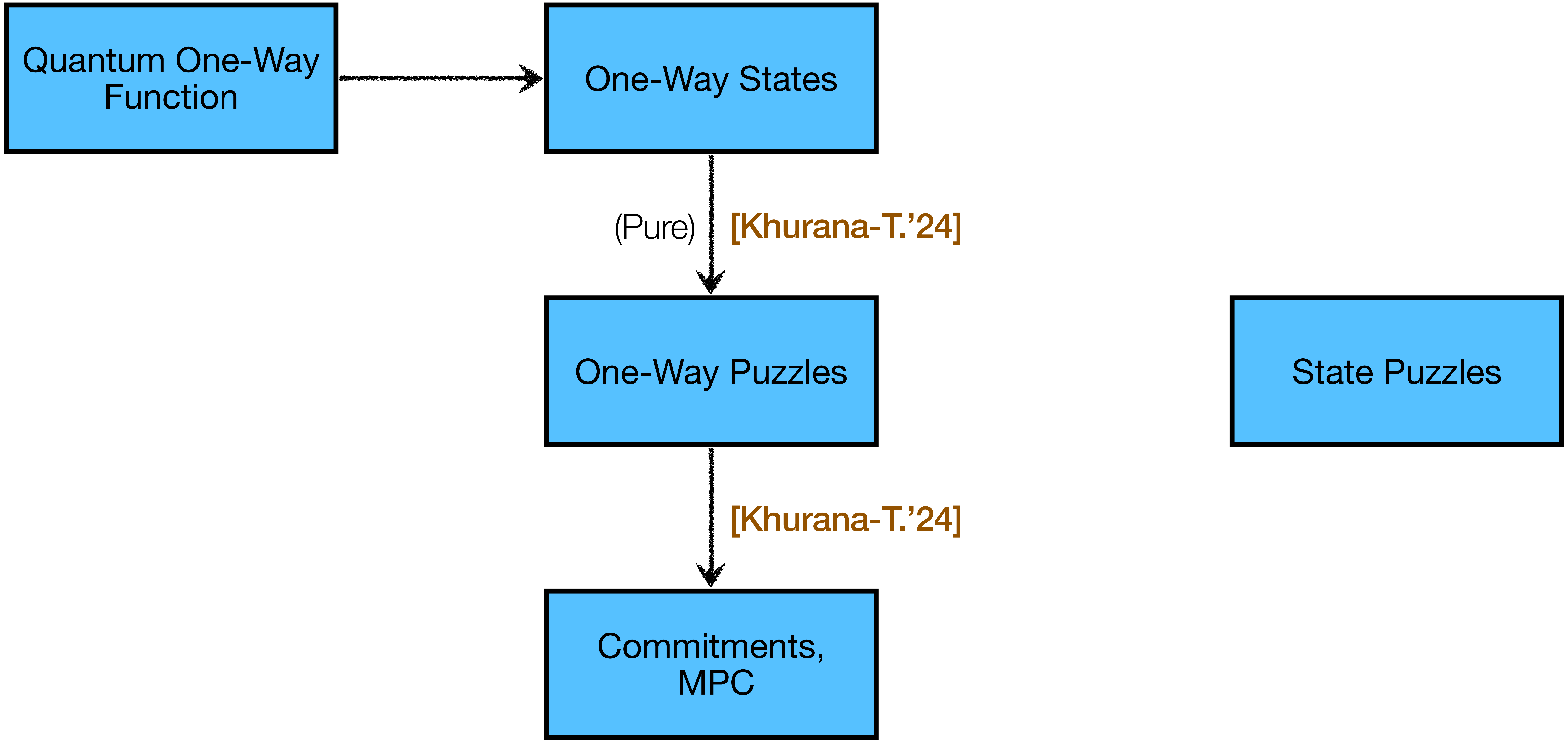
What can we do with one-wayness?



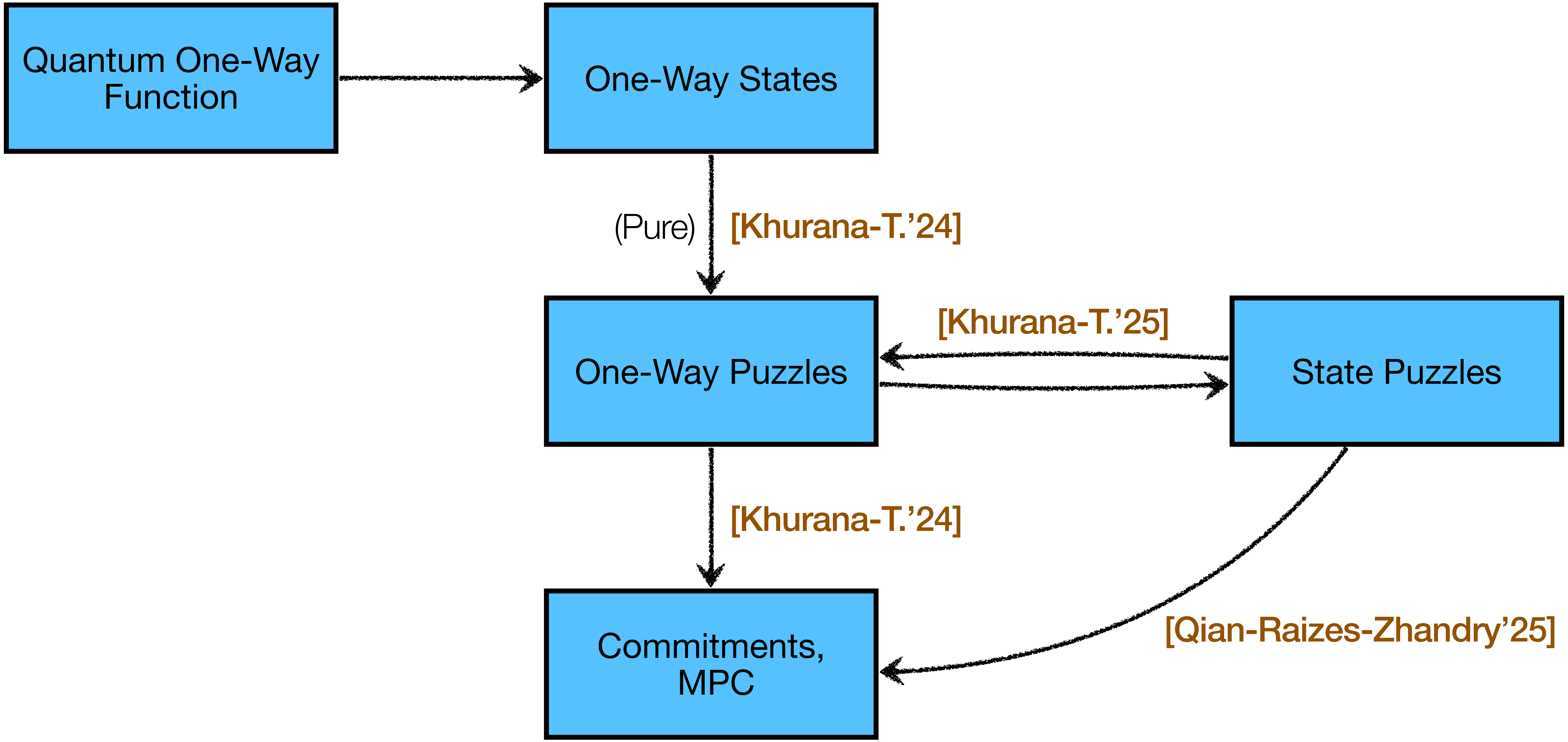
What can we do with one-wayness?



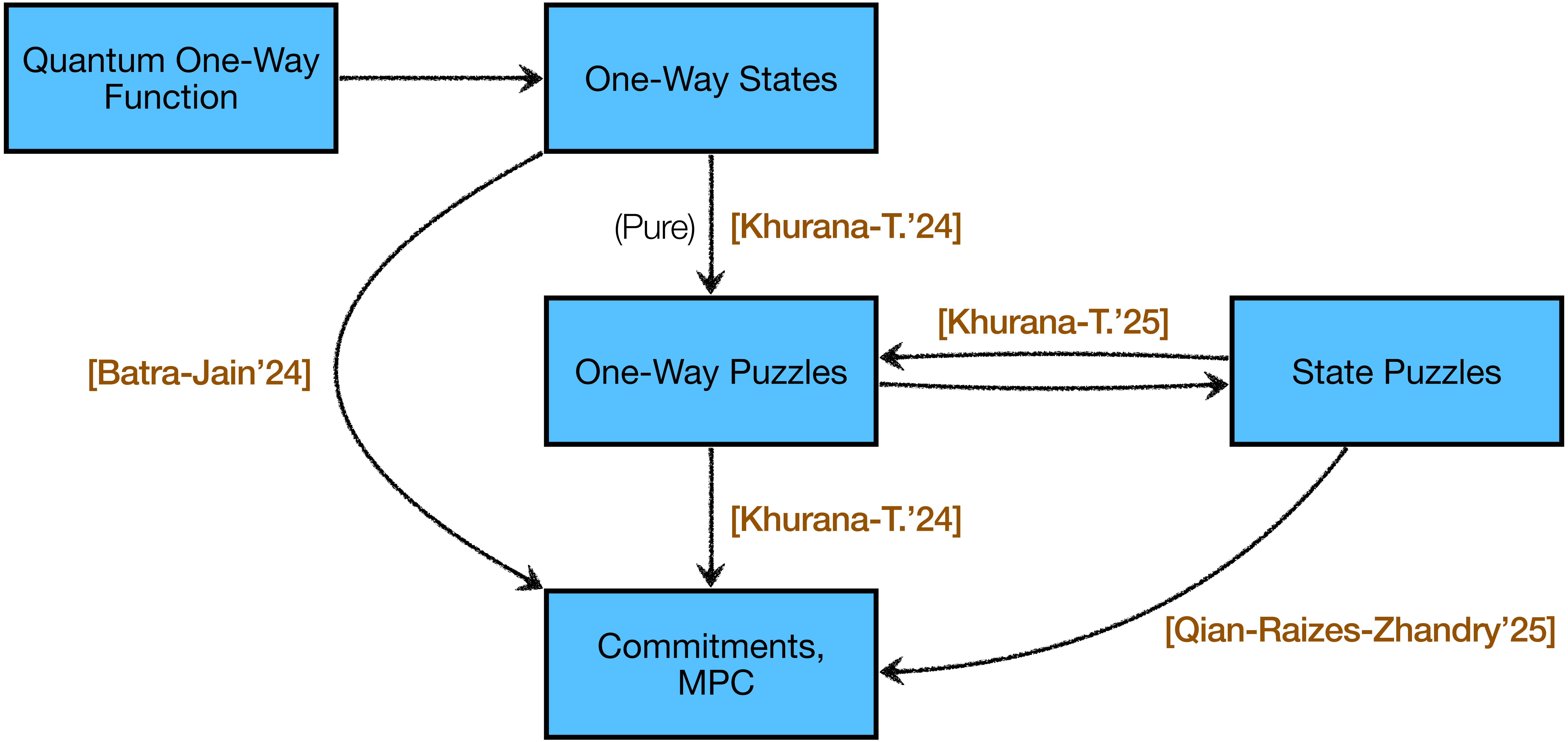
What can we do with one-wayness?



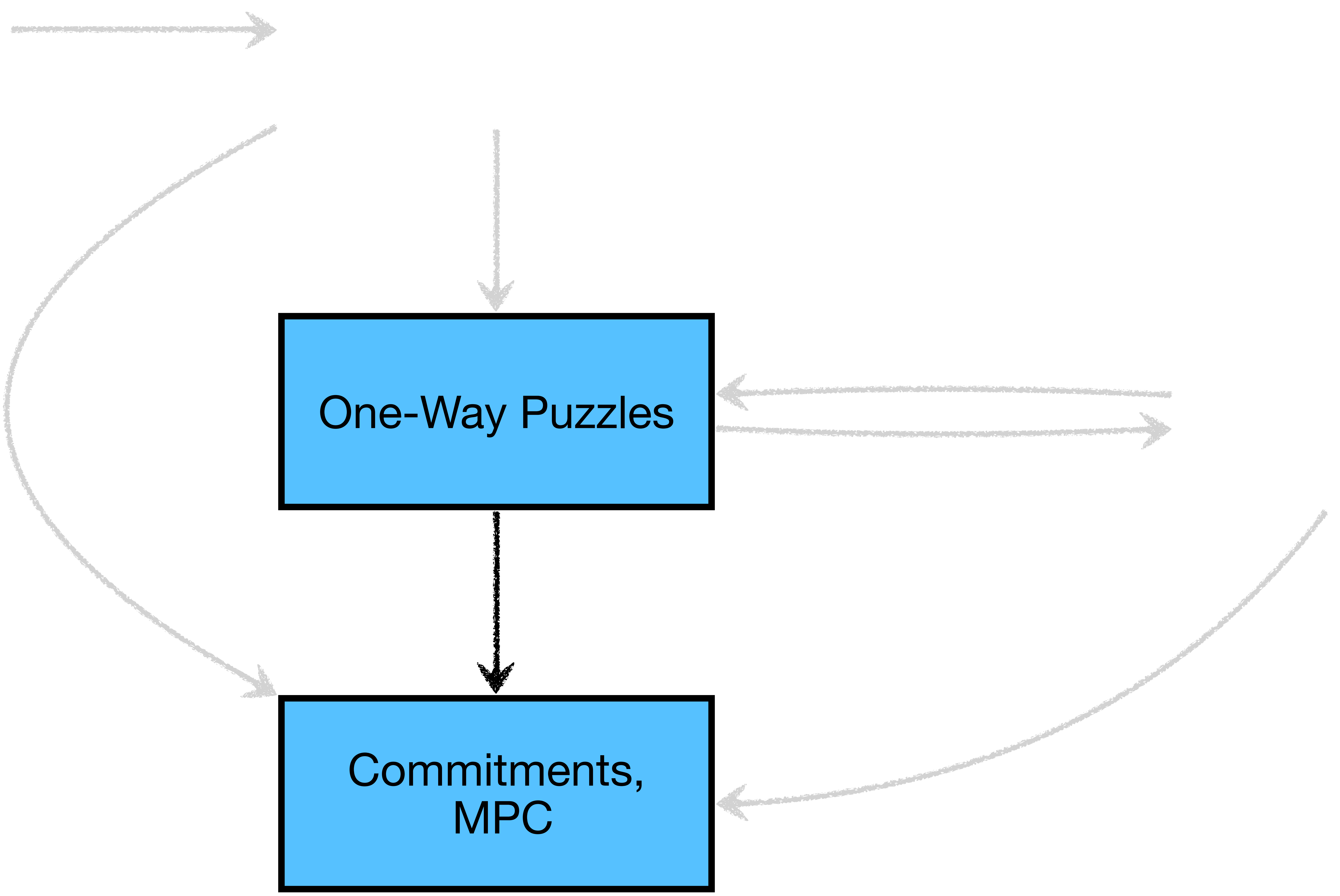
What can we do with one-wayness?



What can we do with one-wayness?



What can we do with one-wayness?



Do we fully understand one-wayness?

- We have considered the hardness of
  - Classical problems with classical solutions (One-way puzzles)
  - Quantum problems with classical solutions (One-way states)
  - Classical problems with quantum solutions (State Puzzles)

Do we fully understand one-wayness?

- We have considered the hardness of
  - Classical problems with classical solutions (One-way puzzles)
  - Quantum problems with classical solutions (One-way states)
  - Classical problems with quantum solutions (State Puzzles)
- What about quantum problems with quantum solutions?
  (Some attempts, see [QRZ’25])

Understanding Microcrypt: Some Lenses

1. Is there a quantum “minimal” primitive/analogue of one-way functions?

2. Can we build cryptosystems from concrete mathematical problems that are harder than inverting one-way functions?

3. Classical cryptography cannot exist if P=NP. What connections does quantum cryptography have with (traditional) complexity theory?

The Scarcity of Concrete Instantiations

The Scarcity of Concrete Instantiations

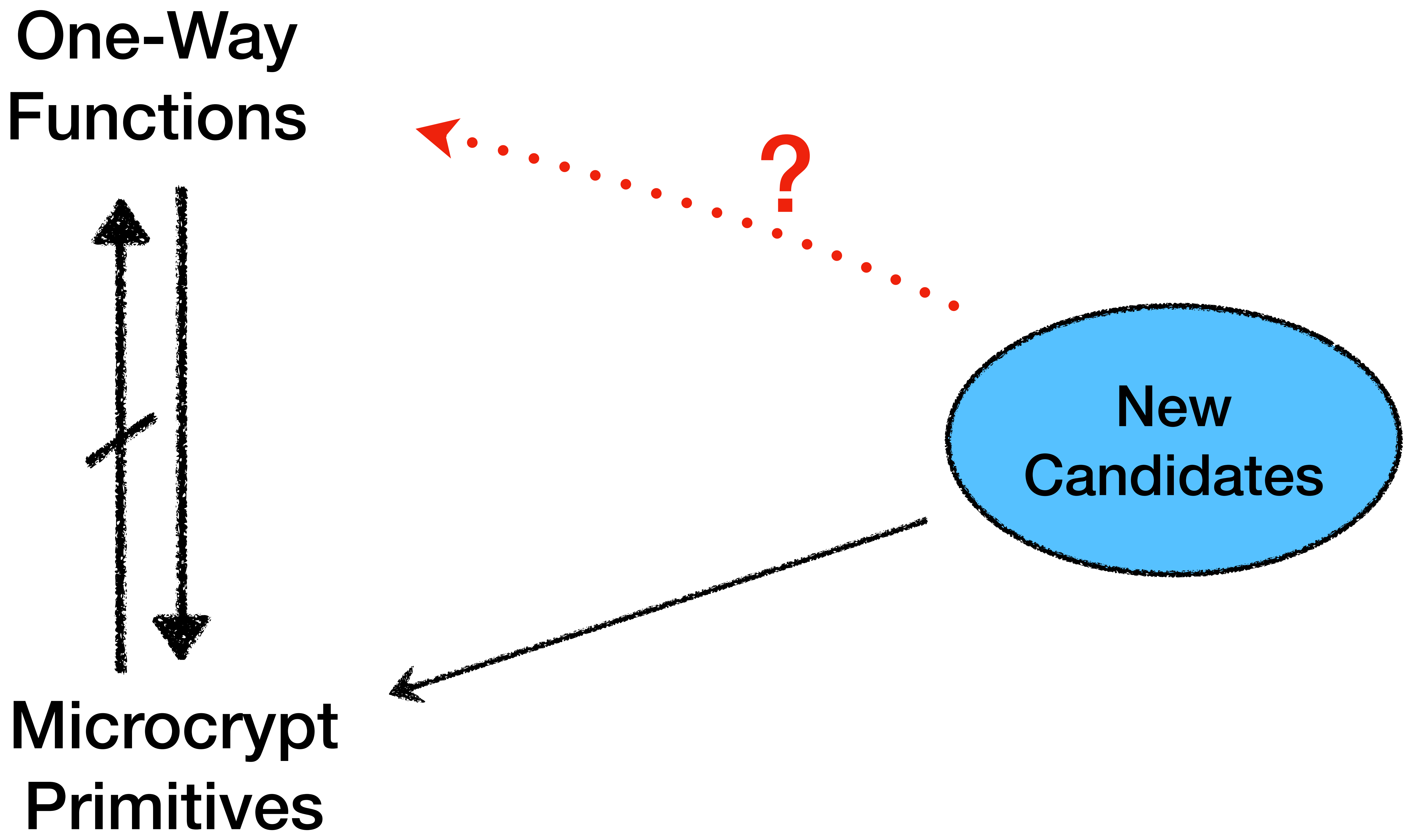
- Microcrypt primitives are implied by (post-quantum) one-way functions.

The Scarcity of Concrete Instantiations

- Microcrypt primitives are implied by (post-quantum) one-way functions.
- Separations from OWFs involve oracle constructions; unknown how to instantiate in the standard model without OWFs.

The Scarcity of Concrete Instantiations

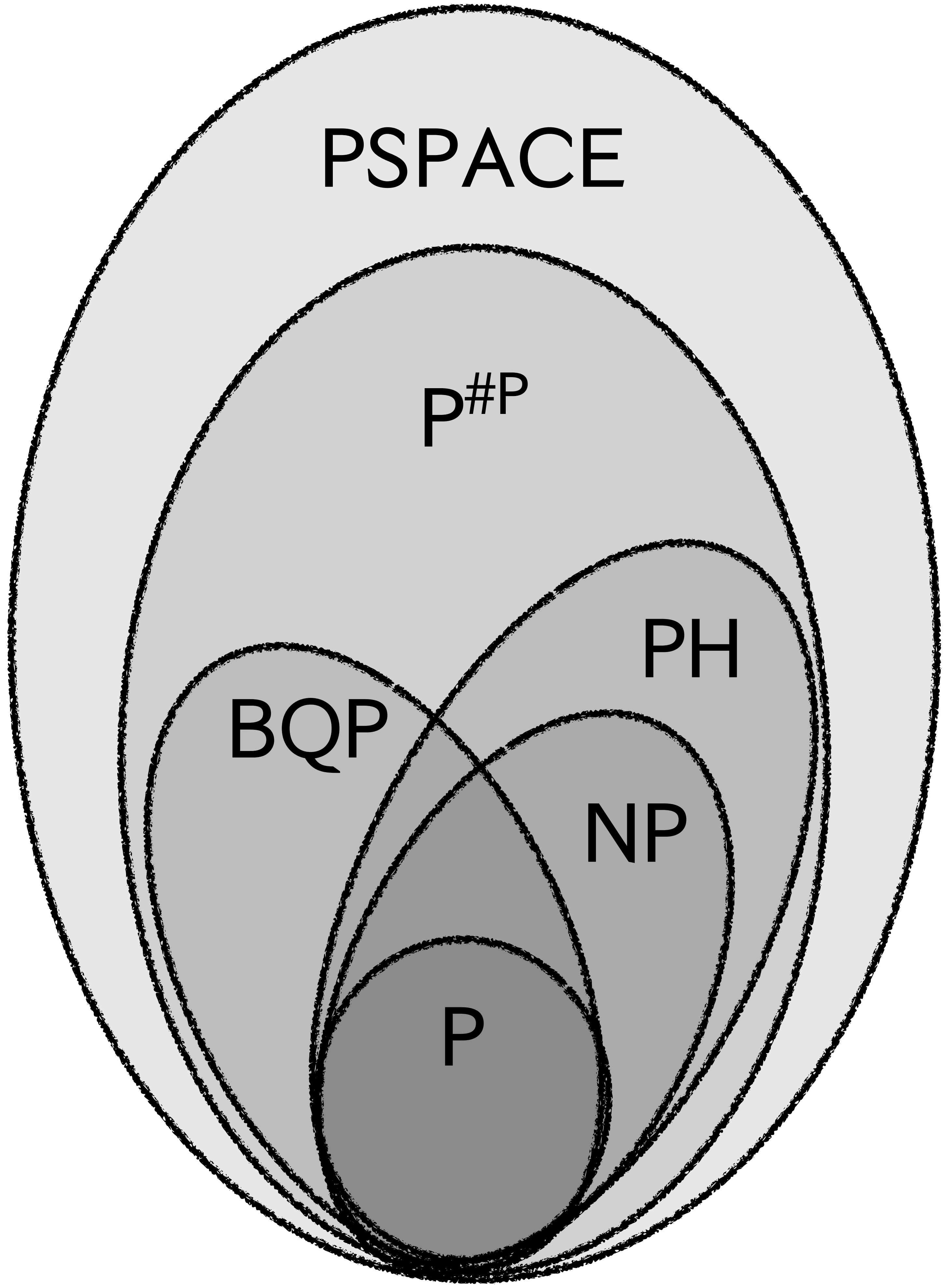
- Microcrypt primitives are implied by (post-quantum) one-way functions.
- Separations from OWFs involve oracle constructions; unknown how to instantiate in the standard model without OWFs.
- Proposed Candidates:
  - For random quantum circuit C, $C|0\rangle$ is conjectured to be pseudorandom [AQY'22][FGSY'25]
  - For random IQP circuit C, $C|0\rangle$ is conjectured to be pseudorandom [BHHP'24]


One-Way Functions
?
New Candidates
Microcrypt Primitives

A Ground-Up Approach:

(1) Look for sources of hardness beyond the polynomial hierarchy.

(2) Build cryptography from these new sources.



The Complexity of Counting

- The class #P captures the complexity of finding the number of satisfying assignments to a boolean formula.

The Complexity of Counting

- The class #P captures the complexity of finding the number of satisfying assignments to a boolean formula.
- $\mathrm{NP} \subseteq \mathrm{PH} \subseteq \mathrm{P}^{\#\mathrm{P}}$ [Toda's Theorem]

The Complexity of Counting

- The class #P captures the complexity of finding the number of satisfying assignments to a boolean formula.
- $\mathrm{NP} \subseteq \mathrm{PH} \subseteq \mathrm{P}^{\#\mathrm{P}}$ [Toda's Theorem]
- But solving #P-complete problems is believed to be *beyond* the power of PH (or even $\mathrm{BQP}^{\mathrm{NP}}$)

The Complexity of Counting

- The class #P captures the complexity of finding the number of satisfying assignments to a boolean formula.
- $\mathrm{NP} \subseteq \mathrm{PH} \subseteq \mathrm{P}^{\#\mathrm{P}}$ [Toda's Theorem]
- But solving #P-complete problems is believed to be *beyond* the power of PH (or even $\mathrm{BQP}^{\mathrm{NP}}$)
- Several #P-complete problems admit worst-case to average-case reductions!

Dream Goal: Build Crypto from a #P-hard problem

$\mathsf{P}^{\#\mathsf{P}} \not\subseteq \mathsf{BQP} \implies$ Quantum Cryptography exists!

- Cryptography from an *extremely* mild worst-case assumption.
- Much weaker than even assuming NP is hard!

Our Results

Main Theorem (informal) [Khurana-**T**'25]

Assume *any one* (from a set of) quantum advantage conjectures:

$$\#\mathrm{P} \not\subseteq \mathrm{BQP} \iff \text{One-Way Puzzles exist}$$

Building One-Way Puzzles

- One-way puzzles are invertible using a #P oracle [CGGHLP'24]
- They can exist only if $P^{\#P} \not\subseteq BQP$

- Can we build one-way puzzles assuming (only) that $P^{\#P} \not\subseteq BQP$?

Permanants are #P-hard on average

- Permanant of a matrix $A :=$ $\text{Perm}(A) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} a_{i,\sigma_i}$

- Computing the permanent is #P-hard on average

- Can we build one-way puzzles from the hardness of computing permanents?

Puzzles from Permanents: First Attempt

- Sampler must *efficiently* sample (x, y) such that given y it is hard to find x.

Puzzles from Permanents: First Attempt

- Sampler must *efficiently* sample (x, y) such that given y it is hard to find x.
- Can we set $(x, y) = (\text{Perm}(A), A)$?

Puzzles from Permanents: First Attempt

- Sampler must *efficiently* sample (x, y) such that given y it is hard to find x.
- Can we set $(x, y) = (\text{Perm}(A), A)$?
- We can efficiently sample A such that finding $\text{Perm}(A)$ is hard.

Puzzles from Permanents: First Attempt

- Sampler must *efficiently* sample (x, y) such that given y it is hard to find x.
- Can we set $(x, y) = (\text{Perm}(A), A)$?
- We can efficiently sample A such that finding $\text{Perm}(A)$ is hard.
- Don't know how to sample $(\text{Perm}(A), A)$

An insight from quantum advantage

[SB09, BJS11, AA11, BMS16, FM17, BIS+18, BFNV19, KMM21, BFLL21, Kro22, Mov23, ZVBL23]

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

An insight from quantum advantage

[SB09, BJS11, AA11, BMS16, FM17, BIS+18, BFNV19, KMM21, BFLL21, Kro22, Mov23, ZVBL23]

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

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

An insight from quantum advantage

[SB09, BJS11, AA11, BMS16, FM17, BIS+18, BFNV19, KMM21, BFLL21, Kro22, Mov23, ZVBL23]

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

- Permanents hard to compute $\implies$ *probabilities of outcomes* are hard to compute

- Can we use this insight to build puzzles?

Puzzles from #P-hardness of computing $\Pr_{\mathsf{D}}[z]$?

- For $z \leftarrow \mathsf{D}$, it is hard to compute $\Pr_{\mathsf{D}}[z]$

Puzzles from #P-hardness of computing $\Pr_{\mathsf{D}}[z]$?

- For $z \leftarrow \mathsf{D}$, it is hard to compute $\Pr_{\mathsf{D}}[z]$
- Can we set our puzzle output to be $(\Pr_{\mathsf{D}}[z], z)$?

Puzzles from #P-hardness of computing $\Pr_{D}[z]$?

- For $z \leftarrow D$, it is hard to compute $\Pr_{D}[z]$
- Can we set our puzzle output to be $(\Pr_{D}[z], z)$?
- Even this is hard to sample!

Puzzles from #P-hardness of computing $\Pr_{D}[z]$?

- For $z \leftarrow$ D, it is hard to compute $\Pr_{D}[z]$
- Can we set our puzzle output to be $(\Pr_{D}[z], z)$?
- Even this is hard to sample!
- All we can do is sample $z \leftarrow$ D efficiently.

Distributional One-Way Puzzles

Capture hardness of *distributional* inversion

(efficient)

$$\boxed{\mathsf{Samp}(1^n)} \longrightarrow (X, Y)$$

Given $y \sim Y$, computationally infeasible to *sample* $x \sim X \mid y$
(unto $1/\mathrm{poly}(n)$ statistical distance)

Hardness Amplification for One-Way Puzzles

Prior work [Chung-Goldin-Gray'24]

Distributional one-way puzzles $\Longleftrightarrow$ one-way puzzles

Distributional one-way puzzles from #P-hardness of computing $\Pr_{D}[z]$

Distributional one-way puzzles from #P-hardness of computing $\Pr_{\mathsf{D}}[z]$

Candidate Distributional One-way Puzzle: $\mathsf{puzz}_{\mathsf{D}}$

(1) Sample $z \leftarrow \mathsf{D}$, where WLOG z is n bits long.

(2) Sample $i \leftarrow [n]$

(3) Set $x := z_i$ and $y := z_1 z_2 \ldots z_{i-1}$

(4) Output $(x, y) = (z_i, z_1 z_2 \ldots z_{i-1})$

Distributional one-way puzzles from #P-hardness of computing $\Pr_{\mathsf{D}}[z]$

Candidate Distributional One-way Puzzle: $\mathsf{puzz}_{\mathsf{D}}$

(1) Sample $z \leftarrow \mathsf{D}$, where WLOG z is n bits long.

(2) Sample $i \leftarrow [n]$

(3) Set $x := z_i$ and $y := z_1 z_2 \ldots z_{i-1}$

(4) Output $(x, y) = (z_i, z_1 z_2 \ldots z_{i-1})$

Hope: Any adversary that *distributionally* inverts the puzzle can be used to compute $\Pr_{\mathsf{D}}[z]$, which will let us compute permanents of matrices (#P-hard!)

Estimating probabilities bit by bit

- Suppose adversary A perfectly inverts the puzzle, i.e. on input $(z_1 z_2 \ldots z_{i-1})$ samples perfectly from the induced distribution $z_i \mid z_1 z_2 \ldots z_{i-1}$

Estimating probabilities bit by bit

- Suppose adversary A perfectly inverts the puzzle, i.e. on input $(z_1 z_2 \ldots z_{i-1})$ samples perfectly from the induced distribution $z_i \mid z_1 z_2 \ldots z_{i-1}$
- For any string z, note that $\Pr_{D}[z] = \Pr_{D}[z_1] \cdot \Pr_{D}[z_2 \mid z_1] \cdot \ldots \cdot \Pr_{D}[z_n \mid z_1 z_2 \ldots z_{n-1}]$

Estimating probabilities bit by bit

- Suppose adversary A perfectly inverts the puzzle, i.e. on input $(z_1 z_2 \ldots z_{i-1})$ samples perfectly from the induced distribution $z_i \mid z_1 z_2 \ldots z_{i-1}$
- For any string z, note that $\Pr_D[z] = \Pr_D[z_1] \cdot \Pr_D[z_2 \mid z_1] \cdot \ldots \cdot \Pr_D[z_n \mid z_1 z_2 \ldots z_{n-1}]$
- We can approximate each term of form $\Pr_D[z_i \mid z_1 z_2 \ldots z_{i-1}]$ by repeatedly calling the adversary on input $(z_1 z_2 \ldots z_{i-1})$ and counting the frequency of each bit in the output.

Dealing with “bad” strings

- The estimate we obtain will have small error only if each of the terms $\Pr_{\mathsf{D}}[z_i \mid z_1 z_2 \ldots z_{i-1}]$ is not too small.

Dealing with "bad" strings

- The estimate we obtain will have small error only if each of the terms $\Pr_{\mathsf{D}}[z_i \mid z_1 z_2 \ldots z_{i-1}]$ is not too small.

- However, note that if $\Pr_{\mathsf{D}}[z_i \mid z_1 z_2 \ldots z_{i-1}]$ is small then $\Pr_{\mathsf{D}}[z]$ must also be small.

Dealing with “bad” strings

- The estimate we obtain will have small error only if each of the terms $\Pr_{D}[z_i \mid z_1 z_2 \ldots z_{i-1}]$ is not too small.

- However, note that if $\Pr_{D}[z_i \mid z_1 z_2 \ldots z_{i-1}]$ is small then $\Pr_{D}[z]$ must also be small.

- Such “bad” z can therefore only arise with small probability.

Dealing with “bad” strings

- The estimate we obtain will have small error only if each of the terms $\Pr_{\mathsf{D}}[z_i \mid z_1 z_2 \dots z_{i-1}]$ is not too small.

- However, note that if $\Pr_{\mathsf{D}}[z_i \mid z_1 z_2 \dots z_{i-1}]$ is small then $\Pr_{\mathsf{D}}[z]$ must also be small.

- Such “bad” z can therefore only arise with small probability.

- Full proof requires dealing with adversaries that make errors and only succeed on infinitely many input lengths.

Limitations

1. We only obtain an *approximation* for $\Pr_{\mathsf{D}}[z]$

2. We only get a *good* approximation with $1 - 1/\text{poly}(n)$ probability over sampling of z

Limitations

1. We only obtain an *approximation* for $\Pr_{D}[z]$

2. We only get a *good* approximation with $1 - 1/\text{poly}(n)$ probability over sampling of z

Is this enough to show security?

Formalizing Probability Approximation

Probability Approximation: For a (quantum) efficiently sampleable distribution D, probability approximation is defined as:

Given $x \leftarrow$ D, compute a $1/\text{poly}(n)$ multiplicative error approximation of $\Pr_{\text{D}}[x]$ with probability $1 - 1/\text{poly}(n)$ over choice of x

Formalizing Probability Approximation

Probability Approximation: For a (quantum) efficiently sampleable distribution D, probability approximation is defined as:

Given $x \leftarrow$ D, compute a $1/\text{poly}(n)$ multiplicative error approximation of $\Pr_{\text{D}}[x]$ with probability $1 - 1/\text{poly}(n)$ over choice of x

Efficient algorithm that distributionally inverts $\text{puzz}_{\text{D}} \Longrightarrow$

Efficient algorithm for **probability approximation**

Puzzles from hardness of probability approximation

Probability Approximation: For a (quantum) efficiently sampleable distribution D, probability approximation is defined as:

Given $x \leftarrow$ D, compute a $1/\text{poly}(n)$ multiplicative error approximation of $\Pr_{\text{D}}[x]$ with probability $1 - 1/\text{poly}(n)$ over choice of x

Theorem 1 [Khurana-**T**'25]

Probability approximation is hard for efficient quantum adversaries $\iff$ One-Way Puzzles exist

How hard is Probability Approximation?

How hard is Probability Approximation?

The literature on quantum advantage conjectures that (for specific choices of experiment D):

Conjecture$_D$: Probability approximation for D is #P-hard

[SB09, BJS11, AA11, BMS16, FM17, BIS+18, BFNV19, KMM21, BFLL21, Kro22, Mov23, ZVBL23]

D $\in$ {BosonSampling, Random Circuit Sampling, IQP Sampling, etc.}

How hard is Probability Approximation?

The literature on quantum advantage conjectures that (for specific choices of experiment D):

> Conjecture$_D$ $\Longrightarrow$ **Probability approximation for D 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….]

Conjectures imply impossibility of classical simulation

$\text{Conjecture}_{D} + (\text{BPP}^{\text{NP}} \neq \#\text{P})$

$\Downarrow$ (Non Trivial)

D cannot be classically simulated

Theorem 1 [Khurana-**T**'25]

Probability approximation is hard for efficient quantum adversaries $\Longleftrightarrow$ One-Way Puzzles exist

Theorem 1 [Khurana-**T**'25]

Probability approximation is hard for efficient quantum adversaries $\Longleftrightarrow$ One-Way Puzzles exist

Conjecture$_{D}$: Probability approximation for D is #P-hard

Theorem 1 [Khurana-**T**'25]

Probability approximation is hard for efficient quantum adversaries $\iff$ One-Way Puzzles exist

Conjecture$_{D}$: Probability approximation for D is #P-hard

Corollary: Assuming Conjecture$_{D}$

$P^{\#P} \not\subseteq BQP$ implies the existence of one-way puzzles.

Ruling out One-Way functions

- Suppose there exists function f such that:

Ruling out One-Way functions

- Suppose there exists function f such that:

Probability approximation for D is hard for efficient quantum adversaries

$$\Longrightarrow$$

f is a secure one way function

Ruling out One-Way functions

- Suppose there exists function f such that:

Probability approximation for D is hard for efficient quantum adversaries

$$\Longrightarrow$$

f is a secure one way function

where security is established via efficient (quantum) black box reduction R, i.e.

Ruling out One-Way functions

- Suppose there exists function f such that :

Probability approximation for D is hard for efficient quantum adversaries

$$\implies$$

f is a secure one way function

where security is established via efficient (quantum) black box reduction R, i.e.

A inverts $f \implies R^A$ performs probability approximation for D

Ruling out One-Way functions

- But any one-way function f can be inverted using an NP oracle.

Ruling out One-Way functions

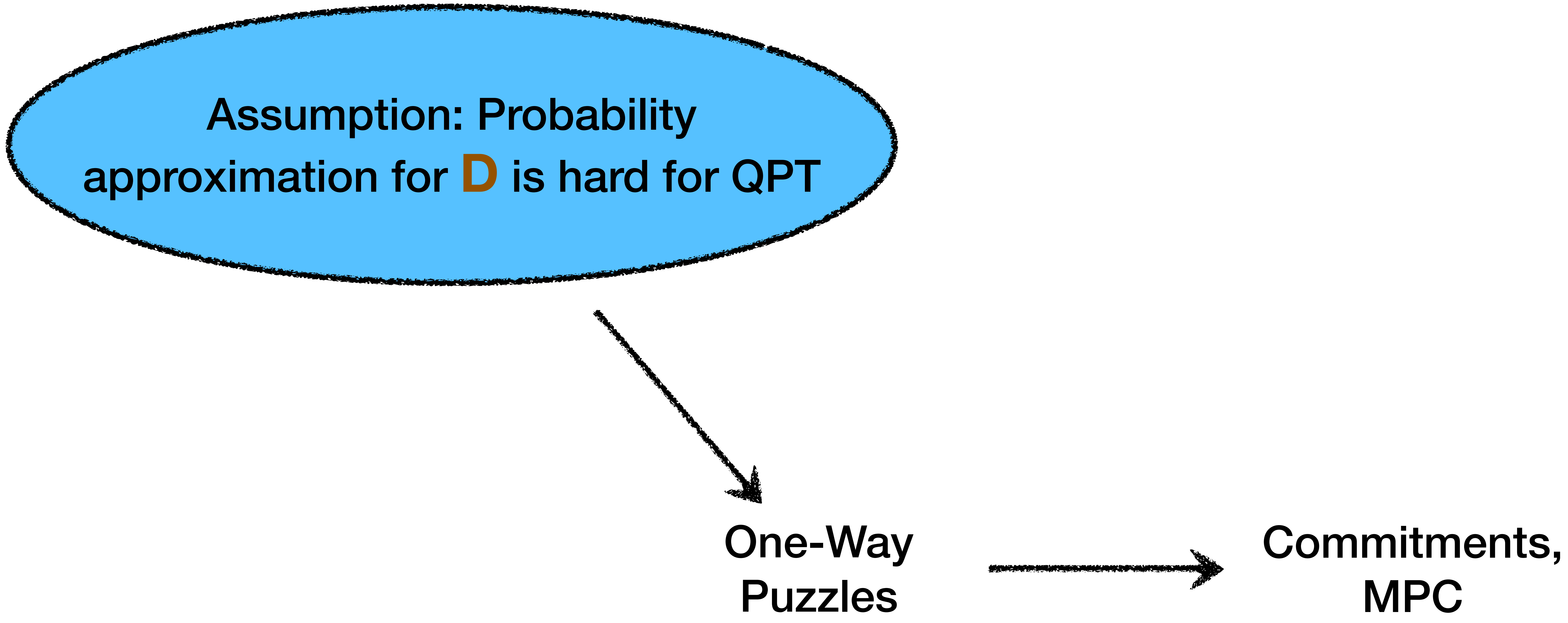
- But any one-way function f can be inverted using an NP oracle.
- Therefore, R^{NP} can perform probability approximation for D.

Ruling out One-Way functions

- But any one-way function f can be inverted using an NP oracle.
- Therefore, R^{NP} can perform probability approximation for D.
- But (by conjectures for BosonSampling, etc.) probability approximation for D is #P-hard!

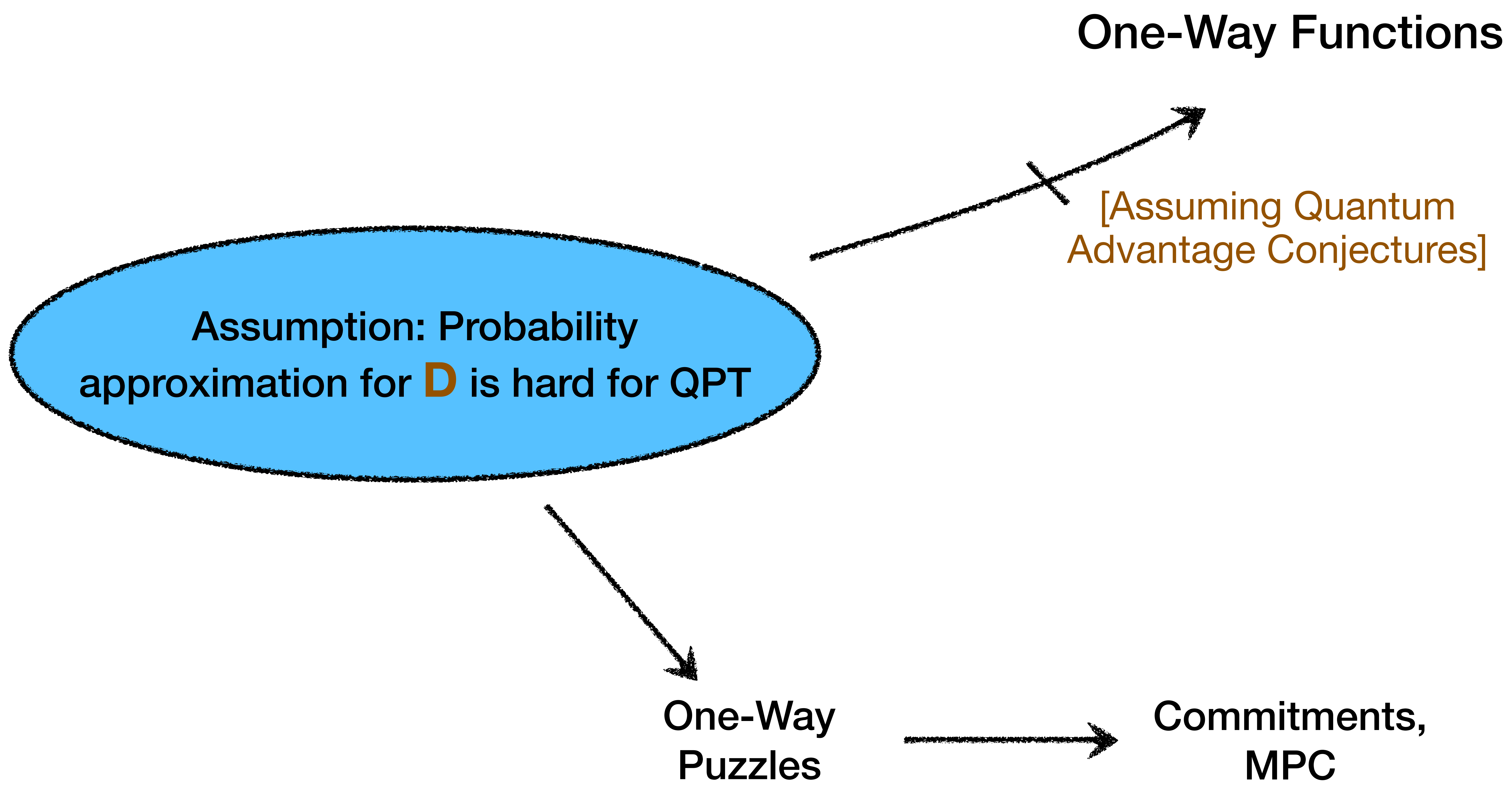
$$\implies \mathsf{P}^{\#\mathsf{P}} \subseteq \mathsf{BQP}^{\mathsf{NP}} \text{ (extremely unlikely!)}$$

Consequences



D ∈ {BosonSampling, Random Circuit Sampling, IQP Sampling, etc.}

Consequences



D $\in$ {BosonSampling, Random Circuit Sampling, IQP Sampling, etc.}

Consequences

$BQP \neq P^{\#P}$

[Assuming Quantum Advantage Conjectures]

Assumption: Probability approximation for **D** is hard for QPT

One-Way Puzzles

Commitments, MPC

D $\in$ {BosonSampling, Random Circuit Sampling, IQP Sampling, etc.}

Understanding Microcrypt: Some Lenses

1. Is there a quantum "minimal" primitive/analogue of one-way functions?

2. Can we build cryptosystems from concrete mathematical problems that are harder than inverting one-way functions?

3. Classical cryptography cannot exist if P=NP. What connections does quantum cryptography have with (traditional) complexity theory?

Open questions:

1. Do commitments imply one-way puzzles? Are they separated?
2. Can one-way puzzles imply interesting primitives *not known to be implied by* commitments?
   - Metacomplexity characterization of one-way puzzles [CGGH25, HM25]
   - One-way puzzles imply (inefficiently verifiable) proofs of quantumness [MSY25]
3. Our new assumptions only get us one-way puzzles. What about pseudorandom states, PKE, signatures, etc?
4. Can we use *even weaker* assumptions to build commitments?

Thank You!

(Questions?)