Complexity Theory for Quantum-Input Decision Problems & Computational Hardness in Quantum Crypto

Kai-Min Chung (Academia Sinica)

https://arxiv.org/abs/2411.03716

Nai-Hui Chia
Rice University, Ken Kennedy Institute and Smalley-Curl Institute

Tzu-Hsiang Huang
UIUC

Jhih-Wei Shih
Academia Sinica

Complexity Theory

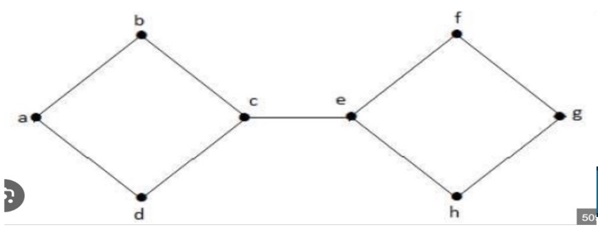
- Goal: how much <u>**computational resource**</u> to <u>**solve**</u> <u>**classical input decision problem**</u>?

Input: classical input problem

output: 1 bit

Is a graph connected?

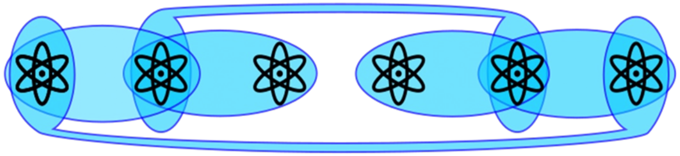
1/0



1 if graph is connected
0 otherwise

Does a local Hamiltonian have ground state energy lower than a or larger than b?

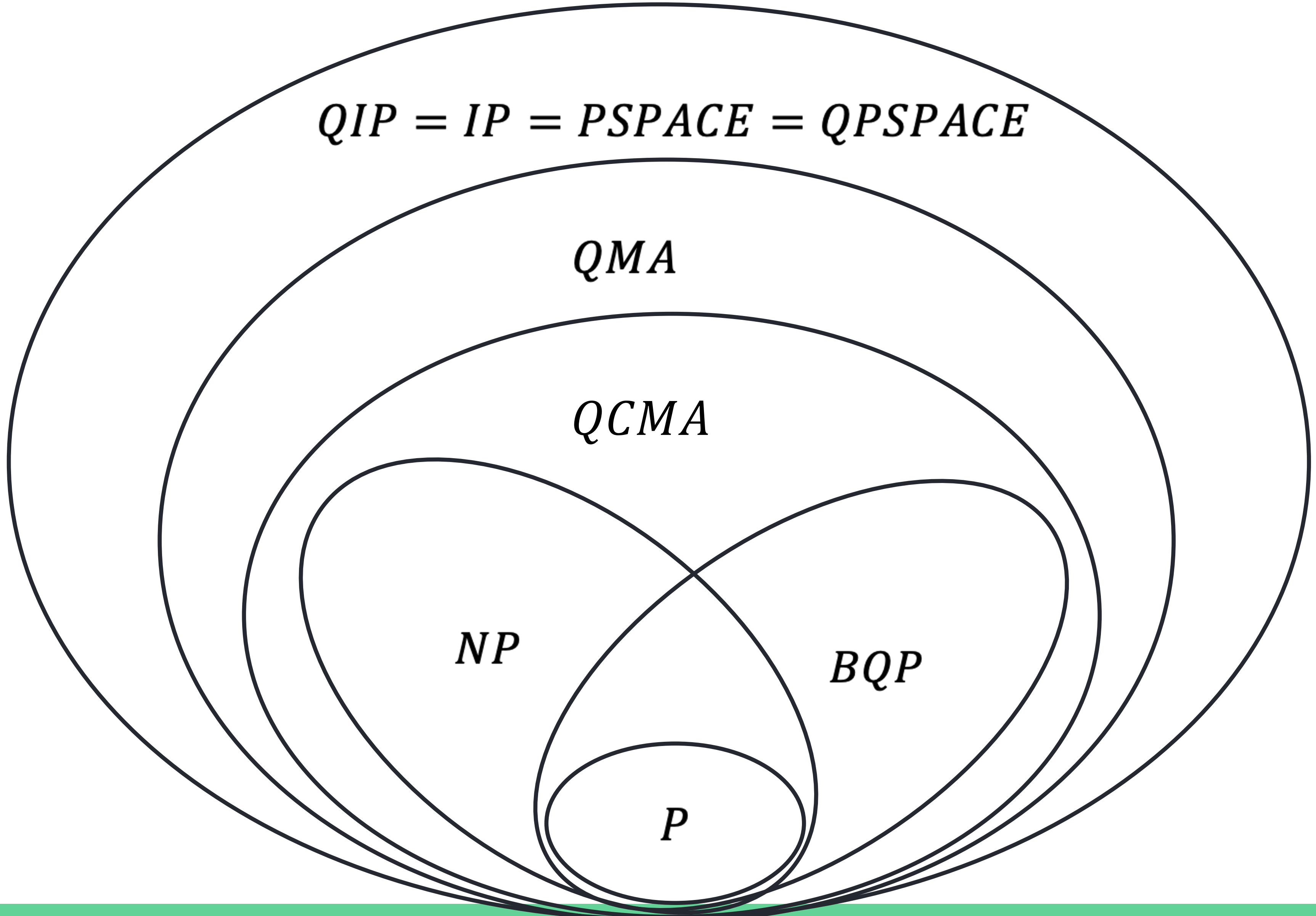
1 if the energy is lower than a
0 if the energy is larger than b



Complexity Theory

- Goal: how much **computational resource** to **solve** **classical input decision problem**?
- Different type of computational resource: **time, space, interaction**
- Time:
  - **P** (**deterministic** polynomial time)
  - **BPP** (**probabilistic** polynomial time)
  - **BQP** (**quantum** polynomial time)
- Space**:**
  - **PSPACE** (**deterministic** polynomial space)
  - **BQPSPACE** (**quantum** polynomial space)
- Interaction**:**
  - **NP** (one **classical** message, **deterministic** polynomial time verifier)
  - **QCMA** (one **classical** message, **quantum** polynomial time verifier)
  - **QMA** (one **quantum** message, **quantum** polynomial time verifier)
  - **IP** (polynomial **classical** round, **probabilistic** polynomial time verifier)
  - **QIP** (polynomial **quantum** round, **quantum** polynomial time verifier)

Complexity Theory



Complexity Theory for Non-decision Problem

There are many types of problems other than decision problems

- Promise problems
- Search problems
- Counting problems
- Sampling problems
- Streaming problems
- Property testing
- Distribution testing
- .....

Complexity Theory for Non-decision Problem

There are many types of problems other than decision problems

- Promise problems
- Search problems
- Counting problems
- Sampling problems
- Streaming problems
- Property testing
- Distribution testing
- .....

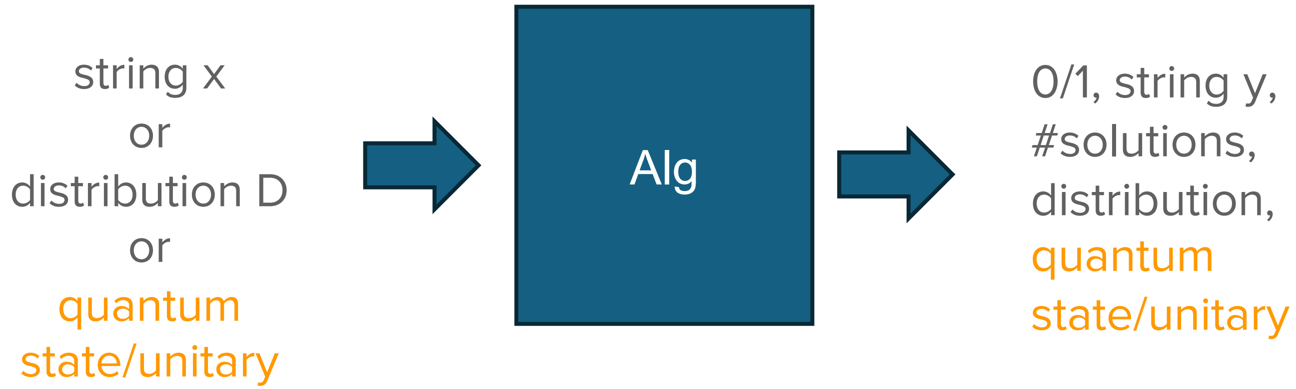
Corresponding complexity classes:

#P, FNP, PPAD, SampBQP, promiseNP, etc.

Various complexity classes and corresponding theory have been studied for these types of problems


string x
or
distribution D
Alg
0/1, string y,
#solutions,
distribution...

What Happen in Quantum World?



What Happen in Quantum World?

More types of problems!

Different Type of Quantum Computational Problem

	Input type	Goal	Complexity Theory
State synthesis problem	classical	synthesize quantum state	[RY22] [MY23] [Ros24]
Unitary synthesis problem	classical	synthesize unitary transform	[BEM+24]

Different Type of Quantum Computational Problem

	Input type	Goal	Complexity Theory
State synthesis problem	classical	synthesize quantum state	[RY22] [MY23] [Ros24]
Unitary synthesis problem	classical	synthesize unitary transform	[BEM+24]
Pure quantum promise problem	pure state	decision	[KA04] and this work
Mixed quantum promise problem	mixed state	decision	[KA04] and this work

Different Type of Quantum Computational Problem

	Input type	Goal	Complexity Theory
State synthesis problem	classical	synthesize quantum state	[RY22] [MY23] [Ros24]
Unitary synthesis problem	classical	synthesize unitary transform	[BEM+24]
Pure quantum promise problem	pure state	decision	[KA04] and this work
Mixed quantum promise problem	mixed state	decision	[KA04] and this work
Quantum-input unitary synthesis problem	pure/mixed state	synthesize unitary transform	

Why Quantum-Input Decision Problem? (Spoiler)

- Decision problems are easy to work with
  - naturally defined complexity classes
  - reduction, complete problems, oracle separation, barrier results
- Nature problems in quantum learning, property testing, crypto
- Useful to understand computational hardness in quantum crypto
  - Allow proving unconditional separation ➔

    Explain hardness in unconditional quantum crypto

Security is only computational:

broken by unbounded adversary

Without making computational assumption

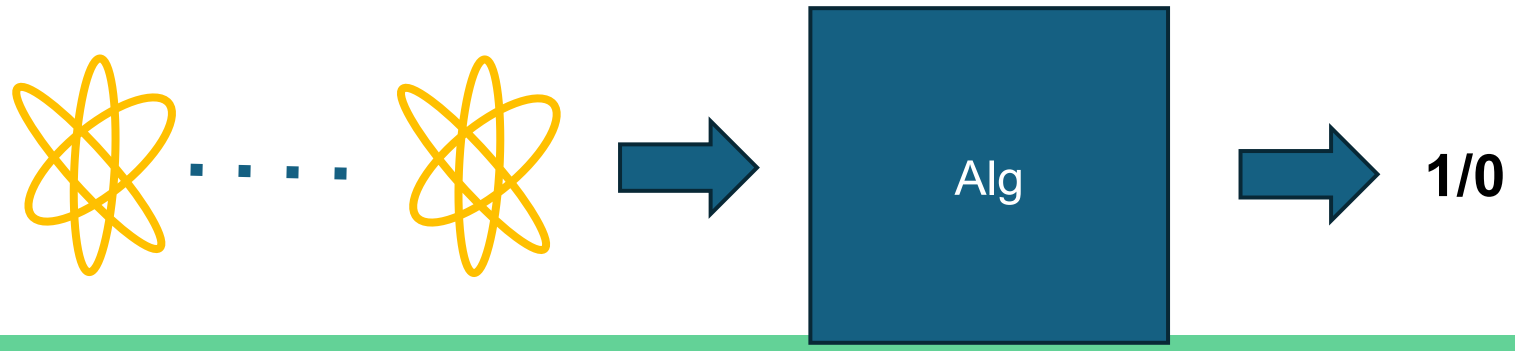
Why Quantum-Input Decision Problem? (Spoiler)

- Decision problems are easy to work with
  - naturally defined complexity classes
  - reduction, complete problems, oracle separation, barrier results
- Nature problems in quantum learning, property testing, crypto
- Useful to understand computational hardness in quantum crypto
  - Allow proving unconditional separation ➔
    Explain hardness in unconditional quantum crypto
- Different landscape comparing to traditional complexity theory

Quantum Promise Problems (QPPs)

Our goal: Build complexity theory for quantum-input decision problem

Input: multiple copies of a quantum state **output:** 1 bit

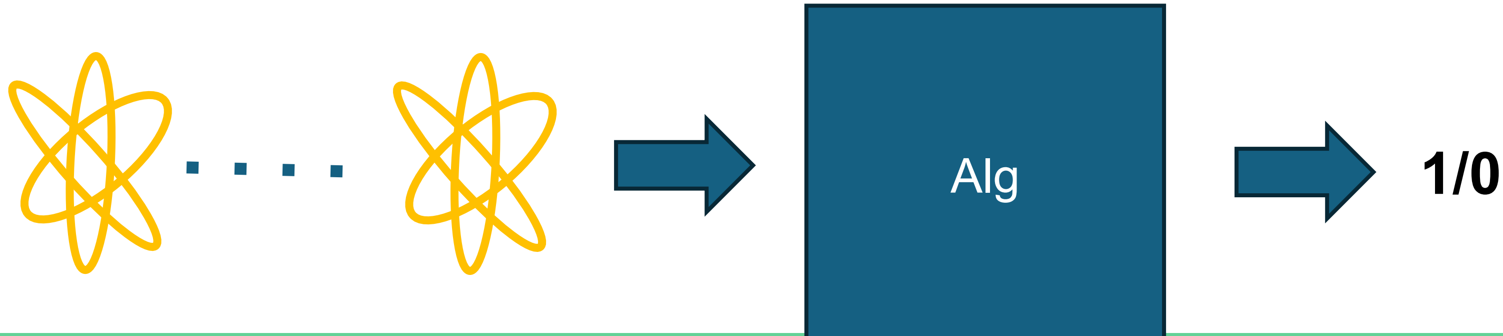


Quantum Promise Problems (QPPs)

Our goal: Build complexity theory for quantum-input decision problem

- Quantum promise problems:
  - $L = (L_Y, L_N)$: L_Y and L_N are subsets of quantum states
  - Given copies of quantum state |s>, decide if |s> is in L_Y or L_N

Input: multiple copies of a quantum state **output:** 1 bit

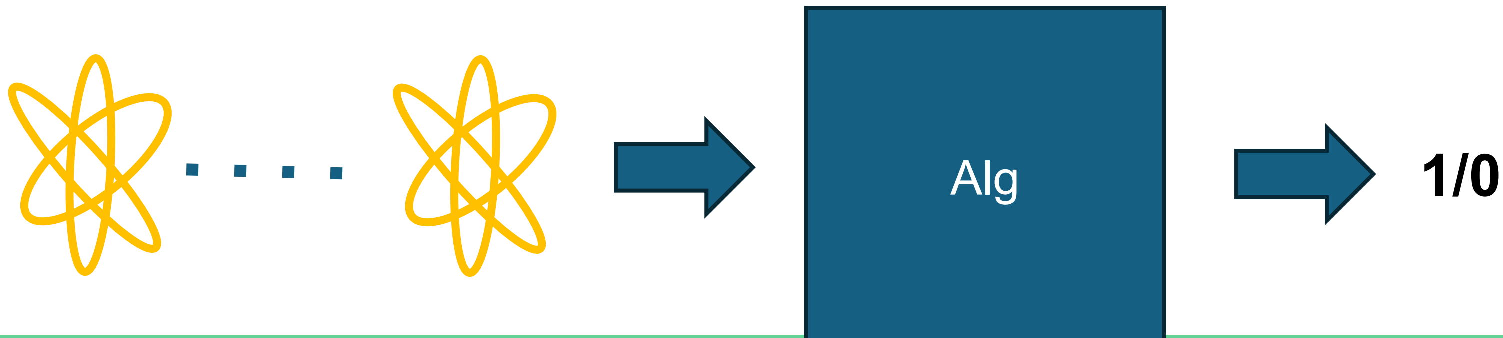


Quantum Promise Problems (QPPs)

Our goal: Build complexity theory for quantum-input decision problem

- Quantum promise problems:
  - $L = (L_Y, L_N)$: L_Y and L_N are subsets of quantum states
  - Given copies of quantum state |s>, decide if |s> is in L_Y or L_N
- Quantum input can be either pure or mixed

Input: multiple copies of a quantum state **output:** 1 bit



Quantum Promise Problems (QPPs)

Our goal: Build complexity theory for quantum-input decision problem

- Quantum promise problems:
  - $L = (L_Y, L_N)$: L_Y and L_N are subsets of quantum states
  - Given copies of quantum state $|s\rangle$, decide if $|s\rangle$ is in L_Y or L_N
- Quantum input can be either pure or mixed
- Capture property testing, promise problems, distribution test
- Standard complexity theory cannot fully characterize QPPs
  - BQP, BPP, NP are for “classical inputs” not “quantum states”

Complexity Theory for QPPs

- Many interesting problems in quantum are in this form
  - Testing: product states, maximally mixed states, stablizer states, matrix product state, etc.
  - Learning: small-depth states, shadow tomography, etc.

Complexity Theory for QPPs

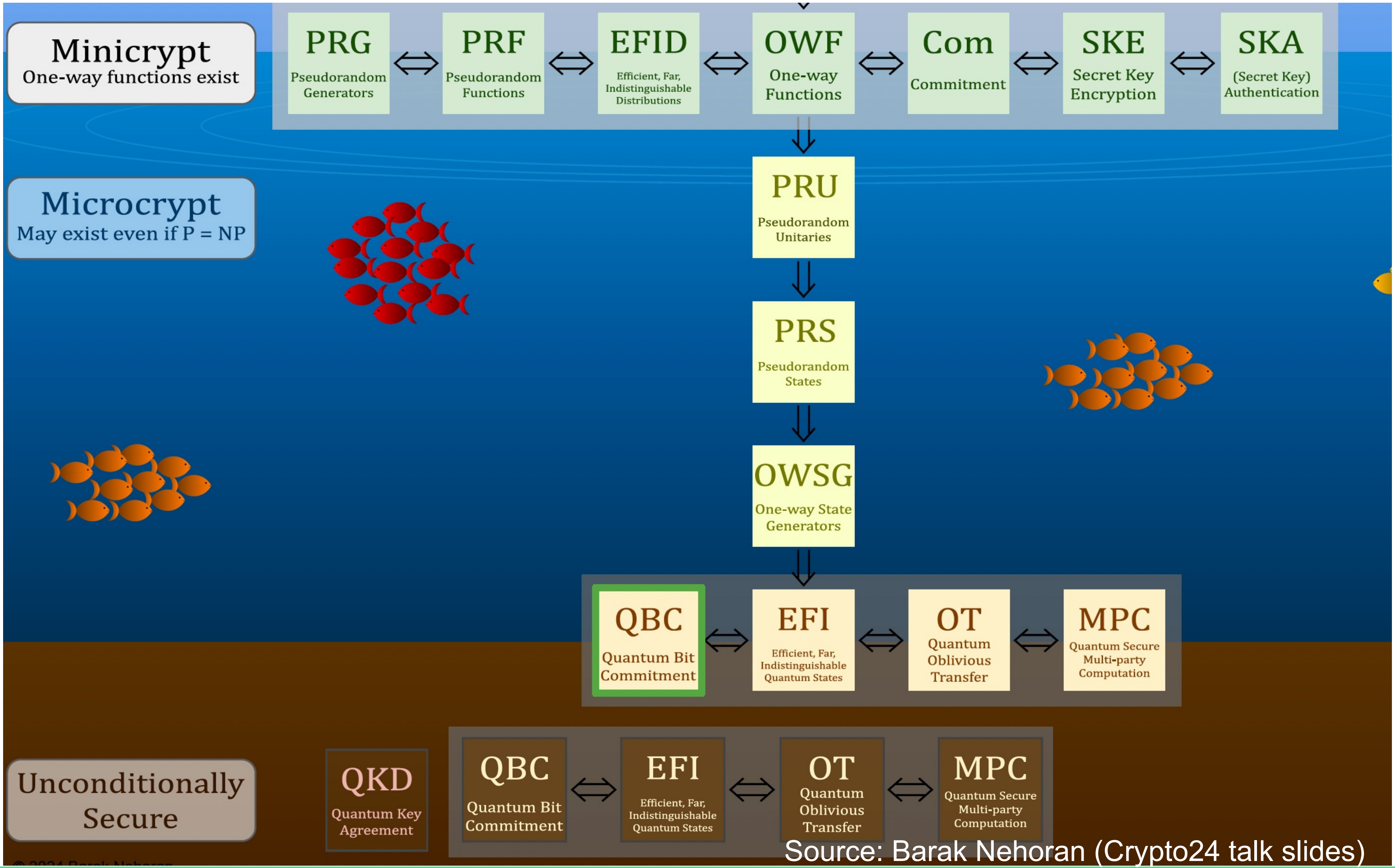
- Many interesting problems in quantum are in this form
  - Testing: product states, maximally mixed states, stablizer states, matrix product state, etc.
  - Learning: small-depth states, shadow tomography, etc.
  - Breaking security in quantum cryptography

Complexity Theory for QPPs

- Many interesting problems in quantum are in this form
  - Testing: product states, maximally mixed states, stablizer states, matrix product state, etc.
  - Learning: small-depth states, shadow tomography, etc.
  - Breaking security in quantum cryptography

Our first motivation: Better characterize the security/hardness in quantum crypto primitives

Quantum Primitives in Q Crypto

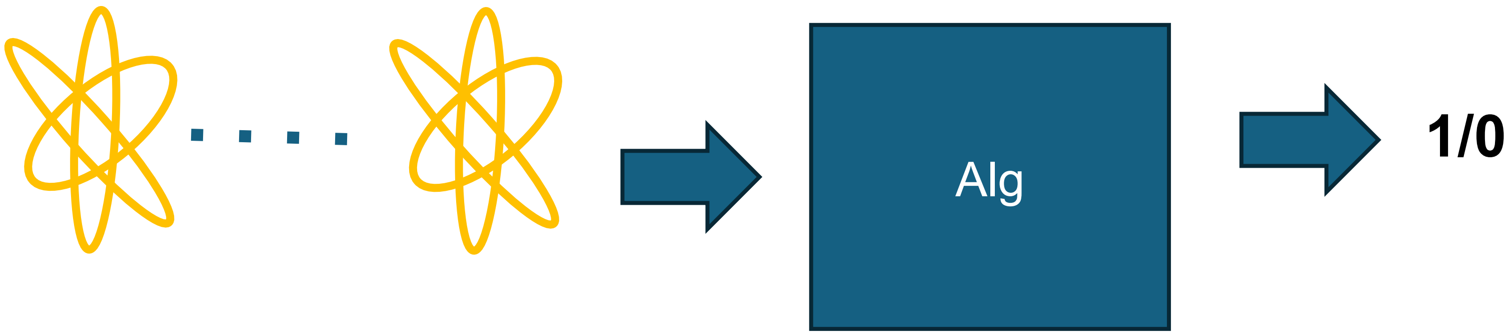


Source: Barak Nehoran (Crypto24 talk slides)

Security of Quantum Crypto Primitive

- **Pseudorandom states (PRS):** Generator generates quantum states G|k> indistinguishable from Haar random states |R>
- **One-way state generator (OWSG):** Generator generates quantum states G|x> hard to invert to classical inputs x
- **EFI pairs:** Generator generates two states ρ_0 and ρ_1 that are statistical far but computational indistinguishable

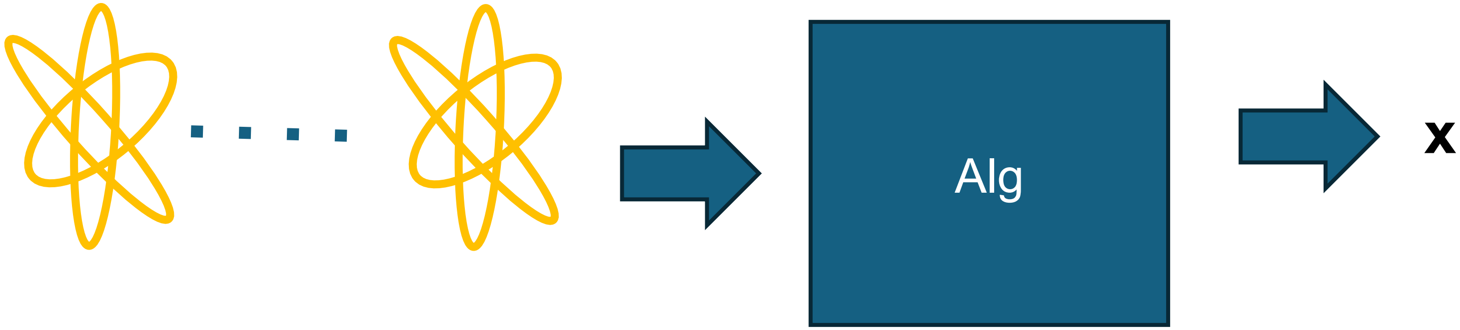
Input: copies of |S> = G|k> or |R> **output:** |S> = G|k> or |R>



Security of Quantum Crypto Primitive

- **Pseudorandom states (PRS):** Generator generates quantum states G|0> indistinguishable from random states |R>
- **One-way state generator (OWSG):** Generator generates quantum states G|x> hard to invert to classical inputs x
- **EFI pairs:** Generator generates two states ρ_0 and ρ_1 that are statistical far but computational indistinguishable

Input: copies of |S> = G|x> **output:** x

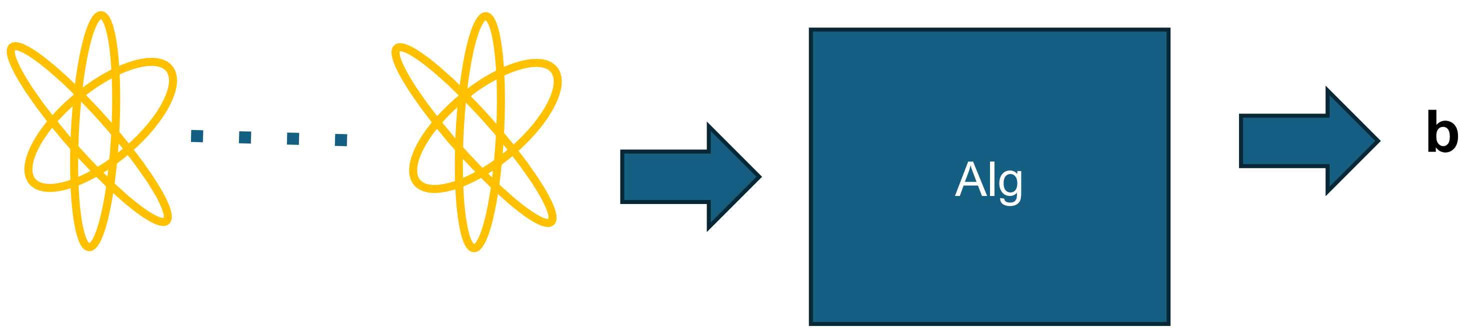


Security of Quantum Crypto Primitive

- **Pseudorandom states (PRS):** Generator generates quantum states G|0> indistinguishable from random states |R>
- **One-way state generator (OWSG):** Generator generates quantum states G|x> hard to invert to classical inputs x
- **EFI pairs:** Generator generates two states ρ_0 and ρ_1 that are statistical far but computational indistinguishable

Input: copies of ρ_b for b=0 or 1

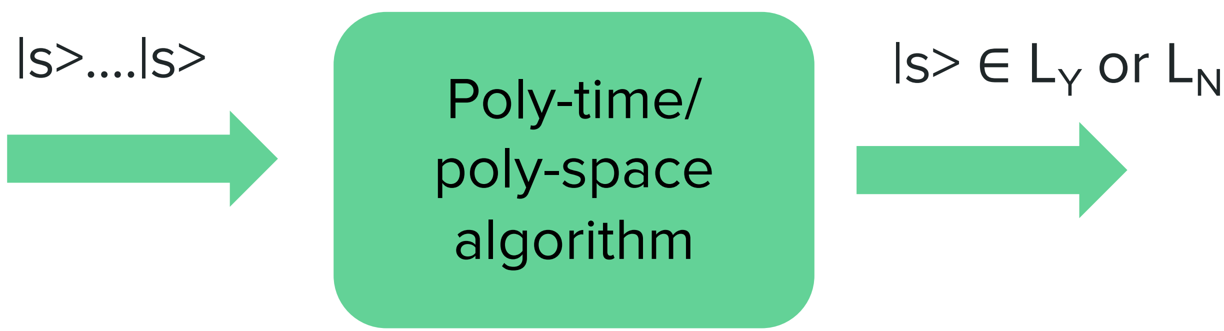
output: b



Complexity Classes for QPPs (pure version)

Let $L=(L_Y,L_N)$

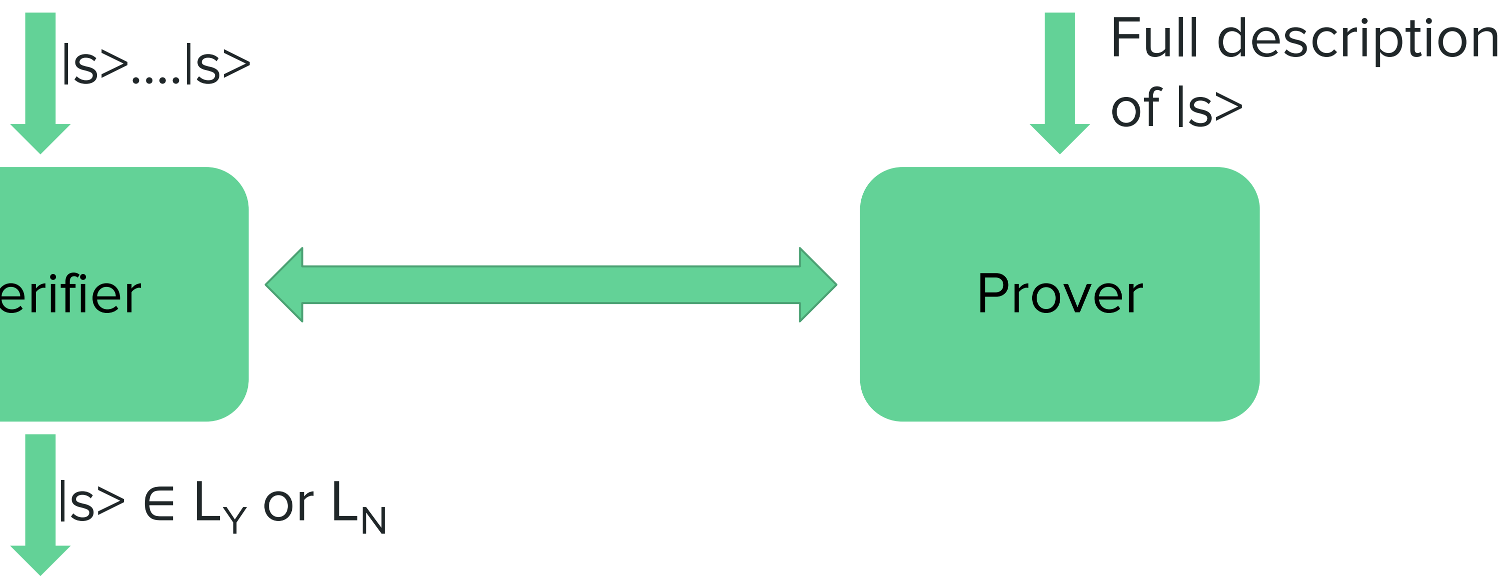
- **pBQP:** Given poly(n) copies of |s>, decide |s> in poly time
- **pPSPACE:** Given poly(n) copies of |s>, decide |s> in poly space
- **pQIP:** Verifier gets poly(n) copies of |s>, decides |s> with the help of a malicious unbounded prover
- **$\mathbf{pQSZK_{hv}}$:** QIP, and the honest verifier cannot get info. other than $|s\rangle \in L_Y$



Complexity Classes for QPPs (pure version)

Let $L=(L_Y,L_N)$

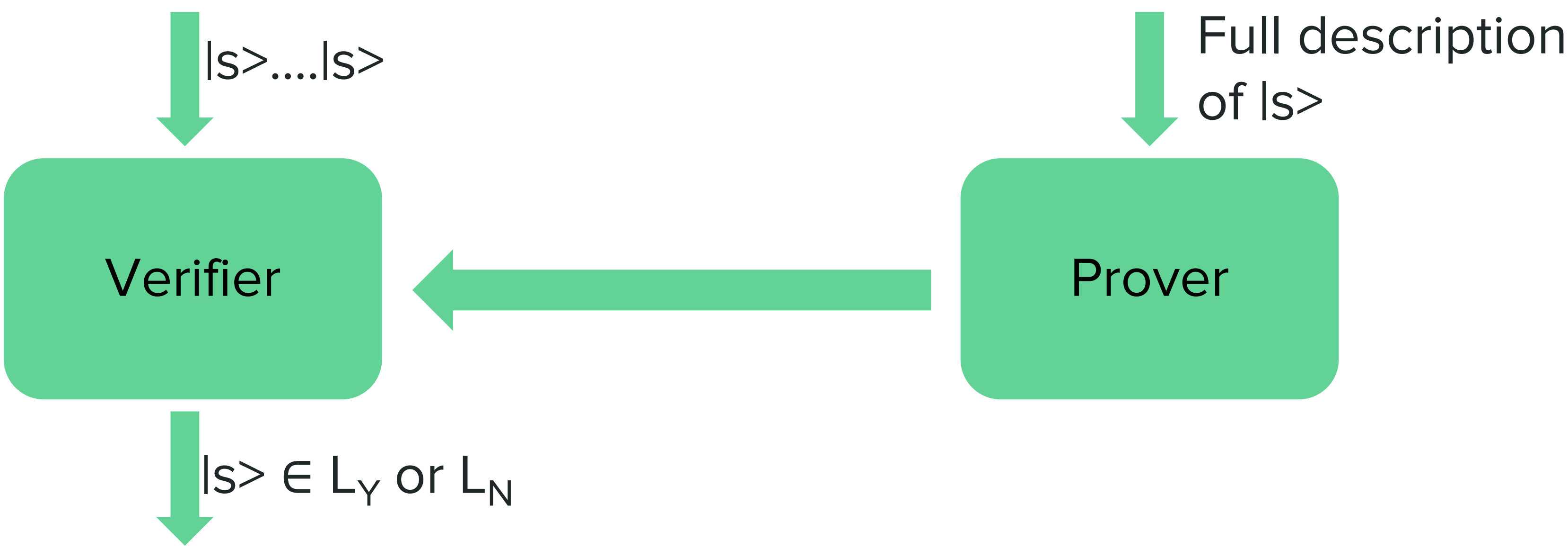
- **pBQP:** Given poly(n) copies of |s>, decide |s> in poly time
- **pPSPACE:** Given poly(n) copies of |s>, decide |s> in poly space
- **pQIP:** Verifier gets poly(n) copies of |s>, decides |s> with the help of a malicious unbounded prover
- **$\mathbf{pQSZK_{hv}}$:** QIP, and the honest verifier cannot get info. other than $|s\rangle \in L_Y$



Complexity Classes for QPPs (pure version)

pQMA and pQCMA are pQIP(one-round) with quantum or classical message from the prover

- **pQIP:** Verifier gets poly(n) copies of |s>, decides |s> with the help of a malicious unbounded prover
- **$\mathbf{pQSZK_{hv}}$:** QIP, and the honest verifier cannot get info. other than |s> ∈ L_Y



Complexity Classes for QPPs (mixed version)

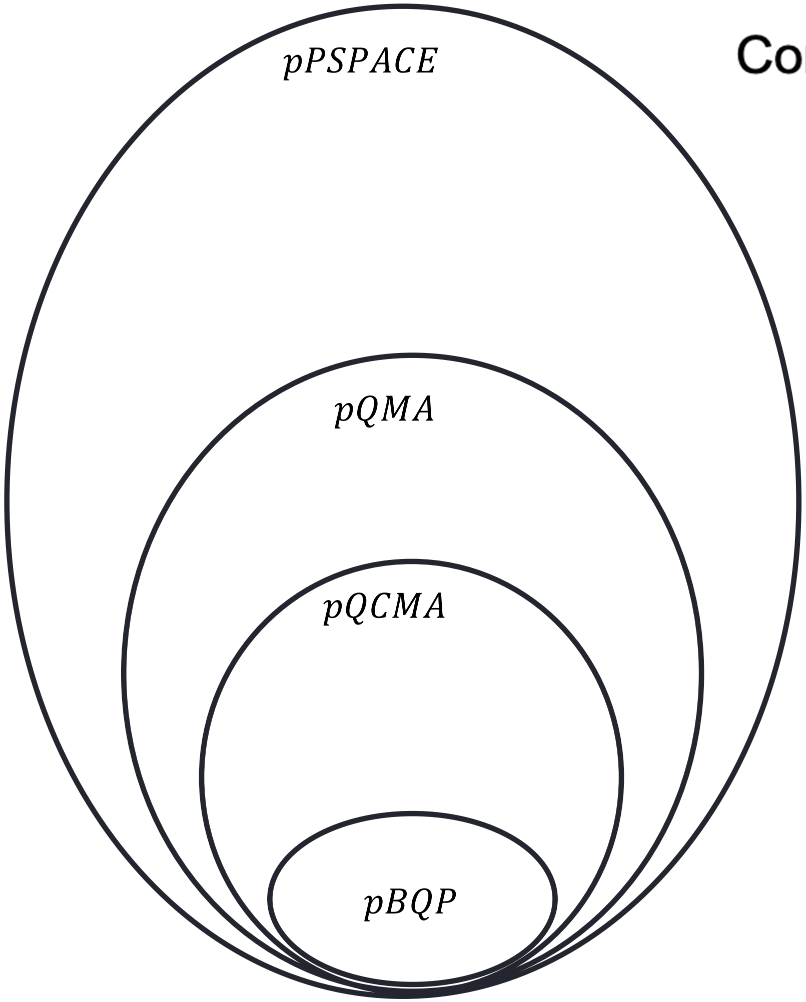
Let $L=(L_Y,L_N)$

- **mBQP:** Given poly(n) copies of ρ_s, decide ρ_s in poly time
- **mPSPACE:** Given poly(n) copies of ρ_s, decide ρ_s in poly space
- **mQIP:** Verifier gets poly(n) copies of ρ_s, decides ρ_s with the help of a malicious unbounded prover
- **mQMA**: one round mQIP
- **mQCMA**: one round mQIP with classical message
- **mQSZK$_{hv}$:** QIP & honest verifier cannot learn info. other than $\rho_s \in L_Y$

of Copies Matter

- Our choice:
  - Single Machine (BQP, PSPACE): polynomial copies
  - Interactive Proofs (QIP, $QSZK_{hv}$): prover unbounded copies
- Also reasonable to consider
  - PSPACE: unbounded copies (require oracle access to the input and able to discard qubits)
  - QIP, $QSZK_{hv}$: prover has polynomial copies
  - lead to different complexity classes

Landscape of Pure QPP Complexity Class

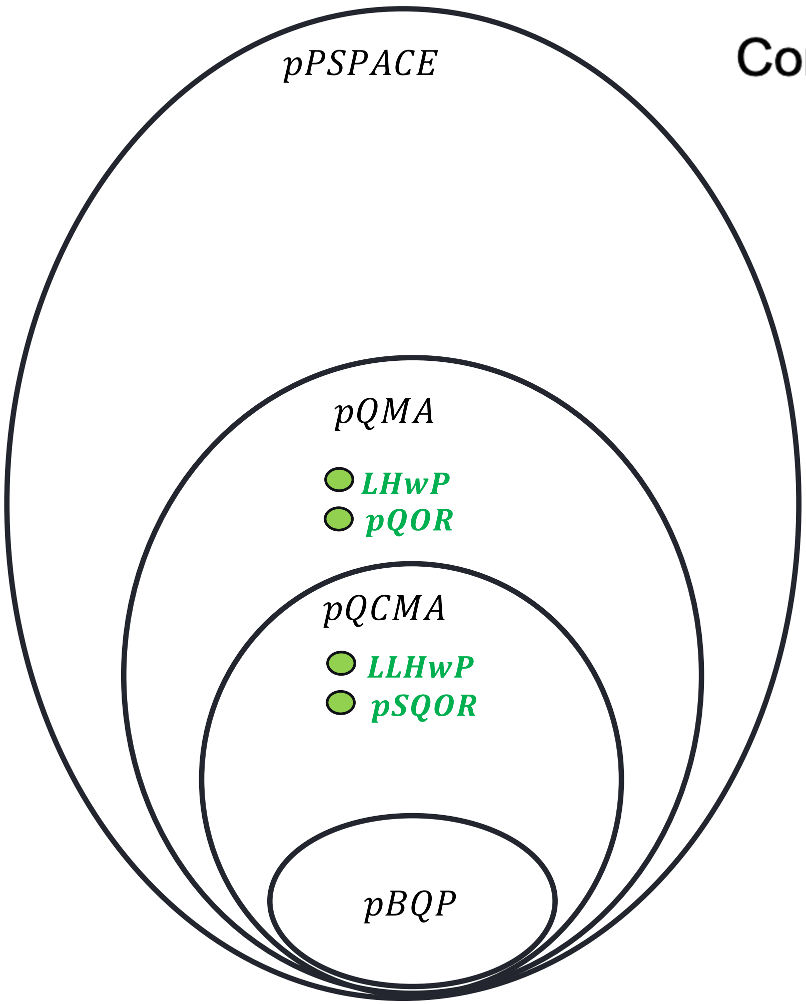


Containment:

$pBQP \subseteq pQCMA \subseteq pQMA \subseteq pPSPACE$

$pQMA \subseteq pPSPACE$ is not trivial because $pPSPACE$ can only access polynomial copies of input state

Landscape of Pure QPP Complexity Class



Containment:

$$pBQP \subseteq pQCMA \subseteq pQMA \subseteq pPSPACE$$

Natural complete problem for $pQCMA, pQMA$

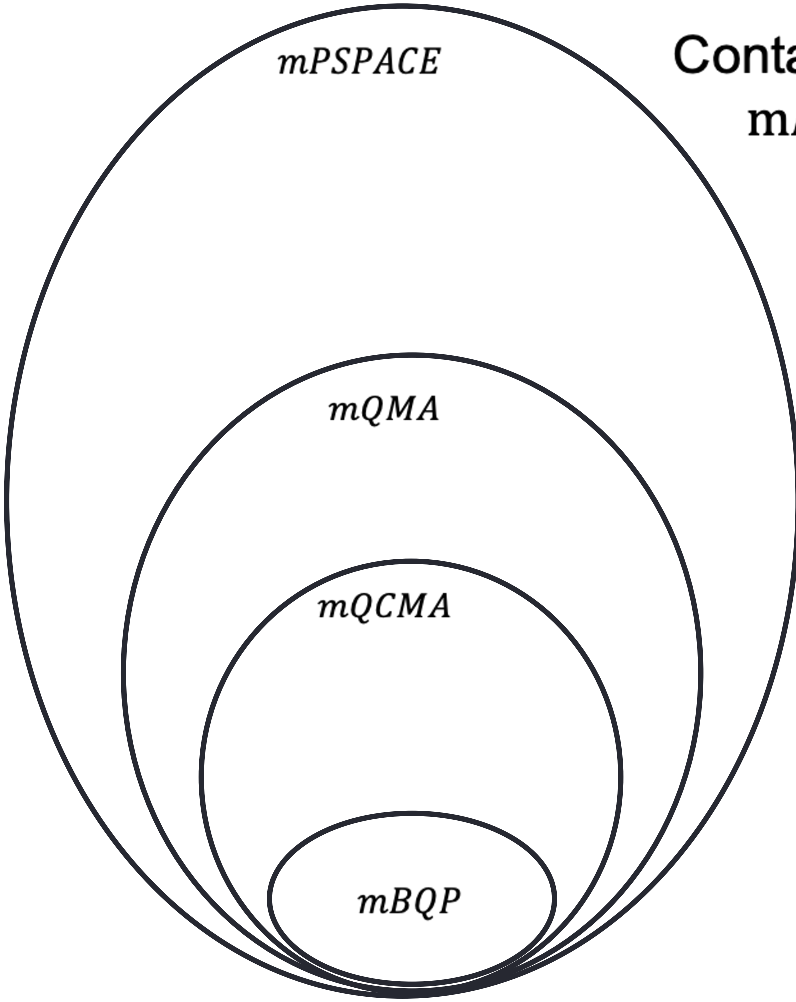
- $LHwP$
- $LLHwP$

variant of local-Hamiltonian problem

- $pQOR$
- $pSQOR$

Quantum OR lemma

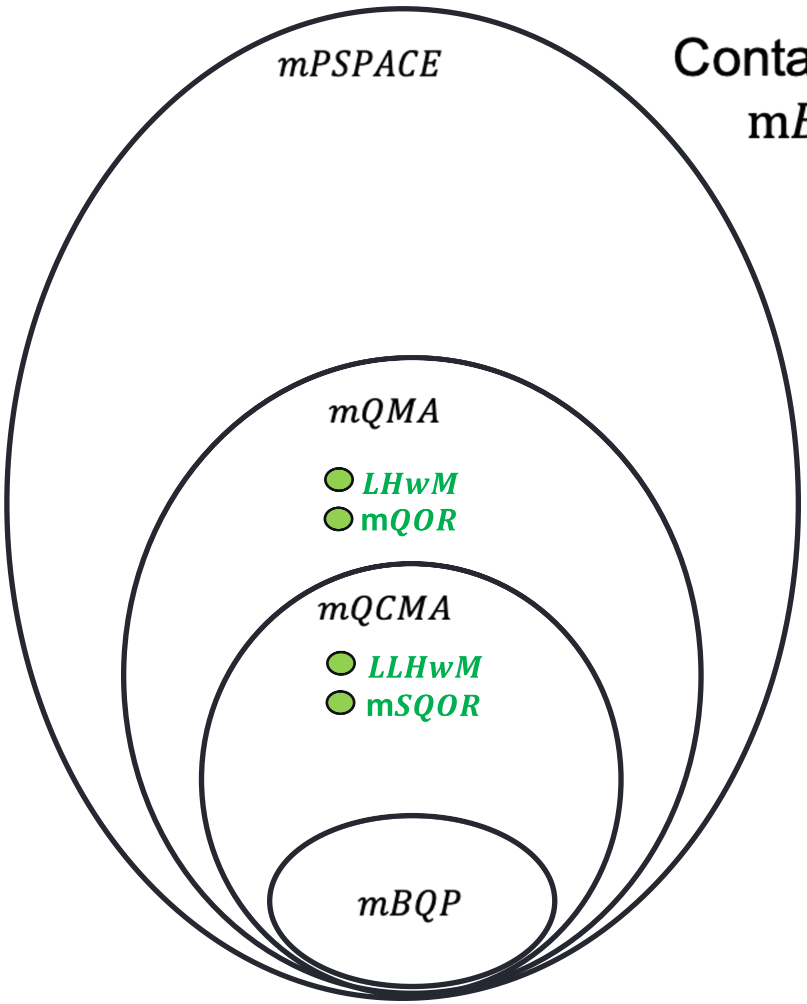
Landscape of Mixed QPP Complexity Class



Containment:

$$\mathrm{m}BQP \subseteq mQCMA \subseteq mQMA \subseteq mPSPACE$$

Landscape of Mixed QPP Complexity Class



Containment:

$$\mathrm{m}BQP \subseteq mQCMA \subseteq mQMA \subseteq mPSPACE$$

Natural complete problem for

$mQCMA, mQMA$

- $LHwM$
- $LLHwM$

variant of local-Hamiltonian problem

Mixed version is non-trivial to define

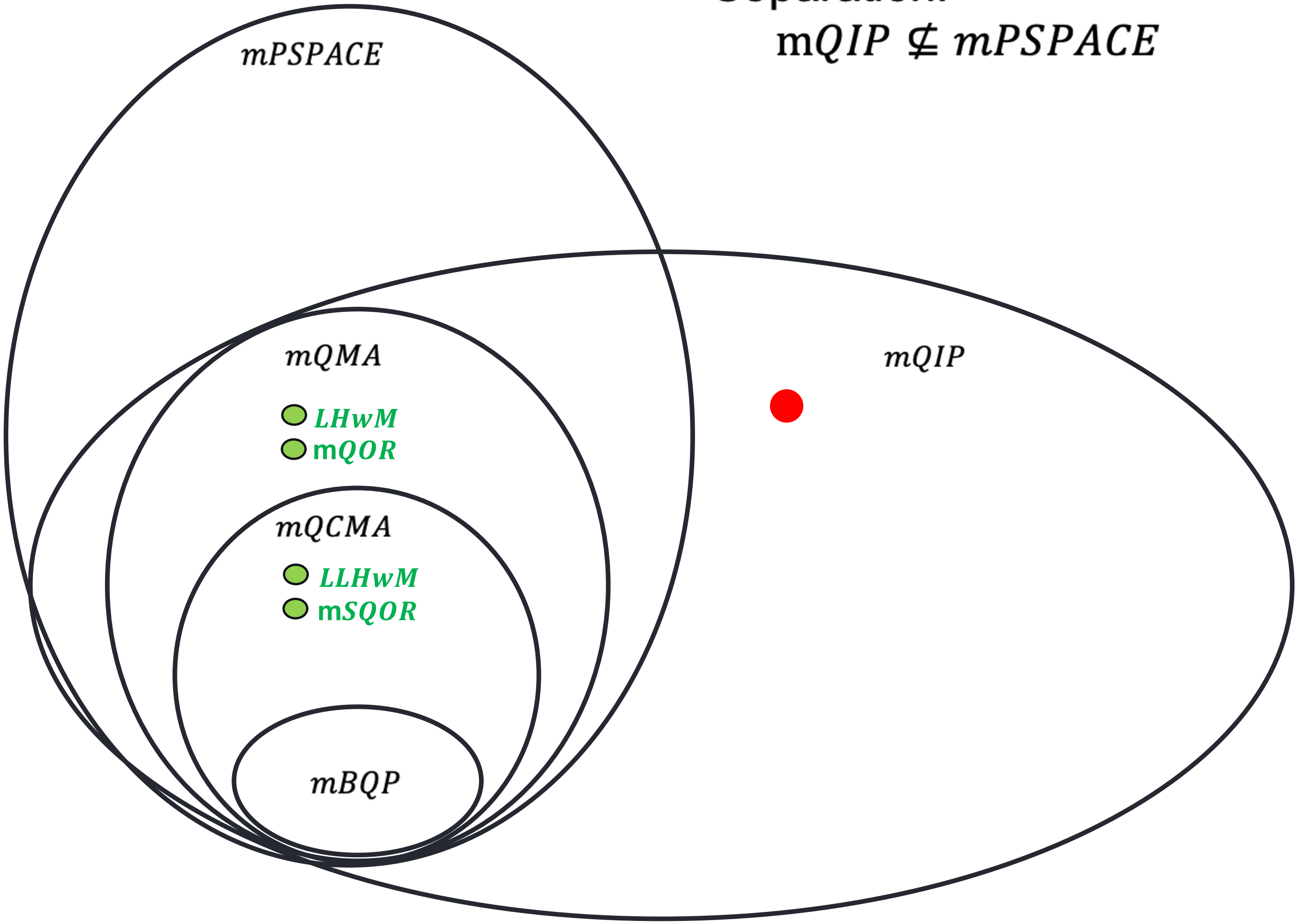
- $\mathrm{m}QOR$
- $\mathrm{m}SQO$

Quantum OR lemma

Landscape of Mixed QPP Complexity Class

Separation:

$$\mathrm{m}QIP \nsubseteq mPSPACE$$



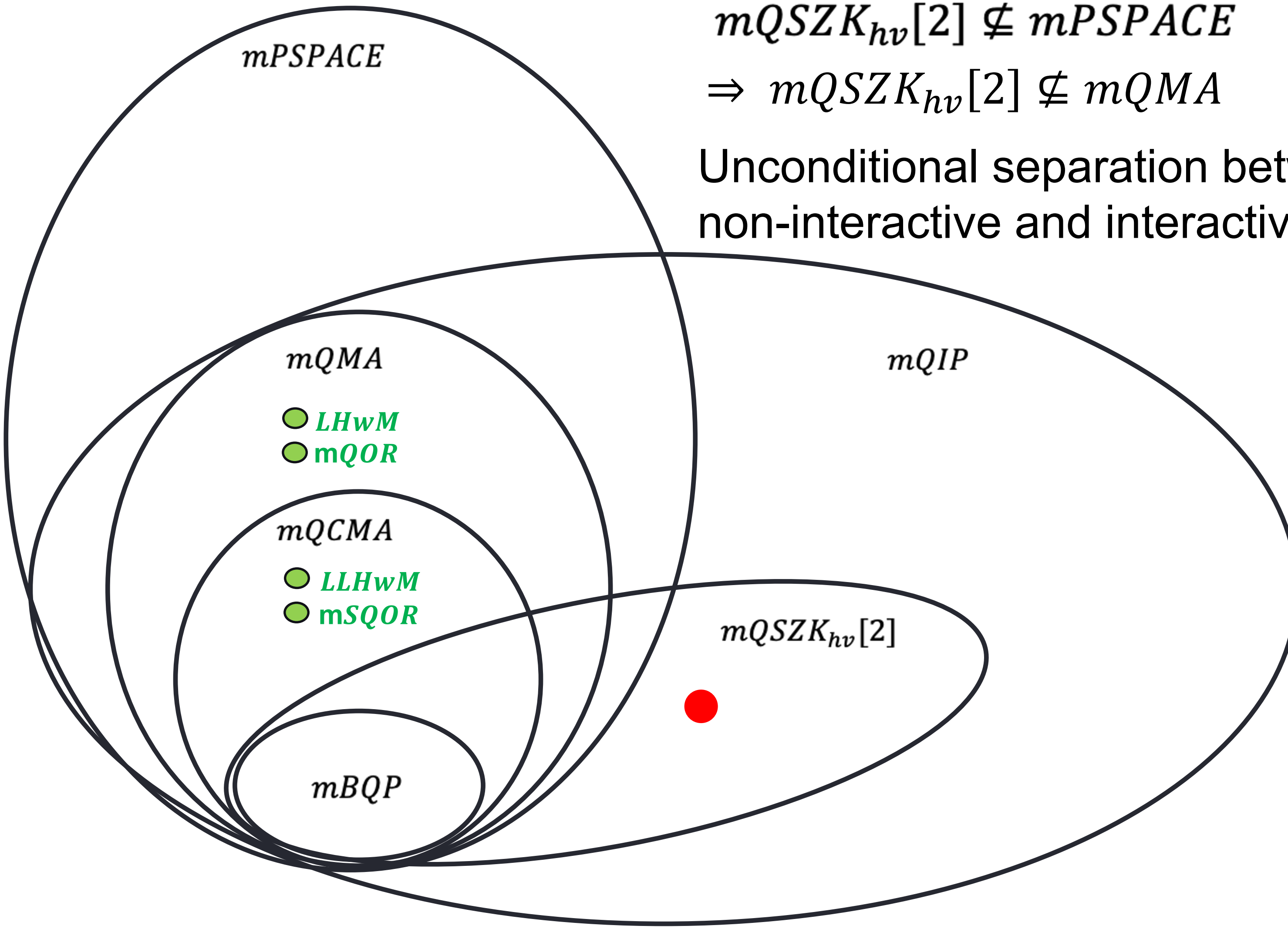
Landscape of Mixed QPP Complexity Class

Separation:

$$mQSZK_{hv}[2] \not\subseteq mPSPACE$$

$$\Rightarrow mQSZK_{hv}[2] \not\subseteq mQMA$$

Unconditional separation between non-interactive and interactive proof.

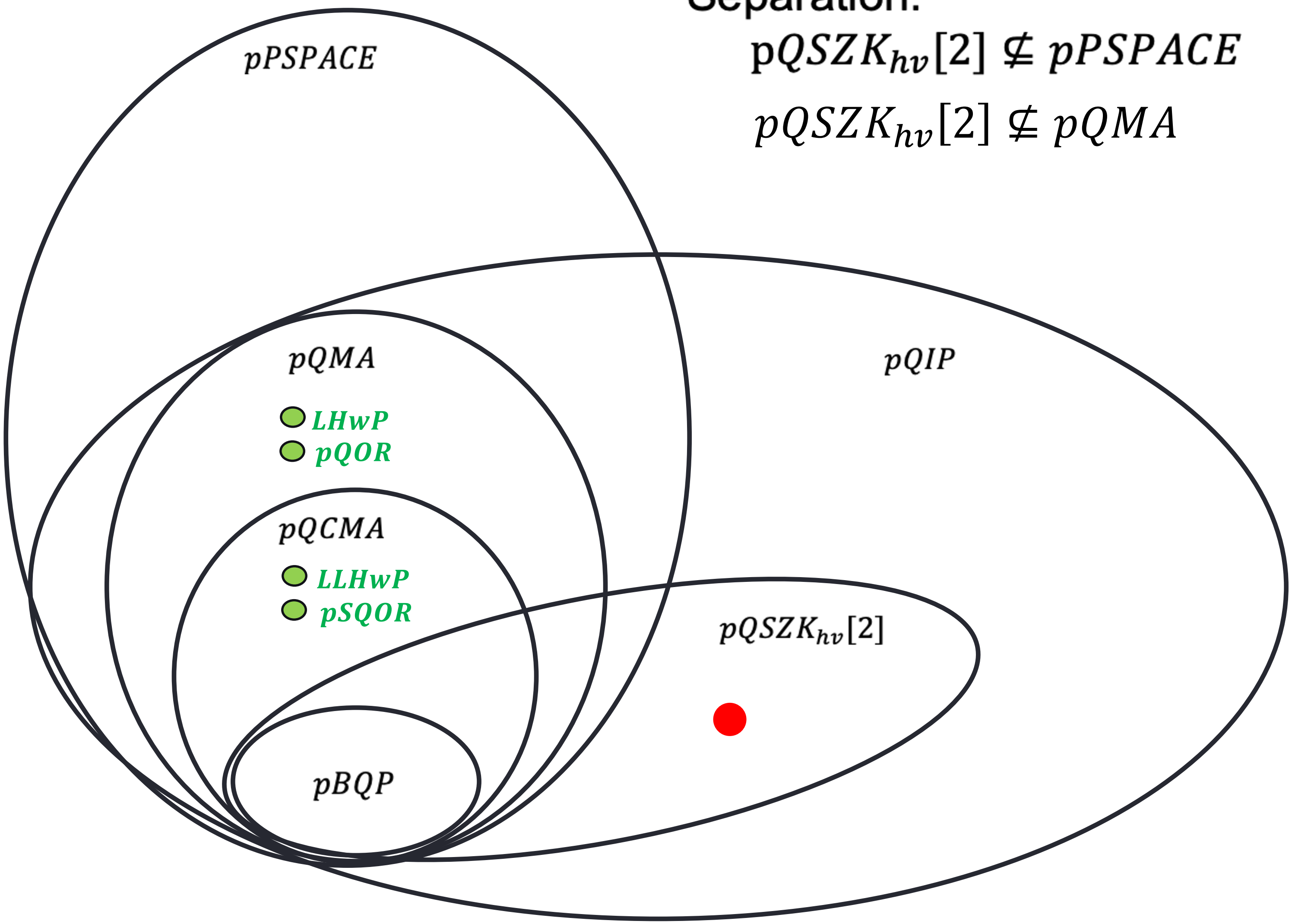


Landscape of Pure QPP Complexity Class

Separation:

$$pQSZK_{hv}[2] \not\subseteq pPSPACE$$

$$pQSZK_{hv}[2] \not\subseteq pQMA$$

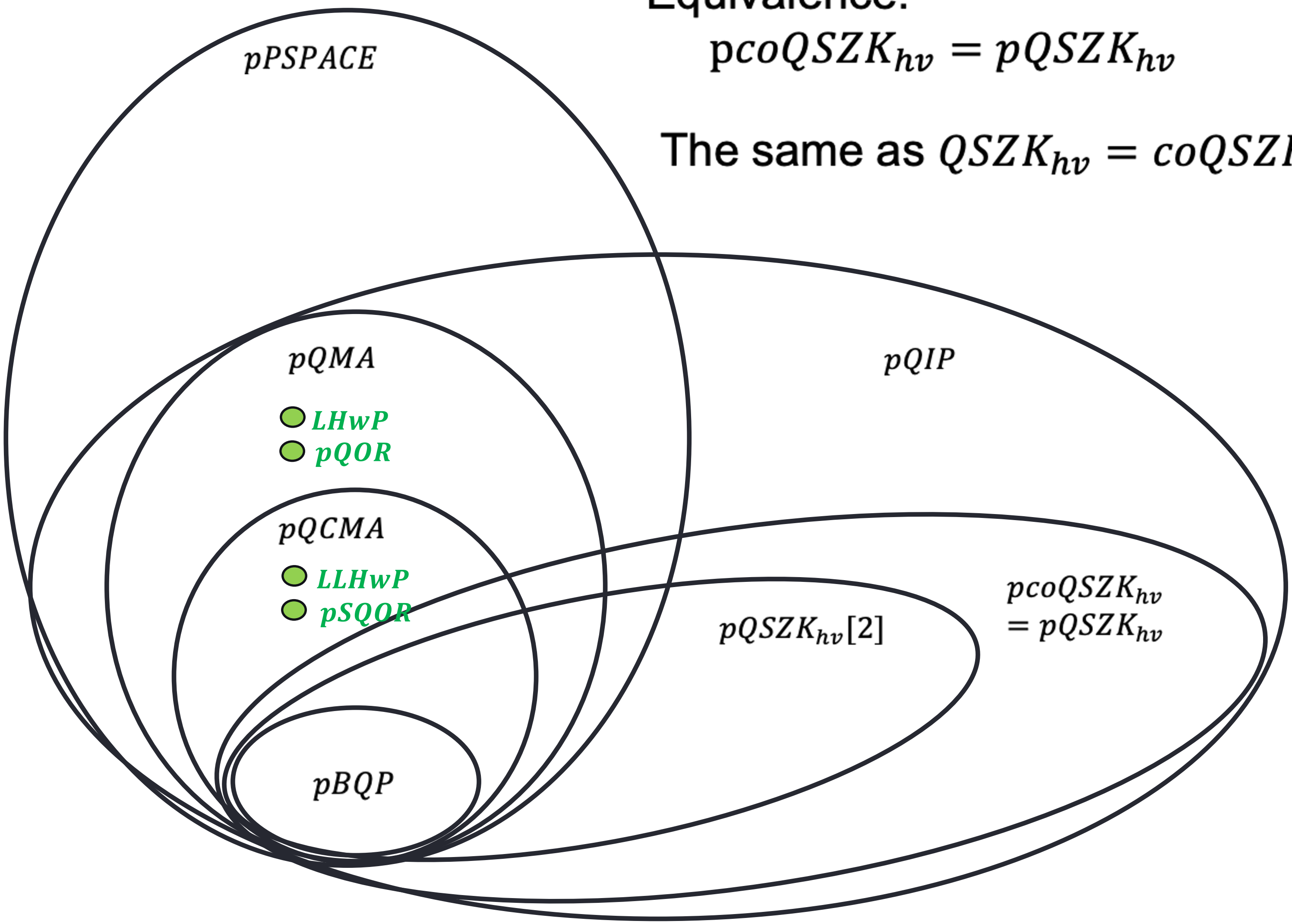


Landscape of Pure QPP Complexity Class

Equivalence:

$pcoQSZK_{hv} = pQSZK_{hv}$

The same as $QSZK_{hv} = coQSZK_{hv}$.

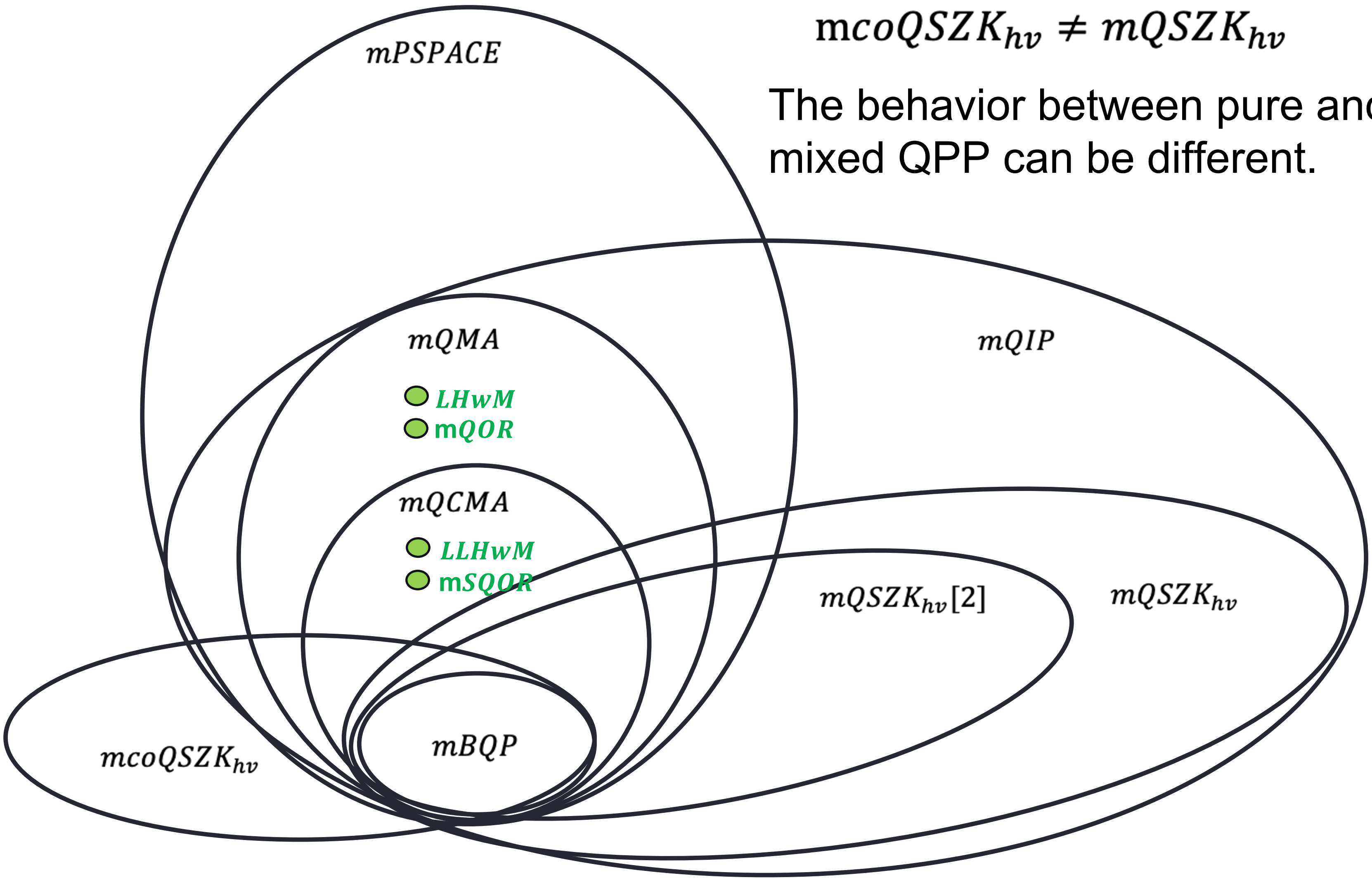


Landscape of Mixed QPP Complexity Class

Separation:

$$mcoQSZK_{hv} \neq mQSZK_{hv}$$

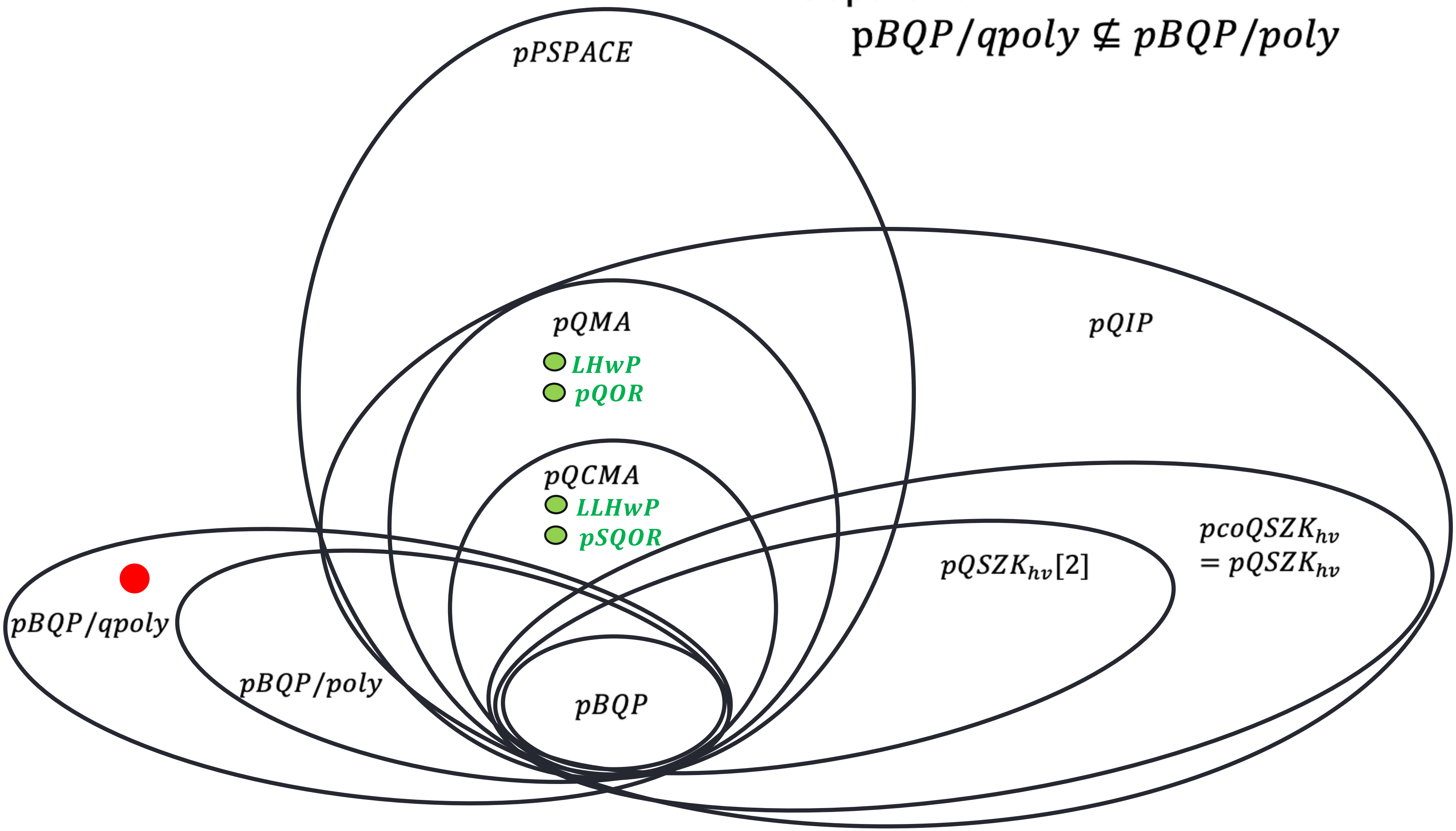
The behavior between pure and mixed QPP can be different.



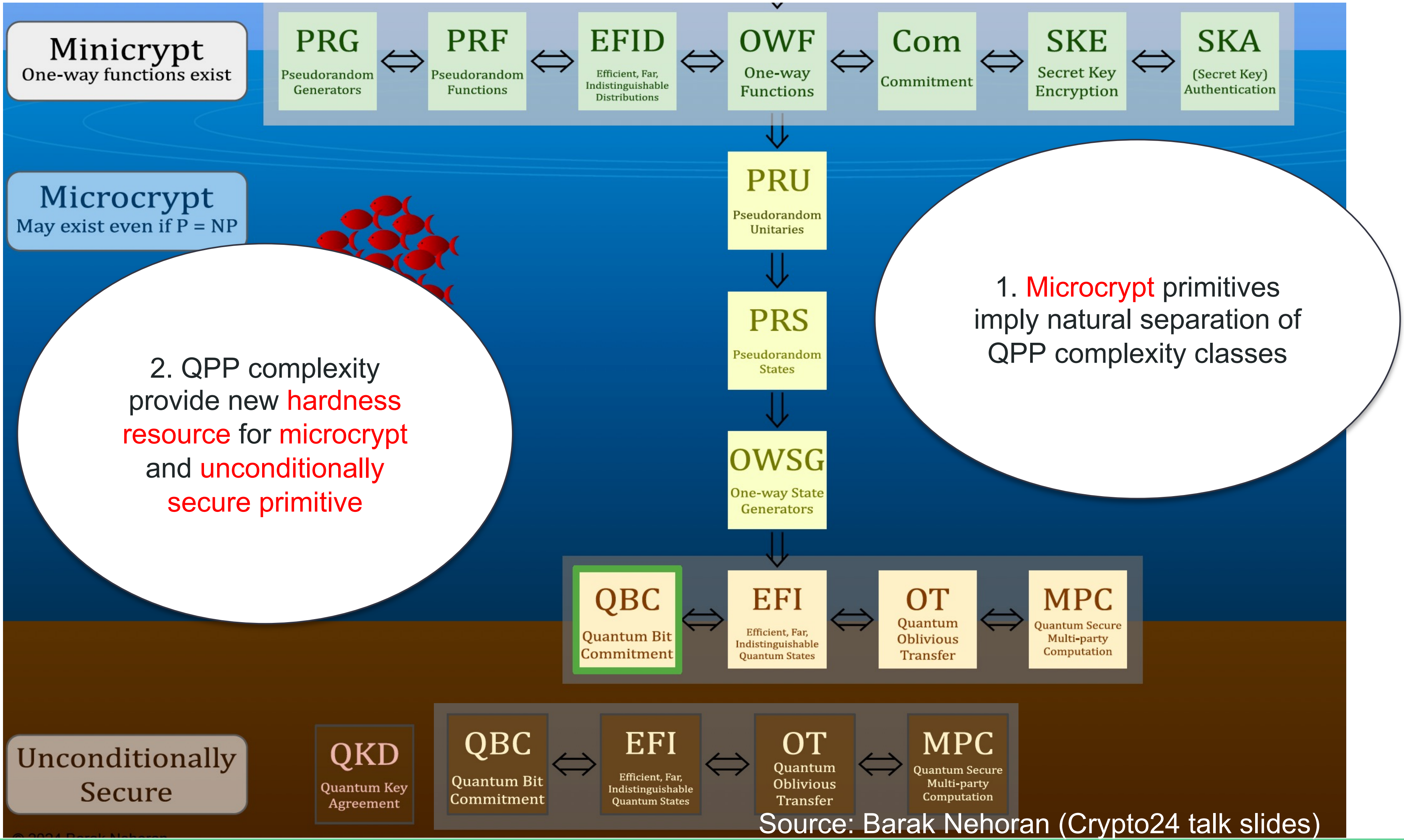
Landscape of Pure QPP Complexity Class

Separation:

$$\mathrm{p}BQP/qpoly \nsubseteq pBQP/poly$$



Characterize Hardness of Quantum Crypto Primitive



Our results: Applications to Crypto

Microcrypt:

PRS, pOWSG

mOWSG

EFI

Unconditional quantum crypto:

Quantum auxiliary-input EFI

Statistical binding, computational hiding commitment (quantum auxiliary model)

Our results: Applications to Crypto

Microcrypt:

PRS, pOWSG $\Rightarrow$ $pBQP \neq pQCMA$

mOWSG $\Rightarrow$ $mBQP \neq mQCMA$

By search to decision for
for $pQCMA$ and $mQCMA$.

EFI

Unconditional quantum crypto:

Quantum auxiliary-input EFI

Statistical binding, computational hiding commitment (auxiliary-input model)

Our results: Applications to Crypto

Microcrypt:

PRS, pOWSG $\Rightarrow$ $pBQP \neq pQCMA$

mOWSG $\Rightarrow$ $mBQP \neq mQCMA$

prover has poly copies input

EFI $\Rightarrow$ $mBQP \neq \boxed{mQSZK_{hv}^{poly}}$

$mBQP \neq mPSPACE$

Unconditional quantum crypto:

Quantum auxiliary-input EFI

Statistical binding, computational hiding commitment (auxiliary-input model)

Our results: Applications to Crypto

Microcrypt:

PRS, pOWSG $\Rightarrow$ $pBQP \neq pQCMA$

mOWSG $\Rightarrow$ $mBQP \neq mQCMA$

EFI $\Rightarrow$ $mBQP \neq mQSZK_{hv}^{poly}$

$\boxed{mBQP \neq mPSPACE}$

$\Longrightarrow$ relativization barrier for EFI!

Unconditional quantum crypto:

Quantum auxiliary-input EFI

Statistical binding, computational hiding commitment (auxiliary-input model)

Our results: Applications to Crypto

Microcrypt:

PRS, pOWSG $\Rightarrow$ $pBQP \neq pQCMA$

mOWSG $\Rightarrow$ $mBQP \neq mQCMA$

avgpQCZK$_{hv}$ is hard $\Rightarrow$ EFI $\Rightarrow$ $mBQP \neq mQSZK_{hv}^{poly}$, $mBQP \neq mPSPACE$

Unconditional quantum crypto:

Quantum auxiliary-input EFI

Statistical binding, computational hiding commitment (auxiliary-input model)

Our results: Applications to Crypto

Microcrypt:

PRS, pOWSG $\Rightarrow$ $pBQP \neq pQCMA$

mOWSG $\Rightarrow$ $mBQP \neq mQCMA$

avgpQCZK$_{hv}$ is hard $\Rightarrow$ EFI $\Rightarrow$ $mBQP \neq mQSZK_{hv}^{poly}$, $mBQP \neq mPSPACE$

Unconditional quantum crypto:

Quantum auxiliary-input EFI

Statistical binding, computational hiding commitment (auxiliary-input model)

$\boxed{\text{Computational binding, perfect hiding commitment (auxiliary-input model)}}$

Unconditional Secure Commitment Scheme

- [Qia24, MNY24] construct a unconditional-secure computational hiding statistically binding commitment scheme in an auxiliary-input model.

Unconditional Secure Commitment Scheme

- [Qia24, MNY24] construct a unconditional-secure computational hiding statistically binding commitment scheme in an auxiliary-input model.

Auxiliary-input model: (setup phase)

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

Committer $\qquad$ Receiver

Unconditional Secure Commitment Scheme

- [Qia24, MNY24] construct a unconditional-secure computational hiding statistically binding commitment scheme in an auxiliary-input model.

Auxiliary-input model: (commit phase)

Committer

On input (b,$|\phi\rangle^{\otimes poly(n)}$), prepare $|\psi_b\rangle_{CR}$ and send register C to receiver.

Register C

Receiver

Unconditional Secure Commitment Scheme

- [Qia24, MNY24] construct a unconditional-secure computational hiding statistically binding commitment scheme in an auxiliary-input model.

Auxiliary-input model: (reveal phase)

Committer

Send bit b and register R to the receiver.

Bit b, Register R $\longrightarrow$

Receiver

Run Verify on register CR, b and $|\phi\rangle^{\otimes n}$, then return the output.

Unconditional Secure Commitment Scheme

- [Qia24, MNY24] Auxiliary-input unconditional-secure computational hiding statistically binding commitment scheme
  - Secure against QPT adversary with quantum advice

Unconditional Computational Hiding:

- C part of $|\psi_0\rangle_{CR}$ and $|\psi_1\rangle_{CR}$ are *only* computational indistinguishable
- *Without using any* computational assumption

Unconditional Secure Commitment Scheme

- [Qia24, MNY24] Auxiliary-input unconditional-secure computational hiding statistically binding commitment scheme
  - Secure against QPT adversary with quantum advice
- **Open question:** Auxiliary-input unconditional-secure statistically hiding computational binding commitment scheme?

Unconditional Secure Commitment Scheme

- [Qia24, MNY24] Auxiliary-input unconditional-secure computational hiding statistically binding commitment scheme
  - Secure against QPT adversary with quantum advice
- **Open question:** Auxiliary-input unconditional-secure statistically hiding computational binding commitment scheme?

Our results:

- Auxiliary-input unconditional-secure perfect hiding computational binding commitment
  - Secure against QPT adversary with classical advice

Unconditional Secure Commitment Scheme

- [Qia24, MNY24] Auxiliary-input unconditional-secure computational hiding statistically binding commitment scheme
  - Secure against QPT adversary with quantum advice
- **Open question:** Auxiliary-input unconditional-secure statistically hiding computational binding commitment scheme?

Our results:

- Auxiliary-input unconditional-secure perfect hiding computational binding commitment
  - Secure against QPT adversary with classical advice
- Lead to unconditional pBQP/qpoly $\neq$ pBQP/poly

Unconditional Separation and Unconditional Cryptography

Unconditional Separation and Unconditional Cryptography

Three Separation Results:

- $Thm: mQSZK_{hv}[2] \nsubseteq mALL^{poly}$
  - $Cor: mQIP \nsubseteq mPSPACE$
- $Thm: pQSZK_{hv}[2] \nsubseteq pALL^{poly}$
  - $Cor: pQIP \nsubseteq pPSPACE$

sample complexity type of separation

$p/mC_1 \nsubseteq p/mALL^{poly}$

- $Thm: pBQP/poly \neq pBQP/qpoly$

computational type of separation

$p/mC_1 \subseteq p/mALL^{poly}$

$\Downarrow$

unconditional cryptography

Three Separation Results:

- Thm: $mQSZK_{hv}[2] \not\subseteq mALL^{poly}$
  - Cor: $mQIP \not\subseteq mPSPACE$
- Thm: $\mathrm{p}QSZK_{hv}[2] \not\subseteq pALL^{poly}$
  - Cor: $\mathrm{p}QIP \not\subseteq pPSPACE$
- Thm: $pBQP/poly \neq pBQP/qpoly$

Quantum Promise Problem L_{mix}

$$\boldsymbol{L_{mix}} := (\boldsymbol{L_Y}, \boldsymbol{L_N})$$

$$L_Y := \{U\rho_{half}U^{\dagger}, \forall\, U \in \mathbb{U}(\mathrm{n})\}$$

$$L_N = \{\frac{I}{2^n}\}$$

$$\rho_{half} := \frac{1}{2^{n-1}} \sum_{i\in\{0,1\}^{n-1}} |i\rangle\langle i|$$

$\mathbb{U}(\mathrm{n})$ be the set of n-qubit unitary

Thm: $L_{mix} \notin mALL^{poly}$

Thm: $L_{mix} \in mQSZK_{hv}[2]$

$\Longrightarrow$ $mQSZK_{hv}[2] \nsubseteq mALL^{poly}$

Cor: $mQIP \nsubseteq mPSPACE$

Theorem: $L_{mix} \notin mALL^{poly}$

$$\rho_{half} \coloneqq \frac{1}{2^{n-1}} \sum_{i \in \{0,1\}^{n-1}} |i\rangle\langle i|$$

- Thm [CHW07] : For any polynomial $q(\cdot)$ and all sufficiently large n, for all algorithm C, the following hold:

$$|\underbrace{\Pr\left[C\left(\left(\frac{I}{2^n}\right)^{\otimes q(n)}\right) = 1\right]}_{\text{NO Instance}} - \Pr_{U \leftarrow Haar_n}\underbrace{\left[C\left(\left(U\rho_{half}U^{\dagger}\right)^{\otimes q(n)}\right) = 1\right]}_{\text{Random Yes Instance}}| \leq \frac{q(n)}{2^n}$$

$L_{mix} := (L_Y, L_N)$

$L_Y := \{U\rho_{half}U^{\dagger}, \forall\, U \in \mathbb{U}(\mathrm{n})\}$

$L_N = \{\frac{I}{2^n}\}$

Theorem: $L_{mix} \in mQSZK_{hv}[2]$

Graph non-Isomorphism Like Protocol:

Prover

Verifier

b = 0

b = 1

$$\left(\left(\frac{I}{2^n}\right)^{\otimes n}, \rho_{in}^{\otimes n}\right) \text{ vs } \left(\rho_{in}^{\otimes n}, \left(\frac{I}{2^n}\right)^{\otimes n}\right) \quad b \leftarrow \{0,1\}$$

b’

Accept if b’= b

Completeness

$L_{mix} \coloneqq (L_Y, L_N)$

$L_Y \coloneqq \{U\rho_{half}U^{\dagger}, \forall\, U \in \mathbb{U}(\mathrm{n})\}$

$L_N = \{\frac{I}{2^n}\}$

Graph non-Isomorphism Like Protocol:

Prover

Verifier

b = 0

b = 1

$$\left(\left(\frac{I}{2^n}\right)^{\otimes n}, \rho_{in}^{\otimes n}\right) \text{ vs } \left(\rho_{in}^{\otimes n}, \left(\frac{I}{2^n}\right)^{\otimes n}\right) \quad b \leftarrow \{0,1\}$$

b'

Accept if b'= b

Completeness: 1 – negl(n):

Trace distance between $\left(\frac{I}{2^n}\right)^{\otimes n}$ and $\rho_{in}^{\otimes n}$ is 1 – negl(n).

$L_{mix} \coloneqq (L_Y, L_N)$

$L_Y \coloneqq \{U\rho_{half}U^{\dagger}, \forall\, U \in \mathbb{U}(\mathrm{n})\}$

$L_N = \{\frac{I}{2^n}\}$

Soundness

Graph non-Isomorphism Like Protocol:

Prover | Verifier

b = 0 | b = 1

$$\left(\left(\frac{I}{2^n}\right)^{\otimes n}, \rho_{in}^{\otimes n}\right) \text{ vs } \left(\rho_{in}^{\otimes n}, \left(\frac{I}{2^n}\right)^{\otimes n}\right) \quad b \leftarrow \{0,1\}$$

b'

Accept if b'= b

Soundness: $\frac{1}{2}$

Because $\rho_{in} = \frac{I}{2^n}$, the case b = 0 or 1 are identical.

$L_{mix} \coloneqq (L_Y, L_N)$

$L_Y \coloneqq \{U\rho_{half}U^{\dagger}, \forall\, U \in \mathbb{U}(\mathrm{n})\}$

$L_N = \{\frac{I}{2^n}\}$

Statistical HV Zero Knowledge

Graph Non-Isomorphism Like Protocol:

Prover

Verifier

b = 0

b = 1

$$\left(\left(\frac{I}{2^n}\right)^{\otimes n}, \rho_{in}^{\otimes n}\right) \text{ vs } \left(\rho_{in}^{\otimes n}, \left(\frac{I}{2^n}\right)^{\otimes n}\right) \quad b \leftarrow \{0,1\}$$

b’

Accept if b’= b

Statistical HV zero knowledge:

Similar to Graph Non-Isomorphism Protocol.

Three Separation Results:

- $Thm: mQSZK[2] \not\subseteq mALL^{poly}$
  - $Cor: mQIP \not\subseteq mPSPACE$
- $Thm: pQSZK[2] \not\subseteq pALL^{poly}$
  - $Cor: pQIP \not\subseteq pPSPACE$
- $Thm: pBQP/poly \neq pBQP/qpoly$

Quantum Promise Problem L_{pure}

$\boldsymbol{L_{mix}} \coloneqq (\boldsymbol{L_Y}, \boldsymbol{L_N})$

$L_Y \coloneqq \{U\rho_{half}U^{\dagger}, \forall\, U \in \mathbb{U}(\mathrm{n})\}$

$L_N = \{\frac{I}{2^n}\}$

$$\rho_{half} \coloneqq \frac{1}{2^{n-1}} \sum_{i \in \{0,1\}^{n-1}} |i\rangle\langle i|$$

purify

$\boldsymbol{L_{pure}} \coloneqq (\boldsymbol{L_Y}, \boldsymbol{L_N})$

$L_Y \coloneqq \{U^1 \otimes U^2 |HALF\rangle, \forall\, U^1, U^2 \in \mathbb{U}(\mathrm{n})\}$

$L_N \coloneqq \{I \otimes U|EPR\rangle, \forall\, U \in \mathbb{U}(\mathrm{n})\}$

$$|EPR\rangle \coloneqq \frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} |i\rangle|i\rangle$$

$$|HALF\rangle \coloneqq \frac{1}{\sqrt{2^{n-1}}} \sum_{i \in \{0,1\}^{n-1}} |0i\rangle|0i\rangle$$

Thm: $L_{pure} \notin pALL^{poly}$

Thm: $L_{pure} \in pQSZK_{hv}[2]$

$\Longrightarrow$ $pQSZK_{hv}[2] \nsubseteq pALL^{poly}$

Cor: $pQIP \nsubseteq pPSPACE$

Theorem: $L_{pure} \notin pALL^{poly}$

- Theorem [CWZ24] (informal) : Let $L = (L_Y, L_N)$ be a mixed QPP. Let L' be the purified version of L. Then sample complexity for deciding L and L' are the same.

$\boldsymbol{L_{mix}} := (\boldsymbol{L_Y}, \boldsymbol{L_N})$

$L_Y := \{U\rho_{half}U^{\dagger}, \forall\, U \in \mathbb{U}(\mathrm{n})\}$

$L_N = \{\frac{I}{2^n}\}$

purify

$\boldsymbol{L_{pure}} := (\boldsymbol{L_Y}, \boldsymbol{L_N})$

$L_Y := \{U^1 \otimes U^2 |HALF\rangle, \forall\, U^1, U^2 \in \mathbb{U}(\mathrm{n})\}$

$L_N := \{I \otimes U|EPR\rangle, \forall\, U \in \mathbb{U}(\mathrm{n})\}$

$L_{pure} \coloneqq (L_Y, L_N)$

$L_Y \coloneqq \{U^1 \otimes U^2 |HALF\rangle, \forall\, U^1, U^2 \in \mathbb{U}(\mathrm{n})\}$

$L_N \coloneqq \{(I \otimes U)|EPR\rangle, \forall\, U \in \mathbb{U}(\mathrm{n})\}$

Theorem: $L_{pure} \in pQSZK_{hv}[2]$

The same Graph Non-Isomorphism Like Protocol except that we set ρ_{in} = first half of $|\phi_{in}\rangle$.

Prover

Verifier

b = 0

b = 1

$\left(\left(\frac{I}{2^n}\right)^{\otimes n}, \rho_{in}^{\otimes n}\right)$ vs $\left(\rho_{in}^{\otimes n}, \left(\frac{I}{2^n}\right)^{\otimes n}\right)$

$b \leftarrow \{0,1\}$

b'

Accept if b'= b

Three Separation Results:

- $Thm: mQSZK[2] \not\subseteq mALL^{poly}$
  - $Cor: mQIP \not\subseteq mPSPACE$
- $Thm: \mathrm{p}QSZK[2] \not\subseteq pALL^{poly}$
  - $Cor: \mathrm{p}QIP \not\subseteq pPSPACE$
- $Thm: pBQP/poly \neq pBQP/qpoly$

Quantum Promise Problem $\boldsymbol{L_{pure^\star}(\{U^\star\})}$

$\boldsymbol{L_{pure}} \coloneqq (\boldsymbol{L_Y}, \boldsymbol{L_N})$

$L_Y \coloneqq \{U^1 \otimes U^2|HALF\rangle, \forall\, U^1, U^2 \in \mathbb{U}(\mathrm{n})\}$

$L_N \coloneqq \{I \otimes U|EPR\rangle, \forall\, U \in \mathbb{U}(\mathrm{n})\}$

$$|EPR\rangle \coloneqq \frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} |i\rangle|i\rangle$$

$$|HALF\rangle \coloneqq \frac{1}{\sqrt{2^{n-1}}} \sum_{i \in \{0,1\}^{n-1}} |0i\rangle|0i\rangle$$

Fix a hard $\boldsymbol{U^\star}$

$\boldsymbol{L_{pure^\star}(\{U^\star\})} \coloneqq (\boldsymbol{L_Y}, \boldsymbol{L_N})$

$L_Y \coloneqq \{U^1 \otimes U^2|HALF\rangle, \forall\, U^1, U^2 \in \mathbb{U}(\mathrm{n})\}$

$L_N \coloneqq \{I \otimes U^\star|EPR\rangle\}$

Thm: Exist $\{U^\star\}$ such that $L_{pure^\star}(\{U^\star\}) \notin pBQP/poly$

Thm: For all $\{U^\star\}$, $L_{pure^\star}(\{U^\star\}) \in pBQP/qpoly$

Cor: $pBQP/poly \neq pBQP/qpoly$

Thm: For all $\{U^\star\}$, $L_{pure^\star}(\{U^\star\}) \in pBQP/qpoly$

$\boldsymbol{L_{pure^\star}} := (\boldsymbol{L_Y}, \boldsymbol{L_N})$

$L_Y := \{U^1 \otimes U^2 |HALF\rangle, \forall\, U^1, U^2 \in \mathbb{U}(\mathrm{n})\}$

$L_N := \{(I \otimes U^\star)|EPR\rangle\}$

Use Swap Test

- Quantum advice: $|\phi^\star\rangle := (\mathrm{I} \otimes U^\star)|EPR\rangle$

- Algorithm: input $|\phi_{in}\rangle$, advice $|\phi^\star\rangle$
  - Apply swap test to $|\phi_{in}\rangle$ and $|\phi^\star\rangle$
  - Output 1 if swap test fail
  - Otherwise output 0.

- Completeness: $\geq \frac{1}{8}$ (because $F(|\phi_{in}\rangle, |\phi^\star\rangle) \leq \frac{3}{4}$)
- Soundness: = 0

Thm: Exist $\{U^\star\}$ such that $L_{pure^\star}(\{U^\star\}) \notin pBQP/poly$

$\boldsymbol{L_{pure}} \coloneqq (\boldsymbol{L_Y}, \boldsymbol{L_N})$

$L_Y \coloneqq \{U^1 \otimes U^2 |HALF\rangle, \forall\, U^1, U^2 \in \mathbb{U}(\mathrm{n})\}$
$L_N \coloneqq \{I \otimes U |EPR\rangle, \forall\, U \in \mathbb{U}(\mathrm{n})\}$

- [CWZ24] & [CHW07] => average case hardness of L_{pure}
- For any polynomial $q(\cdot)$ and all sufficiently large n, for all algorithm C, the following hold:

$$\left| \Pr_{U \leftarrow Haar_n} \Big[C\big(\underbrace{I \otimes U |EPR\rangle^{\otimes q(n)}}_{\text{Uniformly Random No Instance}}\big) = 1\Big] - \Pr_{U^1, U^2 \leftarrow Haar_n} \Big[C\big(\underbrace{U^1 \otimes U^2 |HALF\rangle^{\otimes q(n)}}_{\text{Uniformly Random Yes Instance}}\big) = 1\Big] \right| \leq \frac{q(n)}{2^n}$$

Thm: Exist $\{U^\star\}$ such that $L_{pure^\star}(\{U^\star\}) \notin pBQP/poly$

- By Haar random concentration argument in [Kre21] :
- For any polynomial q(·) and all sufficiently large n, for all algorithm C, with probability $1 - \exp(-2^{\frac{n}{4}})$ over $U \leftarrow Haar_n$ such that:

$$|\, Pr\left[C\left(I \otimes U\, |EPR\rangle\right)^{\otimes q(n)}\right) = 1\right] - \Pr_{U^1, U^2 \leftarrow Haar_n}\left[C\left(U^1 \otimes U^2 |HALF\rangle\,\right)^{\otimes q(n)}\right) = 1\right]| \leq \frac{q(n)}{2^n} + 2^{-\frac{n}{3}}$$

Thm: Exist $\{U^\star\}$ such that $L_{pure^\star}(\{U^\star\}) \notin pBQP/poly$

- Switch quantifier by a union bound:
- For any polynomial q(·) and all sufficiently large n, there exist $U^\star$ such that for all polynomial size circuits C

$$|\, Pr\left[C\left(I \otimes U^\star\, |EPR\rangle\right)^{\otimes q(n)}\right) = 1\right]$$

$$- \Pr_{U^1, U^2 \leftarrow Haar_n}\left[C\left(U^1 \otimes U^2 |HALF\rangle\,\right)^{\otimes q(n)}\right) = 1\right]| \leq \frac{q(n)}{2^n} + 2^{-\frac{n}{3}}$$

Unconditional Separation and Unconditional Cryptography

Thm: There exist a commitment scheme satisfy computational sum-binding* and perfect hiding in auxiliary-input model.

*secure against non-uniform adv with classical advice

Construction – Auxiliary Input State

$|\phi\rangle \coloneqq I \otimes U^\star|EPR\rangle$ Fix $U^\star$ in $L_{pure^\star}(\{U^\star\}) \notin pBQP/poly$

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

Committer

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

Receiver

Construction – Commit Algorithm

$|\phi\rangle \coloneqq I \otimes U^\star |EPR\rangle$ Fix $U^\star$ in $L_{pure^\star}(\{U^\star\}) \notin pBQP/poly$

Com(b, $|\phi\rangle^{\otimes n}) \to |\psi_b\rangle_{CR}$:

$|\psi_0\rangle_{CR} \coloneqq |EPR\rangle_{C_1R_1} \cdots |EPR\rangle_{C_nR_n}$

$|\psi_1\rangle_{CR} \coloneqq |\phi\rangle_{C_1R_1} \cdots |\phi\rangle_{C_nR_n}$

Let $C \coloneqq \{C_i\}_{i=1..n}$, $R \coloneqq \{R_i\}_{i=1..n}$.

Committer

Receiver

Prepare $|\psi_b\rangle_{CR}$ & send register C

Register C $\longrightarrow$

Construction – Verify Algorithm

$|\phi\rangle \coloneqq I \otimes U^\star |EPR\rangle$ Fix $U^\star$ in $L_{pure^\star}(\{U^\star\}) \notin pBQP/poly$

Com(b, $|\phi\rangle^{\otimes n}$) $\rightarrow |\psi_b\rangle_{CR}$:
$|\psi_0\rangle_{CR} \coloneqq |EPR\rangle_{C_1R_1} \cdots |EPR\rangle_{C_nR_n}$
$|\psi_1\rangle_{CR} \coloneqq |\phi\rangle_{C_1R_1} \cdots |\phi\rangle_{C_nR_n}$

Let $C \coloneqq \{C_i\}_{i=1..n}$, $R \coloneqq \{R_i\}_{i=1..n}$.

Verify(b, $|\phi\rangle^{\otimes n}$, CR) $\rightarrow \bot/\top$:
b = 0: check CR == $|\psi_0\rangle$ by $\{|\psi_0\rangle\langle\psi_0|, I - |\psi_0\rangle\langle\psi_0|\}$.
b = 1: check CR == $|\psi_1\rangle$ by swap-test.

Committer		Receiver
Send b & register R	Bit b, Register R →	Run Verify(b, $|\phi\rangle^{\otimes n}$, CR)

Ours Construction:

Fix a hard unitary:

$U^\star: \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$

Auxiliary input state:

$$|\phi\rangle := \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle_C (U^\star |x\rangle)_R$$

Com(b, $|\phi\rangle^{\otimes n}$) → $|\psi_b\rangle_{CR}$:

$|\psi_0\rangle_{CR} := |EPR_n\rangle_{C_1 R_1} \cdots |EPR_n\rangle_{C_n R_n}$

$|\psi_1\rangle_{CR} := |\phi\rangle_{C_1 R_1} \cdots |\phi\rangle_{C_n R_n}$

Let $C := \{C_i\}_{i=1..n}$, $R := \{R_i\}_{i=1..n}$.

Verify(b, $|\phi\rangle^{\otimes n}$, CR) → ⊥/⊤:

b = 0: check CR == $|\psi_0\rangle$ by $\{|\psi_0\rangle\langle\psi_0|, I - |\psi_0\rangle\langle\psi_0|\}$.

b = 1: check CR == $|\psi_1\rangle$ by swap-test.

[Qia24, MNY24]

Fix a “hard” function:

$H^\star: \{0,1\}^n \to \{0,1\}^{3n}$

Auxiliary input state:

$$|\phi\rangle := \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |H^\star(x)\rangle_C |x\rangle_R$$

Com(b, $|\phi\rangle^{\otimes n}$) → $|\psi_b\rangle_{CR}$:

$|\psi_0\rangle_{CR} := |EPR_{3n}\rangle_{C_1 R_1} \cdots |EPR_{3n}\rangle_{C_n R_n}$

$|\psi_1\rangle_{CR} := |\phi\rangle_{C_1 R_1} \cdots |\phi\rangle_{C_n R_n}$

Let $C := \{C_i\}_{i=1..n}$, $R := \{R_i\}_{i=1..n}$.

Verify(b, $|\phi\rangle^{\otimes n}$, CR) → ⊥/⊤ :

b =0/1: Check CR == $|\psi_b\rangle$ by swap-test.

Can also use QPP to capture the unconditional computation hardness of [Qia24,MNY24].

Source of Comp. Hardness in Ours Construction:

$$\boldsymbol{L_{pure^\star}(\{U^\star\}) \coloneqq (L_Y, L_N)}$$

$U^\star: \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$

$$L_Y \coloneqq \{U^1 \otimes U^2 |HALF\rangle, \forall\, U^1, U^2 \in \mathbb{U}(\mathrm{n})\}$$

$$L_N \coloneqq \{(I \otimes U^\star)|EPR\rangle\}$$

Thm: Exist $\{U^\star\}$ such that $L_{pure^\star}(\{U^\star\}) \notin pBQP/poly$

Thm: For all $\{U^\star\}$, $L_{pure^\star}(\{U^\star\}) \in pALL^{poly}$

Source of Comp. Hardness in [Qia24, MNY24]:

$$\boldsymbol{L_{mix^\star}(\{H^\star\}) \coloneqq (L_Y, L_N)}$$

$H^\star: \{0,1\}^n \to \{0,1\}^{3n}$

$$L_Y \coloneqq \{\frac{1}{2^n} \sum_{x \in \{0,1\}^n} |H^\star(x)\rangle\langle H^\star(x)|\}$$

$$L_N \coloneqq \{\frac{I}{2^{3n}}\}$$

Thm: Exist $\{H^\star\}$ such that $L_{mix^\star}(\{H^\star\}) \notin mBQP/qpoly$

Thm: For all $\{H^\star\}$, $L_{pure^\star}(\{H^\star\}) \in mALL^{poly}$

Construction – Commit Algorithm

$|\phi\rangle \coloneqq I \otimes U^{\star}|EPR\rangle$ Fix $U^{\star}$ in $L_{pure^{\star}}(\{U^{\star}\}) \notin pBQP/poly$

Com(b, $|\phi\rangle^{\otimes n}$) $\rightarrow |\psi_b\rangle_{CR}$:
$|\psi_0\rangle_{CR} \coloneqq |EPR\rangle_{C_1R_1} \cdots |EPR\rangle_{C_nR_n}$
$|\psi_1\rangle_{CR} \coloneqq |\phi\rangle_{C_1R_1} \cdots |\phi\rangle_{C_nR_n}$

Let $C \coloneqq \{C_i\}_{i=1..n}$, $R \coloneqq \{R_i\}_{i=1..n}$.

Satisfy perfect hiding

Committer

Receiver

Prepare $|\psi_b\rangle_{CR}$ & send register C

Register C →

Proof of Computational Binding

$$L_{pure^\star}(\{U_n^\star\}) \notin pBQP/poly$$

$$\boxed{\Downarrow}$$

Security of honest binding (0 to 1)

[Yan22] $\Downarrow$

Security of sum binding

Adversary Break Honest Binding ($0 \rightarrow 1$)

$|\phi\rangle \coloneqq I \otimes U^\star |EPR\rangle$ Fix $U^\star$ such that $L_{pure^\star}(\{U^\star\}) \notin pBQP/poly$

Com(b, $|\phi\rangle^{\otimes n}$) $\rightarrow |\psi_b\rangle_{CR}$:

$|\psi_0\rangle_{CR} \coloneqq |EPR\rangle_{C_1R_1} \cdots |EPR\rangle_{C_nR_n}$

$|\psi_1\rangle_{CR} \coloneqq |\phi\rangle_{C_1R_1} \cdots |\phi\rangle_{C_nR_n}$

Let $C \coloneqq \{C_i\}_{i=1..n}$, $R \coloneqq \{R_i\}_{i=1..n}$.

Verify(b, $|\phi\rangle^{\otimes n}$, CR) $\rightarrow \perp/\top$:

b = 0: check CR == $|\psi_0\rangle$ by $\{|\psi_0\rangle\langle\psi_0|, I - |\psi_0\rangle\langle\psi_0|\}$.

b = 1: check CR == $|\psi_1\rangle$ by swap-test.

(Honest Commit):

Adversary

Receiver

Prepare $|\psi_b\rangle_{CR}$ & send register C

Register C $\longrightarrow$

Adversary Break Honest Binding ($0 \rightarrow 1$)

$|\phi\rangle \coloneqq I \otimes U^{\star}|EPR\rangle$ Fix $U^{\star}$ such that $L_{pure^{\star}}(\{U^{\star}\}) \notin pBQP/poly$

Com(b, $|\phi\rangle^{\otimes n}$) $\rightarrow |\psi_b\rangle_{CR}$:

$|\psi_0\rangle_{CR} \coloneqq |EPR\rangle_{C_1R_1} \cdots |EPR\rangle_{C_nR_n}$

$|\psi_1\rangle_{CR} \coloneqq |\phi\rangle_{C_1R_1} \cdots |\phi\rangle_{C_nR_n}$

Let $C \coloneqq \{C_i\}_{i=1..n}$, $R \coloneqq \{R_i\}_{i=1..n}$.

Verify(b, $|\phi\rangle^{\otimes n}$, CR) $\rightarrow \perp/\top$:

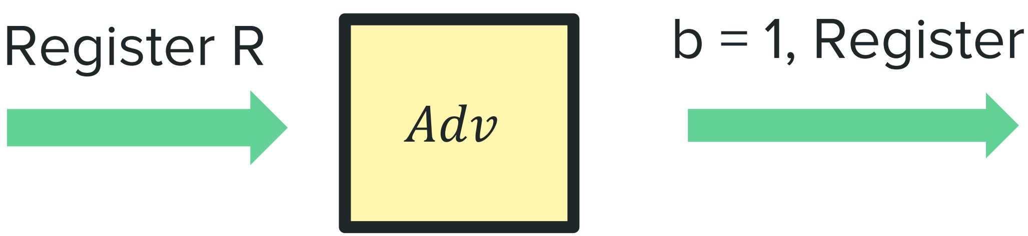
b = 0: check CR == $|\psi_0\rangle$ by $\{|\psi_0\rangle\langle\psi_0|, I - |\psi_0\rangle\langle\psi_0|\}$.

b = 1: check CR == $|\psi_1\rangle$ by swap-test.

(Reveal Phase):

Adversary

Receiver



The CR register $\approx |\psi_1\rangle$

Adversary Break Honest Binding $(0 \rightarrow 1)$

$|\phi\rangle \coloneqq I \otimes U^\star|EPR\rangle$ Fix $U^\star$ such that $L_{pure^\star}(\{U^\star\}) \notin pBQP/poly$

Com(b, $|\phi\rangle^{\otimes n}$) $\rightarrow |\psi_b\rangle_{CR}$:

$|\psi_0\rangle_{CR} \coloneqq |EPR\rangle_{C_1R_1} \cdots |EPR\rangle_{C_nR_n}$

$|\psi_1\rangle_{CR} \coloneqq |\phi\rangle_{C_1R_1} \cdots |\phi\rangle_{C_nR_n}$

Let $C \coloneqq \{C_i\}_{i=1..n}$, $R \coloneqq \{R_i\}_{i=1..n}$.

Verify(b, $|\phi\rangle^{\otimes n}$, CR) $\rightarrow \perp/\top$:

b = 0: check CR == $|\psi_0\rangle$ by $\{|\psi_0\rangle\langle\psi_0|, I - |\psi_0\rangle\langle\psi_0|\}$.

b = 1: check CR == $|\psi_1\rangle$ by swap-test.

$$\boxed{Adv} \approx (U^\star)^{\otimes n}$$

Use Adv to decide $L_{pure^\star}(\{U^\star\})$.

Proof of Honest Binding

$$\boxed{Adv} \approx (U^\star)^{\otimes n}$$

$$\boldsymbol{L_{pure^\star}(\{U^\star\}) \coloneqq (L_Y, L_N)}$$

$$L_Y \coloneqq \{U^1 \otimes U^2|HALF\rangle, \forall\, U^1, U^2 \in \mathbb{U}(\mathrm{n})\}$$

$$L_N \coloneqq \{(I \otimes U^\star)|EPR\rangle\}$$

- Algorithm: input $|\phi_{in}\rangle^{\otimes n}$
  - Generate $|EPR\rangle_{C_1R_1} \cdots |EPR\rangle_{C_nR_n}$ (Let $C \coloneqq \{C_i\}_{i=1..n}$, $R \coloneqq \{R_i\}_{i=1..n}$)
  - Apply Adv to the R part get $|\phi'\rangle$
  - Apply n-swap test to $|\phi'\rangle$ and $|\phi_{in}\rangle^{\otimes n}$
  - Output 0 if n-swap test pass.
  - Otherwise output 1.

- Completeness: $\geq 1 - negl(n)$ (because $F(|\phi_{in}\rangle, |EPR\rangle) \leq \frac{3}{4}$)
- Soundness: $\leq 1 - 1/poly(n)$ (by the binding)

Proof of Computational Binding

$$L_{pure^\star}(\{U_n^\star\}) \notin pBQP/poly$$

Security of honest binding (0 to 1)

[Yan22]

Security of sum binding

Proof of Computational Binding

- Thm [Yan22]: For canonical quantum bit commitment, honest binding imply sum-binding.

- Canonical Quantum Bit Commitment
  - Two efficient unitary $\{Q_0, Q_1\}$.
  - Com(b):$|\psi_b\rangle \coloneqq Q_b|0\rangle$
  - Verify(b,CR): check == $|\psi_b\rangle$ by $\{|\psi_b\rangle\langle\psi_b|, I - |\psi_b\rangle\langle\psi_b|\}$.

- Our construct is "semi-"Canonical Quantum Bit Commitment
  - Com(0): $|\psi_0\rangle \coloneqq |EPR\rangle^{\otimes n}$
  - Verify(0,CR): check == $|\psi_0\rangle$ by $\{|\psi_0\rangle\langle\psi_0|, I - |\psi_0\rangle\langle\psi_0|\}$.

- The technique of [Yan22] can be applied as well

Discussion & Open Problems

- Natural and useful complexity theory to study
  - Different landscape – classical vs pure vs mixed
- Help understand computational hardness in quantum crypto
  - Further characterization? Worst-case hardness <=> EFI?
  - Impagliazzo's five worlds?
- Other applications
  - Interaction helps in quantum property testing
  - Hardness of quantum-input unitary synthesize problem

Discussion & Open Problems

- Many open questions in QPP complexity theory
  - More unconditional separation or barrier?
    - Note: relativize barrier still hold
  - Complete problems for, e.g., PSPACE?
  - $p/mPSPACE^{poly}$ vs. $p/mQIP^{poly}$?
  - $p/mQIP = p/mQIP[3]$?
  - $p/mQSZK_{hv} = p/mQSZK$?
  - ZK for $p/mQMA$? [Mal'25]
  - Complexity of search $p/mQMA$ witness – state synthesize complexity
  - Circuit complexity for QPP?