Uncloneable states are necessary as proofs and advice

Rohit Chatterjee, **Srijita Kundu** & Supartha Podder

SG Crypto 2026

Uncloneabibility of quantum states

No-cloning theorem: No quantum operation can clone an unknown quantum state.

Uncloneabibility of quantum states

No-cloning theorem: No quantum operation can clone an unknown quantum state.

Very useful for cryptography!

Uncloneabibility of quantum states

No-cloning theorem: No quantum operation can clone an unknown quantum state.

Very useful for cryptography!

- Unforgeable quantum money: Wiesner (1969), Aaronson and Christiano (2012), Zhandry (2021), ...

Uncloneabibility of quantum states

No-cloning theorem: No quantum operation can clone an unknown quantum state.

Very useful for cryptography!

- Unforgeable quantum money: Wiesner (1969), Aaronson and Christiano (2012), Zhandry (2021), ...
- Uncloneable encryption and decryption: Broadbent and Lord (2019), Georgiu and Zhandry (2020), ...

Uncloneabibility of quantum states

No-cloning theorem: No quantum operation can clone an unknown quantum state.

Very useful for cryptography!

- Unforgeable quantum money: Wiesner (1969), Aaronson and Christiano (2012), Zhandry (2021), ...
- Uncloneable encryption and decryption: Broadbent and Lord (2019), Georgiu and Zhandry (2020), ...
- Quantum copy protection: Aaronson (2009), Coladangelo, Majenz and Poremba (2020), ...

Uncloneabibility of quantum states

No-cloning theorem: No quantum operation can clone an unknown quantum state.

Very useful for cryptography!

- Unforgeable quantum money: Wiesner (1969), Aaronson and Christiano (2012), Zhandry (2021), ...
- Uncloneable encryption and decryption: Broadbent and Lord (2019), Georgiu and Zhandry (2020), ...
- Quantum copy protection: Aaronson (2009), Coladangelo, Majenz and Poremba (2020), ...
- Secure software leasing: Ananth and La Placa (2021), Broadbent, Jeffery, Lord, Podder and Sundaram (2021), ...

Uncloneability in computation

Is the uncloneability of quantum states useful for computation?

Uncloneability in computation

Is the uncloneability of quantum states useful for computation?

i.e., Are there problems that can only be solved using uncloneable quantum states?

Uncloneability in computation

Is the uncloneability of quantum states useful for computation?

i.e., Are there problems that can only be solved using uncloneable quantum states?

Natural candidate: Quantum proof and advice states

Uncloneability in computation

Is the uncloneability of quantum states useful for computation?

i.e., Are there problems that can only be solved using uncloneable quantum states?

Natural candidate: Quantum proof and advice states

Our results:

1. There is a quantum oracle and a decision problem which can only be solved by a quantum poly-time algorithm using an uncloneable quantum state as quantum proof, with access to the quantum oracle.

Uncloneability in computation

Is the uncloneability of quantum states useful for computation?

i.e., Are there problems that can only be solved using uncloneable quantum states?

Natural candidate: Quantum proof and advice states

Our results:

1. There is a quantum oracle and a decision problem which can only be solved by a quantum poly-time algorithm using an uncloneable quantum state as quantum proof, with access to the quantum oracle.
2. Same as 1. with advice.

Uncloneability in computation

Is the uncloneability of quantum states useful for computation?

i.e., Are there problems that can only be solved using uncloneable quantum states?

Natural candidate: Quantum proof and advice states

Our results:

1. There is a quantum oracle and a decision problem which can only be solved by a quantum poly-time algorithm using an uncloneable quantum state as quantum proof, with access to the quantum oracle.
2. Same as 1. with advice.
3. There is a relational problem which can only be exactly solved by a quantum poly-time algorithm with an uncloneable quantum state as quantum advice.

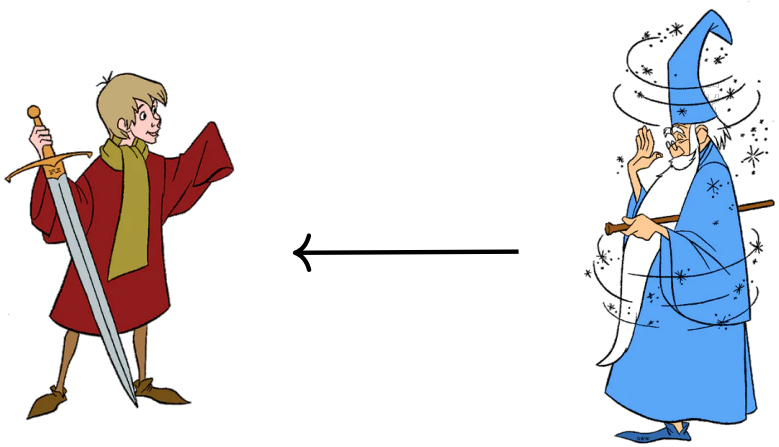
Quantum proofs

Quantum proofs

Quantum generalization of NP

Quantum proofs

Quantum generalization of NP



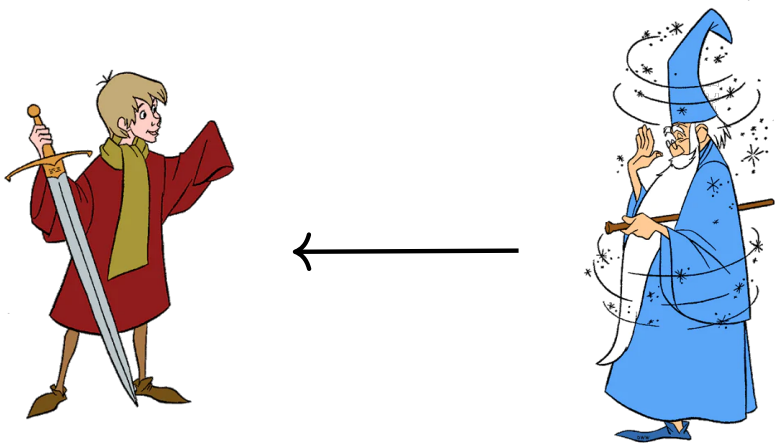
Input $x \in \{0,1\}^*$, is $x \in$ YES?

Knows x

Quantum proofs

Quantum generalization of NP

- If YES instance, exists witness that can convince Arthur w.h.p.
- If NO instance, every witness is rejected by Arthur w.h.p.



Input $x \in \{0,1\}^*$, is $x \in$ YES?

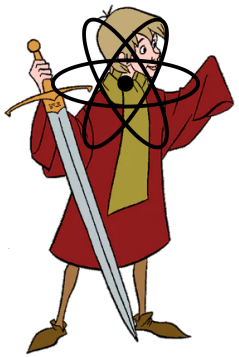
Knows x

Quantum proofs

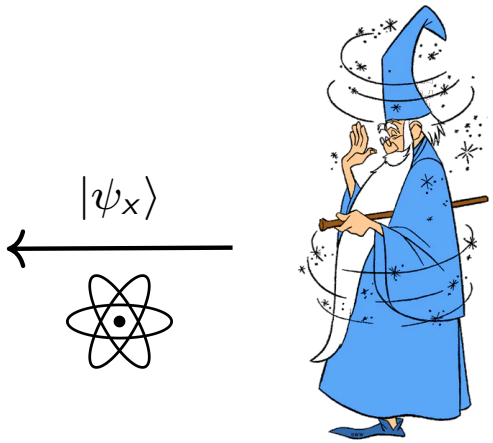
Quantum generalization of NP

- If YES instance, exists witness that can convince Arthur w.h.p.
- If NO instance, every witness is rejected by Arthur w.h.p.

QMA



$|\psi_x\rangle$



Input $x \in \{0,1\}^*$, is $x \in$ YES?

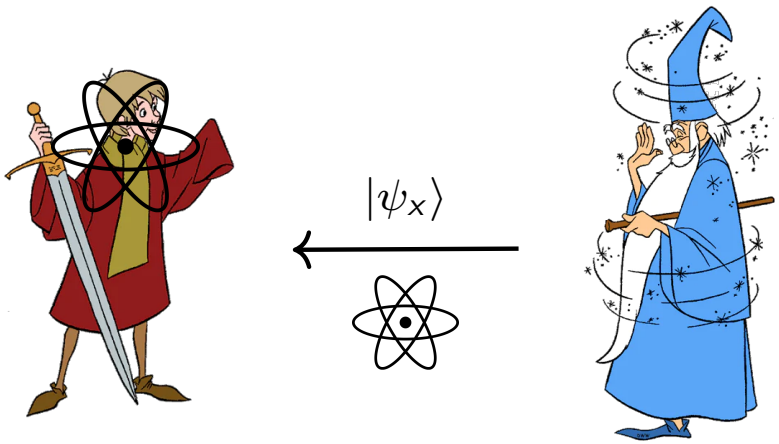
Knows x

Quantum proofs

Quantum generalization of NP

- If YES instance, exists witness that can convince Arthur w.h.p.
- If NO instance, every witness is rejected by Arthur w.h.p.

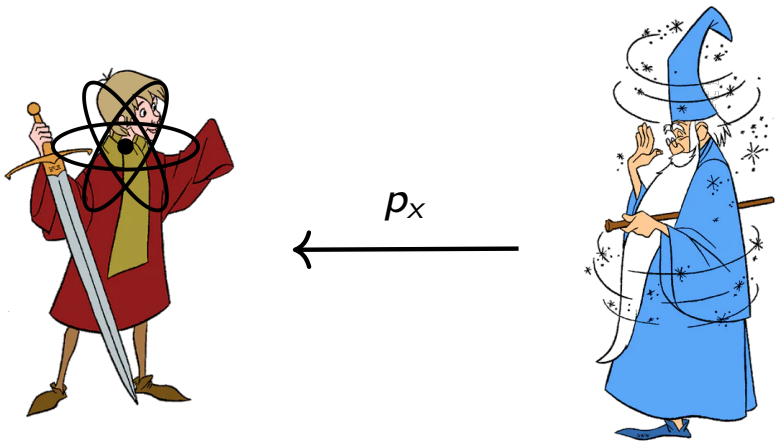
QMA



Input $x \in \{0,1\}^*$, is $x \in$ YES?

Knows x

QCMA



Input $x \in \{0,1\}^*$, is $x \in$ YES?

Knows x

Quantum proofs

Separating QMA and QCMA is one of the most fundamental problems in quantum complexity theory...

Quantum proofs

Separating QMA and QCMA is one of the most fundamental problems in quantum complexity theory...

...But even proving an oracle separation is really hard!

Quantum proofs

Separating QMA and QCMA is one of the most fundamental problems in quantum complexity theory...

...But even proving an oracle separation is really hard!

- All algorithms have access to an oracle, which may be a classical function $\mathcal{O} : \{0,1\}^* \to \{0,1\}^*$ or a sequence of blackbox unitaries $\{U_n\}_n$

Quantum proofs

Separating QMA and QCMA is one of the most fundamental problems in quantum complexity theory...

...But even proving an oracle separation is really hard!

- All algorithms have access to an oracle, which may be a classical function $\mathcal{O} : \{0,1\}^* \to \{0,1\}^*$ or a sequence of blackbox unitaries $\{U_n\}_n$

Quantum oracle separation between QMA and QCMA: Aaronson and Kuperberg (2007)

Quantum proofs

Separating QMA and QCMA is one of the most fundamental problems in quantum complexity theory...

...But even proving an oracle separation is really hard!

- All algorithms have access to an oracle, which may be a classical function $\mathcal{O} : \{0,1\}^* \to \{0,1\}^*$ or a sequence of blackbox unitaries $\{U_n\}_n$

Quantum oracle separation between QMA and QCMA: Aaronson and Kuperberg (2007)

Very recent classical oracle separation: Bostanci, Haferkamp, Nirkhe, Zhandry (2025)

Quantum proofs

Separating QMA and QCMA is one of the most fundamental problems in quantum complexity theory...

...But even proving an oracle separation is really hard!

- All algorithms have access to an oracle, which may be a classical function $\mathcal{O} : \{0,1\}^* \to \{0,1\}^*$ or a sequence of blackbox unitaries $\{U_n\}_n$

Quantum oracle separation between QMA and QCMA: Aaronson and Kuperberg (2007)

Very recent classical oracle separation: Bostanci, Haferkamp, Nirkhe, Zhandry (2025)

Any problem that can only be solved by uncloneable quantum proofs must necessarily separate QMA and QCMA

Quantum proofs

Separating QMA and QCMA is one of the most fundamental problems in quantum complexity theory...

...But even proving an oracle separation is really hard!

- All algorithms have access to an oracle, which may be a classical function $\mathcal{O} : \{0,1\}^* \to \{0,1\}^*$ or a sequence of blackbox unitaries $\{U_n\}_n$

Quantum oracle separation between QMA and QCMA: Aaronson and Kuperberg (2007)

Very recent classical oracle separation: Bostanci, Haferkamp, Nirkhe, Zhandry (2025)

Any problem that can only be solved by uncloneable quantum proofs must necessarily separate QMA and QCMA

- Classical proofs are always cloneable

Quantum proofs

Separating QMA and QCMA is one of the most fundamental problems in quantum complexity theory...

...But even proving an oracle separation is really hard!

- All algorithms have access to an oracle, which may be a classical function $\mathcal{O} : \{0,1\}^* \to \{0,1\}^*$ or a sequence of blackbox unitaries $\{U_n\}_n$

Quantum oracle separation between QMA and QCMA: Aaronson and Kuperberg (2007)

Very recent classical oracle separation: Bostanci, Haferkamp, Nirkhe, Zhandry (2025)

Any problem that can only be solved by uncloneable quantum proofs must necessarily separate QMA and QCMA

- Classical proofs are always cloneable
- We use the AK07 quantum oracle

Quantum advice

Quantum advice

- **BQP/qpoly**: decision BQP with poly-sized quantum advice
- **BQP/poly**: decision BQP with poly-sized classical advice

Quantum advice

- **BQP/qpoly**: decision BQP with poly-sized quantum advice
- **BQP/poly**: decision BQP with poly-sized classical advice
  - Advice only depends on input size
  - Advice is always trusted

Quantum advice

- **BQP/qpoly**: decision BQP with poly-sized quantum advice
- **BQP/poly**: decision BQP with poly-sized classical advice
  - Advice only depends on input size
  - Advice is always trusted

QMA vs QCMA seems related to BQP/qpoly vs BQP/poly: e.g. AK07

Quantum advice

- **BQP/qpoly**: decision BQP with poly-sized quantum advice
- **BQP/poly**: decision BQP with poly-sized classical advice
  - Advice only depends on input size
  - Advice is always trusted

QMA vs QCMA seems related to BQP/qpoly vs BQP/poly: e.g. AK07

Aaronson, Buhrman and Kretschmer (2023): The relational versions of BQP/qpoly and BQP/poly can be **unconditionally** separated!

Quantum advice

- **BQP/qpoly**: decision BQP with poly-sized quantum advice
- **BQP/poly**: decision BQP with poly-sized classical advice
  - Advice only depends on input size
  - Advice is always trusted

QMA vs QCMA seems related to BQP/qpoly vs BQP/poly: e.g. AK07

Aaronson, Buhrman and Kretschmer (2023): The relational versions of BQP/qpoly and BQP/poly can be **unconditionally** separated!

- **FBQP/qpoly**: like BQP/qpoly for polynomially bounded relations $R \subseteq \{0,1\}^* \times \{0,1\}^*$, ...
- In fact the ABK23 construction separates FEQP/qpoly and FBQP/poly
- We use the ABK23 construction

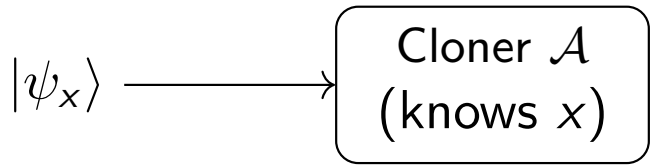
What is an uncloneable proof or advice?

What is an uncloneable proof or advice?

Existence of a family of uncloneable proofs or advice also considered by: Broadbent, Karvonen and Lord (2023), Broadbent, Grilo, Podder and Sikora (2024)

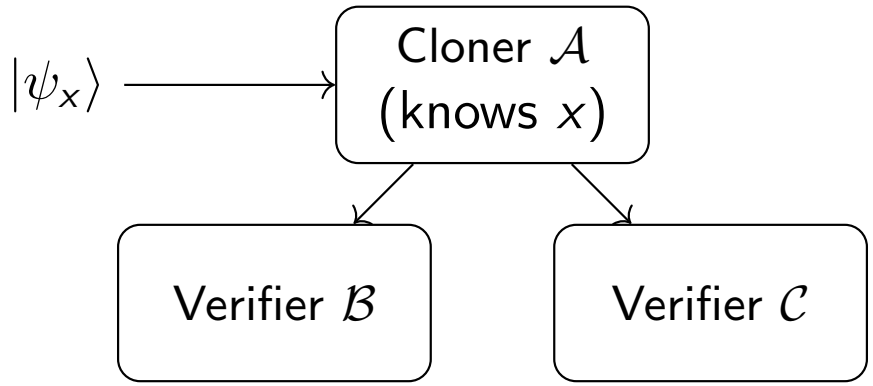
What is an uncloneable proof or advice?

Existence of a family of uncloneable proofs or advice also considered by: Broadbent, Karvonen and Lord (2023), Broadbent, Grilo, Podder and Sikora (2024)



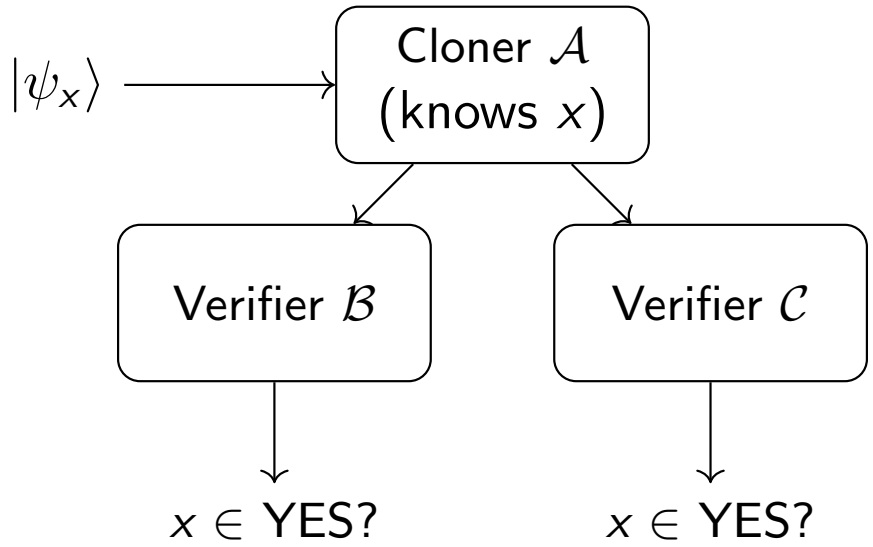
What is an uncloneable proof or advice?

Existence of a family of uncloneable proofs or advice also considered by: Broadbent, Karvonen and Lord (2023), Broadbent, Grilo, Podder and Sikora (2024)



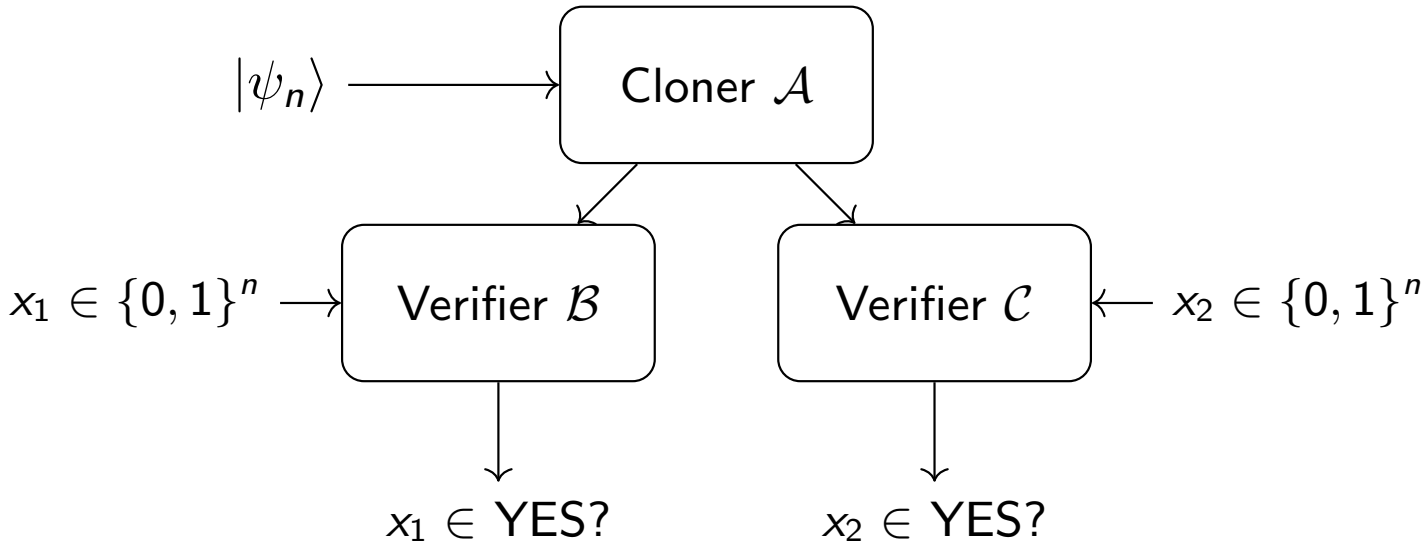
What is an uncloneable proof or advice?

Existence of a family of uncloneable proofs or advice also considered by: Broadbent, Karvonen and Lord (2023), Broadbent, Grilo, Podder and Sikora (2024)



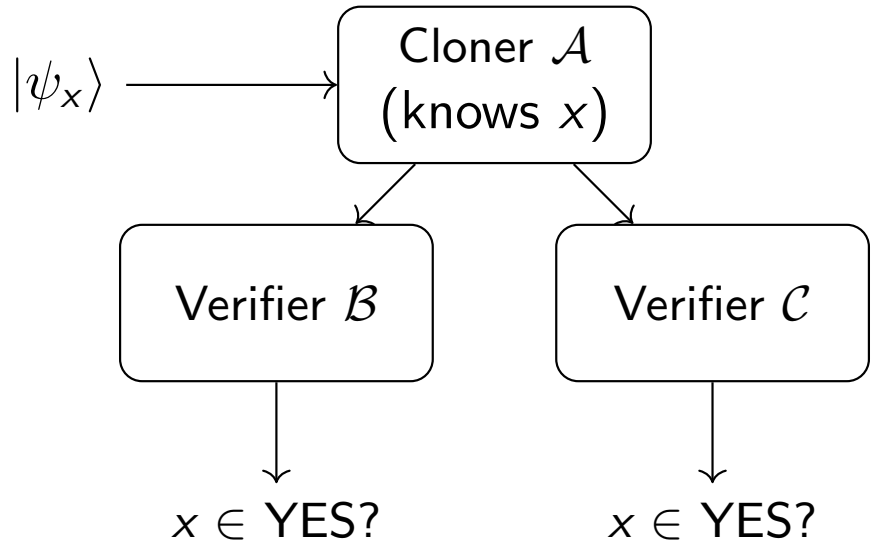
What is an uncloneable proof or advice?

Existence of a family of uncloneable proofs or advice also considered by: Broadbent, Karvonen and Lord (2023), Broadbent, Grilo, Podder and Sikora (2024)



What is an uncloneable proof or advice?

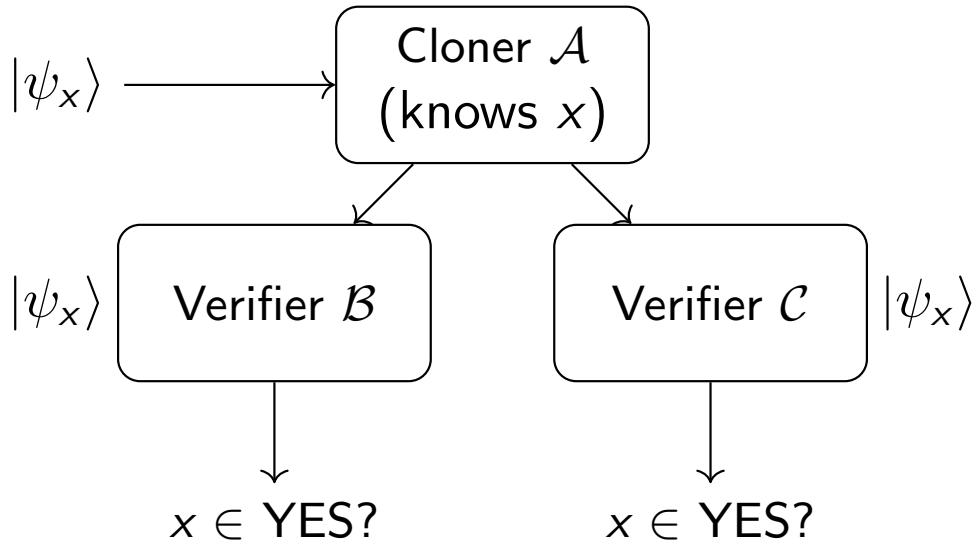
Existence of a family of uncloneable proofs or advice also considered by: Broadbent, Karvonen and Lord (2023), Broadbent, Grilo, Podder and Sikora (2024)



- Functionality of the state $|\psi_x\rangle$ as proof needs to be cloned

What is an uncloneable proof or advice?

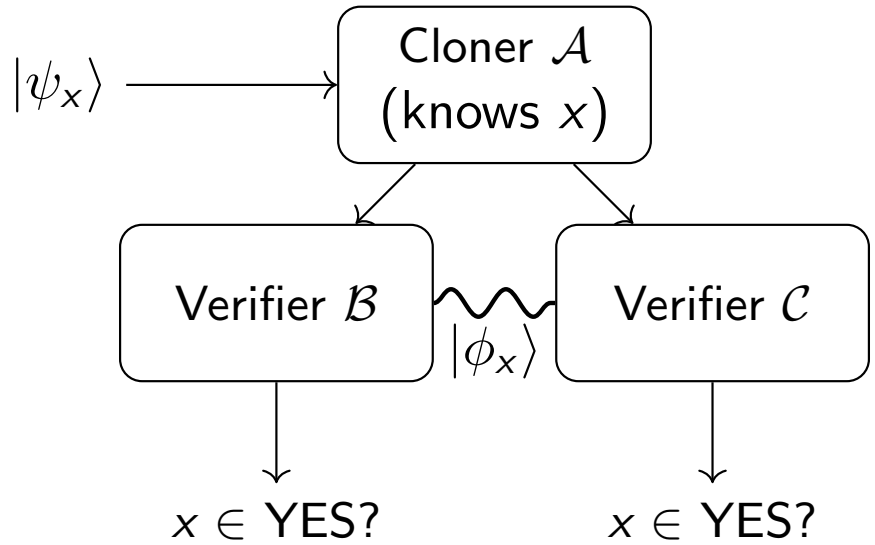
Existence of a family of uncloneable proofs or advice also considered by: Broadbent, Karvonen and Lord (2023), Broadbent, Grilo, Podder and Sikora (2024)



- Functionality of the state $|\psi_x\rangle$ as proof needs to be cloned

What is an uncloneable proof or advice?

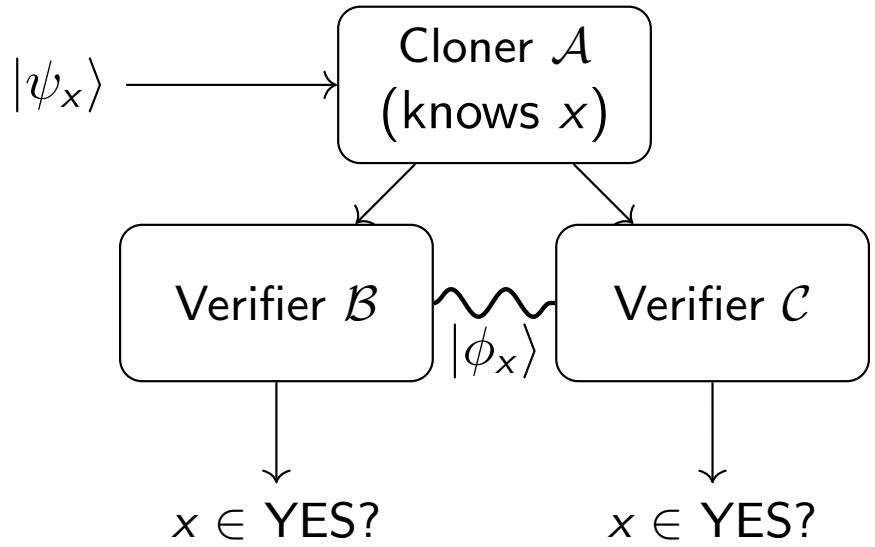
Existence of a family of uncloneable proofs or advice also considered by: Broadbent, Karvonen and Lord (2023), Broadbent, Grilo, Podder and Sikora (2024)



- Functionality of the state $|\psi_x\rangle$ as proof needs to be cloned

What is an uncloneable proof or advice?

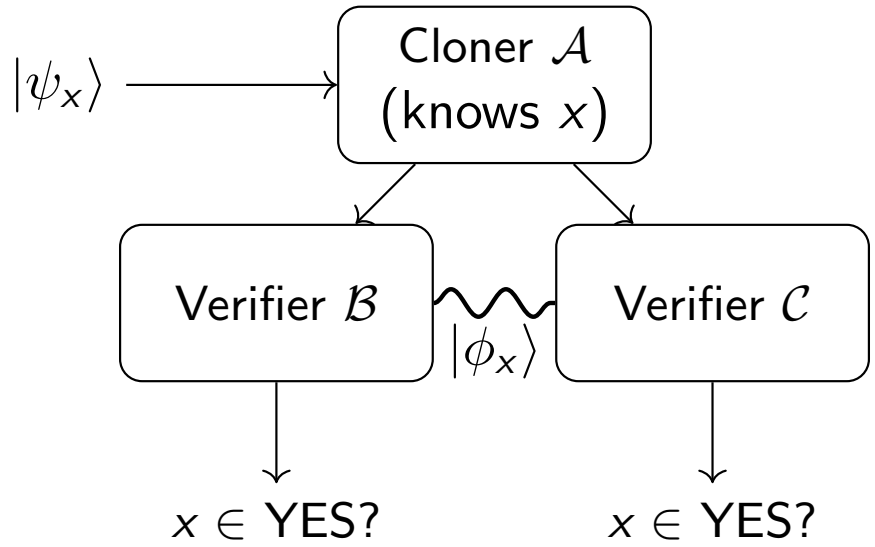
Existence of a family of uncloneable proofs or advice also considered by: Broadbent, Karvonen and Lord (2023), Broadbent, Grilo, Podder and Sikora (2024)



- Functionality of the state $|\psi_x\rangle$ as proof needs to be cloned
- Cloner $\mathcal{A}$ must be computationally bounded (BQP)
  - Verifiers $\mathcal{B}, \mathcal{C}$ are naturally computationally bounded

What is an uncloneable proof or advice?

Existence of a family of uncloneable proofs or advice also considered by: Broadbent, Karvonen and Lord (2023), Broadbent, Grilo, Podder and Sikora (2024)



- Functionality of the state $|\psi_x\rangle$ as proof needs to be cloned
- Cloner $\mathcal{A}$ must be computationally bounded (BQP)
  - Verifiers $\mathcal{B}, \mathcal{C}$ are naturally computationally bounded
- Often average-case uncloneability is considered

Defining strictly uncloneable classes

Defining strictly uncloneable classes

Requirement: Any candidate family of proofs or advice must be uncloneable

Defining strictly uncloneable classes

Requirement: Any candidate family of proofs or advice must be uncloneable

Challenge:

Canonical proofs $\{|\psi_x\rangle\}_{x\in L}$ Another family of proofs $\{|\psi_x\rangle^{\otimes 2}\}_{x\in L}$

Defining strictly uncloneable classes

Requirement: Any candidate family of proofs or advice must be uncloneable

Challenge:

Canonical proofs $\{|\psi_x\rangle\}_{x\in L}$ Another family of proofs $\{|\psi_x\rangle^{\otimes 2}\}_{x\in L}$

Observation: Any polynomial-sized family of proofs can only have polynomially many copies of a canonical proof

Defining strictly uncloneable classes

Requirement: Any candidate family of proofs or advice must be uncloneable

Challenge:

Canonical proofs $\{|\psi_x\rangle\}_{x\in L}$ Another family of proofs $\{|\psi_x\rangle^{\otimes 2}\}_{x\in L}$

Observation: Any polynomial-sized family of proofs can only have polynomially many copies of a canonical proof

$\Rightarrow$ For any polynomial-sized family of proofs, $\exists$ polynomial k s.t. no cloning operation that makes a proof jointly usable by k verifiers?

Defining strictly uncloneable classes

Requirement: Any candidate family of proofs or advice must be uncloneable

Challenge:

Canonical proofs $\{|\psi_x\rangle\}_{x\in L}$ Another family of proofs $\{|\psi_x\rangle^{\otimes 2}\}_{x\in L}$

Observation: Any polynomial-sized family of proofs can only have polynomially many copies of a canonical proof

$\Rightarrow$ For any polynomial-sized family of proofs, $\exists$ polynomial k s.t. no cloning operation that makes a proof jointly usable by k verifiers?

- This turns out to be viable!

Defining strictly uncloneable classes

Requirement: Any candidate family of proofs or advice must be uncloneable

Challenge:

Canonical proofs $\{|\psi_x\rangle\}_{x\in L}$ Another family of proofs $\{|\psi_x\rangle^{\otimes 2}\}_{x\in L}$

Observation: Any polynomial-sized family of proofs can only have polynomially many copies of a canonical proof

$\Rightarrow$ For any polynomial-sized family of proofs, $\exists$ polynomial k s.t. no cloning operation that makes a proof jointly usable by k verifiers?

- This turns out to be viable!
- Non-trivial: classical proofs are not uncloneable in this way

Defining strictly uncloneable classes

Requirement: Any candidate family of proofs or advice must be uncloneable

Challenge:

Canonical proofs $\{|\psi_x\rangle\}_{x\in L}$ Another family of proofs $\{|\psi_x\rangle^{\otimes 2}\}_{x\in L}$

Observation: Any polynomial-sized family of proofs can only have polynomially many copies of a canonical proof

$\Rightarrow$ For any polynomial-sized family of proofs, $\exists$ polynomial k s.t. no cloning operation that makes a proof jointly usable by k verifiers?

- This turns out to be viable!
- Non-trivial: classical proofs are not uncloneable in this way
- Uncloneability is worst-case instead of average case

Strictly uncloneable QMA and FEQP/qpoly

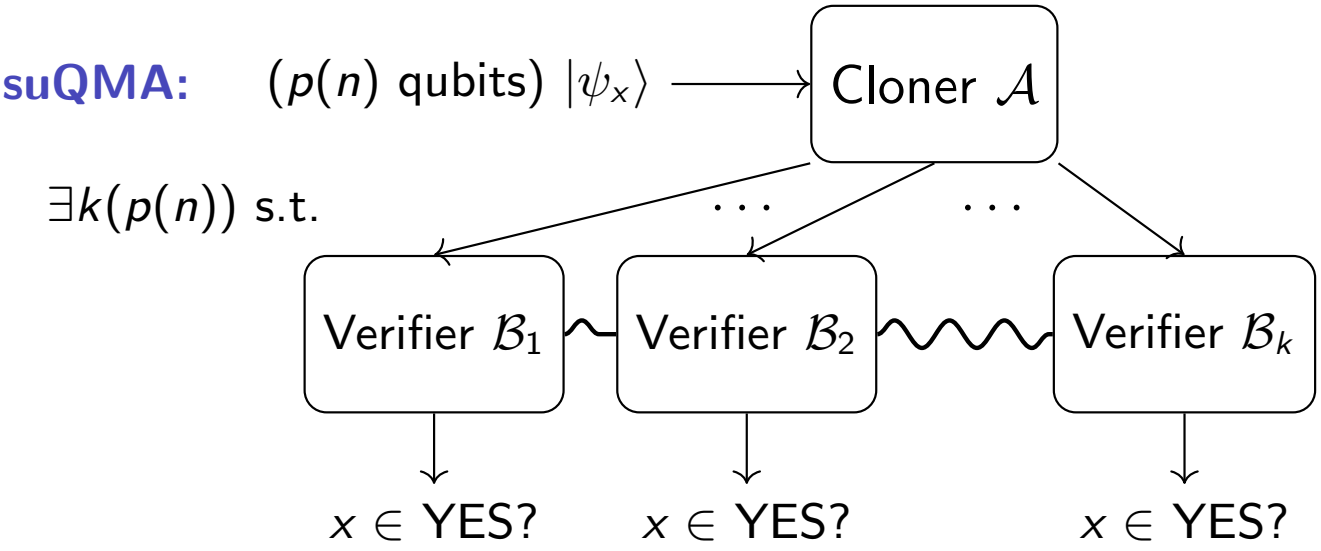
Strictly uncloneable QMA and FEQP/qpoly

QMA $\supseteq$ **suQMA:**

Strictly uncloneable QMA and FEQP/qpoly

suQMA: ($p(n)$ qubits) $|\psi_x\rangle$

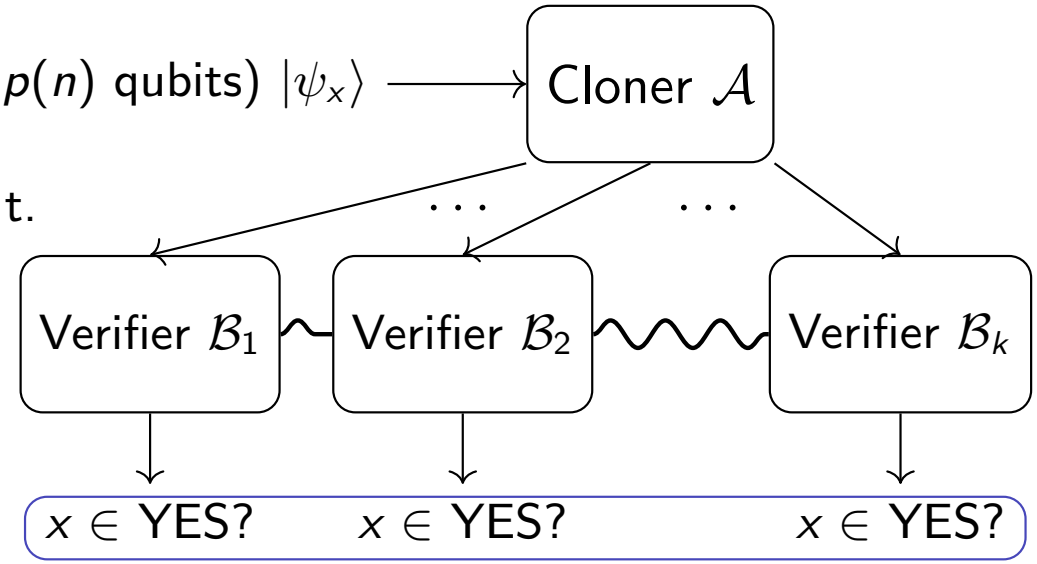
Strictly uncloneable QMA and FEQP/qpoly



Strictly uncloneable QMA and FEQP/qpoly

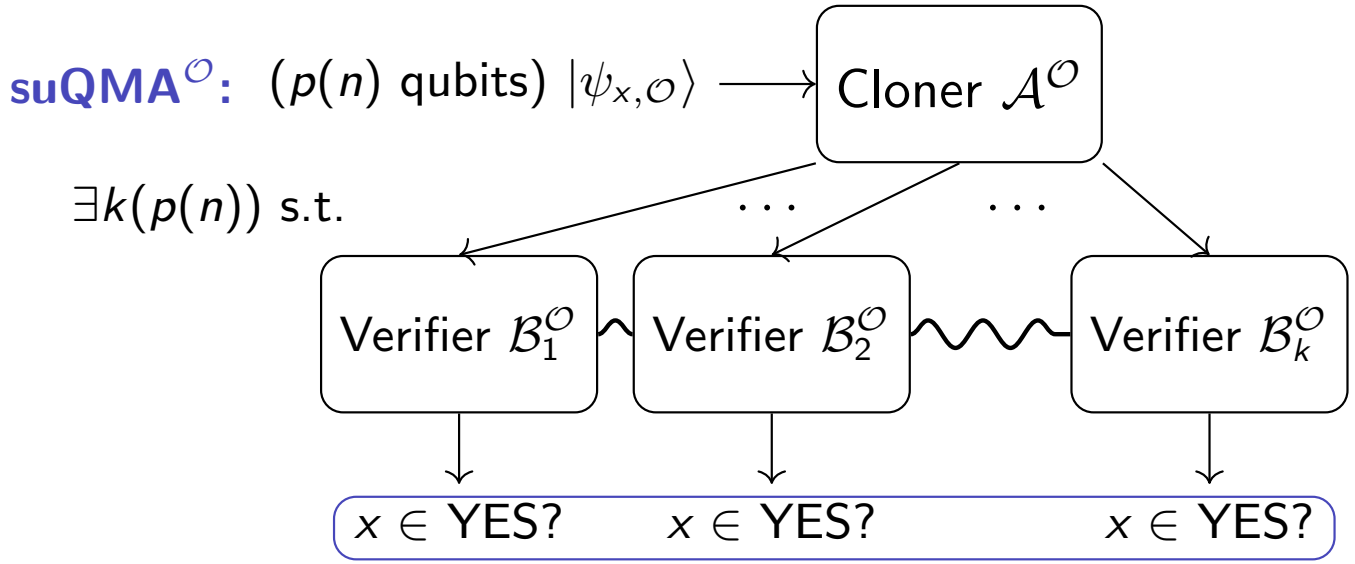
suQMA: $(p(n)$ qubits$)\ |\psi_x\rangle$

$\exists k(p(n))$ s.t.



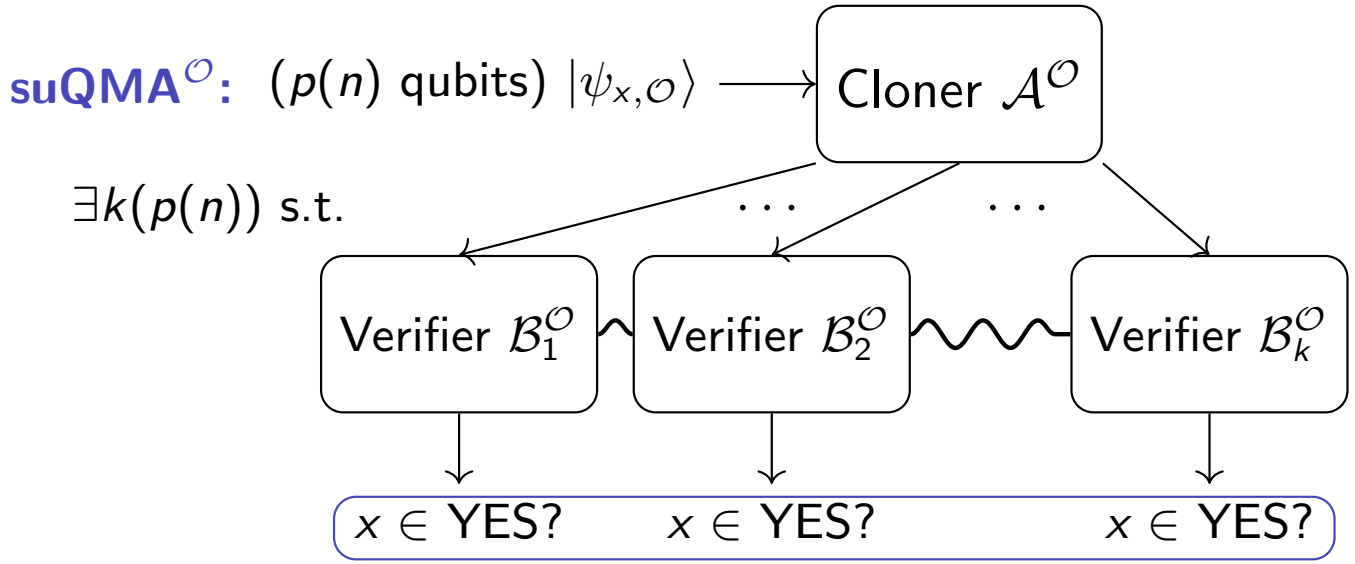
Not jointly correct w.h.p.

Strictly uncloneable QMA and FEQP/qpoly



Not jointly correct w.h.p.

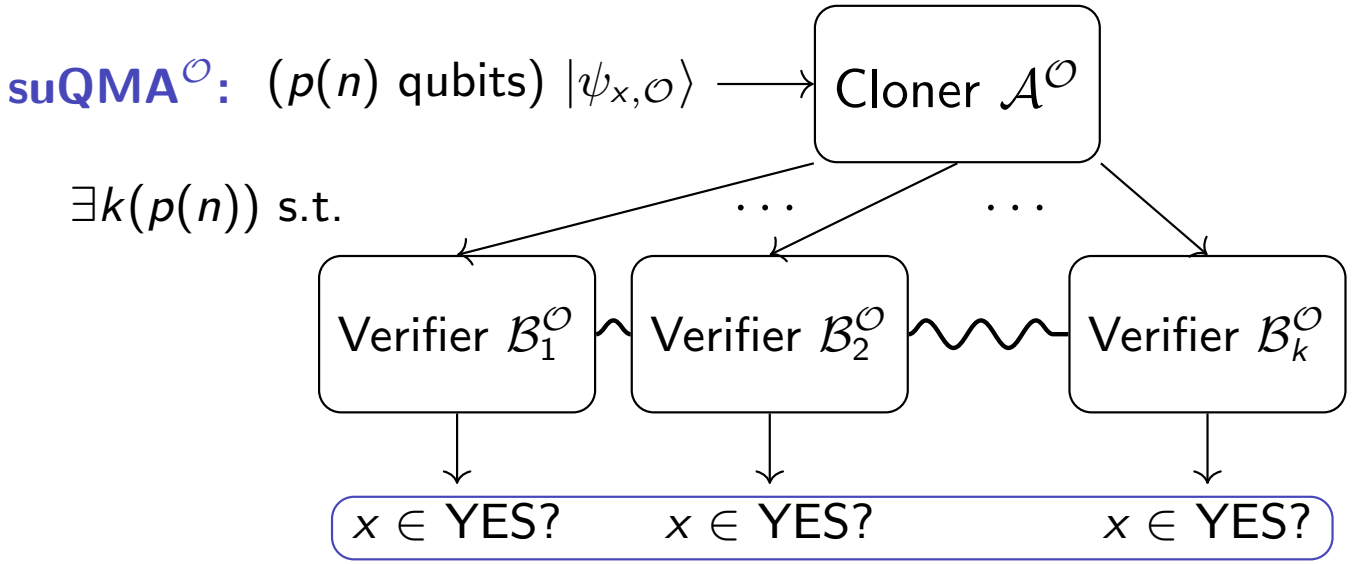
Strictly uncloneable QMA and FEQP/qpoly



Not jointly correct w.h.p.

FEQP/qpoly $\supseteq$ **FEQP/supoly:**

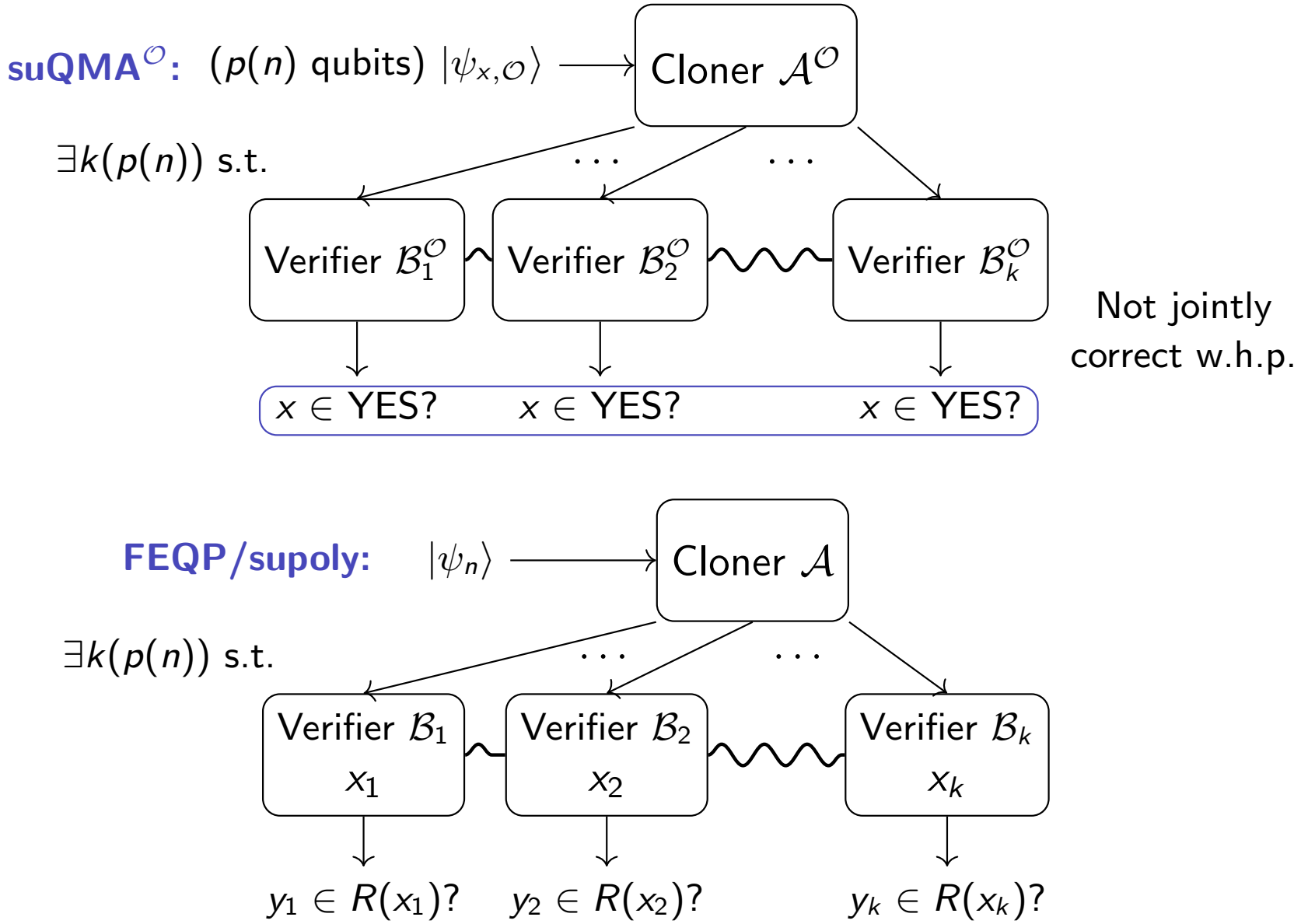
Strictly uncloneable QMA and FEQP/qpoly



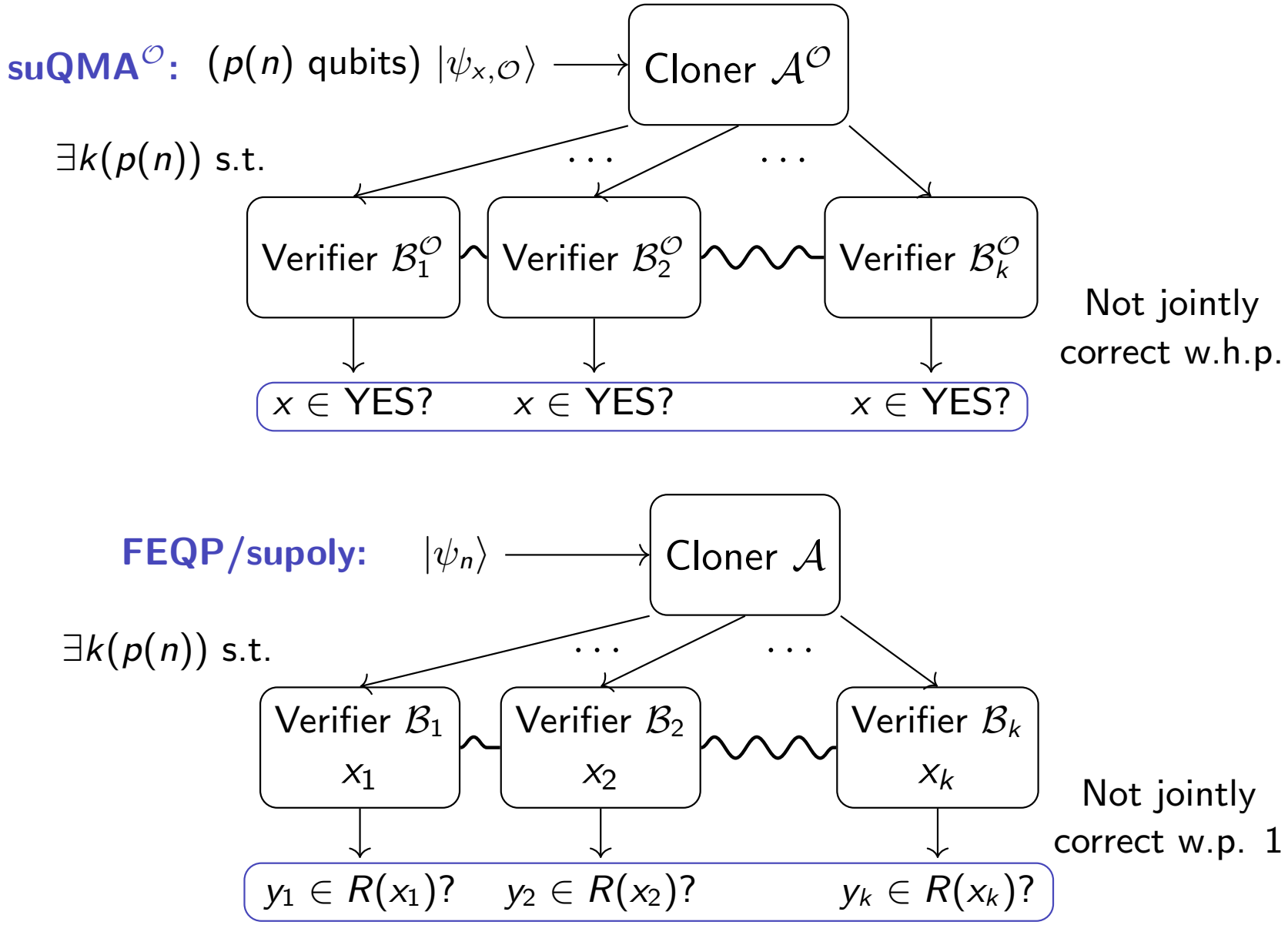
Not jointly correct w.h.p.

FEQP/supoly: $|\psi_n\rangle$

Strictly uncloneable QMA and FEQP/qpoly



Strictly uncloneable QMA and FEQP/qpoly



Constructions

Constructions

suQMA:

AK07 oracle problem (QuantumOR): Given either $\mathbb{1} - 2|\psi\rangle\langle\psi|$ for Haar-random $|\psi\rangle$ (YES) or $\mathbb{1}$ (NO), determine which is the case

Constructions

suQMA:

AK07 oracle problem (QuantumOR): Given either $\mathbb{1} - 2|\psi\rangle\langle\psi|$ for Haar-random $|\psi\rangle$ (YES) or $\mathbb{1}$ (NO), determine which is the case

Canonical proof: The state $|\psi\rangle$ for oracle $\mathbb{1} - 2|\psi\rangle\langle\psi|$

Constructions

suQMA:

AK07 oracle problem (QuantumOR): Given either $\mathbb{1} - 2|\psi\rangle\langle\psi|$ for Haar-random $|\psi\rangle$ (YES) or $\mathbb{1}$ (NO), determine which is the case

Canonical proof: The state $|\psi\rangle$ for oracle $\mathbb{1} - 2|\psi\rangle\langle\psi|$

Good news: Haar-random states are uncloneable!

Constructions

suQMA:

AK07 oracle problem (QuantumOR): Given either $\mathbb{1} - 2|\psi\rangle\langle\psi|$ for Haar-random $|\psi\rangle$ (YES) or $\mathbb{1}$ (NO), determine which is the case

Canonical proof: The state $|\psi\rangle$ for oracle $\mathbb{1} - 2|\psi\rangle\langle\psi|$

Good news: Haar-random states are uncloneable!

FEQP/supoly:

ABK23 problem (Hidden Matching): Family of relations $\{R_f\}_f \subseteq \{0,1\}^n \times \{0,1\}^{n+1}$ indexed by $f : \{0,1\}^n \to \{0,1\}$

$$(x,(y,b)) \in R_f \text{ iff } y \in \{0,1\}^n \text{ and } f(y) \oplus f(y \oplus x) = b$$

Constructions

suQMA:

AK07 oracle problem (QuantumOR): Given either $\mathbb{1} - 2|\psi\rangle\langle\psi|$ for Haar-random $|\psi\rangle$ (YES) or $\mathbb{1}$ (NO), determine which is the case

Canonical proof: The state $|\psi\rangle$ for oracle $\mathbb{1} - 2|\psi\rangle\langle\psi|$

Good news: Haar-random states are uncloneable!

FEQP/supoly:

ABK23 problem (Hidden Matching): Family of relations $\{R_f\}_f \subseteq \{0,1\}^n \times \{0,1\}^{n+1}$ indexed by $f : \{0,1\}^n \to \{0,1\}$

$$(x,(y,b)) \in R_f \text{ iff } y \in \{0,1\}^n \text{ and } f(y) \oplus f(y \oplus x) = b$$

Canonical advice: $\frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle$

Constructions

suQMA:

AK07 oracle problem (QuantumOR): Given either $\mathbb{1} - 2|\psi\rangle\langle\psi|$ for Haar-random $|\psi\rangle$ (YES) or $\mathbb{1}$ (NO), determine which is the case

Canonical proof: The state $|\psi\rangle$ for oracle $\mathbb{1} - 2|\psi\rangle\langle\psi|$

Good news: Haar-random states are uncloneable!

FEQP/supoly:

ABK23 problem (Hidden Matching): Family of relations $\{R_f\}_f \subseteq \{0,1\}^n \times \{0,1\}^{n+1}$ indexed by $f : \{0,1\}^n \to \{0,1\}$

$$(x,(y,b)) \in R_f \text{ iff } y \in \{0,1\}^n \text{ and } f(y) \oplus f(y \oplus x) = b$$

Canonical advice: $\frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle$

Good news: Binary phase states (for random f) are uncloneable!

General proof strategy

General proof strategy

1. **'Rigidity' of the proof or advice**

General proof strategy

1. **'Rigidity' of the proof or advice**
   - If $\mathcal{B}_1, \ldots, \mathcal{B}_k$ can jointly solve the problem with the state given by $\mathcal{A}$, they can jointly prepare something like $|\psi\rangle^{\otimes k}$ (k copies of the canonical proof or advice)

General proof strategy

1. **'Rigidity' of the proof or advice**
   - If $\mathcal{B}_1, \ldots, \mathcal{B}_k$ can jointly solve the problem with the state given by $\mathcal{A}$, they can jointly prepare something like $|\psi\rangle^{\otimes k}$ (k copies of the canonical proof or advice)
   - For suQMA$^{\mathcal{O}}$, if $\mathcal{B}_1, \ldots, \mathcal{B}_k$ can distinguish $\mathbb{1} - 2|\psi\rangle\langle\psi|$ from $\mathbb{1}$ with some joint state, they can also jointly prepare $|\psi\rangle^{\otimes k}$ with a few more queries

General proof strategy

1. **'Rigidity' of the proof or advice**
   - If $\mathcal{B}_1, \ldots, \mathcal{B}_k$ can jointly solve the problem with the state given by $\mathcal{A}$, they can jointly prepare something like $|\psi\rangle^{\otimes k}$ (k copies of the canonical proof or advice)
   - For suQMA$^{\mathcal{O}}$, if $\mathcal{B}_1, \ldots, \mathcal{B}_k$ can distinguish $\mathbb{1} - 2|\psi\rangle\langle\psi|$ from $\mathbb{1}$ with some joint state, they can also jointly prepare $|\psi\rangle^{\otimes k}$ with a few more queries
2. **Use uncloneability of canonical proof or advice**
   - Uncloneability results usually say you can't produce $|\psi\rangle^{\otimes k}$ starting from $|\psi\rangle^{\otimes (k-1)}$, not from arbitrarily states with few qubits

General proof strategy

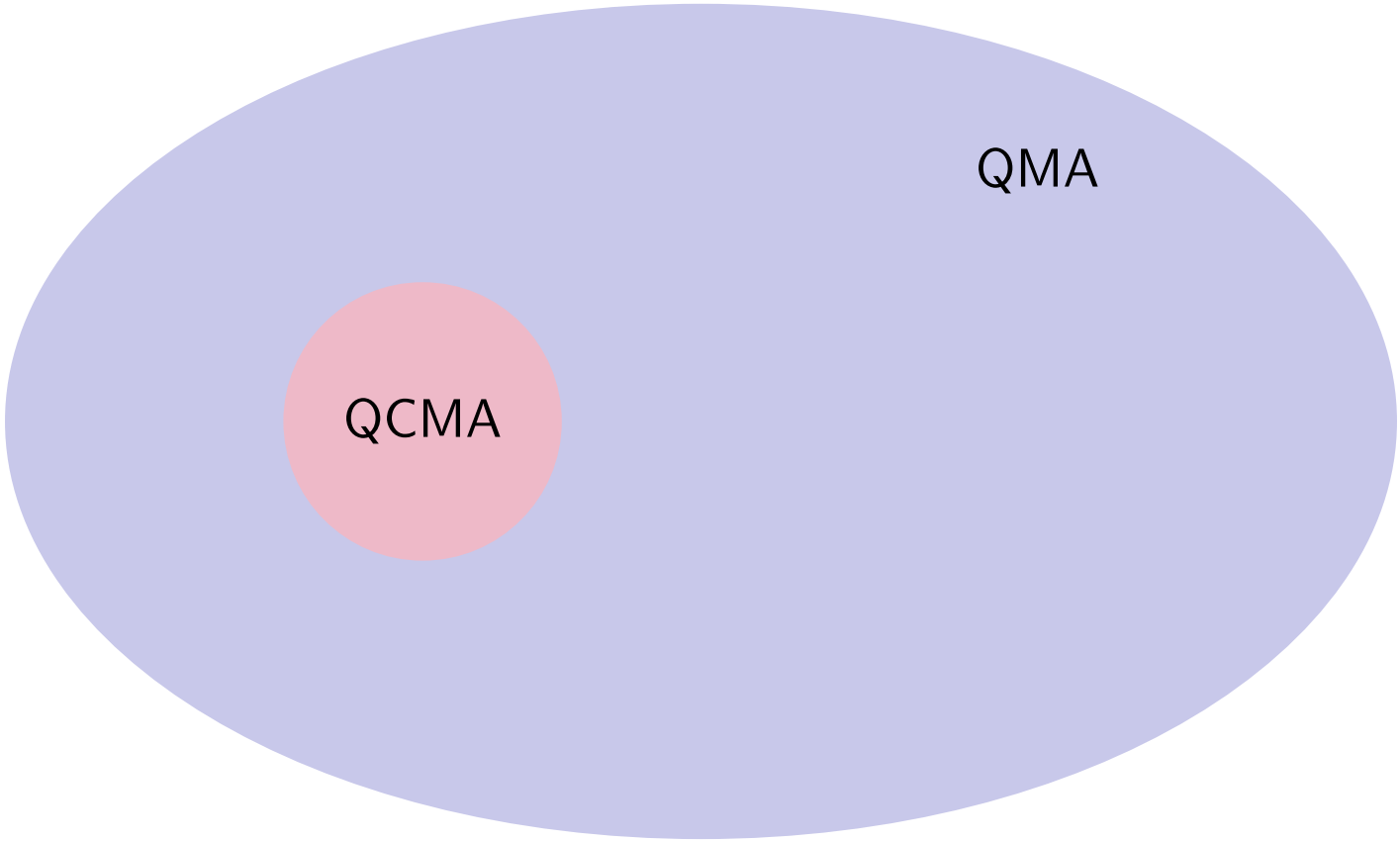
1. **'Rigidity' of the proof or advice**
   - If $\mathcal{B}_1, \ldots, \mathcal{B}_k$ can jointly solve the problem with the state given by $\mathcal{A}$, they can jointly prepare something like $|\psi\rangle^{\otimes k}$ (k copies of the canonical proof or advice)
   - For suQMA$^{\mathcal{O}}$, if $\mathcal{B}_1, \ldots, \mathcal{B}_k$ can distinguish $\mathbb{1} - 2|\psi\rangle\langle\psi|$ from $\mathbb{1}$ with some joint state, they can also jointly prepare $|\psi\rangle^{\otimes k}$ with a few more queries
2. **Use uncloneability of canonical proof or advice**
   - Uncloneability results usually say you can't produce $|\psi\rangle^{\otimes k}$ starting from $|\psi\rangle^{\otimes (k-1)}$, not from arbitrarily states with few qubits
   - Need to generalize known results or use other properties

General proof strategy

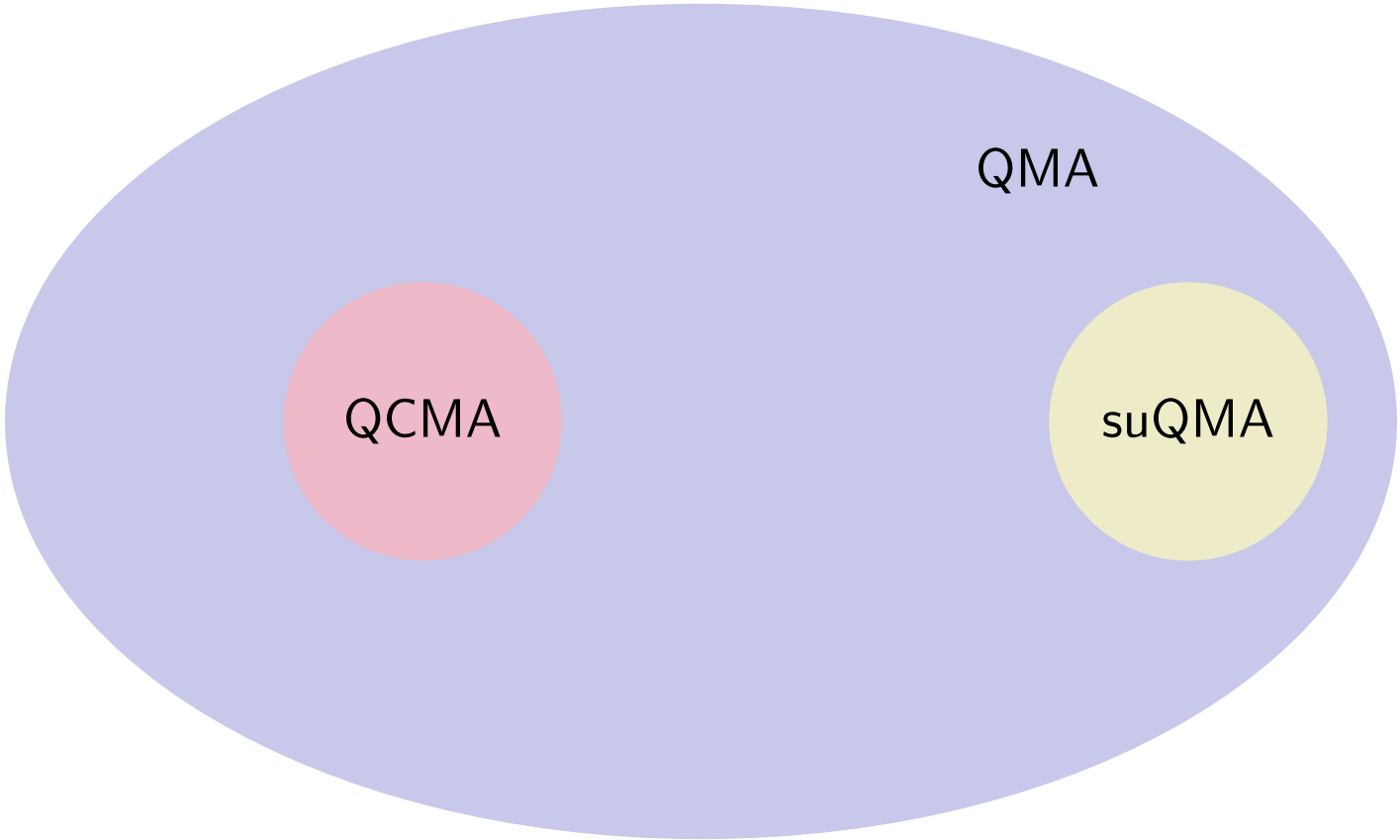
1. **'Rigidity' of the proof or advice**
   - If $\mathcal{B}_1, \ldots, \mathcal{B}_k$ can jointly solve the problem with the state given by $\mathcal{A}$, they can jointly prepare something like $|\psi\rangle^{\otimes k}$ (k copies of the canonical proof or advice)
   - For suQMA$^{\mathcal{O}}$, if $\mathcal{B}_1, \ldots, \mathcal{B}_k$ can distinguish $\mathbb{1} - 2|\psi\rangle\langle\psi|$ from $\mathbb{1}$ with some joint state, they can also jointly prepare $|\psi\rangle^{\otimes k}$ with a few more queries
2. **Use uncloneability of canonical proof or advice**
   - Uncloneability results usually say you can't produce $|\psi\rangle^{\otimes k}$ starting from $|\psi\rangle^{\otimes (k-1)}$, not from arbitrarily states with few qubits
   - Need to generalize known results or use other properties
   - For FEQP/supoly, we show:
     - Proofs $|\psi_f\rangle$ that works jointly for $\mathcal{B}_1, \ldots, \mathcal{B}_k$ must have inner product $|\langle\psi_{f'}|\psi_f\rangle| = 2^{-\Omega(k)}$;
     - In order to achieve the inner products, the states need $\Omega(k)$ qubits.

Other consequences

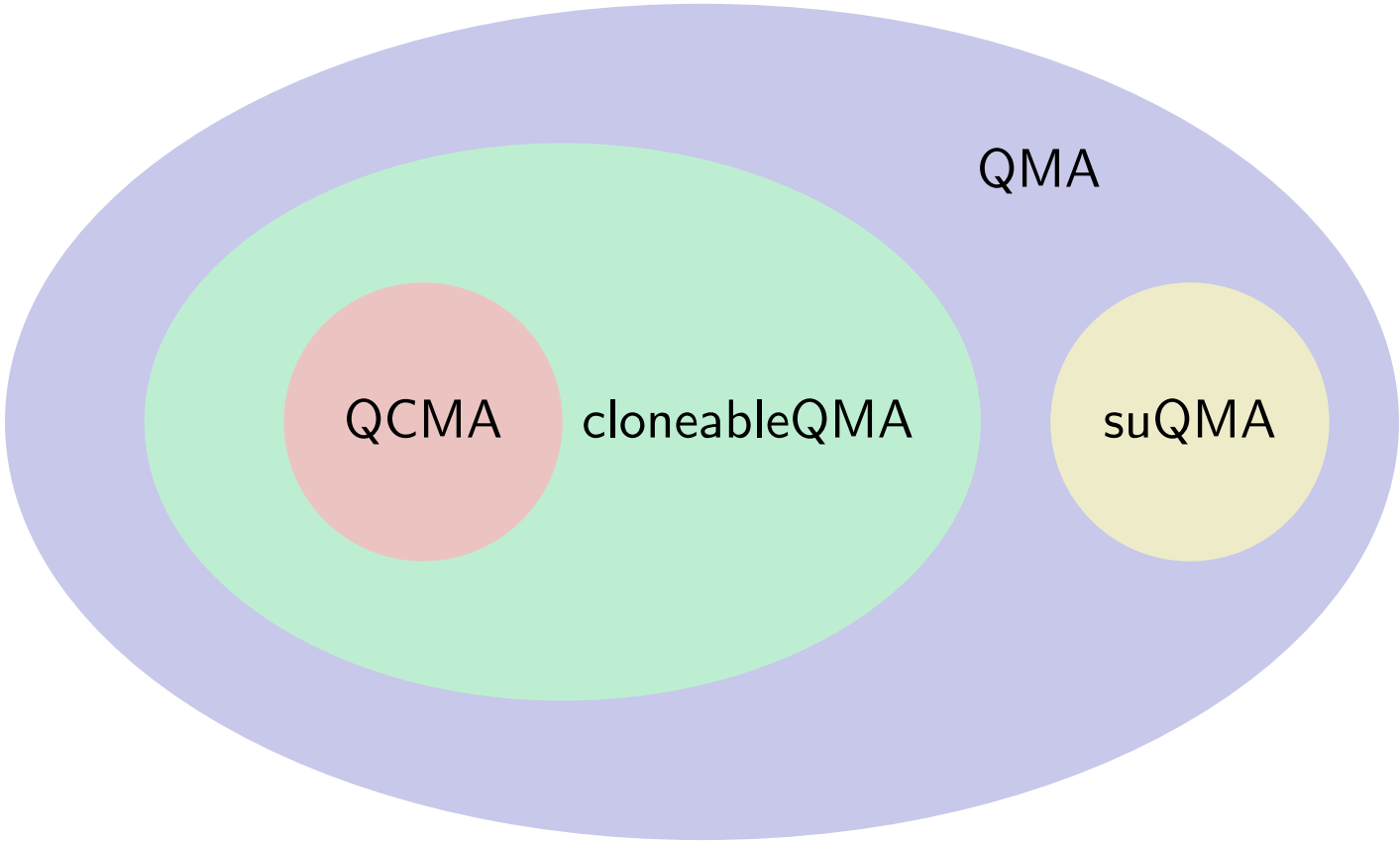
Other consequences



Other consequences

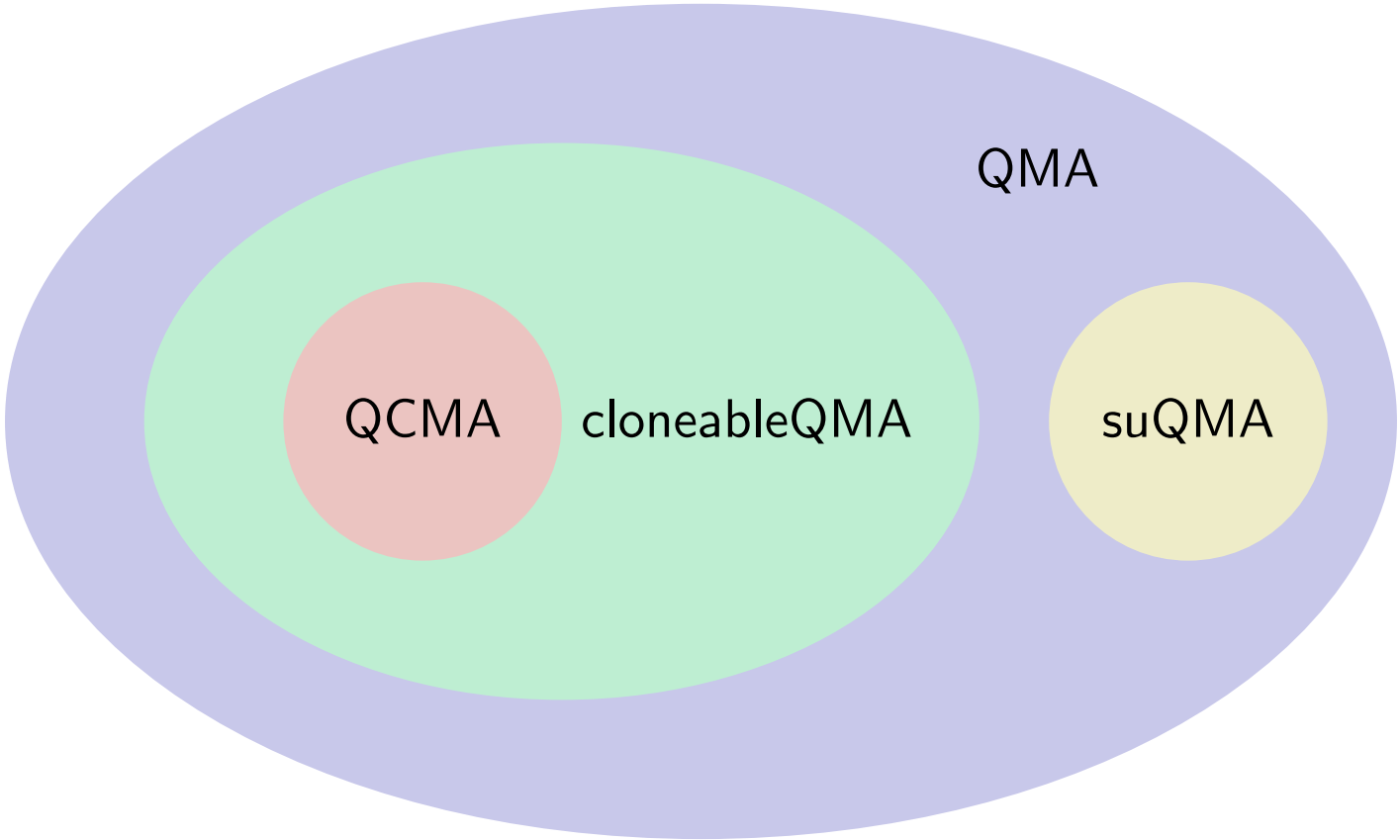


Other consequences



Nehoran and Zhandry (2023): w.r.t. a quantum oracle, cloneableQMA $\neq$ QCMA

Other consequences



Nehoran and Zhandry (2023): w.r.t. a quantum oracle, cloneableQMA $\neq$ QCMA

From definition, suQMA $\subseteq$ QMA $\setminus$ cloneableQMA
$\Rightarrow$ w.r.t. a quantum oracle, QMA $\neq$ cloneableQMA

Open problems

1. Problems in suQMA and BQP/supoly w.r.t. a classical oracle?

Open problems

1. Problems in suQMA and BQP/supoly w.r.t. a classical oracle?

   ...Seems hard, but promising with QMA vs QCMA developments!

Open problems

1. Problems in suQMA and BQP/supoly w.r.t. a classical oracle?

   ...Seems hard, but promising with QMA vs QCMA developments!

2. Problem in strictly uncloneable version of FBQP/qpoly?

Open problems

1. Problems in suQMA and BQP/supoly w.r.t. a classical oracle?

   ...Seems hard, but promising with QMA vs QCMA developments!

2. Problem in strictly uncloneable version of FBQP/qpoly?
   - Unclear how to even define this class! (FBQP/qpoly doesn't have error reduction)

Open problems

1. Problems in suQMA and BQP/supoly w.r.t. a classical oracle?

   ...Seems hard, but promising with QMA vs QCMA developments!

2. Problem in strictly uncloneable version of FBQP/qpoly?
   - Unclear how to even define this class! (FBQP/qpoly doesn't have error reduction)
   - Further refinements of our techniques for FEQP/supoly are needed

Open problems

1. Problems in suQMA and BQP/supoly w.r.t. a classical oracle?

   ...Seems hard, but promising with QMA vs QCMA developments!

2. Problem in strictly uncloneable version of FBQP/qpoly?
   - Unclear how to even define this class! (FBQP/qpoly doesn't have error reduction)
   - Further refinements of our techniques for FEQP/supoly are needed

Thanks!