QMA-hardness of Consistency of local density matrices with applications to quantum ZK

Alex Bredariol Grilo

joint work with Anne Broadbent (U. of Ottawa)

arxiv:1911.07782

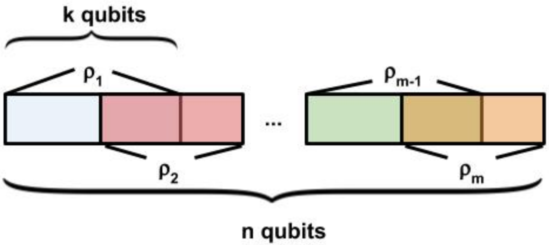
Consistency of local density matrices problem

Consistency of local density matrices problem

Input: Reduced density matrices $\rho_1, ..., \rho_m$ on k-qubits

Output: yes: $\exists \psi$ such that $\forall i : \left\| Tr_{\overline{S_i}}(\psi) - \rho_i \right\| \leq \frac{1}{exp(n)}$

no: $\forall \psi, \exists i : \left\| Tr_{\overline{S_i}}(\psi) - \rho_i \right\| \geq \frac{1}{poly(n)}$

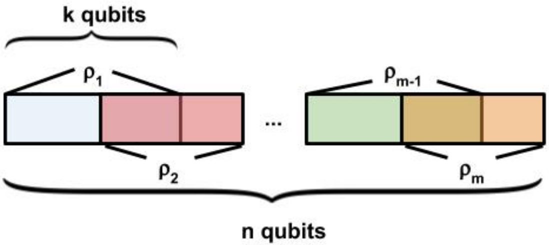


Consistency of local density matrices problem

Input: Reduced density matrices $\rho_1, ..., \rho_m$ on k-qubits

Output: yes: $\exists\psi$ such that $\forall i : \left\| Tr_{\overline{S_i}}(\psi) - \rho_i \right\| \leq \frac{1}{exp(n)}$

no: $\forall\psi$, $\exists i : \left\| Tr_{\overline{S_i}}(\psi) - \rho_i \right\| \geq \frac{1}{poly(n)}$

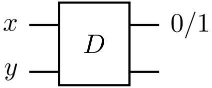


How hard is this problem?

Complexity theory background

Complexity theory background

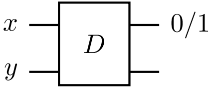
Problem $L \in \text{NP}$



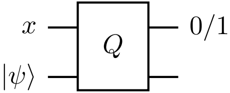
for $x \in L_{yes}$,
 $\exists y \; D(x, y) = 1$
for $x \in L_{no}$,
 $\forall y \; D(x, y) = 0$

Complexity theory background

Problem $L \in \mathrm{NP}$



Problem $L \in \mathrm{QMA}$



for $x \in L_{yes}$,
$\exists y \; D(x, y) = 1$
for $x \in L_{no}$,
$\forall y \; D(x, y) = 0$

for $x \in L_{yes}$,
$\exists \left|\psi\right\rangle \; Pr[Q(x, \left|\psi\right\rangle) = 1] \geq \frac{2}{3}$
for $x \in L_{no}$,
$\forall \left|\psi\right\rangle \; Pr[Q(x, \left|\psi\right\rangle) = 0] \geq \frac{2}{3}$

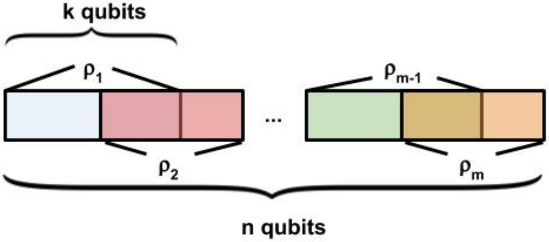
Consistency of local density matrices problem

Consistency of local density matrices problem

Input: Reduced density matrices $\rho_1, ..., \rho_m$ on k-qubits

Output: yes: $\exists\psi$ such that $\forall i : \left\| Tr_{\overline{S_i}}(\psi) - \rho_i \right\| \leq \frac{1}{exp(n)}$

no: $\forall\psi, \exists i : \left\| Tr_{\overline{S_i}}(\psi) - \rho_i \right\| \geq \frac{1}{poly(n)}$

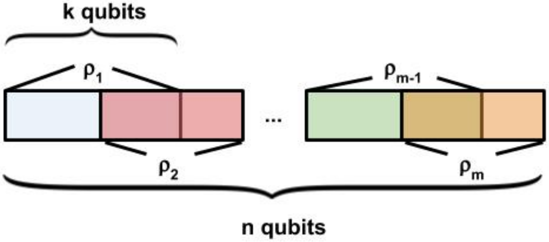


Consistency of local density matrices problem

Input: Reduced density matrices $\rho_1, ..., \rho_m$ on k-qubits

Output: yes: $\exists\psi$ such that $\forall i : \left\| Tr_{\overline{S_i}}(\psi) - \rho_i \right\| \leq \frac{1}{exp(n)}$

no: $\forall\psi$, $\exists i : \left\| Tr_{\overline{S_i}}(\psi) - \rho_i \right\| \geq \frac{1}{poly(n)}$



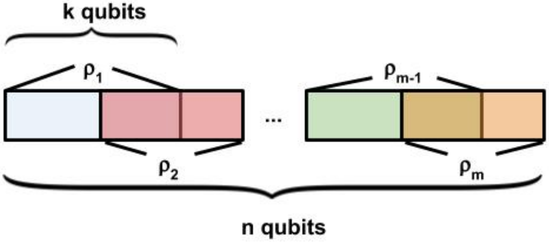
- Liu'06: containment in QMA, and partial result on QMA-hardness

Consistency of local density matrices problem

Input: Reduced density matrices $\rho_1, ..., \rho_m$ on k-qubits

Output: yes: $\exists\psi$ such that $\forall i : \left\| Tr_{\overline{S_i}}(\psi) - \rho_i \right\| \leq \frac{1}{exp(n)}$

no: $\forall\psi$, $\exists i : \left\| Tr_{\overline{S_i}}(\psi) - \rho_i \right\| \geq \frac{1}{poly(n)}$



- Liu'06: containment in QMA, and partial result on QMA-hardness
- Our work:
  - QMA-hardness of CLDM
  - Applications to complexity theory and quantum cryptography

Simulatable codes - warm up

Simulatable codes - warm up

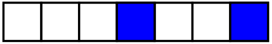
$$
\begin{aligned}
|0\rangle \mapsto \frac{1}{2\sqrt{2}}(\,&|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\
&+ |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle) \\
|1\rangle \mapsto \frac{1}{2\sqrt{2}}(\,&|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle \\
&+ |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle)
\end{aligned}
$$

Simulatable codes - warm up

$$|0\rangle \mapsto \frac{1}{2\sqrt{2}}\big(|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle\big)$$

$$|1\rangle \mapsto \frac{1}{2\sqrt{2}}\big(|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle + |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle\big)$$

$Enc(\rho)$



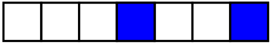
- For every ρ and $i, j \in [7]$, $Tr_{\overline{\{i,j\}}}(Enc(\rho)) = \frac{I}{4}$

Simulatable codes - warm up

$$|0\rangle \mapsto \frac{1}{2\sqrt{2}}\big(|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle\big)$$

$$|1\rangle \mapsto \frac{1}{2\sqrt{2}}\big(|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle + |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle\big)$$

$Enc(\rho)$

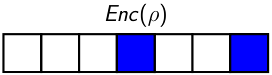


- For every ρ and $i, j \in [7]$, $Tr_{\overline{\{i,j\}}}(Enc(\rho)) = \frac{I}{4}$
  - The reduced density matrix on 2 qubits can be *efficiently computed*

Simulatable codes - warm up

$$|0\rangle \mapsto \frac{1}{2\sqrt{2}}\big(|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle\big)$$

$$|1\rangle \mapsto \frac{1}{2\sqrt{2}}\big(|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle + |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle\big)$$

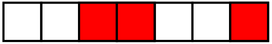


- For every ρ and $i, j \in [7]$, $Tr_{\overline{\{i,j\}}}(Enc(\rho)) = \frac{I}{4}$
  - The reduced density matrix on 2 qubits can be *efficiently computed*
  - Independently of the logical state

Simulatable codes - warm up

$$|0\rangle \mapsto \frac{1}{2\sqrt{2}}\big(|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle$$
$$+ |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle\big)$$
$$|1\rangle \mapsto \frac{1}{2\sqrt{2}}\big(|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle$$
$$+ |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle\big)$$

$Enc(\rho)$



- For every ρ and $i, j \in [7]$, $Tr_{\overline{\{i,j\}}}(Enc(\rho)) = \frac{I}{4}$
  - The reduced density matrix on 2 qubits can be *efficiently computed*
  - Independently of the logical state
- Not true anymore for $i, j, k \in [7]$

Simulatable codes

Simulatable codes

$\log_3(s)$-fold concatenated Steane code is s-simulatable

Simulatable codes

$\log_3(s)$-fold concatenated Steane code is s-simulatable

1. There is a poly(2^s)-time *classical* algorithm that compute any reduced density matrix of Enc(ρ) on s qubits, without knowing ρ

Simulatable codes

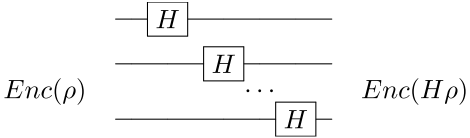
$\log_3(s)$-fold concatenated Steane code is s-simulatable

1. There is a poly(2^s)-time *classical* algorithm that compute any reduced density matrix of Enc(ρ) on s qubits, without knowing ρ
2. There is a poly(2^s)-time *classical* algorithm that compute any reduced density matrix of s qubits of (partial) computation on Enc(ρ)

Simulatable codes

$\log_3(s)$-fold concatenated Steane code is s-simulatable

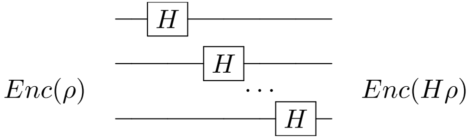
1. There is a poly(2^s)-time *classical* algorithm that compute any reduced density matrix of Enc(ρ) on s qubits, without knowing ρ
2. There is a poly(2^s)-time *classical* algorithm that compute any reduced density matrix of s qubits of (partial) computation on Enc(ρ)
   - transversal Clifford gates

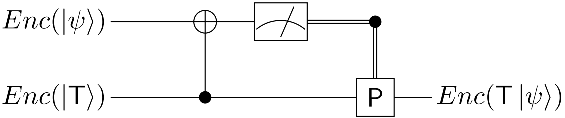


Simulatable codes

$\log_3(s)$-fold concatenated Steane code is s-simulatable

1. There is a poly(2^s)-time *classical* algorithm that compute any reduced density matrix of Enc(ρ) on s qubits, without knowing ρ
2. There is a poly(2^s)-time *classical* algorithm that compute any reduced density matrix of s qubits of (partial) computation on Enc(ρ)
   - transversal Clifford gates
   - T-gadgets





CLDM is QMA-hard

Circuit-to-hamiltonian construction

Given a circuit $V = U_T ... U_1$ and initial state $|\psi_{init}\rangle = |\phi\rangle |0^a\rangle$, there is a reduction to a 5-Local Hamiltonian H_V such that

CLDM is QMA-hard

Circuit-to-hamiltonian construction

Given a circuit $V = U_T \dots U_1$ and initial state $|\psi_{init}\rangle = |\phi\rangle |0^a\rangle$, there is a reduction to a 5-Local Hamiltonian H_V such that

- If V accepts with high probability, then the *history state*

$$\frac{1}{\sqrt{T+1}} \sum_{t \in [T+1]} |t\rangle \otimes U_t \dots U_1 |\psi_{init}\rangle$$

  has low energy in respect to H_V.

CLDM is QMA-hard

Circuit-to-hamiltonian construction

Given a circuit $V = U_T ... U_1$ and initial state $|\psi_{init}\rangle = |\phi\rangle |0^a\rangle$, there is a reduction to a 5-Local Hamiltonian H_V such that

- If V accepts with high probability, then the *history state*

$$\frac{1}{\sqrt{T+1}} \sum_{t \in [T+1]} |t\rangle \otimes U_t ... U_1 |\psi_{init}\rangle$$

  has low energy in respect to H_V.
- If V accepts with low probability, then all states have high energy in respect to H_V.

CLDM is QMA-hard

Circuit-to-hamiltonian construction

Given a circuit $V = U_T \ldots U_1$ and initial state $|\psi_{init}\rangle = |\phi\rangle |0^a\rangle$, there is a reduction to a 5-Local Hamiltonian H_V such that

- If V accepts with high probability, then the *history state*

$$\frac{1}{\sqrt{T+1}} \sum_{t \in [T+1]} |t\rangle \otimes U_t \ldots U_1 |\psi_{init}\rangle$$

  has low energy in respect to H_V.
- If V accepts with low probability, then all states have high energy in respect to H_V.

Goal

Tweak the verification algorithm such that we can compute the reduced density matrices of history states.

CLDM is QMA-hard

Encoded circuit

Instead of $V = U_T ... U_1$ and proof $|\phi\rangle$, we use the following circuit V':

1. Receive $Enc(|\phi\rangle\langle\phi|)$ from Prover
2. Check encoding of the witness
3. Create $Enc(|0\rangle)$ and $Enc(|\mathrm{T}\rangle)$
4. Perform logical V on encoded states
5. Decode the output

CLDM is QMA-hard

Encoded circuit

Instead of $V = U_T \ldots U_1$ and proof $|\phi\rangle$, we use the following circuit V':

1. Receive $\frac{1}{2^n} \sum_{a,b} Enc(|a, b\rangle \langle a, b| \otimes X^a Z^b |\phi\rangle \langle\phi| Z^b X^a)$ from Prover
2. Check encoding of the witness
3. Undoes the OTP of the witness
4. Create $Enc(|0\rangle)$ and $Enc(|T\rangle)$
5. Perform logical V on encoded states
6. Decode the output

CLDM is QMA-hard

Encoded circuit

Instead of $V = U_T \ldots U_1$ and proof $|\phi\rangle$, we use the following circuit V':

1. Receive $\frac{1}{2^n}\sum_{a,b} Enc(|a,b\rangle\langle a,b| \otimes X^a Z^b |\phi\rangle\langle\phi| Z^b X^a)$ from Prover
2. Check encoding of the witness
3. Undoes the OTP of the witness
4. Create $Enc(|0\rangle)$ and $Enc(|T\rangle)$
5. Perform logical V on encoded states
6. Decode the output

Theorem

There is a classical simulator that computes in polynomial time the 5-qubit reduced density matrices of the history state of the encoded verifier.

CLDM is QMA-hard

Encoded circuit

Instead of $V = U_T \ldots U_1$ and proof $|\phi\rangle$, we use the following circuit V':

1. Receive $\frac{1}{2^n} \sum_{a,b} Enc(|a, b\rangle \langle a, b| \otimes X^a Z^b |\phi\rangle \langle\phi| Z^b X^a)$ from Prover
2. Check encoding of the witness
3. Undoes the OTP of the witness
4. Create $Enc(|0\rangle)$ and $Enc(|T\rangle)$
5. Perform logical V on encoded states
6. Decode the output

Theorem

There is a classical simulator that computes in polynomial time the 5-qubit reduced density matrices of the history state of the encoded verifier. Moreover there is a global state consistent with the reduced density matrices iff it is a yes-instance.

CLDM is QMA-hard - Overview of the proof

1. There is a polynomial-time algorithm that computes the density matrices of snapshot of the computation at time t
   - At every step, every qubit is encoded and if it is decoded, we know exactly its value

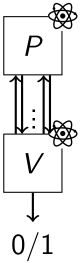
CLDM is QMA-hard - Overview of the proof

1. There is a polynomial-time algorithm that computes the density matrices of snapshot of the computation at time t
   - At every step, every qubit is encoded and if it is decoded, we know exactly its value
2. There is a polynomial-time algorithm that computes the density matrices of “invervals” of the computation
   - Uses the snapshot simulation with some loss in the parameters

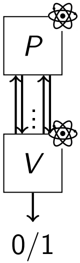
CLDM is QMA-hard - Overview of the proof

1. There is a polynomial-time algorithm that computes the density matrices of snapshot of the computation at time t
   - At every step, every qubit is encoded and if it is decoded, we know exactly its value
2. There is a polynomial-time algorithm that computes the density matrices of "invervals" of the computation
   - Uses the snapshot simulation with some loss in the parameters
3. There is a polynomial-time algorithm that computes the density matrices of the history state
   - Most of clock qubits are traced-out, so the remaining state is a mixture of intervals

Quantum Zero-knowledge for L

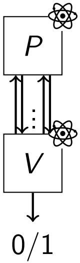


Quantum Zero-knowledge for L



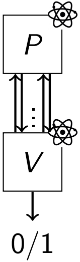
1. If $x \in L_{yes}$, V accepts whp
2. If $x \in L_{no}$, V rejects whp

Quantum Zero-knowledge for L



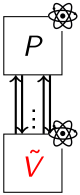
1. If $x \in L_{yes}$, V accepts whp
2. If $x \in L_{no}$, V rejects whp
3. If $x \in L_{yes}$, V learns nothing

Quantum Zero-knowledge for L

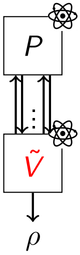


1. If $x \in L_{yes}$, V accepts whp
2. If $x \in L_{no}$, V rejects whp
3. If $x \in L_{yes}$, V learns nothing

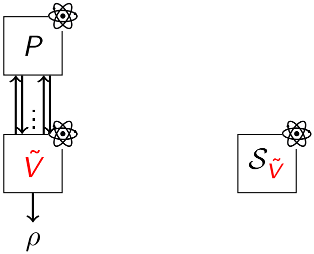
Quantum Zero-knowledge for L



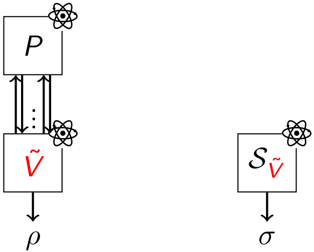
Quantum Zero-knowledge for L



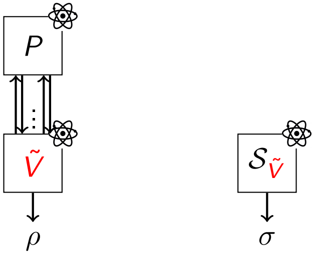
Quantum Zero-knowledge for L



Quantum Zero-knowledge for L



Quantum Zero-knowledge for L



Quantum computational zero-knowledge

ρ and σ cannot be **efficiently** distinguished:

$$\forall \text{ quantum poly-time } \mathcal{A} : |Pr[\mathcal{A}(\rho) = 1] - Pr[\mathcal{A}(\sigma) = 1]| \leq negl(n)$$

Zero-knowledge for QMA

Zero-knowledge for QMA

- Assuming qOWF: QMA $\subseteq$ QZK since PSPACE $=$ CZK $\subseteq$ QZK
  - Need to go through QMA $\subseteq$ PP
  - Desired: Efficient prover with QMA witness
- BJSW'16: QMA $\subseteq$ QZK with efficient prover
  - Multiple rounds of communication
  - Somewhat complicated

Zero-knowledge for QMA

- Assuming qOWF: QMA $\subseteq$ QZK since PSPACE $=$ CZK $\subseteq$ QZK

  Need to go through QMA $\subseteq$ PP

  Desired: Efficient prover with QMA witness
- BJSW'16: QMA $\subseteq$ QZK with efficient prover

  Multiple rounds of communication

  Somewhat complicated
- This work: explore CLDM
  - "commit-and-open" Proof of Knowledge QZK proof for QMA
  - "commit-and-open" Proof of Knowledge QSZK argument for QMA
  - QNISZK for QMA in the secret parameters setup

Zero-knowledge for QMA

- Assuming qOWF: QMA $\subseteq$ QZK since PSPACE $=$ CZK $\subseteq$ QZK
  Need to go through QMA $\subseteq$ PP
  Desired: Efficient prover with QMA witness
- BJSW'16: QMA $\subseteq$ QZK with efficient prover
  Multiple rounds of communication
  Somewhat complicated
- This work: explore CLDM
  - "commit-and-open" Proof of Knowledge QZK proof for QMA
  - "commit-and-open" Proof of Knowledge QSZK argument for QMA
  - QNISZK for QMA in the secret parameters setup

CLDM is in QMA [Liu'06]

Verification algorithm

CLDM is in QMA [Liu'06]

Verification algorithm

Input: $\rho_1, \ldots, \rho_m$

1. Prover sends $\psi^{\otimes \ell}$, where ψ is consistent with all ρ_i
2. Verifier picks i and random k-qubit Pauli P
3. Verifier measures the qubits corresponding to ρ_i on each (supposed) copy of ψ
4. Verifier accepts iff the the average of the measurement outcomes is close to $Tr(P\rho_i)$

CLDM is in QMA [Liu'06]

Verification algorithm

Input: $\rho_1, \ldots, \rho_m$

1. Prover sends $\psi^{\otimes \ell}$, where ψ is consistent with all ρ_i
2. Verifier picks i and random k-qubit Pauli P
3. Verifier measures the qubits corresponding to ρ_i on each (supposed) copy of ψ
4. Verifier accepts iff the the average of the measurement outcomes is close to $Tr(P\rho_i)$

- Completeness

  $Tr(P\psi) \approx Tr(P\rho_i)$ + Hoeffding's inequality

CLDM is in QMA [Liu'06]

Verification algorithm

Input: $\rho_1, \ldots, \rho_m$

1. Prover sends $\psi^{\otimes \ell}$, where ψ is consistent with all ρ_i
2. Verifier picks i and random k-qubit Pauli P
3. Verifier measures the qubits corresponding to ρ_i on each (supposed) copy of ψ
4. Verifier accepts iff the the average of the measurement outcomes is close to $Tr(P\rho_i)$

- Completeness

  $Tr(P\psi) \approx Tr(P\rho_i)$ + Hoeffding's inequality

- Soundness
  - Prover sends state σ
  - Let ψ_j be the register that should be the j-th copy of ψ
  - Let $\tilde{\psi} = \frac{1}{\ell} \sum_j \psi_j$
  - Expected value of the outcomes is $Tr(P\tilde{\psi})$ + Hoeffding's inequality

Very simple ZK proof for QMA

P V

$\rho_1, \ldots, \rho_m$

Very simple ZK proof for QMA

P	V
$\psi^{\otimes \ell}$	$\rho_1, \ldots, \rho_m$

Very simple ZK proof for QMA

P	V
$X^a Z^b \psi^{\otimes \ell} Z^b X^a$	$\rho_1, \ldots, \rho_m$
a_1, b_1	
a_2, b_2	
$\ldots$	
a_{n-1}, b_{n-1}	
a_n, b_n	

Very simple ZK proof for QMA

P V

$X^a Z^b \psi^{\otimes \ell} Z^b X^a$ $\rho_1, \ldots, \rho_m$

Very simple ZK proof for QMA

P

$a_1, b_1 \to 564651$
$a_2, b_2 \to 984565$
$\dots$
$a_n, b_n \to 894102$

V

$\rho_1, \dots, \rho_m$

$X^a Z^b \psi^{\otimes \ell} X^a Z^b$

...

Very simple ZK proof for QMA

P

$a_1, b_1 \rightarrow 564651$

$a_2, b_2 \rightarrow 984565$

$\dots$

$a_n, b_n \rightarrow 894102$

$\xleftarrow{\quad i \quad}$

V

$\rho_1, \dots, \rho_m$

$X^a Z^b \psi^{\otimes \ell} X^a Z^b$

Very simple ZK proof for QMA

P

$a_1, b_1 \rightarrow 564651$
$a_2, b_2 \rightarrow 984565$
$\dots$
$a_n, b_n \rightarrow 894102$

$\longleftarrow i$

$\longrightarrow$ 984565, 894102
keys to open otp of copies of ρ_i

V

$\rho_1, \dots, \rho_m$

$X^a Z^b \psi^{\otimes \ell} X^a Z^b$

Very simple ZK proof for QMA

P

$a_1, b_1 \rightarrow 564651$

$a_2, b_2 \rightarrow 984565$

$\dots$

$a_n, b_n \rightarrow 894102$

V

$\rho_1, \dots, \rho_m$

$X^a Z^b \psi^{\otimes \ell} X^a Z^b$

$\longleftarrow i$

$\longrightarrow$ 984565, 894102

keys to open otp of copies of ρ_i

a_2, b_2

...

a_n, b_n

Very simple ZK proof for QMA

P V

$a_1, b_1 \to 564651$
$a_2, b_2 \to 984565$
$\dots$
$a_n, b_n \to 894102$

$\rho_1, \dots, \rho_m$

$X^a Z^b \psi^{\otimes \ell} X^a Z^b$

$\xleftarrow{\quad i \quad}$

$\xrightarrow{\quad\quad}$ 984565, 894102
keys to open otp of copies of ρ_i

a_2, b_2

...

a_n, b_n

Completeness ✓ Soundness ✓ ZK ✓

Open questions

- Complexity of CLDM with density matrices of size $\{2, 3, 4\}$
- Complexity of approximation of CLDM
- QNIZK protocol for QMA in the CRS model
- More efficient Proof of Quantum knowledge protocols

Open questions

- Complexity of CLDM with density matrices of size $\{2, 3, 4\}$
- Complexity of approximation of CLDM
- QNIZK protocol for QMA in the CRS model
- More efficient Proof of Quantum knowledge protocols

Thank you for your attention!