Secure Certification of Mixed Quantum States

Frédéric Dupuis, Serge Fehr, Philippe Lamontagne and Louis Salvail
Quantum state certification

\[ |\psi\rangle \langle \psi |, I - |\psi\rangle \langle \psi | \]

If the result is \(|\psi\rangle\) for every \(H\), then most of the remaining positions are in state \(|\psi\rangle\) with overwhelming probability [BF10].

The reference state \(|\psi\rangle\) must be pure.
Quantum state certification

- Measure with $|\psi\rangle\langle\psi|$, $I - |\psi\rangle\langle\psi|$.
- If result is $|\psi\rangle$ for every $H$, then most of the remaining positions are in state $|\psi\rangle$ with overwhelming probability $[BF10]$.
- The reference state $|\psi\rangle$ must be pure.
Quantum state certification

Certification

- Measure with \( \{ |\psi\rangle\langle\psi|, \mathbb{I} - |\psi\rangle\langle\psi| \} \)
- If result is \( |\psi\rangle \) for every \( H \), then most of the remaining positions are in state \( |\psi\rangle \) with overwhelming probability [BF10].
- The reference state \( |\psi\rangle \) must be pure.
Quantum state certification

Certification

- Measure $\mathcal{H}$ with $\{ |\psi\rangle\langle\psi|, \mathbb{I} - |\psi\rangle\langle\psi| \}$
- If result is $|\psi\rangle$ for every $\mathcal{H}$, then most of the remaining positions are in state $|\psi\rangle$ with overwhelming probability [BF10].
- The reference state $|\psi\rangle$ must be pure.
Quantum state certification

Certification

- Measure $\mathcal{H}$ with $\{|\psi\rangle\langle\psi|, I - |\psi\rangle\langle\psi|\}$
- If result is $|\psi\rangle$ for every $\mathcal{H}$, then most of the remaining positions are in state $|\psi\rangle$ with overwhelming probability [BF10].
- The reference state $|\psi\rangle$ must be pure.
Quantum state certification

Certification

- Measure $H$ with $\{|\psi\rangle\langle\psi|, \mathbb{I} - |\psi\rangle\langle\psi|\}$
- If result is $|\psi\rangle$ for every $H$, then most of the remaining positions are in state $|\psi\rangle$ with overwhelming probability [BF10].
- The reference state $|\psi\rangle$ must be pure.
What about certifying **mixed** states?

**Usual approach fail**

Notion of *typical subspace* not applicable
What about certifying mixed states?

Usual approach fail

Notion of *typical subspace* not applicable

\[ X_{\text{sample}} = 00\ldots0 \quad \Pr \approx 1 \quad X_{\text{rest}} \in \{ x : x \text{ has less than } \delta n \text{ 1s} \} \]
What about certifying mixed states?

Usual approach fail

Notion of *typical subspace* not applicable

\[ X_{\text{sample}} = 00 \ldots 0 \quad \text{Pr} \approx 1 \quad \Rightarrow \quad X_{\text{rest}} \in \{ x : x \text{ has less than } \delta n \text{ 1s} \} \]
What about certifying mixed states?

Usual approach fail

Notion of *typical subspace* not applicable

\[ X_{\text{sample}} = 00\ldots0 \ \overset{\Pr \approx 1}{\Longrightarrow} \ X_{\text{rest}} \in \{ x : x \ \text{has less than } \delta n \ 1s \} \]
What about certifying mixed states?

**Usual approach fail**

Notion of *typical subspace* not applicable

\[ X_{\text{sample}} = 00\ldots 0 \xrightarrow{\Pr \approx 1} X_{\text{rest}} \in \{ x : x \text{ has less than } \delta n \, 1s \} \]

- For pure states

\[ |\psi_{\text{sample}}\rangle = |0\rangle^\otimes k \xrightarrow{\Pr \approx 1} |\psi_{\text{rest}}\rangle \in \text{span}\{ |x\rangle : x \text{ has less than } \delta n \, 1s \} \]
What about certifying mixed states?

Usual approach fail

Notion of *typical subspace* not applicable

\[ X_{\text{sample}} = 00\ldots0 \overset{\text{Pr} \approx 1}{\Rightarrow} X_{\text{rest}} \in \{ x : x \text{ has less than } \delta n \text{ 1s} \} \]

- For pure states

\[ |\psi_{\text{sample}}\rangle = |0\rangle^\otimes k \overset{\text{Pr} \approx 1}{\Rightarrow} |\psi_{\text{rest}}\rangle \in \text{span}\{|x\rangle : x \text{ has less than } \delta n \text{ 1s} \} \]
What about certifying **mixed** states?

**Usual approach fail**

Notion of *typical subspace* not applicable

\[ X_{\text{sample}} = 00 \ldots 0 \xrightarrow{\text{Pr} \approx 1} X_{\text{rest}} \in \{ x : x \text{ has less than } \delta n \text{ 1s} \} \]

- For pure states

\[ |\psi_{\text{sample}}\rangle = |0\rangle^\otimes k \xrightarrow{\text{Pr} \approx 1} |\psi_{\text{rest}}\rangle \in \text{span}\{|x\rangle : x \text{ has less than } \delta n \text{ 1s} \} \]
What about certifying **mixed** states?

**Usual approach fail**

Notion of *typical subspace* not applicable

\[ X_{\text{sample}} = 00 \ldots 0 \xrightarrow{\Pr \approx 1} X_{\text{rest}} \in \{ x : x \text{ has less than } \delta n \text{ 1s} \} \]

- For pure states

\[ |\psi_{\text{sample}}\rangle = |0\rangle^k \xrightarrow{\Pr \approx 1} |\psi_{\text{rest}}\rangle \in \text{span}\{|x\rangle : x \text{ has less than } \delta n \text{ 1s} \} \]

- For some mixed states \( \varphi \),

\[ \text{supp}(\varphi^\otimes n) = \mathcal{H}^\otimes n \]
What about certifying mixed states?

Usual approach fail

Notion of *typical subspace* not applicable

\[ X_{\text{sample}} = 00 \ldots 0 \overset{\text{Pr} \approx 1}{\rightarrow} X_{\text{rest}} \in \{ x : x \text{ has less than } \delta n \text{ 1s} \} \]

- For pure states

\[ |\psi_{\text{sample}}\rangle = |0\rangle^\otimes k \overset{\text{Pr} \approx 1}{\rightarrow} |\psi_{\text{rest}}\rangle \in \text{span}\{ |x\rangle : x \text{ has less than } \delta n \text{ 1s} \} \]

- For some mixed states \( \varphi \),

\[ \text{supp}(\varphi^\otimes n) = \mathcal{H}^\otimes n \]

No local measurement for a discrete notion of errors for mixed states
A mixed state certification protocol

Possible to verify that a qubit is in state $\varphi$ if we have access to its purifying register.
Possible to verify that a qubit is in state $\varphi$ if we have access to its purifying register.

**Two-player «Game»**

**Verifier** wants to certify that his state is close to $\varphi^\otimes n$.  
**Prover** wants to fool the verifier into thinking he has the right state even though it’s not the case.
A mixed state certification protocol

Possible to verify that a qubit is in state $\varphi$ if we have access to its purifying register.

**Two-player «Game»**

Verifer wants to certify that his state is close to $\varphi^{\otimes n}$.

Prover wants to fool the verifier into thinking he has the right state even though it’s not the case.

**P.** Prepare $|\varphi\rangle^{\otimes n}_{AR}$, send $A^n$ to verifier.

**V.** Choose a random sample, announce it to prover.

**P.** Send $R$ for each position in sample.

**V.** Measure $\{|\varphi\rangle\langle\varphi|_{AR}, \mathbb{I} - |\varphi\rangle\langle\varphi|_{AR}\}$ for each joint system $AR$ in sample.

**V.** Accept if no errors, reject otherwise.
A mixed state certification protocol

Possible to verify that a qubit is in state $\varphi$ if we have access to its purifying register.

Two-player «Game»

Verifier wants to certify that his state is close to $\varphi^{\otimes n}$.

Prover wants to fool the verifier into thinking he has the right state even though it’s not the case.

P. Prepare $|\varphi\rangle^{\otimes n}_{AR}$, send $A^n$ to verifier.

V. Choose a random sample, announce it to prover.

P. Send $R$ for each position in sample.

V. Measure $\{|\varphi\rangle\langle\varphi|_{AR}, \mathbb{I} - |\varphi\rangle\langle\varphi|_{AR}\}$ for each joint system $AR$ in sample.

V. Accept if no errors, reject otherwise.
A mixed state certification protocol

Possible to verify that a qubit is in state $\varphi$ if we have access to its purifying register.

**Two-player «Game»**

Verifier wants to certify that his state is close to $\varphi^\otimes n$.

Prover wants to fool the verifier into thinking he has the right state even though it’s not the case.

**P.** Prepare $|\varphi\rangle^\otimes n_{AR}$, send $A^n$ to verifier.

**V.** Choose a random sample, announce it to prover.

**P.** Send $R$ for each position in sample.

**V.** Measure $\{ |\varphi\rangle\langle \varphi |_{AR}, \mathbb{I} - |\varphi\rangle\langle \varphi |_{AR} \}$ for each joint system $AR$ in sample.

**V.** Accept if no errors, reject otherwise.
A mixed state certification protocol

Possible to verify that a qubit is in state $\varphi$ if we have access to its purifying register.

Two-player «Game»

Verifier wants to certify that his state is close to $\varphi^\otimes n$.

Prover wants to fool the verifier into thinking he has the right state even though it’s not the case.

P. Prepare $|\varphi\rangle^\otimes n_{AR}$, send $A^n$ to verifier.

V. Choose a random sample, announce it to prover.

P. Send $R$ for each position in sample.

V. Measure $\{|\varphi\rangle\langle \varphi|_{AR}, \mathbb{I} - |\varphi\rangle\langle \varphi|_{AR}\}$ for each joint system $AR$ in sample.

V. Accept if no errors, reject otherwise.
A mixed state certification protocol

Possible to verify that a qubit is in state $\varphi$ if we have access to its purifying register.

**Two-player «Game»**

Verifier wants to certify that his state is close to $\varphi \otimes^n$.

Prover wants to fool the verifier into thinking he has the right state even though it’s not the case.

**P.** Prepare $|\varphi\rangle \otimes^n_{AR}$, send $A^n$ to verifier.

**V.** Choose a random sample, announce it to prover.

**P.** Send $R$ for each position in sample.

**V.** Measure $\{|\varphi\rangle\langle\varphi|_{AR}, \mathbb{I} - |\varphi\rangle\langle\varphi|_{AR}\}$ for each joint system $AR$ in sample.

**V.** Accept if no errors, reject otherwise.
A few observations about the protocol

Interaction is necessary

How can you distinguish

\[
\left( \frac{|0\rangle\langle 0|}{2} + \frac{|1\rangle\langle 1|}{2} \right)^\otimes n
\]

from

\[
\approx n/2 \text{ times } |0\rangle|0\rangle \ldots |0\rangle \quad \approx n/2 \text{ times } |1\rangle|1\rangle \ldots |1\rangle
\]
A few observations about the protocol

Interaction is necessary
How can you distinguish

$$\left( \frac{|0\rangle\langle 0|}{2} + \frac{|1\rangle\langle 1|}{2} \right)^{\otimes n}$$

from

$$\approx \frac{n}{2} \text{ times}$$

$$|0\rangle|0\rangle \ldots |0\rangle$$

$$\approx \frac{n}{2} \text{ times}$$

$$|1\rangle|1\rangle \ldots |1\rangle$$

Interaction gives more power to prover

P.  

V.  

4/8
A few observations about the protocol

Interaction is necessary
How can you distinguish
\[
\left( \frac{|0\rangle\langle 0|}{2} + \frac{|1\rangle\langle 1|}{2} \right) \otimes^n \text{ from } |0\rangle|0\rangle \ldots |0\rangle |1\rangle |1\rangle \ldots |1\rangle
\]

Interaction gives more power to prover

1. Learns sample
A few observations about the protocol

**Interaction is necessary**

How can you distinguish

\[
\left(\frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2}\right)^\otimes n
\]

from

\[
|0\rangle|0\rangle \ldots |0\rangle |1\rangle|1\rangle \ldots |1\rangle
\]

\[\approx n/2 \text{ times}\]

\[\approx n/2 \text{ times}\]

**Interaction gives more power to prover**

1. Learns sample
2. Measures qubits
A few observations about the protocol

Interaction is necessary

How can you distinguish

\[ \left( \frac{|0\rangle\langle 0|}{2} + \frac{|1\rangle\langle 1|}{2} \right)^\otimes n \]

from

\[|0\rangle|0\rangle \ldots |0\rangle |1\rangle|1\rangle \ldots |1\rangle\]

\(\approx n/2\) times \(\approx n/2\) times

Interaction gives more power to prover

1. Learns sample
2. Measures qubits
3. Aborts based on result
A few observations about the protocol

**Interaction is necessary**

How can you distinguish

\[
\left( \frac{|0\rangle \langle 0|}{2} + \frac{|1\rangle \langle 1|}{2} \right) \otimes^n \text{ from } |0\rangle |0\rangle \ldots |0\rangle |1\rangle |1\rangle \ldots |1\rangle
\]

\[\approx \frac{n}{2} \text{ times} \quad \frac{n}{2} \text{ times}\]

**Interaction gives more power to prover**

1. **Learns sample**
2. **Measures qubits**
3. **Aborts based on result**

**Post-selection**
A few observations about the protocol

Interaction is necessary
How can you distinguish
\[
\left( \frac{|0\rangle\langle 0|}{2} + \frac{|1\rangle\langle 1|}{2} \right)^\otimes n
\]
from
\[
\approx n/2 \text{ times } |0\rangle|0\rangle \ldots |0\rangle |1\rangle|1\rangle \ldots |1\rangle
\]

Interaction gives more power to prover

1. Learns sample
2. Measures qubits
3. Aborts based on result

Example
Prepare \( \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)^\otimes n \),
measure positions outside of sample, abort if result \( \neq |0\rangle^\otimes n-k \).
Resulting state always \( |0\rangle^\otimes n-k \)
What *can* the *prover* do?

- prepare the honest state, up to a few errors,
- prepare a mixture/superposition of such states,
- purify this mixture, and
- post-select on a measurement outcome.
What *can* the *prover* do?

An “undetectable” attack

The prover can

- prepare the honest state, up to a few errors,
- prepare a mixture/superposition of such states,
- purify this mixture, and
- post-select on a measurement outcome.
What *can* the prover do?

An “undetectable” attack

The prover can

- prepare the **honest state**, up to a few errors,
- prepare a mixture/superposition of such states,
- purify this mixture, and
- post-select on a measurement outcome.

\[ |\phi\rangle^\otimes n = |\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle\]
**What can the prover do?**

**An “undetectable” attack**

The prover can

- prepare the honest state, up to a few errors,
- prepare a mixture/superposition of such states,
- purify this mixture, and
- post-select on a measurement outcome.

\[
|\phi\rangle^\otimes n = |\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle
\]

\[
|\psi_e\rangle = |\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle
\]
What *can* the **prover** do?

**An “undetectable” attack**

The prover can

- prepare the honest state, up to a few errors,
- prepare a *mixture/superposition* of such states,
- purify this mixture, and
- post-select on a measurement outcome.

\[
|\phi\rangle^\otimes n = |\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle
\]

\[
|\psi_e\rangle = |\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle|\phi\rangle
\]

\[
\rho_{A^nR^n} = \sum_e p_e |\psi_e\rangle\langle \psi_e|
\]
What *can* the **prover** do?

**An “undetectable” attack**

The prover can

- prepare the honest state, up to a few errors,
- prepare a mixture/superposition of such states,
- **purify** this mixture, and
- post-select on a measurement outcome.

\[
\rho_{AnR^n} = \sum_{e} p_e |\psi_e\rangle \langle \psi_e|
\]

\[
|\psi\rangle_{AnR^n E} = \sum_{e} \sqrt{p_e} |\psi_e\rangle_{AnR^n} \otimes |\tau_e\rangle_E
\]
What *can* the **prover** do?

An “undetectable” attack

The prover can

- prepare the honest state, up to a few errors,
- prepare a mixture/superposition of such states,
- purify this mixture, and
- **post-select** on a measurement outcome.

\[ \rho_{A^n R^n} = \sum_e p_e |\psi_e\rangle \langle \psi_e| \]

\[ |\psi\rangle_{A^n R^n E} = \sum_e \sqrt{p_e} |\psi_e\rangle_{A^n R^n} \otimes |\tau_e\rangle_E \]

\[ |\hat{\psi}\rangle_{A^n R^n E} = I_{A^n} \otimes M_{R^n E} |\psi\rangle_{A^n R^n E} \]
An “undetectable” attack

The prover can

- prepare the honest state, up to a few errors,
- prepare a mixture/superposition of such states,
- purify this mixture, and
- post-select on a measurement outcome.

\[
\rho_{A^nR^n} = \sum_e p_e |\psi_e\rangle\langle\psi_e|
\]

\[
|\psi\rangle_{A^nR^nE} = \sum_e \sqrt{p_e} |\psi_e\rangle_{A^nR^n} \otimes |\tau_e\rangle_E
\]

\[
|\hat{\Psi}\rangle_{A^nR^nE} = I_{A^n} \otimes M_{R^nE} |\Psi\rangle_{A^nR^nE}
\]
### The mixed state certification Theorem

#### Main Result

For any strategy of the **prover**, if the **verifier** accepts, his output state $\rho_{A^n}$ satisfies

$$\rho_{A^n} \leq p_n \cdot \psi_{A^n} + \sigma$$

where $p_n$ is a fixed-degree polynomial in $n$, $\psi_{A^n}$ is the reduced operator of an ideal state $|\psi\rangle_{A^n R^n E}$ and $\text{tr}(\sigma) \leq \text{negl}(n)$.  

---

---
Main Result

For any strategy of the prover, if the verifier accepts, his output state $\rho_{A^n}$ satisfies

$$\rho_{A^n} \leq p_n \cdot \psi_{A^n} + \sigma$$

where $p_n$ is a fixed-degree polynomial in $n$, $\psi_{A^n}$ is the reduced operator of an ideal state $|\psi\rangle_{A^nR^nE}$ and $\text{tr}(\sigma) \leq \text{negl}(n)$. 
### Main Result

For any strategy of the **prover**, if the **verifier** accepts, his output state $\rho_{A^n}$ satisfies

$$\rho_{A^n} \leq p_n \cdot \psi_{A^n} + \sigma$$

where $p_n$ is a fixed-degree polynomial in $n$, $\psi_{A^n}$ is the reduced operator of an ideal state $|\psi\rangle_{A^nR^nE}$ and $\text{tr}(\sigma) \leq \text{negl}(n)$.
Main Result

For any strategy of the prover, if the verifier accepts, his output state $\rho_{An}$ satisfies

$$\rho_{An} \leq p_n \cdot \psi_{An} + \sigma$$

where $p_n$ is a fixed-degree polynomial in $n$, $\psi_{An}$ is the reduced operator of an ideal state $|\psi\rangle_{AnR^nE}$ and $\text{tr}(\sigma) \leq \text{negl}(n)$.
Main Result

For any strategy of the prover, if the verifier accepts, his output state $\rho_{A^n}$ satisfies

$$\rho_{A^n} \leq p_n \cdot \psi_{A^n} + \sigma$$

where $p_n$ is a fixed-degree polynomial in $n$, $\psi_{A^n}$ is the reduced operator of an ideal state $|\psi\rangle_{A^n R^n E}$ and $\text{tr}(\sigma) \leq \text{negl}(n)$. 
Main Result

For any strategy of the prover, if the verifier accepts, his output state $\rho_{An}$ satisfies

$$\rho_{An} \leq p_n \cdot \psi_{An} + \sigma$$

where $p_n$ is a fixed-degree polynomial in $n$, $\psi_{An}$ is the reduced operator of an ideal state $|\psi\rangle_{A^n R^n E}$ and $\text{tr}(\sigma) \leq \text{negl}(n)$. 
### The mixed state certification Theorem

#### Main Result

For any strategy of the prover, if the verifier accepts, his output state $\rho_{A^n}$ satisfies

$$\rho_{A^n} \leq p_n \cdot \psi_{A^n} + \sigma$$

where $p_n$ is a fixed-degree polynomial in $n$, $\psi_{A^n}$ is the reduced operator of an ideal state $|\psi\rangle_{A^nR^nE}$ and $\text{tr}(\sigma) \leq \text{negl}(n)$.

#### Application to Cryptography

For any POVM operator $E^{bad}$ of a “bad” outcome,

$$\text{tr} \left( E^{bad} \rho_{A^n} \right) \leq p_n \cdot \text{tr} \left( E^{bad} \psi_{A^n} \right) + \text{negl}(n)$$

Bad outcome on real state has negligible probability if $\text{tr}(E^{bad}\psi_{A^n})$ is negligible.
The mixed state certification Theorem

Main Result
For any strategy of the prover, if the verifier accepts, his output state $\rho_{A^n}$ satisfies

$$\rho_{A^n} \leq p_n \cdot \psi_{A^n} + \sigma$$

where $p_n$ is a fixed-degree polynomial in $n$, $\psi_{A^n}$ is the reduced operator of an ideal state $|\psi\rangle_{A^nR^nE}$ and $\text{tr}(\sigma) \leq \text{negl}(n)$.

Application to Cryptography
For any POVM operator $E^{bad}$ of a “bad” outcome,

$$\text{tr} \left( E^{bad} \rho_{A^n} \right) \leq p_n \cdot \text{tr} \left( E^{bad} \psi_{A^n} \right) + \text{negl}(n)$$

Bad outcome on real state has negligible probability if $\text{tr}(E^{bad}\psi_{A^n})$ is negligible.
Generalisations and special cases

Sufficient conditions

**Invariance under permutations.** Equivalent to protocol where verifier permutes his registers with random $\pi$ and announces $\pi$ to the prover.

Behaves well on “easy” state. The verifier detects any cheating attempt with overwhelming probability on a state of the form $\sigma^{\otimes n}$ for $\sigma$ distant from reference state $\varphi$. 

Corollary

Theorem implies security of

- a local measurement certification protocol for $\varphi = I_2$,
- pure state certification [BF10], and
- a “distributed” pure state certification protocol [DDN14] not covered by [BF10].
**Generalisations and special cases**

| Sufficient conditions |
|------------------------|
| **Invariance under permutations.** *Equivalent* to protocol where **verifier** permutes his registers with random $\pi$ and announces $\pi$ to the **prover**. |
| **Behaves well on “easy” state.** The **verifier** detects any cheating attempt with overwhelming probability on a state of the form $\sigma \otimes^n$ for $\sigma$ *distant* from reference state $\varphi$. |
Generalisations and special cases

**Sufficient conditions**

**Invariance under permutations.** *Equivalent* to protocol where verifier permutes his registers with random $\pi$ and announces $\pi$ to the prover.

**Behaves well on “easy” state.** The verifier detects any cheating attempt with overwhelming probability on a state of the form $\sigma \otimes n$ for $\sigma$ distant from reference state $\varphi$.

**Corollary**

*Theorem* implies security of

- a local measurement certification protocol for $\varphi = \frac{I}{2}$,
- pure state certification [BF10], and
- a “distributed” pure state certification protocol [DDN14] not covered by [BF10].
Generalisations and special cases

Sufficient conditions

Invariance under permutations. Equivalent to protocol where verifier permutes his registers with random $\pi$ and announces $\pi$ to the prover.

Behaves well on “easy” state. The verifier detects any cheating attempt with overwhelming probability on a state of the form $\sigma \otimes^n$ for $\sigma$ distant from reference state $\varphi$.

Corollary

Theorem implies security of
• a local measurement certification protocol for $\varphi = \mathbb{I}/2$,
• pure state certification [BF10], and
• a “distributed” pure state certification protocol [DDN14] not covered by [BF10].
Generalisations and special cases

Sufficient conditions

Invariance under permutations. *Equivalent* to protocol where verifier permutes his registers with random $\pi$ and announces $\pi$ to the prover.

Behaves well on “easy” state. The verifier detects any cheating attempt with overwhelming probability on a state of the form $\sigma \otimes n$ for $\sigma$ distant from reference state $\varphi$.

Corollary

*Theorem implies security of*

- a local measurement certification protocol for $\varphi = \frac{I}{2}$,
- pure state certification [BF10], and
- a “distributed” pure state certification protocol [DDN14] not covered by [BF10].
Sufficient conditions

**Invariance under permutations.** Equivalent to protocol where verifier permutes his registers with random $\pi$ and announces $\pi$ to the prover.

Behaves well on “easy” state. The verifier detects any cheating attempt with overwhelming probability on a state of the form $\sigma \otimes^n$ for $\sigma$ distant from reference state $\varphi$.

Corollary

*Theorem implies security of*
- a local measurement certification protocol for $\varphi = \frac{I}{2}$,
- pure state certification [BF10], and
- a “distributed” pure state certification protocol [DDN14] not covered by [BF10].
Application: secure two-party randomness generation
Secure Two-Party Randomness Generation

Goal

Produce $X_A, X_B \in \{0, 1\}^n$ such that

- $X_A = X_B$ if Alice and Bob are both honest,
- $H_\infty(X_A) \geq (1 - \epsilon)n$ and $H_\infty(X_B) \geq (1 - \epsilon)n$ except with negligible probability.
## Secure Two-Party Randomness Generation

### Goal

Produce $X_A, X_B \in \{0, 1\}^n$ such that

- $X_A = X_B$ if Alice and Bob are both honest,
- $H_\infty(X_A) \geq (1 - \epsilon)n$ and $H_\infty(X_B) \geq (1 - \epsilon)n$ except with negligible probability.

| Protocol |
|---|
| Alice prepares $|\Psi\rangle \otimes N_{AB}$ and sends $B_N$ to Bob. |
| Bob certifies that most of his registers are close to $I_2$. |
| Alice and Bob measure their remaining $n$ registers. |
Secure Two-Party Randomness Generation

Goal

Produce $X_A, X_B \in \{0, 1\}^n$ such that

- $X_A = X_B$ if Alice and Bob are both honest,
- $H_\infty(X_A) \geq (1 - \epsilon)n$ and $H_\infty(X_B) \geq (1 - \epsilon)n$ except with negligible probability.
Secure Two-Party Randomness Generation

Goal

Produce $X_A, X_B \in \{0, 1\}^n$ such that

- $X_A = X_B$ if Alice and Bob are both honest,
- $H_\infty(X_A) \geq (1 - \epsilon)n$ and $H_\infty(X_B) \geq (1 - \epsilon)n$ except with negligible probability.

Protocol

- Alice prepares $|\Psi\rangle^N_{AB}$ and sends $B^N$ to Bob.
- Bob certifies that most of his registers are close to $\frac{I}{2}$.
- Alice and Bob measure their remaining $n$ registers.
Secure Two-Party Randomness Generation

Goal

Produce $X_A, X_B \in \{0, 1\}^n$ such that

- $X_A = X_B$ if Alice and Bob are both honest,
- $H_\infty(X_A) \geq (1 - \epsilon)n$ and $H_\infty(X_B) \geq (1 - \epsilon)n$ except with negligible probability.

Protocol

- Alice prepares $|\psi\rangle^{\otimes N}_{AB}$ and sends $B^N$ to Bob.
- Bob certifies that most of his registers are close to $\frac{I}{2}$.
- Alice and Bob measure their remaining $n$ registers.
Secure Two-Party Randomness Generation

Goal

Produce $X_A, X_B \in \{0, 1\}^n$ such that

- $X_A = X_B$ if Alice and Bob are both honest,
- $H_\infty(X_A) \geq (1 - \epsilon)n$ and $H_\infty(X_B) \geq (1 - \epsilon)n$ except with negligible probability.

Protocol

- Alice prepares $|\psi\rangle_{AB}^\otimes N$ and sends $B^N$ to Bob.
- Bob certifies that most of his registers are close to $\frac{I}{2}$.
- Alice and Bob measure their remaining $n$ registers.
Secure Two-Party Randomness Generation

Goal

Produce $X_A, X_B \in \{0, 1\}^n$ such that

- $X_A = X_B$ if Alice and Bob are both honest,
- $H_\infty(X_A) \geq (1 - \epsilon)n$ and $H_\infty(X_B) \geq (1 - \epsilon)n$ except with negligible probability.

Protocol

- Alice prepares $|\psi\rangle^{\otimes N}_{AB}$ and sends $B^N$ to Bob.
- Bob *certifies* that most of his registers are close to $\frac{I}{2}$.
- Alice and Bob measure their remaining $n$ registers.
Secure Two-Party Randomness Generation

Goal
Produce $X_A, X_B \in \{0, 1\}^n$ such that

- $X_A = X_B$ if Alice and Bob are both honest,
- $H_\infty(X_A) \geq (1 - \epsilon)n$ and $H_\infty(X_B) \geq (1 - \epsilon)n$ except with negligible probability.

Protocol
- Alice prepares $|\psi\rangle^N_{AB}$ and sends $B^N$ to Bob.
- Bob certifies that most of his registers are close to $\frac{I}{2}$.
- Alice and Bob measure their remaining $n$ registers.

Our main result ensures that the measurement outcome will have near maximal min-entropy.
Thank you!
Niek J. Bouman and Serge Fehr.
**Sampling in a quantum population, and applications.**
In *Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference*, volume 6223 of *Lecture Notes in Computer Science*, pages 724–741. Springer, 2010.

Ivan Damgård, Frédéric Dupuis, and Jesper Buus Nielsen.
**On the orthogonal vector problem and the feasibility of unconditionally secure leakage resilient computation.**
Cryptology ePrint Archive, Report 2014/282, 2014. [http://eprint.iacr.org/](http://eprint.iacr.org/).