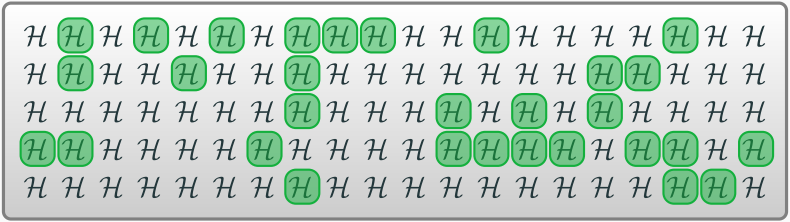
Secure Certification of Mixed Quantum States

Frédéric Dupuis, Serge Fehr, **Philippe Lamontagne** and Louis Salvail

Quantum state certification

$\mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}$
$\mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}$
$\mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}$
$\mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}$
$\mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}\ \mathcal{H}$

Quantum state certification



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 $\{|\psi\rangle\langle\psi|, \mathbb{I} - |\psi\rangle\langle\psi|\}$
- 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 $\{|\psi\rangle\langle\psi|, \mathbb{I} - |\psi\rangle\langle\psi|\}$
- 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 $\{|\psi\rangle\langle\psi|, \mathbb{I} - |\psi\rangle\langle\psi|\}$
- 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.

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

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

What about certifying mixed states ?

Usual approach fail

Notion of *typical subspace* not applicable

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

What about certifying mixed states ?

Usual approach fail

Notion of *typical subspace* not applicable

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

What about certifying mixed states ?

Usual approach fail

Notion of *typical subspace* not applicable

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

- For pure states

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

What about certifying mixed states ?

Usual approach fail

Notion of *typical subspace* not applicable

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

- For pure states

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

What about certifying mixed states ?

Usual approach fail

Notion of *typical subspace* not applicable

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

- For pure states

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

What about certifying mixed states ?

Usual approach fail

Notion of *typical subspace* not applicable

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

- For pure states

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

- For some mixed states φ,

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

What about certifying mixed states ?

Usual approach fail

Notion of *typical subspace* not applicable

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

- For pure states

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

- For some mixed states φ,

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

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 φ if we have access to its purifying register.

A mixed state certification protocol

Possible to verify that a qubit is in state φ 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 φ 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 $|\varphi\rangle_{AR}^{\otimes n}$, 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 φ 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 $|\varphi\rangle_{AR}^{\otimes n}$, 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 φ 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 $|\varphi\rangle_{AR}^{\otimes n}$, 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 φ 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 $|\varphi\rangle_{AR}^{\otimes n}$, 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 φ 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 $|\varphi\rangle_{AR}^{\otimes n}$, 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

$$\left(\frac{|0\rangle\langle 0|}{2}+\frac{|1\rangle\langle 1|}{2}\right)^{\otimes n} \quad \text{from} \quad \overbrace{|0\rangle|0\rangle\ldots|0\rangle}^{\approx n/2 \text{ times}}\overbrace{|1\rangle|1\rangle\ldots|1\rangle}^{\approx n/2 \text{ times}}$$

A few observations about the protocol

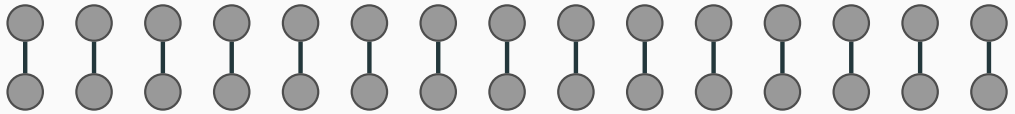
Interaction is necessary

How can you distinguish

$$\left(\frac{|0\rangle\langle 0|}{2}+\frac{|1\rangle\langle 1|}{2}\right)^{\otimes n} \quad \text{from} \quad \overbrace{|0\rangle|0\rangle\ldots|0\rangle}^{\approx n/2 \text{ times}}\overbrace{|1\rangle|1\rangle\ldots|1\rangle}^{\approx n/2 \text{ times}}$$

Interaction gives more power to prover

P.
V.



A few observations about the protocol

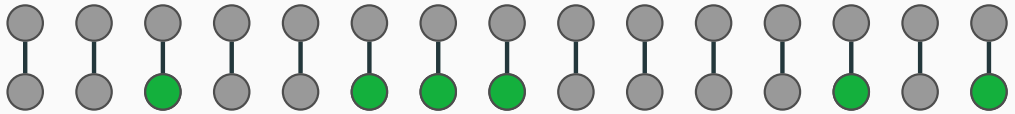
Interaction is necessary

How can you distinguish

$$\left(\frac{|0\rangle\langle 0|}{2}+\frac{|1\rangle\langle 1|}{2}\right)^{\otimes n} \quad \text{from} \quad \overbrace{|0\rangle|0\rangle\ldots|0\rangle}^{\approx n/2 \text{ times}}\overbrace{|1\rangle|1\rangle\ldots|1\rangle}^{\approx n/2 \text{ times}}$$

Interaction gives more power to prover

P.
V.



1. Learns sample

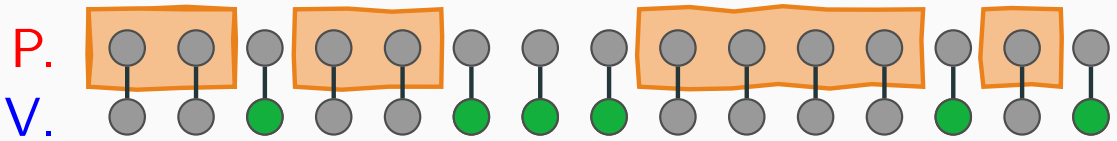
A few observations about the protocol

Interaction is necessary

How can you distinguish

$$\left(\frac{|0\rangle\langle 0|}{2}+\frac{|1\rangle\langle 1|}{2}\right)^{\otimes n} \quad \text{from} \quad \overbrace{|0\rangle|0\rangle\ldots|0\rangle}^{\approx n/2 \text{ times}}\overbrace{|1\rangle|1\rangle\ldots|1\rangle}^{\approx n/2 \text{ times}}$$

Interaction gives more power to prover



1. Learns sample
2. Measures qubits

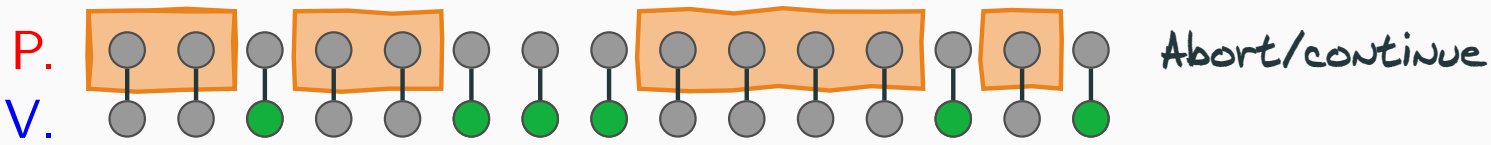
A few observations about the protocol

Interaction is necessary

How can you distinguish

$$\left(\frac{|0\rangle\langle 0|}{2} + \frac{|1\rangle\langle 1|}{2}\right)^{\otimes n} \quad \text{from} \quad \overbrace{|0\rangle|0\rangle\ldots|0\rangle}^{\approx n/2 \text{ times}}\overbrace{|1\rangle|1\rangle\ldots|1\rangle}^{\approx n/2 \text{ times}}$$

Interaction gives more power to prover



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

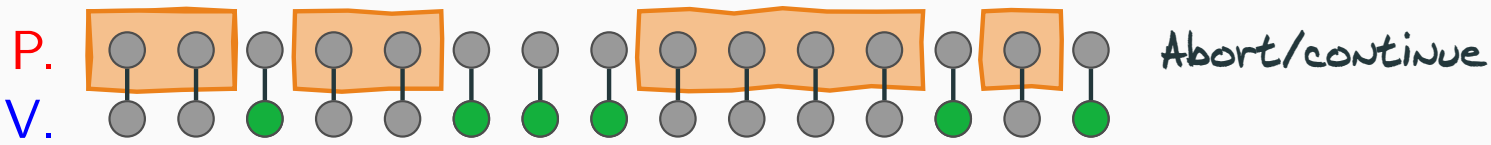
A few observations about the protocol

Interaction is necessary

How can you distinguish

$$\left(\frac{|0\rangle\langle 0|}{2} + \frac{|1\rangle\langle 1|}{2}\right)^{\otimes n} \quad \text{from} \quad \overbrace{|0\rangle|0\rangle\ldots|0\rangle}^{\approx n/2 \text{ times}}\overbrace{|1\rangle|1\rangle\ldots|1\rangle}^{\approx n/2 \text{ times}}$$

Interaction gives more power to prover



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

Post-selection

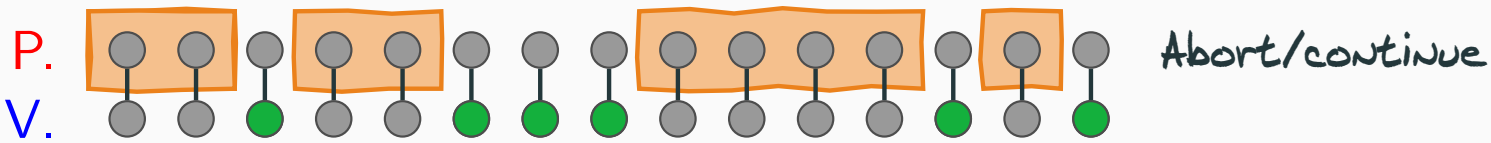
A few observations about the protocol

Interaction is necessary

How can you distinguish

$$\left(\frac{|0\rangle\langle 0|}{2}+\frac{|1\rangle\langle 1|}{2}\right)^{\otimes n} \quad \text{from} \quad \overbrace{|0\rangle|0\rangle\ldots|0\rangle}^{\approx n/2 \text{ times}}\overbrace{|1\rangle|1\rangle\ldots|1\rangle}^{\approx n/2 \text{ times}}$$

Interaction gives more power to prover



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

Post-selection

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 ?

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.

$$|\varphi\rangle^{\otimes n} = |\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle$$

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.

$$|\varphi\rangle^{\otimes n} = |\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle$$

$$|\psi_e\rangle = |\varphi\rangle \not\varphi |\varphi\rangle|\varphi\rangle|\varphi\rangle \not\varphi |\varphi\rangle \not\varphi |\varphi\rangle|\varphi\rangle|\varphi\rangle \not\varphi |\varphi\rangle|\varphi\rangle \not\varphi |\varphi\rangle|\varphi\rangle$$

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.

$$|\varphi\rangle^{\otimes n} = |\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle|\varphi\rangle$$

$$|\psi_e\rangle = |\varphi\rangle \not|\varphi\rangle |\varphi\rangle|\varphi\rangle|\varphi\rangle \not|\varphi\rangle |\varphi\rangle \not|\varphi\rangle|\varphi\rangle|\varphi\rangle \not|\varphi\rangle |\varphi\rangle|\varphi\rangle \not|\varphi\rangle|\varphi\rangle$$

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

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.

$$|\psi_e\rangle = |\varphi\rangle\,\cancel{|\varphi\rangle}\,|\varphi\rangle|\varphi\rangle|\varphi\rangle\,\cancel{|\varphi\rangle}\,|\varphi\rangle\,\widehat{\cancel{|\varphi\rangle}}|\varphi\rangle|\varphi\rangle|\varphi\rangle\,\cancel{|\varphi\rangle}\,|\varphi\rangle|\varphi\rangle\,\cancel{|\varphi\rangle}\,|\varphi\rangle|\varphi\rangle \quad \dots$$

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

$$|\Psi\rangle_{A^nR^nE} = \sum_e \sqrt{p_e}|\psi_e\rangle_{A^nR^n} \otimes |\tau_e\rangle_E$$

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.

$$\rho_{A^n R^n} = \sum_e p_e |\psi_e\rangle\langle\psi_e| \quad \cdots$$

$$|\Psi\rangle_{A^n R^n E} = \sum_e \sqrt{p_e} |\psi_e\rangle_{A^n R^n} \otimes |\tau_e\rangle_E$$

$$|\hat{\Psi}\rangle_{A^n R^n E} = \mathbb{I}_{A^n} \otimes M_{R^n E} |\Psi\rangle_{A^n R^n E}$$

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.

$$\rho_{A^n R^n} = \sum_e p_e |\psi_e\rangle\langle\psi_e| \quad \cdots$$

$$|\Psi\rangle_{A^n R^n E} = \sum_e \sqrt{p_e} |\psi_e\rangle_{A^n R^n} \otimes |\tau_e\rangle_E$$

ideal state

$$|\hat{\Psi}\rangle_{A^n R^n E} = \mathbb{I}_{A^n} \otimes M_{R^n E} |\Psi\rangle_{A^n R^n E}$$

The mixed state certification Theorem

Main Result

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

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

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

The mixed state certification Theorem

Main Result

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

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

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

The mixed state certification Theorem

Main Result

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

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

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

The mixed state certification Theorem

Main Result

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

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

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

The mixed state certification Theorem

Main Result

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

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

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

The mixed state certification Theorem

Main Result

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

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

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

The mixed state certification Theorem

Main Result

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

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

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

Application to Cryptography

For any POVM operator E^{bad} of a "bad" outcome,

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

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

The mixed state certification Theorem

Main Result

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

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

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

Application to Cryptography

For any POVM operator E^{bad} of a "bad" outcome,

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

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

Generalisations and special cases

Sufficient conditions

Invariance under permutations. *Equivalent* to protocol where verifier permutes his registers with random π and announces π 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 σ *distant* from reference state φ.

Generalisations and special cases

Sufficient conditions

Invariance under permutations. *Equivalent* to protocol where verifier permutes his registers with random π and announces π 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 σ *distant* from reference state φ.

Generalisations and special cases

Sufficient conditions

Invariance under permutations. *Equivalent* to protocol where verifier permutes his registers with random π and announces π 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 σ *distant* from reference state φ.

Corollary

Theorem implies security of

- *a local measurement certification protocol for* $\varphi = \frac{\mathbb{I}}{2}$,
- *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 π and announces π 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 σ *distant* from reference state φ.

Corollary

Theorem implies security of

- *a local measurement certification protocol for* $\varphi = \frac{\mathbb{I}}{2}$,
- *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 π and announces π 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 σ *distant* from reference state φ.

Corollary

Theorem implies security of

- *a local measurement certification protocol for* $\varphi = \frac{\mathbb{I}}{2}$,
- *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 π and announces π 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 σ *distant* from reference state φ.

Corollary

Theorem implies security of

- *a local measurement certification protocol for* $\varphi = \frac{\mathbb{I}}{2}$,
- *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,
- $\mathrm{H}_\infty(X_A) \geq (1-\epsilon)n$ and $\mathrm{H}_\infty(X_B) \geq (1-\epsilon)n$ 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,
- $\mathrm{H}_\infty(X_A) \geq (1-\epsilon)n$ and $\mathrm{H}_\infty(X_B) \geq (1-\epsilon)n$ 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,
- $\mathrm{H}_\infty(X_A) \geq (1-\epsilon)n$ and $\mathrm{H}_\infty(X_B) \geq (1-\epsilon)n$ 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,
- $\mathrm{H}_\infty(X_A) \geq (1-\epsilon)n$ and $\mathrm{H}_\infty(X_B) \geq (1-\epsilon)n$ 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 $\frac{\mathbb{I}}{2}$.
- 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,
- $\mathrm{H}_\infty(X_A) \geq (1-\epsilon)n$ and $\mathrm{H}_\infty(X_B) \geq (1-\epsilon)n$ 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 $\frac{\mathbb{I}}{2}$.
- 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,
- $\mathrm{H}_\infty(X_A) \geq (1-\epsilon)n$ and $\mathrm{H}_\infty(X_B) \geq (1-\epsilon)n$ 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 $\frac{\mathbb{I}}{2}$.
- 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,
- $\mathrm{H}_\infty(X_A) \geq (1-\epsilon)n$ and $\mathrm{H}_\infty(X_B) \geq (1-\epsilon)n$ 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 $\frac{\mathbb{I}}{2}$.
- 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,
- $\mathrm{H}_\infty(X_A) \geq (1-\epsilon)n$ and $\mathrm{H}_\infty(X_B) \geq (1-\epsilon)n$ 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 $\frac{\mathbb{I}}{2}$.
- 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/`.