The Quantum Bit Commitment

A complete classification of protocols

Giacomo Mauro D’Ariano

Quantum Optics & Information Group

Istituto Nazionale di Fisica della Materia, Unità di Pavia

Dipartimento di Fisica “A. Volta”, via Bassi 6, I-27100 Pavia, Italy

Dept. of Electrical and Computer Engineering, Northwestern University, Evanston, IL 60208

Index

- **Dispute:** Are there unconditionally secure quantum bit commitment protocols?

Index

- **Dispute:** Are there unconditionally secure quantum bit commitment protocols?
- Complete classification of all possible protocols and cheating attacks (ask for preprint or look at quant-ph/ next weeks).

Index

- **Dispute:** Are there unconditionally secure quantum bit commitment protocols?
- Complete classification of all possible protocols and cheating attacks (ask for preprint or look at quant-ph/ next weeks).
- **Main point:** The most general encoding is on quantum operations (QO)—instead on quantum states.

Index

- **Dispute:** Are there unconditionally secure quantum bit commitment protocols?
- Complete classification of all possible protocols and cheating attacks (ask for preprint or look at quant-ph/ next weeks).
- **Main point:** The most general encoding is on quantum operations (QO)—instead on quantum states.
- Bound for the cheating probabilities, for *non-aborting, perfect-verification* protocols.

Index

- **Dispute:** Are there unconditionally secure quantum bit commitment protocols?
- Complete classification of all possible protocols and cheating attacks (ask for preprint or look at quant-ph/ next weeks).
- **Main point:** The most general encoding is on quantum operations (QO)—instead on quantum states.
- Bound for the cheating probabilities, for *non-aborting, perfect-verification* protocols.

Definition of the problem

- Commitment:  provides  with a piece of evidence that she has chosen a bit $b = 0, 1$ which she commits to him.

Definition of the problem

- Commitment:  provides  with a piece of evidence that she has chosen a bit $b = 0, 1$ which she commits to him.
- Opening: Later  will open the commitment, revealing b to  , and proving that it is indeed the committed bit with the evidence in Bob's possession, i. e.  will check the commited bit.

Definition of the problem

- Therefore, Alice and Bob should agree on a protocol which satisfies simultaneously the three requirements:

Definition of the problem

- Therefore, Alice and Bob should agree on a protocol which satisfies simultaneously the three requirements:

(1) The evidence should be *concealing*, namely  should not be able to retrieve b before the opening.

Definition of the problem

- Therefore, Alice and Bob should agree on a protocol which satisfies simultaneously the three requirements:

(1) The evidence should be *concealing*, namely  should not be able to retrieve b before the opening.

(2) The evidence should be *binding*, namely  should not be able to change b after the commitment.

Definition of the problem

- Therefore, Alice and Bob should agree on a protocol which satisfies simultaneously the three requirements:

(1) The evidence should be *concealing*, namely  should not be able to retrieve b before the opening.

(2) The evidence should be *binding*, namely  should not be able to change b after the commitment.

(3) The evidence should be *verifiable*, namely  must be able to check b unambiguously against the evidence in his possession.

Definition of the problem

- Therefore, Alice and Bob should agree on a protocol which satisfies simultaneously the three requirements:

(1) The evidence should be *concealing*, namely  should not be able to retrieve b before the opening.

(2) The evidence should be *binding*, namely  should not be able to change b after the commitment.

(3) The evidence should be *verifiable*, namely  must be able to check b unambiguously against the evidence in his possession.

- Both parties are supposed to possess unlimited technology, and the protocol is said *unconditionally secure* if neither Alice nor Bob can cheat with significant probability of success as a consequence of physical laws.

History

[1984] C. H. Bennet and G. Brassard,

History

[1984] C. H. Bennet and G. Brassard, [1993] G. Brassard, C. Crépeau, R. Jozsa, D. Langlois,

History

[1984] C. H. Bennet and G. Brassard, [1993] G. Brassard, C. Crépeau, R. Jozsa, D. Langlois, [1997] D. Mayers, H. K. Lo, H. F. Chau,

History

[1984] C. H. Bennet

[1993] G. Brassard, C. Crépeau, R. Jozsa, D. Langlois, [1997] D. Mayers, H. K. Lo, H. F. Chau, [2000] H. P. Yuen,

History

[1984] C. H. Bennet [1993] G. Brassard, C. Crépeau, R. Jozsa, D. Langlois, [1997] D. Mayers, H. K. Lo, H. F. Chau, [2000] H. P. Yuen, [2001] C. F. Li and G.-C. Guo, . . .

History

[1984] C. H. Bennet [1993] G. Brassard, C. Crépeau, R. Jozsa, D. Langlois, [1997] D. Mayers, H. K. Lo, H. F. Chau, [2000] H. P. Yuen, [2001] C. F. Li and G.-C. Guo, . . .

Commitment step

Commitment step

-  prepares the Hilbert space H with the anonymous state $|\varphi\rangle \in \mathcal{H}$. He then sends H to  .

Commitment step

-  prepares the Hilbert space H with the anonymous state $|\varphi\rangle \in \mathrm{H}$. He then sends H to  .
-  modulates the value b of the committed bit on the anonymous state $|\varphi\rangle$ and sends the output back to  .

The most general bit modulation

- Bit modulation: QO parametrized by $b = 0, 1$.

The most general bit modulation

- Bit modulation: QO parametrized by $b = 0, 1$.
- To make the protocol concealing and at the same time verifiable, the modulation is a choice between two ensembles of QO's $\{\mathrm{M}_j^{(b)}\}$ for $b = 0, 1$ from $\mathsf{S}(\mathsf{H})$ to $\mathsf{S}(\mathsf{K})$.

The most general bit modulation

- Bit modulation: QO parametrized by $b = 0, 1$.
- To make the protocol concealing and at the same time verifiable, the modulation is a choice between two ensembles of QO's $\{\mathrm{M}_j^{(b)}\}$ for $b = 0, 1$ from $\mathsf{S}(\mathsf{H})$ to $\mathsf{S}(\mathsf{K})$.

– $\mathsf{K} \supseteq \mathsf{H}$: *extending modulation*, (e. g. adding decoy systems).

The most general bit modulation

- Bit modulation: QO parametrized by $b = 0, 1$.
- To make the protocol concealing and at the same time verifiable, the modulation is a choice between two ensembles of QO's $\{\mathrm{M}_j^{(b)}\}$ for $b = 0, 1$ from $\mathsf{S}(\mathsf{H})$ to $\mathsf{S}(\mathsf{K})$.
  - $\mathsf{K} \supseteq \mathsf{H}$: *extending modulation*, (e. g. adding decoy systems).
  - $\mathsf{K} \subseteq \mathsf{H}$: *restricting modulation*

The most general bit modulation

- Bit modulation: QO parametrized by $b = 0, 1$.
- To make the protocol concealing and at the same time verifiable, the modulation is a choice between two ensembles of QO's $\{\mathrm{M}_j^{(b)}\}$ for $b = 0, 1$ from $\mathsf{S}(\mathsf{H})$ to $\mathsf{S}(\mathsf{K})$.

– $\mathsf{K} \supseteq \mathsf{H}$: *extending modulation*, (e. g. adding decoy systems).

– $\mathsf{K} \subseteq \mathsf{H}$: *restricting modulation*

– j: secret parameter known only to  parametrizing the choice of different forms for the modulation.

The space of secret parameters

-  has always the option of choosing j by preparing the secret-parameter space P in the state $|j\rangle$ and performing $\mathbb{M}^{(b)}$ on H $\otimes$ P:

$$\mathbb{M}^{(b)} = \sum_j \mathrm{M}_j^{(b)} \otimes \mathrm{P}_j,$$

where P_j represents the orthonormal projection

$$\mathrm{P}_j(\rho) = |j\rangle\langle j|\rho|j\rangle\langle j|.$$

The space of secret parameters

-  has always the option of choosing j by preparing the secret-parameter space P in the state $|j\rangle$ and performing $\mathbb{M}^{(b)}$ on H $\otimes$ P:

$$\mathbb{M}^{(b)} = \sum_j \mathrm{M}_j^{(b)} \otimes \mathrm{P}_j,$$

where P_j represents the orthonormal projection

$$\mathrm{P}_j(\rho) = |j\rangle\langle j|\rho|j\rangle\langle j|.$$

- The actually performed QO depends on the state preparation ρ_{P} that  choses for the secret-parameter space P:

$$\mathrm{Tr}_{\mathsf{P}}[\mathbb{M}^{(b)}(\,|\varphi\rangle\langle\varphi| \otimes \rho_{\mathsf{P}}^{(b)})] = \sum_j \mathrm{M}_j^{(b)}(|\varphi\rangle\langle\varphi|)\,\underbrace{\langle j|\rho_{\mathsf{P}}^{(b)}|j\rangle}_{p_j^{(b)}}.$$

Reduction to trace-preserving

- The quantum operations $\mathrm{M}_j^{(b)}$ are generally trace-decreasing, i. e. they may be achieved with nonunit probability.

Reduction to trace-preserving

- The quantum operations $\mathrm{M}_j^{(b)}$ are generally trace-decreasing, i. e. they may be achieved with nonunit probability.
- In terms of the Kraus decomposition

$$\mathrm{M}_j^{(b)}(\rho) = \sum_i E_{ji}^{(b)} \rho E_{ji}^{(b)\dagger},$$

this means that

$$\sum_i E_{ji}^{(b)\dagger} E_{ji}^{(b)} \leq I.$$

Reduction to trace-preserving

- The quantum operations $\mathrm{M}_j^{(b)}$ are generally trace-decreasing, i. e. they may be achieved with nonunit probability.
- In terms of the Kraus decomposition

$$\mathrm{M}_j^{(b)}(\rho) = \sum_i E_{ji}^{(b)} \rho E_{ji}^{(b)\dagger},$$

this means that

$$\sum_i E_{ji}^{(b)\dagger} E_{ji}^{(b)} \leq I.$$

- When  doesn't succeed in achieving the map, the protocol is aborted. Abortion must be declared by  !

Reduction to trace-preserving

- The quantum operations $\mathrm{M}_j^{(b)}$ are generally trace-decreasing, i. e. they may be achieved with nonunit probability.
- In terms of the Kraus decomposition

$$\mathrm{M}_j^{(b)}(\rho) = \sum_i E_{ji}^{(b)} \rho E_{ji}^{(b)\dagger},$$

this means that

$$\sum_i E_{ji}^{(b)\dagger} E_{ji}^{(b)} \leq I.$$

- When  doesn't succeed in achieving the map, the protocol is aborted. Abortion must be declared by  !
- A trace decreasing map is equivalent to a trace preserving one with additional "outcomes" i.

Reduction to unitary

-  has unlimited technology,

Reduction to unitary

-  has unlimited technology, whence she can always achieve $E_{ji}^{(b)}$ knowingly,

Reduction to unitary

-  has unlimited technology, whence she can always achieve $E^{(b)}_{ji}$ knowingly, i. e. she has the option of achieving each trace-preserving map $\mathrm{M}^{(b)}_j$ as a perfect pure measurement.

Reduction to unitary

-  has unlimited technology, whence she can always achieve $E_{ji}^{(b)}$ knowingly, i. e. she has the option of achieving each trace-preserving map $\mathrm{M}_j^{(b)}$ as a perfect pure measurement.
- This can be done as follows

  (in the following we will temporarily drop the indices b and j).

Reduction to unitary

- A trace-preserving QO can be written in the form

$$\mathrm{M}(\rho) = \mathrm{Tr}_{\mathsf{F}}[E\rho E^\dagger], \quad E = \sum_i E_i \otimes |i\rangle \in \mathsf{B}(\mathsf{H}, \mathsf{K} \otimes \mathsf{F}) \text{ isometry.}$$

Reduction to unitary

- A trace-preserving QO can be written in the form

$$\mathrm{M}(\rho) = \mathrm{Tr}_{\mathsf{F}}[E\rho E^\dagger], \quad E = \sum_i E_i \otimes |i\rangle \in \mathsf{B}(\mathsf{H}, \mathsf{K} \otimes \mathsf{F}) \text{ isometry.}$$

- Unitary embedding of H into $\mathsf{K} \otimes \mathsf{F} \simeq \mathsf{H} \otimes \mathsf{A}$:

$$E = U(I_{\mathsf{H}} \otimes |\omega\rangle_{\mathsf{A}}),$$

Reduction to unitary

- A trace-preserving QO can be written in the form

$$\mathrm{M}(\rho) = \mathrm{Tr}_{\mathsf{F}}[E\rho E^\dagger], \quad E = \sum_i E_i \otimes |i\rangle \in \mathsf{B}(\mathsf{H}, \mathsf{K} \otimes \mathsf{F}) \text{ isometry.}$$

- Unitary embedding of H into $\mathsf{K} \otimes \mathsf{F} \simeq \mathsf{H} \otimes \mathsf{A}$:

$$E = U(I_{\mathsf{H}} \otimes |\omega\rangle_{\mathsf{A}}),$$

- we have

$$\mathrm{M}(\rho) = \mathrm{Tr}_{\mathsf{F}}[U(\rho \otimes |\omega\rangle\langle\omega|_{\mathsf{A}})U^\dagger],$$

Reduction to unitary

- Therefore  achieves the trace-preserving QO $\mathrm{M}(\rho) = \sum_i E_i \rho E_i^\dagger$ knowingly by:

Reduction to unitary

- Therefore  achieves the trace-preserving QO $\mathrm{M}(\rho) = \sum_i E_i \rho E_i^\dagger$ knowingly by:

(1) preparing an ancilla/decoy state $|\omega\rangle_{\mathsf{A}} \in \mathsf{A}$,

Reduction to unitary

- Therefore  achieves the trace-preserving QO $\mathrm{M}(\rho) = \sum_i E_i \rho E_i^\dagger$ knowingly by:

(1) preparing an ancilla/decoy state $|\omega\rangle_{\mathsf{A}} \in \mathsf{A}$,

(2) performing a unitary transformation U on $\mathsf{H} \otimes \mathsf{A}$,

Reduction to unitary

- Therefore  achieves the trace-preserving QO $\mathrm{M}(\rho) = \sum_i E_i \rho E_i^\dagger$ knowingly by:

(1) preparing an ancilla/decoy state $|\omega\rangle_{\mathsf{A}} \in \mathsf{A}$,

(2) performing a unitary transformation U on $\mathsf{H} \otimes \mathsf{A}$,

(3) performing a complete von Neumann measurement on F, with $\mathsf{K} \otimes \mathsf{F} \simeq \mathsf{H} \otimes \mathsf{A}$ and outcome i,

Reduction to unitary

- Therefore  achieves the trace-preserving QO $\mathrm{M}(\rho) = \sum_i E_i \rho E_i^\dagger$ knowingly by:

(1) preparing an ancilla/decoy state $|\omega\rangle_{\mathsf{A}} \in \mathsf{A}$,

(2) performing a unitary transformation U on $\mathsf{H} \otimes \mathsf{A}$,

(3) performing a complete von Neumann measurement on F, with $\mathsf{K} \otimes \mathsf{F} \simeq \mathsf{H} \otimes \mathsf{A}$ and outcome i,

(4) sending K to  .

Reduction to unitary

- Therefore  achieves the trace-preserving QO $\mathrm{M}(\rho) = \sum_i E_i \rho E_i^\dagger$ knowingly by:

(1) preparing an ancilla/decoy state $|\omega\rangle_{\mathsf{A}} \in \mathsf{A}$,

(2) performing a unitary transformation U on $\mathsf{H} \otimes \mathsf{A}$,

(3) performing a complete von Neumann measurement on F, with $\mathsf{K} \otimes \mathsf{F} \simeq \mathsf{H} \otimes \mathsf{A}$ and outcome i,

(4) sending K to  .

- Notice that we can have both situations $\mathsf{H} \subseteq \mathsf{K}$ and $\mathsf{H} \supseteq \mathsf{K}$, depending on the choice of A and F.

The BIG unitary

- Now, if we consider also the preparation of the secret parameter space P, the bit commitment step can be achieved as follows:

$$\sum_j p_j^{(b)} \mathrm{M}_j^{(b)}(|\varphi\rangle\langle\varphi|) = \sum_j p_j^{(b)} E_{ji}^{(b)} |\varphi\rangle\langle\varphi| E_{ji}^{(b)\dagger}$$

$$= \sum_j p_j^{(b)} \mathrm{Tr}_{\mathsf{F}}[U_j^{(b)}(|\varphi\rangle\langle\varphi| \otimes |\omega\rangle\langle\omega|_{\mathsf{A}})U_j^{(b)\dagger}] =$$

The BIG unitary

- Now, if we consider also the preparation of the secret parameter space P, the bit commitment step can be achieved as follows:

$$\sum_j p_j^{(b)} \mathrm{M}_j^{(b)}(|\varphi\rangle\langle\varphi|) = \sum_j p_j^{(b)} E_{ji}^{(b)} |\varphi\rangle\langle\varphi| E_{ji}^{(b)\dagger}$$

$$= \sum_j p_j^{(b)} \mathrm{Tr}_{\mathsf{F}}[U_j^{(b)}(|\varphi\rangle\langle\varphi| \otimes |\omega\rangle\langle\omega|_{\mathsf{A}}) U_j^{(b)\dagger}] =$$

$$= \mathrm{Tr}_{\mathsf{F}\otimes\mathsf{P}}[U^{(b)}(|\varphi\rangle\langle\varphi| \otimes |\omega\rangle\langle\omega|_{\mathsf{A}} \otimes \rho_{\mathsf{P}}) U^{(b)\dagger}],$$

The BIG unitary

- Now, if we consider also the preparation of the secret parameter space P, the bit commitment step can be achieved as follows:

$$\sum_j p_j^{(b)} \mathrm{M}_j^{(b)}(|\varphi\rangle\langle\varphi|) = \sum_j p_j^{(b)} E_{ji}^{(b)} |\varphi\rangle\langle\varphi| E_{ji}^{(b)\dagger}$$

$$= \sum_j p_j^{(b)} \operatorname{Tr}_{\mathsf{F}}[U_j^{(b)}(|\varphi\rangle\langle\varphi| \otimes |\omega\rangle\langle\omega|_{\mathsf{A}})U_j^{(b)\dagger}] =$$

$$= \operatorname{Tr}_{\mathsf{F}\otimes\mathsf{P}}[U^{(b)}(|\varphi\rangle\langle\varphi| \otimes |\omega\rangle\langle\omega|_{\mathsf{A}} \otimes \rho_{\mathsf{P}})U^{(b)\dagger}],$$

- where $|\omega\rangle_{\mathsf{A}}$ and ρ_{P} are independent on j and b, and

$$U^{(b)} = \sum_j U_j^{(b)} \otimes |j\rangle\langle j| \quad \text{unitary over } \mathsf{H} \otimes \mathsf{A} \otimes \mathsf{P} \simeq \mathsf{K} \otimes \mathsf{F} \otimes \mathsf{P}.$$

The BIG unitary

- However, for aborting protocols we have:

$$\sum_j p_j^{(b)} \mathrm{M}_j^{(b)}(|\varphi\rangle\langle\varphi|)$$
$$= \sum_j p_j^{(b)} \,\mathrm{Tr}_{\mathsf{F}}[(I_{\mathsf{K}} \otimes \Sigma_{j\mathsf{F}}^{(b)})U_j^{(b)}(|\varphi\rangle\langle\varphi| \otimes |\omega\rangle\langle\omega|_{\mathsf{A}})U_j^{(b)\dagger}],$$

where $\Sigma_{j\mathsf{F}}^{(b)}$ denotes an orthonogonal projector on a subspace of F, whose rank generally depends on j and b.

The BIG unitary

- However, for aborting protocols we have:

$$\sum_j p_j^{(b)} \mathrm{M}_j^{(b)}(|\varphi\rangle\langle\varphi|)$$
$$= \sum_j p_j^{(b)} \,\mathrm{Tr}_{\mathsf{F}}[(I_{\mathsf{K}} \otimes \Sigma_{j\mathsf{F}}^{(b)}) U_j^{(b)} (|\varphi\rangle\langle\varphi| \otimes |\omega\rangle\langle\omega|_{\mathsf{A}}) U_j^{(b)\dagger}],$$

  where $\Sigma_{j\mathsf{F}}^{(b)}$ denotes an orthonogonal projector on a subspace of F, whose rank generally depends on j and b.

- From now we focus attention on the simplest case of non aborting protocols.

Opening step

- In a perfectly verifiable protocol  tells b along with the secret parameter j and the secret outcome i to , who verifies the pure state $E_{ji}^{(b)}|\varphi\rangle$.

Opening step

- In a perfectly verifiable protocol  tells b along with the secret parameter j and the secret outcome i to  , who verifies the pure state $E_{ji}^{(b)}|\varphi\rangle$.

- However, since the local QO's on K and F $\otimes$ P commute,  has the possibility of: (1) first sending K to  ; (2) then performing the measurement on F $\otimes$ P at the very last moment of the opening. This is the basis of the EPR cheating attack!

Opening step

- In a perfectly verifiable protocol  tells b along with the secret parameter j and the secret outcome i to  , who verifies the pure state $E_{ji}^{(b)}|\varphi\rangle$.
- However, since the local QO's on K and F $\otimes$ P commute,  has the possibility of: (1) first sending K to  ; (2) then performing the measurement on F $\otimes$ P at the very last moment of the opening. This is the basis of the EPR cheating attack!
- However, strictly trace-decreasing QO—i. e. aborting protocols—pose limitations to Alice's EPR cheating, since Alice cannot delay the abortion of the protocol up to the opening, but she must declare it at the commitment.

Simplifying

- Since both secret parameters j and i can be conveniently measured by , they can be treated on equal footings as a single parameter $J \equiv (j, i)$.

Simplifying

- Since both secret parameters j and i can be conveniently measured by  , they can be treated on equal footings as a single parameter $J \equiv (j, i)$.
- The two maps are then:

$$\sum_j p_j^{(b)} \mathrm{M}_j^{(b)}(|\varphi\rangle\langle\varphi|) = \sum_J E_J^{(b)} |\varphi\rangle\langle\varphi| E_J^{(b)\dagger},$$

where $E_J^{(b)} \doteq \sqrt{p_j^{(b)}} E_{ji} \in \mathsf{B}(\mathsf{H}, \mathsf{K})$.

The principle of *delayed reading*

- For non aborting protocols we can reduce a multistep commitment to a single step one, using the principle of delayed reading.

The principle of *delayed reading*

- For non aborting protocols we can reduce a multistep commitment to a single step one, using the principle of delayed reading.
- Principle: Any conditioned QO on H can be regarded as unconditioned on $H \otimes N$ followed by a measurement on N.

The principle of *delayed reading*

- For non aborting protocols we can reduce a multistep commitment to a single step one, using the principle of delayed reading.
- Principle: Any conditioned QO on H can be regarded as unconditioned on H $\otimes$ N <u>followed</u> by a measurement on N.

1) Bob is requested to make a different QO, say $\{\mathrm{N}^{(x)}\}$, depending on the outcome x of previous Alice's QO.

The principle of *delayed reading*

- For non aborting protocols we can reduce a multistep commitment to a single step one, using the principle of delayed reading.
- Principle: Any conditioned QO on H can be regarded as unconditioned on H $\otimes$ N followed by a measurement on N.

1) Bob is requested to make a different QO, say $\{\mathrm{N}^{(x)}\}$, depending on the outcome x of previous Alice's QO.

2) Bob instead automatizes the conditioned QO, using the un-conditioned one on H $\otimes$ N:

$$\mathbb{N} = \sum_x \mathrm{N}^{(x)} \otimes |x\rangle\langle x|$$

The principle of *delayed reading*

- For non aborting protocols we can reduce a multistep commitment to a single step one, using the principle of delayed reading.
- Principle: Any conditioned QO on H can be regarded as unconditioned on H $\otimes$ N followed by a measurement on N.

1) Bob is requested to make a different QO, say $\{\mathrm{N}^{(x)}\}$, depending on the outcome x of previous Alice's QO.

2) Bob instead automatizes the conditioned QO, using the un-conditioned one on H $\otimes$ N:

$$\mathbb{N} = \sum_x \mathrm{N}^{(x)} \otimes |x\rangle\langle x|$$

3) When Bob will measure N, the actual QO $\mathrm{N}^{(x)}$ will result.

Reduction to one commitment step

- If the knowledge of x is needed only at the opening (non aborting protocols), then the measurement $|x\rangle\langle x|$ can be delayed up to then.

Reduction to one commitment step

- If the knowledge of x is needed only at the opening (non aborting protocols), then the measurement $|x\rangle\langle x|$ can be delayed up to then.
- Again, each QO can be achieved *knowingly*, by means of a pure measurement.

Reduction to one commitment step

- If the knowledge of x is needed only at the opening (non aborting protocols), then the measurement $|x\rangle\langle x|$ can be delayed up to then.
- Again, each QO can be achieved *knowingly*, by means of a pure measurement.
- In this way we have a sequence of interlaced unitary operators, say $\ldots U'^{(b)}_A U_B U^{(b)}_A$.

Reduction to one commitment step

- If the knowledge of x is needed only at the opening (non aborting protocols), then the measurement $|x\rangle\langle x|$ can be delayed up to then.
- Again, each QO can be achieved *knowingly*, by means of a pure measurement.
- In this way we have a sequence of interlaced unitary operators, say $\ldots U'^{(b)}_A U_B U^{(b)}_A$.
- For $U_B \in \{U_l\}$, Bob can use instead the unitary $\mathbb{U}_B = \sum_l U_l \otimes |l\rangle\langle l|$. This is equivalent to another anonymous-state preparation.

Reduction to one commitment step

- If the knowledge of x is needed only at the opening (non aborting protocols), then the measurement $|x\rangle\langle x|$ can be delayed up to then.
- Again, each QO can be achieved *knowingly*, by means of a pure measurement.
- In this way we have a sequence of interlaced unitary operators, say $\ldots U'^{(b)}_A U_B U^{(b)}_A$.
- For $U_B \in \{U_l\}$, Bob can use instead the unitary $\mathbb{U}_B = \sum_l U_l \otimes |l\rangle\langle l|$. This is equivalent to another anonymous-state preparation.
- In conclusion, the whole multi-step protocol is equivalent to a single-step one, with larger spaces H, K, A, F, and P.

Commitment: summary

- Classification of protocols $\equiv$ classifications of QO extensions

Commitment: summary

- Classification of protocols $\equiv$ classifications of QO extensions

Symbol	Hilbert space	Symbol	Hilbert space
H	Anonymous state	K	Output
A	Preparation ancilla/decoy	P	Secret parameter
F	Measurement ancilla	R	Bob cheating space
$\mathrm{Rng}(\Sigma)$	Range of Σ (abortion)		

Commitment: summary

- Classification of protocols $\equiv$ classifications of QO extensions

Symbol	Hilbert space	Symbol	Hilbert space
H	Anonymous state	K	Output
A	Preparation ancilla/decoy	P	Secret parameter
F	Measurement ancilla	R	Bob cheating space
$\mathrm{Rng}(\Sigma)$	Range of Σ (abortion)		

The Church of Larger Hilbert Space!

Cheating!

-  Pre and post-cheating

Cheating!

-  Pre and post-cheating

- post-cheating:  can try to cheat by performing a unitary V on F $\otimes$ P. This will not change the QO, however, it changes the Kraus decomposition:

Cheating!

-  Pre and post-cheating

- post-cheating:  can try to cheat by performing a unitary V on F $\otimes$ P. This will not change the QO, however, it changes the Kraus decomposition:

  $\{E_J^{(b)}\} \rightarrow \{E_J^{(b)}(V)\}$ (same cardinality)

Cheating!

-  Pre and post-cheating

- post-cheating:  can try to cheat by performing a unitary V on F $\otimes$ P. This will not change the QO, however, it changes the Kraus decomposition:

  $\{E_J^{(b)}\} \to \{E_J^{(b)}(V)\}$ (same cardinality)

- with

$$E_J^{(b)}(V) = \sum_L E_L^{(b)} V_{LJ}, \qquad V_{LJ} = \langle L|V|J\rangle.$$

Cheating!

- The probability that  can cheat successfully in pretending having committed $b = 1$, whereas she committed $b = 0$ instead, is given by

$$\overline{P_c^A} = \max_V \int \mathrm{d}\,\mu(\varphi) P_c^A(V, \varphi),$$

Cheating!

- The probability that  can cheat successfully in pretending having committed $b = 1$, whereas she committed $b = 0$ instead, is given by

$$\overline{P_c^A} = \max_V \int \mathrm{d}\,\mu(\varphi) P_c^A(V, \varphi),$$

where

$$P_c^A(V, \varphi) = \sum_J \frac{|\langle \varphi | E_J^{(0)}(V)^\dagger E_J^{(1)} |\varphi\rangle|^2}{\left\| E_J^{(1)} \varphi \right\|^2}.$$

Cheating!

-  can try to cheat by making the best discrimination between the two maps $\mathrm{M}^{(b)} = \sum_j p_j^{(b)} \mathrm{M}_j^{(b)}$.

Cheating!

-  can try to cheat by making the best discrimination between the two maps $\mathrm{M}^{(b)} = \sum_j p_j^{(b)} \mathrm{M}_j^{(b)}$.
- Instead of preparing $|\varphi\rangle \in$ H  prepares an entangled state $|\varphi\rangle \in$ H $\otimes$ R and sends only H to  .

Cheating!

-  can try to cheat by making the best discrimination between the two maps $\mathrm{M}^{(b)} = \sum_j p_j^{(b)} \mathrm{M}_j^{(b)}$.

- Instead of preparing $|\varphi\rangle \in \mathsf{H}$  prepares an entangled state $|\varphi\rangle \in \mathsf{H} \otimes \mathsf{R}$ and sends only H to  .

- Cheating probability

$$P_c^B - \frac{1}{2} \leq \max_{|\varphi\rangle \in \mathsf{H} \otimes \mathsf{R}} \frac{1}{4} \left\| [\mathrm{M}^{(1)} - \mathrm{M}^{(0)}] \otimes \mathrm{I}_{\mathsf{R}}(|\varphi\rangle\langle\varphi|) \right\|_1 \leq \frac{1}{4} \left\| \mathrm{M}^{(1)} - \mathrm{M}^{(0)} \right\|_{cb}$$

Perfectly concealing protocols

$$\left\| \mathrm{M}^{(1)} - \mathrm{M}^{(0)} \right\|_{cb} = 0.$$

- Then one has $\mathrm{M}^{(1)} = \mathrm{M}^{(0)}$! Therefore, the two Kraus are connected via a unitary transformation V on F $\otimes$ P.

Perfectly concealing protocols

$$\left\| \mathrm{M}^{(1)} - \mathrm{M}^{(0)} \right\|_{cb} = 0.$$

- Then one has $\mathrm{M}^{(1)} = \mathrm{M}^{(0)}$! Therefore, the two Kraus are connected via a unitary transformation V on $\mathrm{F} \otimes \mathrm{P}$.
- It follows that  can cheat with probability one!

Perfectly concealing protocols

$$\left\| \mathrm{M}^{(1)} - \mathrm{M}^{(0)} \right\|_{cb} = 0.$$

- Then one has $\mathrm{M}^{(1)} = \mathrm{M}^{(0)}$! Therefore, the two Kraus are connected via a unitary transformation V on F $\otimes$ P.
- It follows that  can cheat with probability one!
- The protocol is not binding!

Approximate concealing

$$\left\| \mathrm{M}^{(1)} - \mathrm{M}^{(0)} \right\|_{cb} = \varepsilon,$$

- where generally ε infinitesimal with $\dim(\mathrm{K})^{-1}$.

Approximate concealing

$$\left\| \mathrm{M}^{(1)} - \mathrm{M}^{(0)} \right\|_{cb} = \varepsilon,$$

- where generally ε infinitesimal with $\dim(\mathsf{K})^{-1}$.
- Problem: is it true that then $1 - \overline{P_c^A}$ is infinitesimal with ε?

Approximate concealing

$$\left\| \mathrm{M}^{(1)} - \mathrm{M}^{(0)} \right\|_{cb} = \varepsilon,$$

- where generally ε infinitesimal with $\dim(\mathrm{K})^{-1}$.
- Problem: is it true that then $1 - \overline{P_c^A}$ is infinitesimal with ε?
- A affermative answer would provide the impossibility proof for non aborting protocols.

Bounds for cheating probabilities

$$P_c^A(V,\varphi) \geq \sqrt{1 - \sum_J \left\| E_J^{(0)}(V) - E_J^{(1)} \right\|^2},$$

$$\left\| \mathrm{M}^{(1)} - \mathrm{M}^{(0)} \right\|_{cb} \leq \sqrt{\sum_J \left\| E_J^{(0)}(V) - E_J^{(1)} \right\|^2}.$$

Bounds for cheating probabilities

$$P_c^A(V,\varphi) \geq \sqrt{1 - \sum_J \left\| E_J^{(0)}(V) - E_J^{(1)} \right\|^2},$$

$$\left\| \mathrm{M}^{(1)} - \mathrm{M}^{(0)} \right\|_{cb} \leq \sqrt{\sum_J \left\| E_J^{(0)}(V) - E_J^{(1)} \right\|^2}.$$

- However, is it true that there is a V such that

$$\sum_J \left\| E_J^{(0)}(V) - E_J^{(1)} \right\|^2 \leq \omega \left(\left\| \mathrm{M}^{(1)} - \mathrm{M}^{(0)} \right\|_{cb} \right),$$

with $\omega(\varepsilon)$ vanishing with ε?

Bounds for cheating probabilities

- For $\mathrm{M}^{(1)}$ random unitary, i. e. $E_J^{(1)} = \sqrt{p_J^{(1)}} U_J^{(1)}$ we have $[d = \dim(\mathsf{H})]$

$$\overline{P_c^A} = \frac{1}{d+1} + \frac{1}{d(d+1)} \max_V \sum_J \left| \sum_L \mathrm{Tr}\left(U_J^{(1)\dagger} E_L^{(0)} \right) V_{JL} \right|^2 .$$

Bounds for cheating probabilities

- For $\mathrm{M}^{(1)}$ random unitary, i. e. $E_J^{(1)} = \sqrt{p_J^{(1)}} U_J^{(1)}$ we have $[d = \dim(\mathsf{H})]$

$$\overline{P_c^A} = \frac{1}{d+1} + \frac{1}{d(d+1)} \max_V \sum_J \left| \sum_L \mathrm{Tr}\left(U_J^{(1)\dagger} E_L^{(0)} \right) V_{JL} \right|^2 .$$

- An upper bound is given by

$$\frac{1}{d+1} \leq \overline{P_c^A} \leq \frac{1}{d+1} + \frac{1}{d(d+1)} \left\| \mathbb{Z} \right\|_1 ,$$

$$\mathbb{Z}_{(JL)K} = \mathrm{Tr}[U_K^{(1)\dagger} E_J^{(0)}]\, \mathrm{Tr}[U_K^{(1)} E_L^{(0)\dagger}]$$

Conclusion

Conclusion

- There is no general impossibility proof.

Conclusion

- There is no general impossibility proof.
- From the general classification we still don't know if there are proved secure protocols.

Conclusion

- There is no general impossibility proof.
- From the general classification we still don't know if there are proved secure protocols.
- Bound for cheating probabilities such that:

Conclusion

- There is no general impossibility proof.
- From the general classification we still don't know if there are proved secure protocols.
- Bound for cheating probabilities such that:

⇒ if violated for all choices of $\{p_j^{(b)}\}$, it will provide a secure perfect-verification non-aborting protocol;

Conclusion

- There is no general impossibility proof.
- From the general classification we still don't know if there are proved secure protocols.
- Bound for cheating probabilities such that:

$\Rightarrow$ if violated for all choices of $\{p_j^{(b)}\}$, it will provide a secure perfect-verification non-aborting protocol;

$\Rightarrow$ if proved always valid, it would provide an impossibility proof for non-aborting perfect-verification protocols, but we still may have unconditionally secure protocols in the complementary class, e. g. for aborting protocols.

Missed things in the imp. proof

(1) The bit is encoded on maps instead of states.

Missed things in the imp. proof

(1) The bit is encoded on maps instead of states.

(2) The spaces H and K are not isomorphic.

Missed things in the imp. proof

(1) The bit is encoded on maps instead of states.

(2) The spaces H and K are not isomorphic.

(3) There are aborting protocols: this limits  EPR cheating.

Missed things in the imp. proof

(1) The bit is encoded on maps instead of states.

(2) The spaces H and K are not isomorphic.

(3) There are aborting protocols: this limits  EPR cheating.

(4)  probability of cheating <u>is not</u> a fidelity.

Missed things in the imp. proof

(1) The bit is encoded on maps instead of states.

(2) The spaces H and K are not isomorphic.

(3) There are aborting protocols: this limits  EPR cheating.

(4)  probability of cheating is not a fidelity.

(5) There is no proved continuity argument between concealing and binding.

Missed things in the imp. proof

(1) The bit is encoded on maps instead of states.

(2) The spaces H and K are not isomorphic.

(3) There are aborting protocols: this limits  EPR cheating.

(4)  probability of cheating <u>is not</u> a fidelity.

(5) There is no proved continuity argument between concealing and binding.

(6) No probability can be assumed for any secret parameter.

Missed things in the imp. proof

(1) The bit is encoded on maps instead of states.

(2) The spaces H and K are not isomorphic.

(3) There are aborting protocols: this limits  EPR cheating.

(4)  probability of cheating <u>is not</u> a fidelity.

(5) There is no proved continuity argument between concealing and binding.

(6) No probability can be assumed for any secret parameter.

(7) Reduction to a single step holds only for non aborting protocols.

Missed things in the imp. proof

(1) The bit is encoded on maps instead of states.

(2) The spaces H and K are not isomorphic.

(3) There are aborting protocols: this limits  EPR cheating.

(4)  probability of cheating is not a fidelity.

(5) There is no proved continuity argument between concealing and binding.

(6) No probability can be assumed for any secret parameter.

(7) Reduction to a single step holds only for non aborting protocols.

(8) . . .