Title: A New Protocol for Loss-Tolerant Quantum Coin Tossing

Date: Jun 01, 2007 03:20 PM

URL: http://pirsa.org/07060005

Abstract: Quantum coin tossing is a cryptographic task in which two parties, Alice and Bob, wish to generate a shared random bit but do not necessarily trust each other. This task is completely impossible to realize with classical asynchronous communication but becomes at least partially feasible when quantum communication is also available. The best quantum protocol known so far, due to Ambainis, uses qutrits and is near optimal in the sense that either party can bias the outcome with at most a 75% probability of success. However, when the transmission of the link is below 50%, Ambainis' protocol can be easily broken by a cheating Bob. This problem arises whenever there exists a conclusive measurement allowing Bob to obtain with certainty, although with a probability less than one, relevant information about the state sent by Alice. In this talk, we will present a new protocol for quantum coin tossing that does not suffer from this weakness and, as a consequence, is loss-tolerant. We discuss possible attacks and argue that the protocol is secure. Technologically, the implementation of this protocol is no more difficult than implementing entangled quantum key distribution with qubits. This is joint work with Guido Berlin, Gilles Brassard and Nicolas Godbout.

A New Protocol for Loss-Tolerant Quantum Coin Tossing

Guido Berlin, Gilles Brassard, **Félix Bussières** and Nicolas Godbout

Ph.D. Student
felix.bussieres@polymtl.ca

Centre d'optique, photonique et laser and Laboratoire des fibres optiques
École Polytechnique de Montréal
Laboratoire d'informatique théorique et quantique
Université de Montréal

Fourth Canadian Quantum Information Students' Conference
University of Waterloo / Perimeter Institute
June 2007

Overview

1. Introduction : BB84 and Ambainis' protocols
2. A New Loss-Tolerant Protocol
3. Concluding remarks and future work

Coin-tossing (flipping) is a cryptographic primitive

COIN FLIPPING BY TELEPHONE:
A Protocol for Solving Impossible Problems

Manuel Blum*

Department of Electrical Engineering and Computer Sciences
Computer Science Division
University of California at Berkeley
November 10, 1981

Coin-tossing is a cryptographic primitive

Abstract

Alice and Bob want to flip a coin by telephone. (They have just divorced, live in different cities, want to decide who gets the car.) Bob would not like to tell Alice HEADS and hear Alice (at the other end of the line) say "Here goes... I'm flipping the coin.... You lost!"

Coin-tossing (flipping) is a cryptographic primitive

> Coin-flipping in the SPECIAL way done here has a serious purpose. Indeed, it should prove an INDISPENSABLE TOOL of the protocol designer. Whenever a protocol requires one of two adversaries, say Alice, to pick a sequence of bits at random, and whenever it serves Alice's interests best NOT to pick her sequence of bits at random, then coin-flipping (Bob flipping coins to Alice) as defined here achieves the desired goal:

In other words, we want to force **Alice' and Bob's answer to contain a certain degree of randomness**, ideally complete randomness, to prevent one of them to determine the outcome of the coin-toss with certainty.

Coin-tossing (flipping) is a cryptographic primitive

> Coin-flipping has already proved useful in solving a number of problems once thought impossible: mental poker, certified mail, and exchange of secrets. It will certainly prove a useful tool in solving other problems as well.

These tasks have the common goal of **realizing a bipartite cryptographic task, possibly comprising one dishonest player, without the need for a trusted third party.**

Classically : Coin-Tossing is secure only under unproven computational assumptions (like factoring is hard) or under relativistic configurations (that can be unpractical). Otherwise, a dishonest player can win anytime.

Interestingly, Quantum mechanics succeeds where classical physics doesn't!

Coin-tossing (flipping) is a cryptographic primitive

> Coin-flipping has already proved useful in solving a number of problems once thought impossible: mental poker, certified mail, and exchange of secrets. It will certainly prove a useful tool in solving other problems as well.

These tasks have the common goal of **realizing a bipartite cryptographic task, possibly comprising one dishonest player, without the need for a trusted third party.**

Classically : Coin-Tossing is secure only under unproven computational assumptions (like factoring is hard) or under relativistic configurations (that can be unpractical). **Otherwise, a dishonest player can win anytime.**

Interestingly, Quantum mechanics succeeds where classical physics doesn't!

Coin-tossing (flipping) is a cryptographic primitive

> Coin-flipping has already proved useful in solving a number of problems once thought impossible: mental poker, certified mail, and exchange of secrets. It will certainly prove a useful tool in solving other problems as well.

These tasks have the common goal of **realizing a bipartite cryptographic task, possibly comprising one dishonest player, without the need for a trusted third party.**

Classically : Coin-Tossing is secure only under unproven computational assumptions (like factoring is hard) or under relativistic configurations (that can be unpractical). **Otherwise, a dishonest player can win anytime.**

Interestingly, **Quantum mechanics** succeeds where classical physics doesn't !

BB84 Quantum Coin-Tossing

To get an idea of what's possible and what's not, we first describe the BB84 Coin-Tossing protocol which can be **broken by a dishonest Alice by using entanglement**.

Excerpt of the BB84 paper :

> tially. We also present a protocol for coin-tossing by exchange of quantum messages, which is secure against traditional kinds of cheating, even by an opponent with unlimited computing power, but ironically can be subverted by use of a still subtler quantum phenomemon, the Einstein-Podolsky-Rosen paradox.

Charles H. Bennett and Gilles Brassard,
Quantum cryptography : public key distribution and coin tossing,
Proc. of the IEEE Int. conf. on Computers, Systems & Signal Processing, Bangalore, India, 1984, pp. 175.

BB84 Quantum Coin-Tossing

$|\psi_x\rangle$ → Bob measures

x' chosen randomly ←

Classical description of $|\psi_x\rangle$ → Bob tries to verify if Alice is honest

Coin toss result $x \oplus x'$

BB84 Quantum Coin-Tossing

BB84 Set

$$\left.\begin{aligned} |\psi_{0,0}\rangle &= |0\rangle \\ |\psi_{0,1}\rangle &= |1\rangle \end{aligned}\right\} x = 0$$

$$\left.\begin{aligned} |\psi_{1,0}\rangle &= |+\rangle \\ |\psi_{1,1}\rangle &= |-\rangle \end{aligned}\right\} x = 1$$

$|\psi_{x,b}\rangle$ chosen randomly →

Bob measures in the rectilinear or diagonal basis

← x' chosen randomly

$x\ ,\ b$ →

Bob can verify if Alice is honest only when the received state is coherent with his measurement basis

Coin toss result $x \oplus x'$

BB84 Quantum Coin-Tossing

BB84 Set

$$\left.\begin{aligned}|\psi_{0,0}\rangle &= |0\rangle \\ |\psi_{0,1}\rangle &= |1\rangle\end{aligned}\right\} x=0 \qquad \left.\begin{aligned}|\psi_{1,0}\rangle &= |+\rangle \\ |\psi_{1,1}\rangle &= |-\rangle\end{aligned}\right\} x=1$$

$$\rho_0 = \tfrac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$$
$$\rho_1 = \tfrac{1}{2}(|+\rangle\langle +| + |-\rangle\langle -|)$$
$$\rho_0 = \rho_1$$ Bob can't cheat at all!

$|\psi_{x,b}\rangle$ chosen randomly →

Bob measures in the rectilinear or diagonal basis

← x' chosen randomly

$x\ ,\ b$ →

Bob can verify if Alice is honest only when the received state is coherent with his measurement basis

Coin toss result $x \oplus x'$

BB84 Quantum Coin-Tossing

BB84 Set

$$\left.\begin{aligned}|\psi_{0,0}\rangle &= |0\rangle\\ |\psi_{0,1}\rangle &= |1\rangle\end{aligned}\right\} x=0 \qquad \left.\begin{aligned}|\psi_{1,0}\rangle &= |+\rangle\\ |\psi_{1,1}\rangle &= |-\rangle\end{aligned}\right\} x=1$$

$$\rho_0 = \tfrac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$$
$$\rho_1 = \tfrac{1}{2}(|+\rangle\langle +| + |-\rangle\langle -|)$$
$$\rho_0 = \rho_1$$ Bob can't cheat at all!

But Alice can break the protocol using entanglement

$|\psi_{x,b}\rangle$ chosen randomly →

Bob measures in the rectilinear or diagonal basis

← x' chosen randomly

$x\ ,\ b$ →

Bob can verify if Alice is honest only when the received state is coherent with his measurement basis

Coin toss result $x \oplus x'$

Breaking BB84 Coin-Toss protocol with entanglement

- Alice sends one half of $|00\rangle + |11\rangle$ to Bob.
- Bob measures in a secret basis and declares x' randomly.
- Alice measures in the basis x that would make her win the coin-toss.
- Alice declares x and the b she measured.
- Because $|00\rangle + |11\rangle = |++\rangle + |--\rangle$, whenever Alice and Bob measured in the same basis their measurement results are the same, hence **Alice is never caught cheating and can always declare the x that makes her win.**

This is always possible when the 2 choices of Alice produces 2 density matrices ρ_0 and ρ_1 that are identical at Bob's side. This is known as the **HJW theorem**.

Breaking BB84 Coin-Toss protocol with entanglement

- Alice sends one half of $|00\rangle + |11\rangle$ to Bob.
- Bob measures in a secret basis and declares x' randomly.
- Alice measures in the basis x that would make her win the coin-toss.
- Alice declares x and the b she measured.
- Because $|00\rangle + |11\rangle = |++\rangle + |--\rangle$, whenever Alice and Bob measured in the same basis their measurement results are the same, hence **Alice is never caught cheating and can always declare the x that makes her win**.

This is always possible when the 2 choices of Alice produces 2 density matrices ρ_0 and ρ_1 that are identical at Bob's side. This is known as the **HJW theorem**.

Breaking BB84 Coin-Toss protocol with entanglement

- Alice sends one half of $|00\rangle + |11\rangle$ to Bob.
- Bob measures in a secret basis and declares x' randomly.
- Alice measures in the basis x that would make her win the coin-toss.
- Alice declares x and the b she measured.
- Because $|00\rangle + |11\rangle = |++\rangle + |--\rangle$, whenever Alice and Bob measured in the same basis their measurement results are the same, hence **Alice is never caught cheating and can always declare the x that makes her win.**

This is always possible when the 2 choices of Alice produces 2 density matrices ρ_0 and ρ_1 that are identical at Bob's side. This is known as the **HJW theorem**.

Breaking BB84 Coin-Toss protocol with entanglement

- Alice sends one half of $|00\rangle + |11\rangle$ to Bob.
- Bob measures in a secret basis and declares x' randomly.
- Alice measures in the basis x that would make her win the coin-toss.
- Alice declares x and the b she measured.
- Because $|00\rangle + |11\rangle = |++\rangle + |--\rangle$, whenever Alice and Bob measured in the same basis their measurement results are the same, hence **Alice is never caught cheating and can always declare the x that makes her win.**

This is always possible when the 2 choices of Alice produces 2 density matrices ρ_0 and ρ_1 that are identical at Bob's side. This is known as the **HJW theorem**.

Breaking BB84 Coin-Toss protocol with entanglement

- Alice sends one half of $|00\rangle + |11\rangle$ to Bob.
- Bob measures in a secret basis and declares x' randomly.
- Alice measures in the basis x that would make her win the coin-toss.
- Alice declares x and the b she measured.
- Because $|00\rangle + |11\rangle = |++\rangle + |--\rangle$, whenever Alice and Bob measured in the same basis their measurement results are the same, hence **Alice is never caught cheating and can always declare the x that makes her win.**

This is always possible when the 2 choices of Alice produces 2 density matrices ρ_0 and ρ_1 that are identical at Bob's side. This is known as the **HJW theorem**.

Breaking BB84 Coin-Toss protocol with entanglement

- Alice sends one half of $|00\rangle + |11\rangle$ to Bob.
- Bob measures in a secret basis and declares x' randomly.
- Alice measures in the basis x that would make her win the coin-toss.
- Alice declares x and the b she measured.
- Because $|00\rangle + |11\rangle = |++\rangle + |--\rangle$, whenever Alice and Bob measured in the same basis their measurement results are the same, hence **Alice is never caught cheating and can always declare the x that makes her win**.

This is always possible when the 2 choices of Alice produces 2 density matrices ρ_0 and ρ_1 that are identical at Bob's side. This is known as the **HJW theorem**.

The Ambainis Protocol

To overcome HJW, Andris Ambainis introduced a protocol using qutrits (2002) :

$$|\phi_{b,x}\rangle = \begin{cases} \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle & \text{if} \quad x=0, b=0 \\ \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle & \text{if} \quad x=0, b=1 \\ \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|2\rangle & \text{if} \quad x=1, b=0 \\ \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|2\rangle & \text{if} \quad x=1, b=1 \end{cases}$$

$|\psi_{x,b}\rangle$ chosen randomly →

Bob stores the state in a memory

← x' chosen randomly

$x\ ,\ b$ →

Bob measures and verifies if Alice is honest

Coin toss result $x \oplus x'$

The Ambainis Protocol

To overcome HJW, Andris Ambainis introduced a protocol using qutrits (2002) :

$$|\phi_{b,x}\rangle = \begin{cases} \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle & \text{if} \quad x=0, b=0 \\ \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle & \text{if} \quad x=0, b=1 \\ \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|2\rangle & \text{if} \quad x=1, b=0 \\ \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|2\rangle & \text{if} \quad x=1, b=1 \end{cases}$$

$$\rho_0 = \begin{pmatrix} \frac{1}{2} & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} \frac{1}{2} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \frac{1}{2} \end{pmatrix}$$

Alice can still cheat but not break the protocol using HJW

$$\rho_0 \neq \rho_1$$

Bob can cheat a little!

Some numbers... and tolerance to losses

Ambainis showed that :

If only **Alice cheats**, she can win with probability **0.75** without being caught.
If only **Bob cheats**, he can win with probability **0.75** without being caught.

Remark : Kitaev showed (2002) that for any protocol, at least one party can win with probability higher or equal to $1/\sqrt{2} \approx 0.71$.

Why is Ambainis' protocol not loss-tolerant ?

Whenever the spans of ρ_0 and ρ_1 are different, Bob can do a **conclusive measurement** that, once in a while, will allow Bob to **distinguish** ρ_0 **from** ρ_1 **with certainty**.

In the presence of losses, Bob is allowed to declare that he hasn't received the photon. To win with certainty, a cheating Bob only has to wait for this conclusive measurement to succeed to declare having measured the photon !

Some numbers... and tolerance to losses

Ambainis showed that :

If only **Alice cheats**, she can win with probability **0.75** without being caught.
If only **Bob cheats**, he can win with probability **0.75** without being caught.

Remark : Kitaev showed (2002) that for any protocol, at least one party can win with probability higher or equal to $1/\sqrt{2} \approx 0.71$.

Why is Ambainis' protocol not loss-tolerant ?

Whenever the spans of ρ_0 and ρ_1 are different, Bob can do a **conclusive measurement** that, once in a while, will allow Bob to **distinguish** ρ_0 **from** ρ_1 **with certainty**.

In the presence of losses, Bob is allowed to declare that he hasn't received the photon. To win with certainty, a cheating Bob only has to wait for this conclusive measurement to succeed to declare having measured the photon !

The Ambainis Protocol

To overcome HJW, Andris Ambainis introduced a protocol using qutrits (2002) :

$$|\phi_{b,x}\rangle = \begin{cases} \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle & \text{if} \quad x=0, b=0 \\ \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle & \text{if} \quad x=0, b=1 \\ \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|2\rangle & \text{if} \quad x=1, b=0 \\ \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|2\rangle & \text{if} \quad x=1, b=1 \end{cases}$$

$|\psi_{x,b}\rangle$ chosen randomly →

Bob stores the state in a memory

← x' chosen randomly

$x\ ,\ b$ →

Bob measures and verifies if Alice is honest

Coin toss result $x \oplus x'$

Some numbers... and tolerance to losses

Ambainis showed that :

If only **Alice cheats**, she can win with probability **0.75** without being caught.
If only **Bob cheats**, he can win with probability **0.75** without being caught.

Remark : Kitaev showed (2002) that for any protocol, at least one party can win with probability higher or equal to $1/\sqrt{2} \approx 0.71$.

Why is Ambainis' protocol not loss-tolerant ?

Whenever the spans of ρ_0 and ρ_1 are different, Bob can do a **conclusive measurement** that, once in a while, will allow Bob to **distinguish** ρ_0 **from** ρ_1 **with certainty**.

In the presence of losses, Bob is allowed to declare that he hasn't received the photon. To win with certainty, a cheating Bob only has to wait for this conclusive measurement to succeed to declare having measured the photon !

Some numbers... and tolerance to losses

Ambainis showed that :

If only **Alice cheats**, she can win with probability **0.75** without being caught.
If only **Bob cheats**, he can win with probability **0.75** without being caught.

Remark : Kitaev showed (2002) that for any protocol, at least one party can win with probability higher or equal to $1/\sqrt{2} \approx 0.71$.

Why is Ambainis' protocol not loss-tolerant ?

Whenever the spans of ρ_0 and ρ_1 are different, Bob can do a **conclusive measurement** that, once in a while, will allow Bob to **distinguish** ρ_0 **from** ρ_1 **with certainty**.

In the presence of losses, Bob is allowed to declare that he hasn't received the photon. To win with certainty, a cheating Bob only has to wait for this conclusive measurement to succeed to declare having measured the photon !

Some numbers... and tolerance to losses

Ambainis showed that :

If only **Alice cheats**, she can win with probability **0.75** without being caught.
If only **Bob cheats**, he can win with probability **0.75** without being caught.

Remark : Kitaev showed (2002) that for any protocol, at least one party can win with probability higher or equal to $1/\sqrt{2} \approx 0.71$.

Why is Ambainis' protocol not loss-tolerant ?

Whenever the spans of ρ_0 and ρ_1 are different, Bob can do a **conclusive measurement** that, once in a while, will allow Bob to **distinguish** ρ_0 **from** ρ_1 **with certainty**.

In the presence of losses, Bob is allowed to declare that he hasn't received the photon. To win with certainty, a cheating Bob only has to wait for this conclusive measurement to succeed to declare having measured the photon !

A little twist of BB84...

$$\text{BB84 Set} \quad \left.\begin{aligned} |\psi_{0,0}\rangle &= |0\rangle \\ |\psi_{1,0}\rangle &= |+\rangle \end{aligned}\right\} b = 0 \qquad \left.\begin{aligned} |\psi_{0,1}\rangle &= |1\rangle \\ |\psi_{1,1}\rangle &= |-\rangle \end{aligned}\right\} b = 1$$

$|\psi_{x,b}\rangle$ chosen randomly →

Bob measures in the rectilinear or diagonal basis (no memory!)

← b' chosen randomly

$x\ ,\ b$ →

Bob can verify if Alice is honest only when the received state is coherent with his measurement basis

Coin toss result $b \oplus b'$

A little twist of BB84...

BB84 Set

$$\left.\begin{aligned}|\psi_{0,0}\rangle &= |0\rangle \\ |\psi_{1,0}\rangle &= |+\rangle\end{aligned}\right\} b=0$$

$$\left.\begin{aligned}|\psi_{0,1}\rangle &= |1\rangle \\ |\psi_{1,1}\rangle &= |-\rangle\end{aligned}\right\} b=1$$

$$\rho_0 = \tfrac{1}{2}(|0\rangle\langle 0| + |+\rangle\langle +|)$$
$$\rho_1 = \tfrac{1}{2}(|1\rangle\langle 1| + |-\rangle\langle -|)$$

$\rho_0 \neq \rho_1$ Bob can't do a conclusive measurement

$|\psi_{x,b}\rangle$ chosen randomly →

Bob measures in the rectilinear or diagonal basis (no memory!)

← b' chosen randomly

$x\ ,\ b$ →

Coin toss result $b \oplus b'$

Bob can verify if Alice is honest only when the received state is coherent with his measurement basis

A little twist of BB84...

BB84 Set $\left.\begin{array}{l} |\psi_{0,0}\rangle = |0\rangle \\ |\psi_{1,0}\rangle = |+\rangle \end{array}\right\} b=0$ $\left.\begin{array}{l} |\psi_{0,1}\rangle = |1\rangle \\ |\psi_{1,1}\rangle = |-\rangle \end{array}\right\} b=1$

$$\rho_0 = \tfrac{1}{2}(|0\rangle\langle 0| + |+\rangle\langle +|)$$
$$\rho_1 = \tfrac{1}{2}(|1\rangle\langle 1| + |-\rangle\langle -|)$$
$$\rho_0 \neq \rho_1$$

$|\psi_{x,b}\rangle$ chosen randomly →

Bob measures in the rectilinear or diagonal basis (no memory!)

← b' chosen randomly

Alice can't use HJW

$x\ ,\ b$ →

Bob can verify if Alice is honest only when the received state is coherent with his measurement basis

Coin toss result $b \oplus b'$

Security against a cheating Bob

- Since Bob can't perform a conclusive measurement, this new protocol is loss-tolerant.
- For individual attacks, the probability for Bob to correctly guess the state is

$$\frac{1}{2} + \frac{Tr(|\rho_0 - \rho_1|)}{4} = \cos^2 \pi/8 \approx 85.4\%$$

obtained by measuring in the Briedbart basis, i.e. halfway between $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$.
- The protocol is not optimal.

Security against a cheating Bob

- Since Bob can't perform a conclusive measurement, this new protocol is loss-tolerant.
- For individual attacks, the probability for Bob to correctly guess the state is

$$\frac{1}{2} + \frac{Tr(|\rho_0 - \rho_1|)}{4} = \cos^2 \pi/8 \approx 85.4\%$$

obtained by measuring in the Briedbart basis, i.e. halfway between $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$.

- The protocol is not optimal.

Security against a cheating Alice

Alice's cheating strategy is constrained by having to **answer a b that is consistent with her preparation basis x and the measurement basis of Bob.**

It can be shown that given entanglement and projective measurements, Alice's cheating strategy is such that :

- she can't increase her probability of winning over 1/2,
- only measurements in the $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ basis allow her not to get caught cheating.

Hence it seems that **Alice has to follow the protocol to avoid getting caught cheating** and therefore she **can't cheat at all.**

We are currently working on a complete security proof.

Security against a cheating Alice

Alice's cheating strategy is constrained by having to **answer a b that is consistent with her preparation basis x and the measurement basis of Bob**.

It can be shown that given entanglement and projective measurements, Alice's cheating strategy is such that :

- she can't increase her probability of winning over $1/2$,
- only measurements in the $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ basis allow her not to get caught cheating.

Hence it seems that Alice has to follow the protocol to avoid getting caught cheating and therefore she can't cheat at all.

We are currently working on a complete security proof.

Security against a cheating Alice

Alice's cheating strategy is constrained by having to **answer a b that is consistent with her preparation basis x and the measurement basis of Bob**.

It can be shown that given entanglement and projective measurements, Alice's cheating strategy is such that :

- she can't increase her probability of winning over $1/2$,
- only measurements in the $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ basis allow her not to get caught cheating.

Hence it seems that Alice has to follow the protocol to avoid getting caught cheating and therefore she can't cheat at all.

We are currently working on a complete security proof.

Security against a cheating Alice

Alice's cheating strategy is constrained by having to **answer a b that is consistent with her preparation basis x and the measurement basis of Bob**.

It can be shown that given entanglement and projective measurements, Alice's cheating strategy is such that :

- she can't increase her probability of winning over $1/2$,
- only measurements in the $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ basis allow her not to get caught cheating.

Hence it seems that **Alice has to follow the protocol to avoid getting caught cheating** and therefore she **can't cheat at all**.

We are currently working on a complete security proof.

Concluding remarks

- We proposed a new protocol that is tolerant to losses and doesn't require a quantum memory
- Bob's best cheating strategy allows him to win with probability 85.4% without being caught cheating
- To avoid getting caught cheating, Alice has to follow the protocol hence she can't cheat at all (working on complete proof).
- Whether a loss-tolerant protocol can reach Kitaev's lower bound or not is still an open question.
- We are currently working on an experimental demonstration of this protocol.

Security against a cheating Alice

Alice's cheating strategy is constrained by having to **answer a b that is consistent with her preparation basis x and the measurement basis of Bob**.

It can be shown that given entanglement and projective measurements, Alice's cheating strategy is such that :

- she can't increase her probability of winning over $1/2$,
- only measurements in the $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ basis allow her not to get caught cheating.

Hence it seems that **Alice has to follow the protocol to avoid getting caught cheating** and therefore she **can't cheat at all**.

We are currently working on a complete security proof.

Concluding remarks

- We proposed a new protocol that is tolerant to losses and doesn't require a quantum memory
- Bob's best cheating strategy allows him to win with probability 85.4% without being caught cheating
- To avoid getting caught cheating, Alice has to follow the protocol hence she can't cheat at all (working on complete proof).
- Whether a loss-tolerant protocol can reach Kitaev's lower bound or not is still an open question.
- We are currently working on an experimental demonstration of this protocol.

Concluding remarks

- We proposed a new protocol that is tolerant to losses and doesn't require a quantum memory
- Bob's best cheating strategy allows him to win with probability 85.4% without being caught cheating
- To avoid getting caught cheating, Alice has to follow the protocol hence she can't cheat at all (working on complete proof).
- Whether a loss-tolerant protocol can reach Kitaev's lower bound or not is still an open question.
- We are currently working on an experimental demonstration of this protocol.

Concluding remarks

- We proposed a new protocol that is tolerant to losses and doesn't require a quantum memory
- Bob's best cheating strategy allows him to win with probability 85.4% without being caught cheating
- To avoid getting caught cheating, Alice has to follow the protocol hence she can't cheat at all (working on complete proof).
- Whether a loss-tolerant protocol can reach Kitaev's lower bound or not is still an open question.
- We are currently working on an experimental demonstration of this protocol.

Concluding remarks

- We proposed a new protocol that is tolerant to losses and doesn't require a quantum memory
- Bob's best cheating strategy allows him to win with probability 85.4% without being caught cheating
- To avoid getting caught cheating, Alice has to follow the protocol hence she can't cheat at all (working on complete proof).
- Whether a loss-tolerant protocol can reach Kitaev's lower bound or not is still an open question.
- We are currently working on an experimental demonstration of this protocol.

Concluding remarks

- We proposed a new protocol that is tolerant to losses and doesn't require a quantum memory
- Bob's best cheating strategy allows him to win with probability 85.4% without being caught cheating
- To avoid getting caught cheating, Alice has to follow the protocol hence she can't cheat at all (working on complete proof).
- Whether a loss-tolerant protocol can reach Kitaev's lower bound or not is still an open question.
- We are currently working on an experimental demonstration of this protocol.