Practical Quantum Coin Flipping

A. Pappa, A. Chailloux, E. Diamanti, I. Kerenidis

Phys. Rev. A 84, 052305 (2011)

What is Quantum Coin Flipping?

$$\frac{\text{quantum}}{\text{classical}}$$

$$\frac{\text{channel}}{\text{channel}}$$

- Strong CF : the players want to end up with a random bit
- Weak CF : the players have a preference on the outcome

Definitions

A strong coin flipping protocol with bias ε (SCF(ε)) has the following properties :

- If Alice and Bob are honest then $\Pr[c = 0] = \Pr[c = 1] = ½$
- If Alice cheats and Bob is honest then $P^*_A = \max\{\Pr[c = 0], \Pr[c = 1]\} \leq 1/2 + \varepsilon$.
- If Bob cheats and Alice is honest then $P^*_B = \max\{\Pr[c = 0], \Pr[c = 1]\} \leq 1/2 + \varepsilon$.

The cheating probability of the protocol is defined as $\max\{P^*_A, P^*_B\}$.
We say that the coin flipping is *perfect* if $\varepsilon=0$.

Background

- Introduced by Blum in 1981
- Impossibility of classical CF $=1$
- Impossibility of perfect quantum CF (LC98) $>1/2$
- Several non-perfect protocols:
  - Aharonov et al ('00) $= (2+\sqrt{2})/4$
  - SR('02), Ambainis('02) $=3/4$
- Kitaev's theoretical proof ('03) $\geq 1/\sqrt{2}$
- Chailloux, Kerenidis protocol ('09) $\approx 1/\sqrt{2}$

Practical Considerations

- Channel noise
- System transmission efficiency, losses
- Multi-photon pulses
- Detectors’ dark counts
- Detectors’ finite quantum efficiency

Ambainis protocol

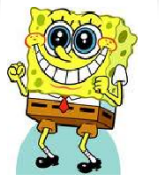
The Protocol uses the states $\left|\phi_{a,x}\right\rangle$ on qutrits, where *α* is the basis and *x* is the bit:

$$\left|\phi_{0,x}\right\rangle = \frac{1}{\sqrt{2}}\left|0\right\rangle + (-1)^x \frac{1}{\sqrt{2}}\left|1\right\rangle \ , \ \left|\phi_{1,x}\right\rangle = \frac{1}{\sqrt{2}}\left|0\right\rangle + (-1)^x \frac{1}{\sqrt{2}}\left|2\right\rangle$$

The measurement basis is defined for $\alpha \in \{0,1\}$:

$$B_a = \{\left|\phi_{a,0}\right\rangle, \left|\phi_{a,1}\right\rangle, \left|2-a\right\rangle\}$$

Ambainis protocol



$a, x \in_R \{0,1\}$

$|\phi_{a,x}\rangle$ →

$|\phi_{a,x}\rangle$ memory

← b

$b \in_R \{0,1\}$

$a,\ x$ →

measure in B_a

⇓

$\hat{x}$

If $x \neq \hat{x}$, then Bob aborts the protocol. If he doesn't abort, the outcome of the coin flip is $a \oplus b$.

Ambainis protocol with losses

Unavoidable losses in channel, quantum memory and detector

Bob accepts Alice's bit on faith

- Alice sends nothing

Bob asks to restart the protocol

- Bob declares loss when he is not happy with a

Some practical results

- Berlin et al (‘09)

Loss-tolerant with cheating probability 0.9

- Chailloux (‘10)

Loss-tolerant with cheating probability 0.86

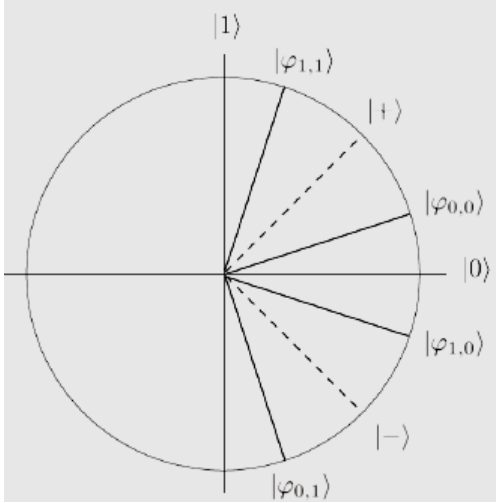
Berlin et al protocol

The Protocol uses the states $\left|\phi_{a,x}\right\rangle$, where *α* is the basis and *x* is the bit:

$$\left|\phi_{a,0}\right\rangle = \sqrt{\alpha}\left|0\right\rangle + (-1)^a\sqrt{1-\alpha}\left|1\right\rangle \quad , \quad \left|\phi_{a,1}\right\rangle = \sqrt{1-\alpha}\left|0\right\rangle - (-1)^a\sqrt{\alpha}\left|1\right\rangle$$

The measurement basis is defined for $a \in \{0,1\}$:

$$B_a = \{\left|\phi_{a,0}\right\rangle, \left|\phi_{a,1}\right\rangle\}$$



Berlin et al protocol

$a, x \in_R \{0,1\}$

$|\phi_{a,x}\rangle$ →

$\hat{a} \in_R \{0,1\}$

measure in $B_{\hat{a}} \Longrightarrow \hat{x}$

← "Start over" or b

Declare "loss" or choose $b \in_R \{0,1\}$

$a,\ x$ →

If $a = \hat{a}$ and $x \neq \hat{x}$, then Bob aborts the protocol. If he doesn't abort, the outcome of the coin flip is $x \oplus b$.

Berlin et al protocol

Properties

- Allows for infinite ammount losses
- Doesn’t allow for conclusive measurement (the two distinct density matrices cannot be distringuished conclusively)
- Cheating probability is equal to 90%.

Disadvantages

- Not secure against multi-photon pulses (ex: for 2-photon pulses, there is a conclusive measurement with probability 64%)
- Doesn’t take into account noise, dark counts and system’s finite efficiency.

Our Protocol

The Protocol uses *K* states $\left|\phi_{a_i,x_i}\right\rangle$ (i=1,...,K), where α_i is the basis and x_i is the bit:

$$\left|\phi_{a_i,0}\right\rangle = \sqrt{\alpha}\left|0\right\rangle + (-1)^{a_i}\sqrt{1-\alpha}\left|1\right\rangle \quad , \quad \left|\phi_{a_i,1}\right\rangle = \sqrt{1-\alpha}\left|0\right\rangle - (-1)^{a_i}\sqrt{\alpha}\left|1\right\rangle$$

The measurement basis is defined for $\alpha_i \in \{0,1\}$:

$$B_{a_i} = \{\left|\phi_{a_i,0}\right\rangle, \left|\phi_{a_i,1}\right\rangle\}$$

Our Protocol

For i=1,...,K

$a_i, x_i \in_R \{0,1\}$ $\xrightarrow{\left|\phi_{a_i, x_i}\right\rangle}$ $\hat{a}_i \in_R \{0,1\}$

measure in $B_{\hat{a}_i}$

Our Protocol

For i=1,...,K

$a_i, x_i \in_R \{0,1\}$ $\xrightarrow{\left|\phi_{a_i, x_i}\right\rangle}$ $\hat{a}_i \in_R \{0,1\}$

measure in $B_{\hat{a}_i}$

If Bob's detectors don't click for any pulse, he aborts. Else let *j* be the first pulse he detects.

$\xleftarrow{c,\ j}$ $c \in_R \{0,1\}$

$\xrightarrow{x_j,\ a_j}$

If $a_i = a_j$, Bob checks the correctness of the outcome and aborts if not correct. If he doesn't abort, then the outcome is $b = x_j + c$.

Properties of the protocol

- We take into account all experimental parameters.
- We use an attenuated laser pulse (the number of photons μ follows the Poisson distribution), instead of a perfect single photon source or an entangled source.
- We bound the number of sent pulses.
- We allow some honest abort probability due to the imperfections of the system (noise).

Coin flipping with honest abort

Hanggi and Wullschleger (2010) defined CF that is characterized by 6 parameters: $CF(\underbrace{p_{00}, p_{11}}_{\text{Two honest players output } i}, p_{*0}, p_{*1}, p_{0*}, p_{1*})$

Coin flipping with honest abort

Hanggi and Wullschleger (2010) defined CF that is characterized by 6 parameters: $CF(p_{00}, p_{11}, \underbrace{p_{*0}, p_{*1}}, p_{0*}, p_{1*})$

1st player forces the honest player to output i

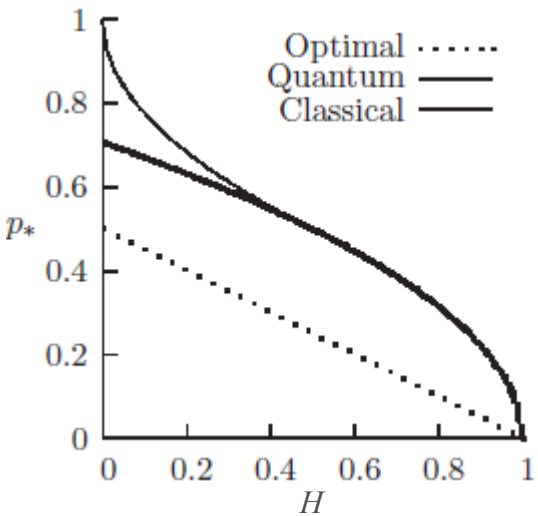
Coin flipping with honest abort

Hanggi and Wullschleger (2010) defined CF that is characterized by 6 parameters: $CF(p_{00}, p_{11}, p_{*0}, p_{*1}, \underbrace{p_{0*}, p_{1*}}_{\text{2nd player forces the honest player to output } i})$

Coin flipping with honest abort

Hanggi and Wullschleger (2010) defined CF that is characterized by 6 parameters: $CF(p_{00}, p_{11}, p_{*0}, p_{*1}, p_{0*}, p_{1*})$

- The honest players will abort with probability $H = 1 - p_{00} - p_{11}$.



$$\text{quantum: } p_* = \sqrt{\frac{1-H}{2}}$$

$$\text{classical : } p_* = \sqrt{\frac{1-H}{2}} \text{ for H} \geq \frac{1}{2}$$

$$p_* = 1 - \sqrt{\frac{H}{2}} \text{ for H} < \frac{1}{2}$$

Honest Abort

The Abort Probability depends on:

- the detectors' finite quantum efficiency (η) and dark counts (d_B)
- the probability of wrong measurement outcome due to noise e
- the system transmission efficiency F

$$H = Z^K(1-d_B)^K + \frac{1}{4}\sum_{i=1}^{K}(1-d_B)^{i-1}d_B Z^i + \left[1 - Z^K(1-d_B)^K - \sum_{i=1}^{K}(1-d_B)^{i-1}d_B Z^i\right]\frac{e}{2}$$

where: $Z = p_0 + (1-p_0)(1-F\eta)$ is the probability that no signal arrives at Bob's detectors.

$F = 10^{-(\beta L + k)/10}$ is the system transmission efficiency.

Honest Abort

The Abort Probability depends on:

- the detectors' finite quantum efficiency and dark counts
- the probability of wrong measurement outcome due to noise
- the system transmission efficiency

$$H = \underbrace{Z^K(1-d_B)^K}_{\text{Bob's detectors don't click in any of the K rounds}} + \frac{1}{4}\sum_{i=1}^{K}(1-d_B)^{i-1}d_B Z^i + \left[1 - Z^K(1-d_B)^K - \sum_{i=1}^{K}(1-d_B)^{i-1}d_B Z^i\right]\frac{e}{2}$$

Honest Abort

The Abort Probability depends on:

- the detectors' finite quantum efficiency and dark counts
- the probability of wrong measurement outcome due to noise
- the system transmission efficiency

$$H = Z^K (1-d_B)^K + \underbrace{\frac{1}{4}\sum_{i=1}^{K}(1-d_B)^{i-1} d_B Z^i}_{\text{Bob's first click is a dark count}} + \left[1 - Z^K (1-d_B)^K - \sum_{i=1}^{K}(1-d_B)^{i-1} d_B Z^i\right]\frac{e}{2}$$

Honest Abort

The Abort Probability depends on:

- the detectors' finite quantum efficiency and dark counts
- the probability of wrong measurement outcome due to noise
- the system transmission efficiency

$$H = Z^K(1-d_B)^K + \frac{1}{4}\sum_{i=1}^{K}(1-d_B)^{i-1}d_B Z^i + \underbrace{\left[1 - Z^K(1-d_B)^K - \sum_{i=1}^{K}(1-d_B)^{i-1}d_B Z^i\right]\frac{e}{2}}_{\text{The channel noise alters the state of the photon}}$$

Malicious Alice

Alice's Cheating Probability depends only on the amplitude of the state.

$$A \leq \left(3 + 2\sqrt{\alpha(1-\alpha)}\right)/4$$

Malicious Bob

Bob's Cheating Probability depends on the number of photons that are contained in the received pulses (determined by *K* and μ).

$$B \le \sum_{i=1}^{4} P(A_i) * P\left(b' \middle| A_i\right) + \left(1 - \sum_{i=1}^{4} P(A_i)\right) * 1$$

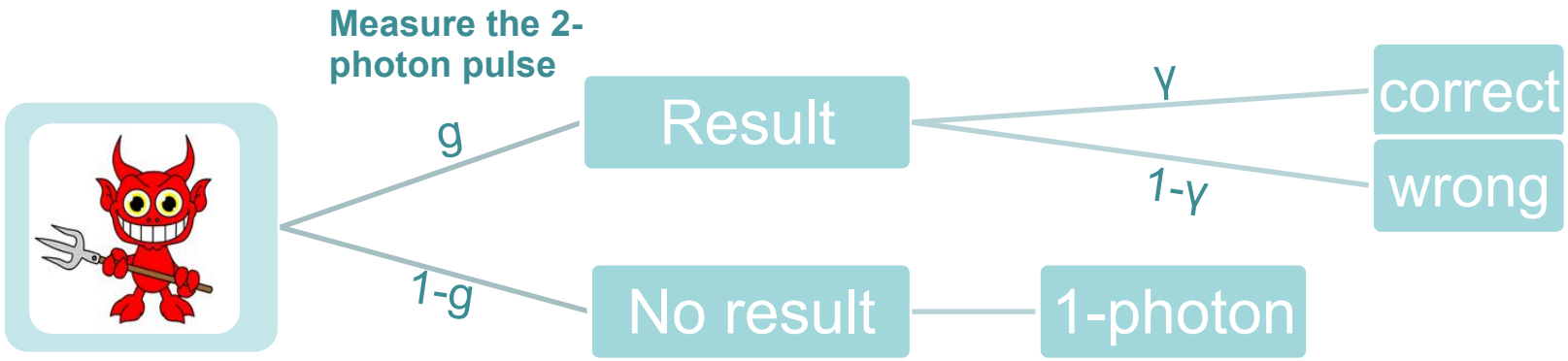
A_1: all 0-photon pulses ⇒ $P(b' \mid A_1) = 1/2$
A_2: at least one 1-photon pulse ⇒ $P(b' \mid A_2) = \alpha$
A_3: one 2-photon pulse (rest are 0-photon pulses) ⇒ $P(b' \mid A_3) = \alpha$
A_4: one 2-photon pulse, at least 1-photon pulse (rest are 0-photon pulses)

Malicious Bob

What can Bob do in the case of event A_4 ?

1. Optimal distinguishing measurement(Helstrom) on the two photons. The cheating probability is equal to α.
2. Conclusive measurement on the 2-photon pulse and if the answer is not conclusive then he can play with one of the 1-photon.

Optimal strategy ?? NONE OF THE ABOVE



Malicious Bob

What can Bob do in the case of event A_4 ?

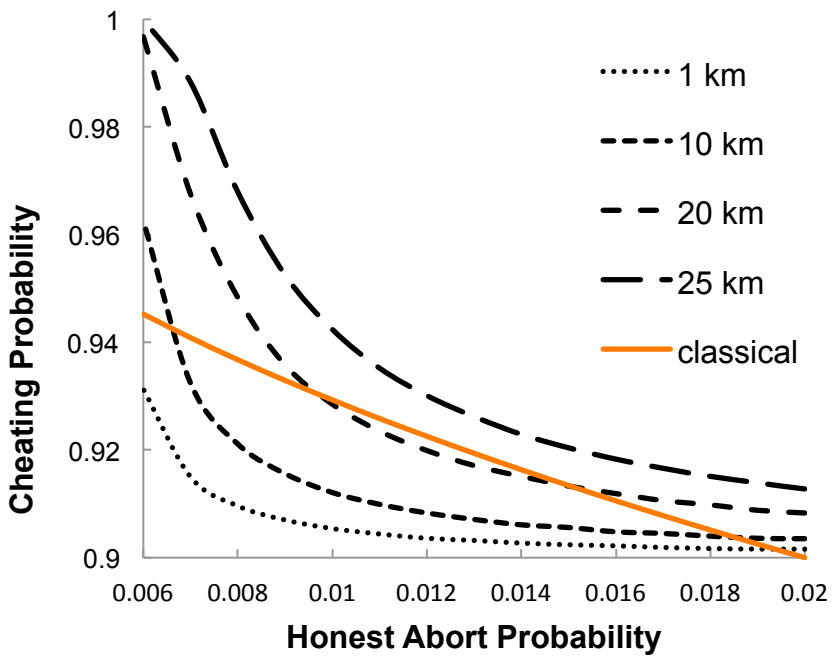
1. Optimal distinguishing measurement(Helstrom) on the two photons. The cheating probability is equal to α.
2. Conclusive measurement on the 2-photon pulse and if the answer is not conclusive then he can play with one of the 1-photon.

Optimal strategy ?? NONE OF THE ABOVE

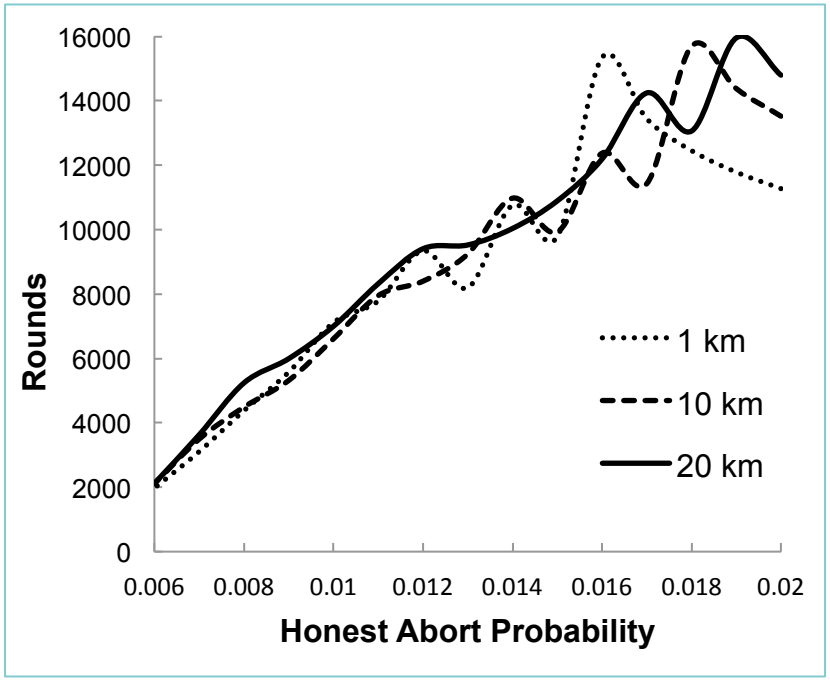
$$P(b' \mid A_4) = g\gamma + (1-g)\alpha \leq -2\alpha^2 + 4\alpha - 1$$

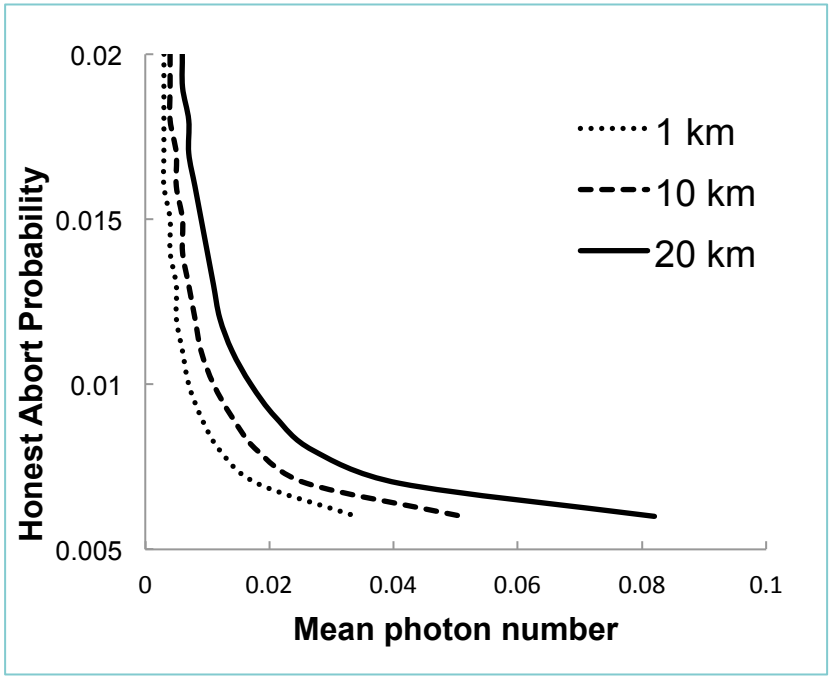
Our Results

Parameter		Value
Detector constant loss [dB]	k	1
Absorption coefficient [dB/km]	β	0.2
Detection efficiency	η	0.2
Dark counts (per slot)	d_B	10^{-5}
Signal error rate	e	0.01



Our Results





Implementations

1. G. Molina-Terriza, A. Vaziri, R. Ursin and A. Zeilinger (2005)

2. A.T. Nguyen, J. Frison, K. Phan Huy and S. Massar (2008)

3. G. Berlin, G. Brassard, F. Bussières, N. Godbout, J.A.Slater and W. Tittel (2009)

Implementation coming soon!

Thank you