Practical Quantum Coin Flipping

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

What is Quantum Coin Flipping?

• Strong CF: the players want to end up with a random bit
• Weak CF: the players have a preference on the outcome
A strong coin flipping protocol with bias $\varepsilon$ (SCF($\varepsilon$)) has the following properties:

- If Alice and Bob are honest then $\Pr[c = 0] = \Pr[c = 1] = \frac{1}{2}$
- If Alice cheats and Bob is honest then $P_A^* = \max\{\Pr[c = 0],\Pr[c = 1]\} \leq \frac{1}{2} + \varepsilon$.
- If Bob cheats and Alice is honest then $P_B^* = \max\{\Pr[c = 0],\Pr[c = 1]\} \leq \frac{1}{2} + \varepsilon$.

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) = \(\frac{2+\sqrt{2}}{4}\)
  - SR(‘02), Ambainis(‘02) = 3/4
- Kitaev’s theoretical proof (‘03) ≥ 1/√2
- Chailloux, Kerenidis protocol (‘09) ≈ 1/√2
Practical Considerations

• Channel noise
• System transmission efficiency, losses
• Multi-photon pulses
• Detectors’ dark counts
• Detectors’ finite quantum efficiency
The Protocol uses the states $|\phi_{a,x}\rangle$ on qutrits, where $\alpha$ is the basis and $x$ is the bit:

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

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

$$B_\alpha = \{|\phi_{\alpha,0}\rangle, |\phi_{\alpha,1}\rangle, |2-\alpha\rangle\}$$
Ambainis protocol

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)

- Chailloux (‘10)

  Loss-tolerant with cheating probability 0.9

  Loss-tolerant with cheating probability 0.86
The Protocol uses the states $|\phi_{a,x}\rangle$, where $\alpha$ is the basis and $x$ is the bit:

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

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

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

$$B_a = \{ |\phi_{a,0}\rangle, |\phi_{a,1}\rangle \}$$
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 amount losses
- Doesn’t allow for conclusive measurement (the two distinct density matrices cannot be distinguished 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 $\left| \phi_{a_i, x_i} \right\rangle (i=1,\ldots,K)$, where $\alpha_i$ is the basis and $x_i$ is the bit:

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

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

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

For $i=1,\ldots,K$

$a_i, x_i \in \mathbb{R} \{0,1\} \quad \left| \phi_{a_i, x_i} \right> \quad \hat{a}_i \in \mathbb{R} \{0,1\}

\text{measure in } B_{\hat{a}_i}$
Our Protocol

For $i=1,\ldots,K$

\[ a_i, x_i \in_R \{0,1\} \]

\[ \left| \phi_{a_i, x_i} \right\rangle \]

\[ \hat{a}_i \in_R \{0,1\} \]

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.

\[ c, j \]

\[ x_j, a_j \]

\[ c \in_R \{0,1\} \]

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 $\mu$ 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:

\[ CF(p_{00}, p_{11}, p^*_0, p^*_1, p^*_0, p^*_1) \]

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

1st player forces the honest player to output \( i \)
Hanggi and Wullschleger (2010) defined CF that is characterized by 6 parameters: \( CF(p_{00}, p_{11}, p^*_0, p^*_1, p_0^*, p_1^*) \).
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 \( H = 1 - p_{00} - p_{11} \).

\[ p_* = \sqrt{\frac{1 - H}{2}} \]

- Quantum: \( p_* = \sqrt{\frac{1 - H}{2}} \) for \( H \geq \frac{1}{2} \)
- Classical: \( p_* = 1 - \sqrt{\frac{H}{2}} \) for \( H < \frac{1}{2} \)
Honest Abort

The Abort Probability depends on:

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

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

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

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

Bob's detectors don't click in any of the K rounds
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

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

Bob’s first click is a dark count
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

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

The channel noise alters the state of the photon.
Malicious Alice

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

\[ A \leq \frac{3 + 2\sqrt{\alpha(1-\alpha)}}{4} \]
Malicious Bob

Bob’s Cheating Probability depends on the number of photons that are contained in the received pulses (determined by $K$ and $\mu$).

\[ B \leq \sum_{i=1}^{4} P(A_i) \cdot P\left(b' \mid A_i\right) + \left(1 - \sum_{i=1}^{4} P(A_i)\right) \cdot 1 \]

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detector constant loss [dB]</td>
<td>$k = 1$</td>
</tr>
<tr>
<td>Absorption coefficient [dB/km]</td>
<td>$\beta = 0.2$</td>
</tr>
<tr>
<td>Detection efficiency</td>
<td>$\eta = 0.2$</td>
</tr>
<tr>
<td>Dark counts (per slot)</td>
<td>$d_B = 10^{-5}$</td>
</tr>
<tr>
<td>Signal error rate</td>
<td>$e = 0.01$</td>
</tr>
</tbody>
</table>

---

Our Results

![Graph showing cheating probability vs. honest abort probability for different distances: 1 km, 10 km, 20 km, 25 km, and classical.]
Our Results

- Honest Abort Probability vs. Rounds
- Honest Abort Probability vs. Mean photon number

Distance:
- 1 km
- 10 km
- 20 km

Graphs show the relationship between Rounds, Honest Abort Probability, and Mean photon number for different distances.


Implementation coming soon!

Thank you