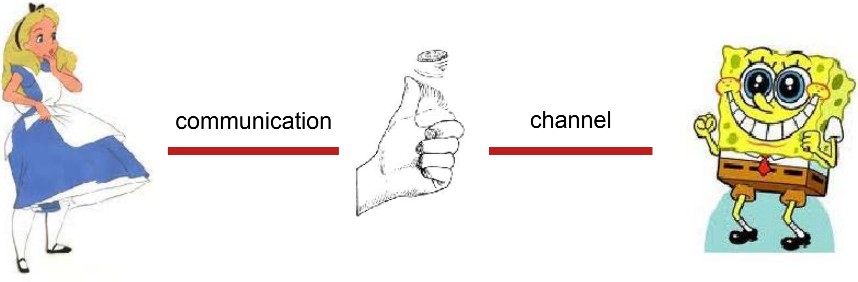
Experimental plug&play quantum coin flipping

Anna Pappa

1 September 2014

Coin Flipping



Why do we need it?

1. Bit commitment
2. Leader election and zero-knowledge protocols
3. Secure identification

Coin Flipping with bias ϵ

- If Alice and Bob are honest then

$$\Pr[c=0] = \Pr[c=1] = \frac{1}{2}$$

- If Alice cheats and Bob is honest then

$$p_*^A := \max_A \{\Pr[c=0], \Pr[c=1]\} \leq \frac{1}{2} + \epsilon$$

- If Bob cheats and Alice is honest then

$$p_*^B := \max_B \{\Pr[c=0], \Pr[c=1]\} \leq \frac{1}{2} + \epsilon$$

Coin Flipping with bias ϵ

- If Alice and Bob are honest then

$$\Pr[c=0] = \Pr[c=1] = \frac{1}{2}$$

- If Alice cheats and Bob is honest then

$$p_*^A := \max_A \{\Pr[c=0], \Pr[c=1]\} \le \frac{1}{2} + \epsilon$$

- If Bob cheats and Alice is honest then

$$p_*^B := \max_B \{\Pr[c=0], \Pr[c=1]\} \ \le \frac{1}{2} + \epsilon$$

The **cheating probability** of the CF protocol is $p_* = \max\{p_*^A, p_*^B\}$.

Coin flipping with information-theoretic security

Impossibility of classical CF	$p_c = 1$
Impossibility of perfect quantum CF (May97,LC98)	$p_q > 1/2$
Several non-perfect protocols (ATVY00, SR02, Amb04)	$p_q \leq 3/4$
Kitaev's SDP proof (2003)	$p_q \geq 1/\sqrt{2}$
Chailloux, Kerenidis (2009)	$p_q \approx 1/\sqrt{2}$

In practice

Practical Considerations :

- Technological state of the art (ex: state generation)
- System transmission losses and noise
- Detectors' dark counts and finite quantum efficiency
- Quantum memory

In practice

Practical Considerations :

- Technological state of the art (ex: state generation)
- System transmission losses and noise
- Detectors' dark counts and finite quantum efficiency
- Quantum memory

Loss-tolerant Protocols :

- Berlin *et al* (2009): $p_q = 0.9$
- Chailloux (2010): $p_q = 0.86$

In practice

Practical Considerations :

- Technological state of the art (ex: state generation)
- System transmission losses and noise
- Detectors' dark counts and finite quantum efficiency
- Quantum memory

Loss-tolerant Protocols :

- Berlin *et al* (2009): $p_q = 0.9$
- Chailloux (2010): $p_q = 0.86$

Implementations :

- Molina-Terriza *et al* (2005)
- Nguyen *et al* (2008)
- Berlin *et al* (2011)

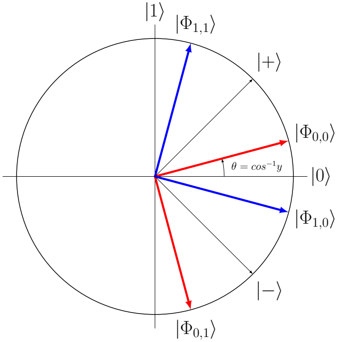
The Protocol

The protocol uses K states $|\Phi_{\alpha_i,c_i}\rangle$, where α_i: basis and c_i: bit

$$
\begin{aligned}
|\Phi_{\alpha_i,0}\rangle &= \sqrt{y}|0\rangle + (-1)^{\alpha_i}\sqrt{1-y}|1\rangle \\
|\Phi_{\alpha_i,1}\rangle &= \sqrt{1-y}|0\rangle - (-1)^{\alpha_i}\sqrt{y}|1\rangle
\end{aligned}
$$

For any bit $\beta \in \{0,1\}$, we define the measurement basis:

$$\mathcal{B}_\beta = \{|\Phi_{\beta,0}\rangle, |\Phi_{\beta,1}\rangle\}$$



The Protocol

Alice		**Bob**
choose $\{\alpha_i, c_i\}_1^K$	$\xrightarrow{\{\lvert\Phi_{\alpha_i,c_i}\rangle\}_1^K}$	choose $\{\beta_i\}_1^K$ measure in $\{\mathcal{B}_{\beta_i}\}_1^K$
	$\xleftarrow{j,\ b}$	j: first measured pulse, c'_j: outcome, $b \in_R \{0,1\}$
	$\xrightarrow{\alpha_j,\ c_j}$	If $\alpha_j = \beta_j$ and $c_j \neq c'_j$, abort. Else $\boxed{x = c_j \oplus b}$

The Protocol

Alice		**Bob**
choose $\{\alpha_i, c_i\}_1^K$	$\xrightarrow{\{\lvert\Phi_{\alpha_i,c_i}\rangle\}_1^K}$	choose $\{\beta_i\}_1^K$ measure in $\{\mathcal{B}_{\beta_i}\}_1^K$
	$\xleftarrow{j,\ b}$	j: first measured pulse, c'_j: outcome, $b \in_R \{0,1\}$
	$\xrightarrow{\alpha_j,\ c_j}$	If $\alpha_j = \beta_j$ and $c_j \neq c'_j$, abort. Else $\boxed{x = c_j \oplus b}$

Properties

- No need for entanglement, use of attenuated laser source
- No need for a quantum memory
- Tolerance to losses and noise
- Small probability of honest players' abort

Security Analysis

Protocol Parameters : μ (photon number), K (number of pulses), y (state coefficient), d_B (dark counts), e (channel noise), Z (losses).

Security Analysis

Protocol Parameters : μ (photon number), K (number of pulses), y (state coefficient), d_B (dark counts), e (channel noise), Z (losses).

Honest Players - Abort :

$$\underbrace{Z^K(1-d_B)^K}_{\Pr(\text{no click})} + \underbrace{\frac{1}{4}\sum_{i=1}^{K}(1-d_B)^{i-1}d_B Z^i}_{\Pr(\text{dark count})} + \frac{e}{2}\underbrace{\left[1 - Z^K(1-d_B)^K - \sum_{i=1}^{K}(1-d_B)^{i-1}d_B Z^i\right]}_{\Pr(\text{channel noise})}$$

Security Analysis

Protocol Parameters : μ (photon number), K (number of pulses), y (state coefficient), d_B (dark counts), e (channel noise), Z (losses).

Honest Players - Abort :

$$\underbrace{Z^K(1-d_B)^K}_{\Pr\text{ (no click)}} + \underbrace{\frac{1}{4}\sum_{i=1}^{K}(1-d_B)^{i-1}d_B Z^i}_{\Pr\text{ (dark count)}} + \frac{e}{2}\underbrace{\left[1-Z^K(1-d_B)^K-\sum_{i=1}^{K}(1-d_B)^{i-1}d_B Z^i\right]}_{\Pr\text{ (channel noise)}}$$

Dishonest Alice : $p_q^A \leq \frac{3}{4} + \frac{1}{2}\sqrt{y(1-y)}$

Security Analysis

Protocol Parameters : μ (photon number), K (number of pulses), y (state coefficient), d_B (dark counts), e (channel noise), Z (losses).

Honest Players - Abort :

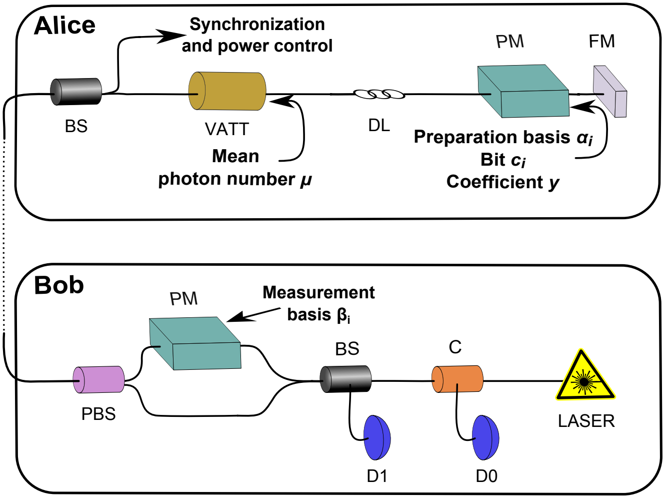
$$\underbrace{Z^K(1-d_B)^K}_{\Pr(\text{no click})} + \underbrace{\frac{1}{4}\sum_{i=1}^{K}(1-d_B)^{i-1}d_B Z^i}_{\Pr(\text{dark count})} + \frac{e}{2}\underbrace{\left[1-Z^K(1-d_B)^K-\sum_{i=1}^{K}(1-d_B)^{i-1}d_B Z^i\right]}_{\Pr(\text{channel noise})}$$

Dishonest Alice : $p_q^A \leq \frac{3}{4}+\frac{1}{2}\sqrt{y(1-y)}$

Dishonest Bob : Depends on the distribution of the number of multiple photons in pulses (function of K, μ, y).

The Clavis2 system

The Clavis2 system



C: Circulator, BS: Beam Splitter, D0,D1: APD detectors, PM: Phase Modulator, FM: Faraday Mirror
VATT: Variable Attenuator, PBS: Polarization Beam Splitter, BF: Bandpass Filter, DL: Delay Line

HW and SW enhancements on the Clavis2

Hardware Changes

- Changed the detectors to high efficiency/low noise ones.

Software Changes

- Use of rotated BB84 states $\Rightarrow$ set coefficient y both in Alice and Bob.
- Use of very low μ: average photon number per pulse.

Adapting the security proofs

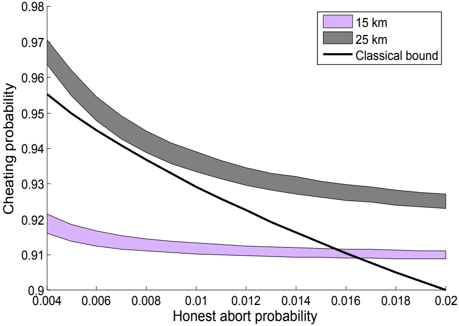
Assumptions

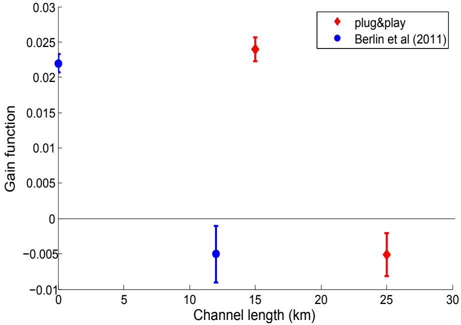
- Alice can create each state with equal probability and independently of Bob.
- Bob's basis β_j and bit b are chosen uniformly at random and independently of Alice.
- Bob's detectors have the same efficiencies.

Adaptation

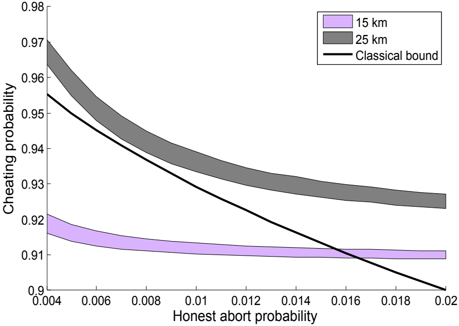
- Symmetrization of losses: Bob makes the two detection efficiencies equal by throwing away some detection events.

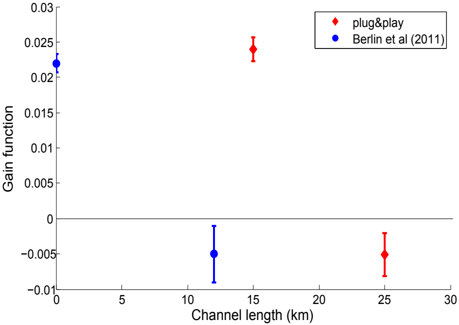
Experimental Results





Experimental Results





- Strictly stronger-than-classical security
- Practical implementation, off-the-shelf equipment

Enhancing security against limited adversaries

Our protocol has information-theoretic security	$\rightarrow$	Pr[cheat] is high
CF protocols against bounded adversaries	$\rightarrow$	Pr[cheat] ≈ 0.5

Enhancing security against limited adversaries

Our protocol has information-theoretic security	$\rightarrow$	Pr[cheat] is high
CF protocols against bounded adversaries	$\rightarrow$	Pr[cheat] ≈ 0.5

Computationally bounded: based on the inability to invert 1-way functions.

Noisy storage: based on the inability to maintain quantum information in a memory for a long period of time.

Enhancing security against limited adversaries

Our protocol has information-theoretic security	$\rightarrow$	Pr[cheat] is high
CF protocols against bounded adversaries	$\rightarrow$	Pr[cheat] ≈ 0.5

Computationally bounded: based on the inability to invert 1-way functions.

Noisy storage: based on the inability to maintain quantum information in a memory for a long period of time.

Combined protocols

The security of our QCF protocol lies on top of the perfect security of the bounded protocols, adding a guarantee against unbounded adversaries.

Coin Flipping

Summary

- We have shown, both theoretically and experimentally, that flipping a single coin with security guarantees strictly better than classical, can be achieved with present day technology.
- We provided security proofs that take into account all standard imperfections, including asymmetries in detection efficiencies, multi-photon pulses, losses and noise.

Open Questions

- Side-channel or other types of attacks?
- Use of decoy states or some kind of error-correcting code?
- Further study of other types of bounded adversaries?

Coin Flipping

Summary

- We have shown, both theoretically and experimentally, that flipping a single coin with security guarantees strictly better than classical, can be achieved with present day technology.
- We provided security proofs that take into account all standard imperfections, including asymmetries in detection efficiencies, multi-photon pulses, losses and noise.

Open Questions

- Side-channel or other types of attacks?
- Use of decoy states or some kind of error-correcting code?
- Further study of other types of bounded adversaries?

Publications

A. Pappa, A. Chailloux, E. Diamanti, and I. Kerenidis, *Practical Quantum Coin Flipping*, Phys. Rev. A **84**, 052305 (2011).

A. Pappa, P. Jouguet, T. Lawson, A. Chailloux, M. Legré, P. Trinkler, I. Kerenidis and E. Diamanti, *Experimental plug and play quantum coin flipping*, Nature Communications. **5**, 3717 (2014).