INSTITUTO SUPERIOR TÉCNICO
Universidade Técnica de Lisboa

instituto de telecomunicações

# Quantum Commitments Based on Complementarity - Contract Signing

N. Paunković, P. Mateus and J. Bouda

*Phys. Rev. A,* ***84****, 062331 (2011)*

*Workshop on Quantum Telecommunications, 15 – 17 May 2013, Lisbon*

# Context and objectives

Objective:

Alice and Bob want to sign a contract message **m** remotely, but do not trust each other.

Problem:

Devise a *fair* and *viable* contract signing protocol.

- *Fair* – either *both* Alice and Bob *receive* each others' signed messages *or none* of them *does*.
- *Viable* – if *both* agents are *honest*, then they *receive* each others' signed messages.

# Context and objectives

- Ideal fair contract signing protocol

  Alice and Bob exchange the signed messages ***through*** a third trusted party (the Trent) that verifies the validity of the signatures.

  *Is it possible to eliminate the information exchange with the third trusted party (Trent)?*

- Impossibility result

  There exists no fair contract signing protocol without communicating with a third trusted party.

# Context and objectives

- Optimistic protocols:

  The third trusted party in involved *only* when one party is *cheating* or the communication is *interrupted*;

- Probabilistic protocols:

  Signatures are obtained with certain probabilities. *Probabilistic fairness* – no significant advantage over the other side.

Agents exchange each others' *commitments*.

Using them, they can *bind* the contract:

obtain *signed certificates* (contracts) from Trent.

# The Protocol

In order for it to be fair, any contract signing protocol has to force a client to make *only one* out of two possible choices – *accept* or *reject* the contract.

Agents reveal their choices by measuring *one* of the *two complementary* observables.

Gaining information about one corresponds to the *acceptance*, while acquiring it about the other corresponds to *rejection* of the contract.

The *Accept* basis

$$\mathcal{B}_A = \{|0\rangle, |1\rangle\}$$

The *Accept* Observable

$$\hat{A} = 1 \cdot |1\rangle\langle 1| + 0 \cdot |0\rangle\langle 0|$$

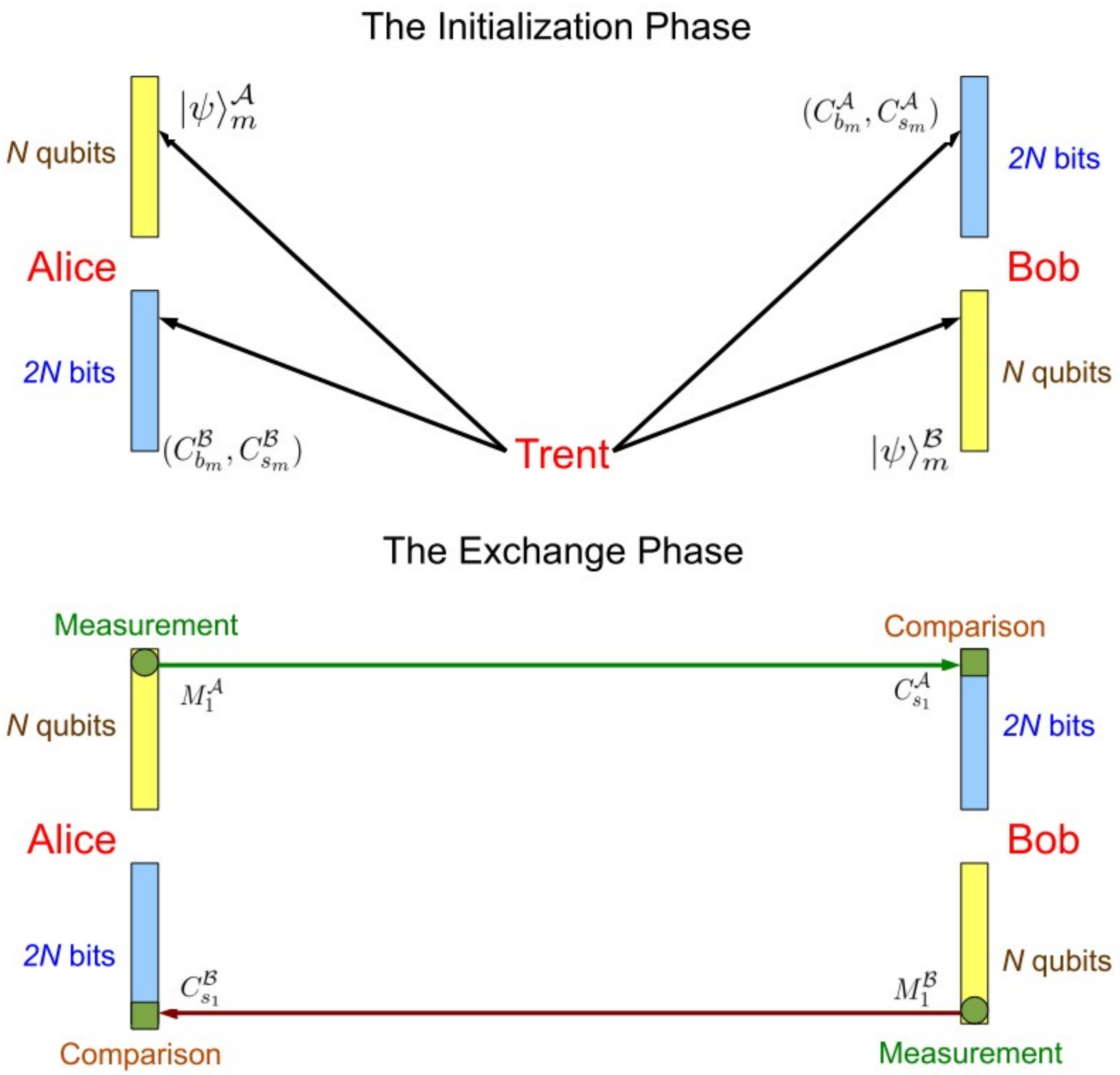
The *Reject* basis

$$\mathcal{B}_R = \{|-\rangle, |+\rangle\}$$

The *Reject* observable

$$\hat{R} = 1 \cdot |+\rangle\langle +| + 0 \cdot |-\rangle\langle -|$$

Each qubit state $|\psi\rangle \in \{|0\rangle, |1\rangle, |-\rangle, |+\rangle\}$ is defined by two classical bits $C = (C_b, C_s)$, first of which defines the basis ($C_b = 1$ if $|\psi\rangle \in \mathcal{B}_\mathcal{A}$, while $C_b = 0$ otherwise) while the second defines the particular state from a given basis ($C_s = 1$ if $|\psi\rangle \in \{|1\rangle, |+\rangle\}$, while $C_s = 0$ otherwise).


The Initialization Phase
$|\psi\rangle_m^{\mathcal{A}}$
$(C_{b_m}^{\mathcal{A}}, C_{s_m}^{\mathcal{A}})$
N qubits
2N bits
Alice
Bob
2N bits
N qubits
$(C_{b_m}^{\mathcal{B}}, C_{s_m}^{\mathcal{B}})$
Trent
$|\psi\rangle_m^{\mathcal{B}}$
The Exchange Phase
Measurement
Comparison
$M_1^{\mathcal{A}}$
$C_{s_1}^{\mathcal{A}}$
N qubits
2N bits
Alice
Bob
2N bits
N qubits
$C_{s_1}^{\mathcal{B}}$
$M_1^{\mathcal{B}}$
Comparison
Measurement

# The Protocol – Binding Phase

Agent can *bind* the contract if:

- (s)he *accepted* the contract,
- the other agent did *not reject* it.

Passing the accept/reject test:

A client has to establish *perfect correlations*

on $\alpha|A|$ ($\alpha|R|$) qubits from the Accept (Reject) basis.

*Acceptance ratio*: $1/2 < \alpha < 1$.

Acceptance ratio is *random*, given by $p(\alpha)$.

# Fairness of the Protocol

Working assumption: only Accept or Reject allowed.

Exchange phase *finished*: *no both* accept and reject (security of BB84).

Exchange phase *interrupted*:

- to *bind*, a client measures the *Accept* observable;
- *otherwise*, the *Reject*.

Cheating is *detected fast* (exponentially): *no* client is *privileged*.

Probabilities to accept the contract stay high, to reject decrease (but stay almost equal).

The protocol is *fair*!

# Fairness of the Protocol

Working assumption: only Accept or Reject allowed.

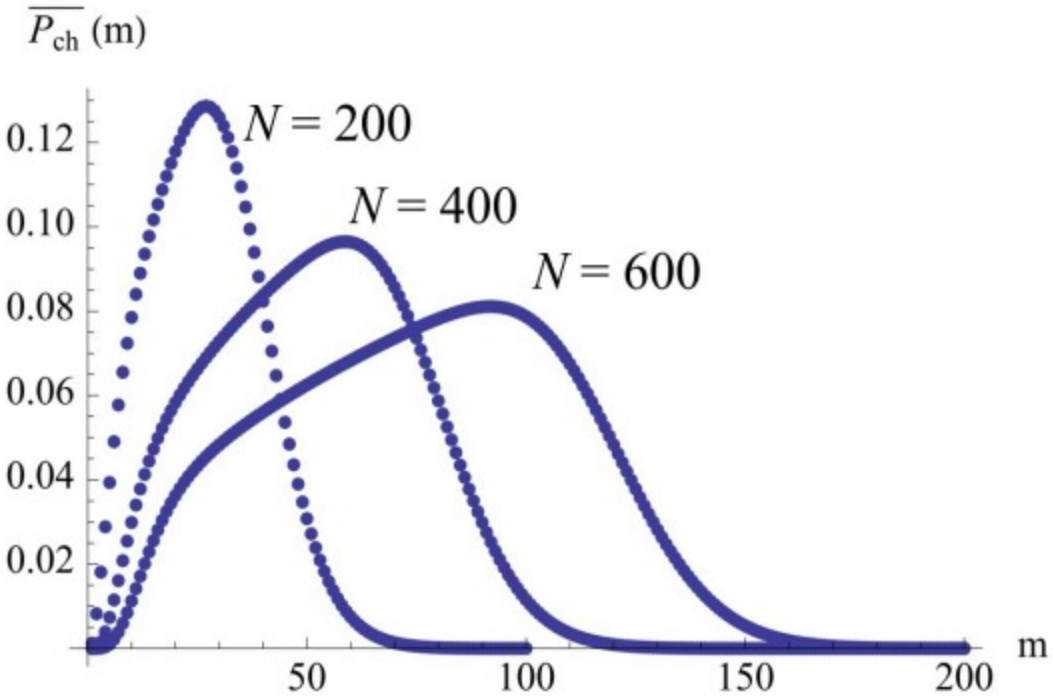
The probability for a client to be able to reject the contract after playing the accept strategy for $m$ steps, for a fixed acceptance ratio $\alpha$ is $P_R(m, \alpha)$.

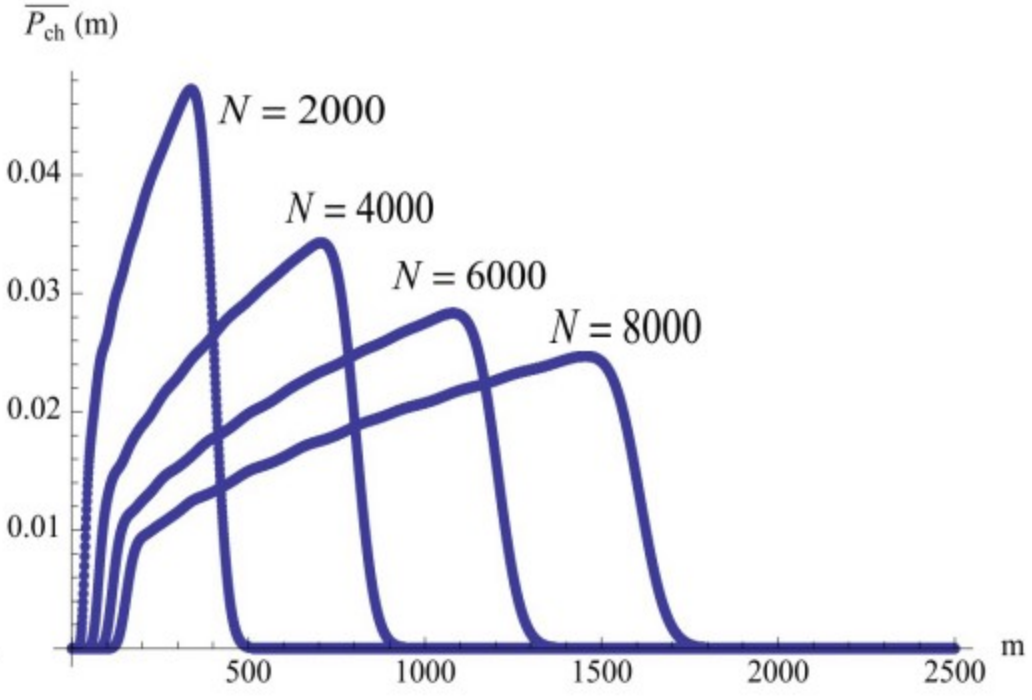
The probability for Bob's successful cheating is the product of the probability that he can still reject the contract and the probability that Alice cannot:

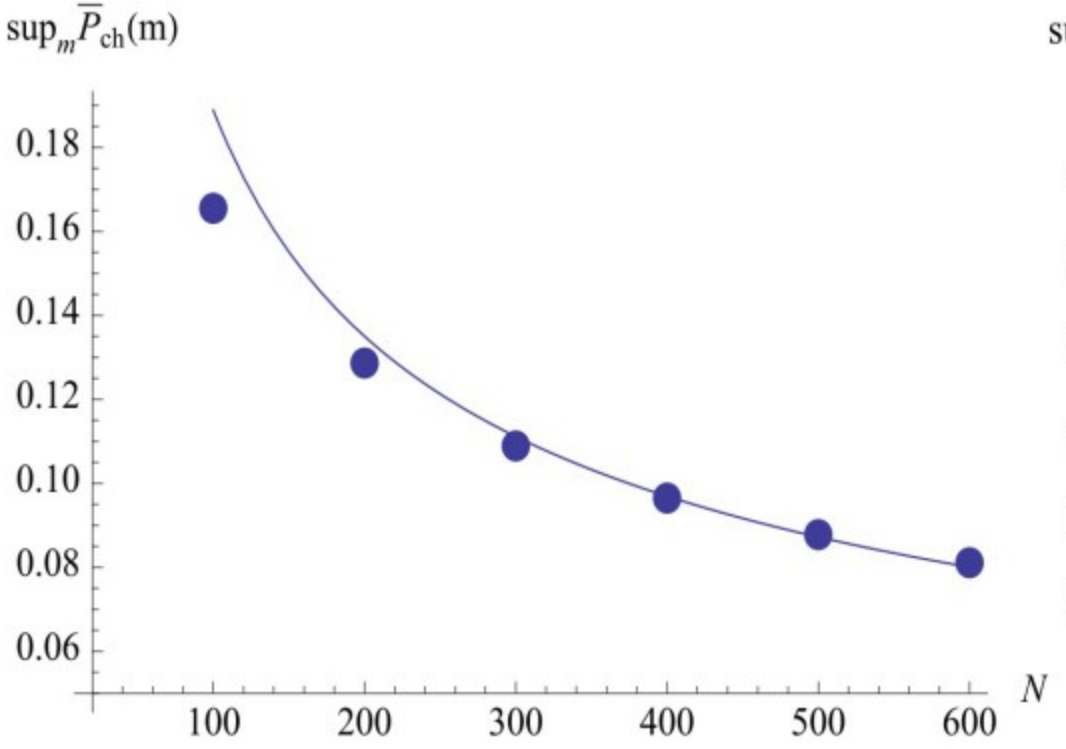
$$P_{ch}(m; \alpha) = P_R(m; \alpha)(1 - P_R(m; \alpha)).$$

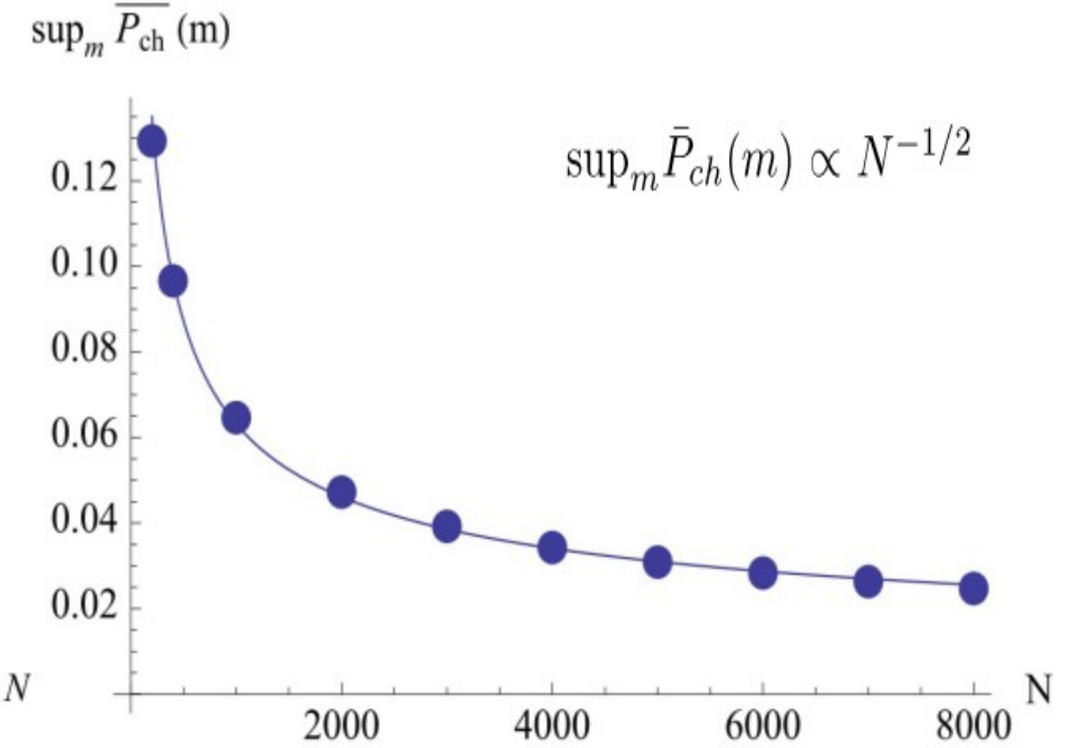
The *expected* probability for successful cheating, for a given probability distribution $p(\alpha)$:

$$\bar{P}_{ch}(m) = \int_{I_\alpha} p(\alpha) P_{ch}(m; \alpha) \mathbf{d}\alpha.$$


$\overline{P_{ch}}$ (m)
N = 200
N = 400
N = 600
0.12
0.10
0.08
0.06
0.04
0.02
50
100
150
200
m


$\overline{P_{ch}}$ (m)
N = 2000
N = 4000
N = 6000
N = 8000
0.04
0.03
0.02
0.01
500
1000
1500
2000
2500
m


$\sup_m \overline{P}_{ch}$(m)
0.18
0.16
0.14
0.12
0.10
0.08
0.06
100
200
300
400
500
600
N


$\sup_m \overline{P_{ch}}$ (m)
$\sup_m \bar{P}_{ch}(m) \propto N^{-1/2}$
0.12
0.10
0.08
0.06
0.04
0.02
2000
4000
6000
8000
N

# Fairness of the Protocol

## General one-qubit orthogonal measurements (assuming perfect measurements and channels)

Assumption: Alice notices cheating after $m$ steps

**Only $\hat{R}/\hat{A}$ measurements allowed.** Alice performs $m$ measurements of $\hat{A}$, while Bob performs $(m-\delta m)$ measurements of $\hat{A}$ and $\delta m$ measurements of $\hat{R}$. The probability to cheat (for a given $\alpha$) is:

$$P_{ch}(m;\alpha) = P_R(m-\delta m,\alpha)[1-P_R(m,\alpha)].$$

The probability to obtain wrong result in measuring $\delta m$ times the observable $\hat{R}$ on states prepared in the Accept basis is $p_w(\delta m) = 1-(3/4)^{\delta m}$, therefore $\delta m \approx 1$.

# Fairness of the Protocol

## General one-qubit orthogonal measurements (assuming perfect measurements and channels)

Assumption: Alice notices cheating after *m* steps

**All one-qubit orthogonal measurements allowed.** Bob measures $k = k_a + k_r$ times "rotated" observable $\hat{K}$ (out of total $m = m_a + m_r$ measurements), which is equivalent to:

- $q_a \cdot k_a$ measurements of $\hat{A}$ and $\delta m_a = [1 - q_a] \cdot k_a$ measurements of $\hat{R}$ on qubits from the Accept basis, where $q_a = \cos\theta$. Thus, the probability to notice cheating after $k_a$ measurements of $\hat{K}$ is $\tilde{p}_w(\delta m_a) = \tilde{p}_w([1 - q_a]k_a) = 1 - (1/2)^{[1-q_a]k_a}$ and Bob's probability to accept the contract is $P_A(m - \delta m_a, \alpha)$;

- $q_r \cdot k_r$ measurements of $\hat{A}$ and $\delta m_r = [1 - q_r] \cdot k_r$ measurements of $\hat{R}$ on qubits from the Reject basis, where $q_r = \cos\theta'$. Thus, Bob's measurements are equivalent to $(m_r - \delta m_r)$ measurements of $\hat{A}$ on qubits from Reject basis and his probability to reject is smaller or equal than $P_R(m - \delta m_r, \alpha)$.

Since $\tilde{p}_w(\delta m_a) = 1 - (1/2)^{[1-q_a]k_a}$, either $k_a$ is small, or $q_a \approx 1$. In case of $q_a \approx 1$, we have that $q_r \approx 0$: the observable $\hat{K}$ is close to $\hat{A}$ and Bob's strategy is close to that of an honest client. In case, $k_a$ is small, we have that $\delta m_a$ is also small and Bob's probability to accept the contract is close to one, $P_A(m, \alpha) \approx 1$. Moreover, since for typical cases $k_a \approx k_r$, we have that typically Bob's probability to reject the contract is approximatelly $P_R(m, \alpha)$. Therefore, the corrected probability to cheat, averaged over all possible distribution of states (from the Accept and the Reject bases) and all possible strategies of the clients, will not be considerably altered and the protocol would still be fair, even if arbitrary number of observables $\hat{K}_i$ is allowed.

# Fairness of the Protocol

## Real-life scenario – imperfect channels and measurements

In the case of measurement errors, imperfect quantum memories and noisy channels, one must introduce the error tolerance $\eta = M_w/M$, where $M_w = \langle m_w \rangle \equiv \eta M$ is the expected number of wrong results obtained in measuring an observable on $M$ qubits prepared in states from the observable's eigenbasis. Coefficient $\eta$ gives the ratio of unavoidably produced wrong results: to detect cheating would then mean to obtain more than expected, according to $\eta$, wrong results. For $\eta < (1 - \alpha)$ and big enough $N$, our protocol would therefore still be fair.

# Advantages

- *No Trent* during the *commitment* phase (avoiding bottlenecks);
- *Optimistic*: Trent is *rarely* asked to bind the contract, due to its fairness (*decreasing* expensive *resources*);
- Low use of signatures: *small number of keys* needed to be generated;
- *Abuse-free*: only Trent and Bob have information about Alice's qubits. Bob has *no proof* to anybody else that *he communicated* with Alice;
- *Easy to implement* with the current technology (modulo stable memories – practical quantum bit commitment);
- *Conceptually novel* approach to the problem.

# Future Lines of Research

- Prove *analytics* for *asymptotic* behavior;
- Analyze *fairness* against global *coherent* measurements;
- Analyze *real-life scenario* with explicit noise and measurement models;
- Analyze protocol with *two* instead of four *states* (B92);
- Analyze protocols with *entangled states*;
- Analyze generalizations to *more than two clients;*
- *Analyze practical quantum bit commitment protocol;*
- *Design other quantum security protocols that need timely decisions – simultaneous dense coding and teleportation (arXiv:1106.3956 [quant-ph]).*