Quantum contract signing

N. Paunković[1], P. Mateus[1] and J. Bouda[2]
[1]*SQIG – Instituto de Telecomunicações, IST, Lisbon, P-1049-001 Lisbon, Portugal and*
[2]*Faculty of Informatics, Masaryk University, Botanická 68a, 60200, Brno*

We present a probabilistic quantum contract signing protocol between two clients that requires no communication with the third trusted party during the commitment (i.e. signature exchange) phase. We discuss its fairness and show that it is possible to design such a protocol for which the probability of a dishonest client to cheat becomes negligible, and scales as $N^{-1/2}$, where N is the size of the signature, in bits. This way, our protocol over performs the classical probabilistic protocol by Ben-Or *et. al.* [4], for which the probability to cheat can be as high as $1/4$. We discuss the real-life scenario when the measurement errors and qubit state corruption due to noisy channels occur and argue that for real, good enough measurement apparatus and transmission channels, our protocol would still be fair. Our protocol could be implemented by today's technology, as it requires in essence the same type of apparatus as the one needed for BB84 cryptography protocol. Finally, we show that it is possible to generalize our protocol to an arbitrary number of clients.

PACS numbers:

Contract signing [1] is an important security task with many applications, namely to stock market and others [2]. It is a two party protocol between Alice and Bob who share a common contract and want to exchange each others' commitments to it, thus binding to the terms of the contract. Usually, commitment is done by signing the contract: the two parties meet and sign the document on the spot.

With the technology development, situations when parties involved are physically far apart from each other become more relevant every day - distant people can communicate using ordinary or e-mail, internet, etc. This poses new challenges to the problem. Forcing two spatially distant parties to exchange signatures opens the possibility of a fraud. For example, Bob may get the commitment from Alice without committing himself, which creates an *unfair situation*. Indeed, having Alice's commitment enables Bob to appeal to a judge to bind (i.e. to enforce) the contract, by showing Alice's commitment to the contract (together with his). On the other hand, although, Alice did commit, she cannot prove that she sent her commitment to Bob and thus cannot appeal to a judge. Moreover, she cannot prove that she did not receive Bob's commitment. The problem when distant parties wish to commit to a common contract lies in the impossibility for an agent, say Alice, to prove whether she has indeed committed to it or not. Note that initially Bob did not commit, but having Alice's commitment puts him in a position to later in time choose whether to bind the contract or not, while Alice has no power to do either of the two.

A simple solution to this unfair situation is to have a trusted third party (usually referred to as Trent) mediating the transaction - Alice and Bob send their commitments to Trent, who then returns the receipts to the senders, and performs the message exchange *only* upon receiving both of the commitments. However, Trent's time and resources are expensive and should be avoided as much as possible. Unfortunately, it has been shown that there is no fair and viable contract signing protocol [1], unless during the commitment phase (i.e., the signature exchange phase) the signing parties communicate with a common trusted agent, i.e., Trent. By *fair* protocol we mean that either both parties get each other's commitment or none gets. By *viable* protocol we mean that, if both parties behave honestly, they will both get each others' commitments. The proof of the above impossibility result is rather simple, and is related with the impossibility of establishing distributed consensus in asynchronous networks [3].

One way to come around this difficulty is to relax the fairness condition probabilistically. *Probabilistic fairness* allows one agent to have ϵ more probability of binding the contract over the other agent. In this case, for an arbitrarily small ϵ solutions have been found where the number of exchanged messages between the agents is minimized [4]. Another workaround is to consider optimistic protocols that do not require communication with Trent unless something wrong comes up [5].

In this paper, we present a contract signing protocol where *no information* with a trusted third party (Trent) is exchanged during the commitment phase. The information exchange takes place during the initialization phase and possibly later during the (contract) binding phase. It is a probabilistic protocol: an agent has at most $\epsilon << 1$ more probability of binding the contract over the other agent. Moreover, our protocol satisfies even stronger condition: the probability of an agent to cheat can be made negligible. By *probability to cheat* we mean the probability that an agent, say Bob, can bind a contract, while Alice cannot. If $P_{bind}^{\mathcal{B}/\mathcal{A}}$ is a probability that, upon completing the commitment phase, Alice/Bob can bind the contract, then Bob's probability to cheat is $P_{ch}^{\mathcal{B}} = P_{bind}^{\mathcal{B}}(1 - P_{bind}^{\mathcal{A}})$. Obviously, the condition $P_{ch}^{\mathcal{B}/\mathcal{A}} < \epsilon$ is stronger than the condition $|P_{bind}^{\mathcal{B}} - P_{bind}^{\mathcal{A}}| < \epsilon$, as $P_{ch}^{\mathcal{B}} - P_{ch}^{\mathcal{A}} = P_{bind}^{\mathcal{B}} - P_{bind}^{\mathcal{A}}$. In the classical protocol proposed by Ben-Or *et. al.* [4], the probability to cheat could be as high as $1/4$. To achieve negligible probability to cheat, we exploit *quantum* systems, that has shown to be useful in wide range of problems, such as quantum cryptography [6, 7], factorizing prime numbers [8], decreasing communication complexity [9], etc.

In the following, we present our quantum contract signing protocol that requires no communication with Trent during the commitment phase. Then, we discuss its fairness and show that it is possible to design such a protocol for which the probability of a dishonest client to cheat becomes negligible. We also argue that under the assumption of noisy channels and realistic measurements with error rates, it is still possible to design a fair protocol. An alternative version that uses entanglement and the many-party generalization of the protocol are discussed. In conclusions, we give an overview of the results and suggest some of the possible future lines of research.

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. A conceptually similar situation occurs in quantum physics, where an observer has to choose to measure *only one* out of the two possible observables (say, position and momentum) and gain information about only one out of two complementary properties of a system.

This basic feature of quantum physics is essential for our protocol: instead of sending information (a physical system in a definite state) to Trent about accepting or rejecting the contract, Alice reveals her choice by measuring one of the two complementary observables, thus acquiring information about only one of the two possible features of the system given to her by Trent. Gaining information about one feature thus corresponds to the acceptance, while acquiring information about the other corresponds to rejection of the contract.

As the act of a client's measurement is local, no information is exchanged between a client and Trent, during the commitment phase. Only latter, during the possible binding phase, this (classical) information obtained in a measurement is confronted with Trent's and used as verification of client's choice.

To ensure timely decisions, Trent provides Alice with the classical information of the quantum state in which Bob's quantum system is prepared, and vice versa. This way, the clients can confront each others' measurement results with the classical data provided by Trent, thus obtaining each others' commitment choices before a certain fixed moment in time. Since quantum mechanics is essentially a probabilistic theory, the clients are supplied by a number of qubits, giving rise to the probabilistic fairness of the protocol.

In our protocol, we use the simplest two-dimensional quantum systems called qubits. The complementary observables could be seen as spin components (for electrons), or linear polarizations (for photons), along two mutually orthogonal axes. We will denote the two observables measured on single qubits as *the Accept* observable $\hat{A}$ and *the Reject* observable $\hat{R}$. Measuring $\hat{A}$ corresponds to the acceptance, while measuring $\hat{R}$ corresponds to the rejection of the contract. The two observables $\hat{A}$ and $\hat{R}$ are required to be mutually complementary and are given by mutually unbiased bases [10] $\mathcal{B}_A = \{|0\rangle, |1\rangle\}$ (*the Accept* basis) and $\mathcal{B}_R = \{|-\rangle, |+\rangle\}$ (*the Reject* basis), respectively, such that $|\pm\rangle = (|1\rangle \pm |0\rangle)/\sqrt{2}$. Both observables have the same eigenvalues, 0 and 1, such that $\hat{A} = 1 \cdot |1\rangle\langle 1| + 0 \cdot |0\rangle\langle 0|$ and $\hat{R} = 1 \cdot |+\rangle\langle +| + 0 \cdot |-\rangle\langle -|$. Trent randomly prepares qubits each in one of the four states $\{|0\rangle, |1\rangle, |-\rangle, |+\rangle\}$ from the Accept or the Reject basis. For each qubit in a state $|\psi\rangle$ sent to, say Alice, Trent sends to Bob classical bits $C(|\psi\rangle)$ assigned to this state. Alice then measures either of the observables $\hat{A}$ or $\hat{R}$, depending on whether she decides to accept or reject the contract, respectively, and then communicates her result to Bob.

This way, by choosing one of the two measurements performed on a sequence of qubits, Alice produces one of two mutually exclusive sets of measurement outcomes that serve as a signature of her choice. By sending the results to Bob, she informs him of her decision by some fixed moment in time t_0. The same is done by Bob. In the binding phase, each party is asked to confront her/his measurement results with the Trent's corresponding classical bits. The perfect correlation between measurement results and the corresponding classical information for qubits prepared in the Accept/Reject basis confirms a client's Accept/Reject choice.

Obviously, the commitment phase as described above suffers from the same problem as any classical protocol not involving information exchange with Trent: upon receiving Alice's results, Bob can stop communication and safely postpone his decision to accept or reject the contract to a later moment in time. Thus, we require that the exchange of measurement outcomes between clients happens in steps, (qu)bit by (qu)bit. Nevertheless, if we require perfect correlations between the measuring results and the corresponding classical information for *all* qubits distributed to a client, a dishonest party has still probability of $1/4$ to successfully cheat.

Thus, we require that in order to accept/reject the contract, a client has to establish perfect correlations on $\alpha N_{A/R}$ qubits prepared in the Accept/Reject basis (with the total number of qubits $N = N_A + N_R$), where $1/2 < \alpha < 1$. We call α the *acceptance ratio* (note that, for a protocol to be viable, it is necessary that $\alpha > 1/2$). In this scenario, a client is allowed to obtain $(1-\alpha)N_{A/R}$ wrong results for the states prepared in the basis of her/his choice (Accept or Reject). If α is sufficiently large, this eliminates the possibility of obtaining good enough correlations for both group of qubits. On the other hand, for a fixed α and large enough N, an honest client will be given a possibility to make a few "wrong" measurements before (s)he detects a dishonest side measurements in the Reject basis and change her/his strategy by rejecting the contract.

Unfortunately, even this protocol allows for a strategy of a dishonest client to successfully cheat with probability $1/4$. But if α, determined by Trent by sampling a random variable described by a publicly known probability distribution $p(\alpha)$, is itself unknown to the clients, and revealed only later, during the binding phase, the probability to cheat becomes negligible, for big enough N, and our protocol becomes *fair*.

The protocol is divided into three phases: the Initialization, the Commitment (see Fig. 1) and the Binding phase.

The Initialization Phase: Trent produces N pairs of qubits in states $(|\psi\rangle_m^{\mathcal{A}}, |\psi\rangle_m^{\mathcal{B}})$ with the corresponding classical bits $(C_m^{\mathcal{A}}, C_m^{\mathcal{B}}) = ((C_{b_m}^{\mathcal{A}}, C_{s_m}^{\mathcal{A}}), (C_{b_m}^{\mathcal{B}}, C_{s_m}^{\mathcal{B}}))$, with $m \in \{1, \ldots N\}$. The rule of assigning the classical data to the corresponding qubit states is the following: $C_{b_m}^{\mathcal{A}/\mathcal{B}} = 1$ if

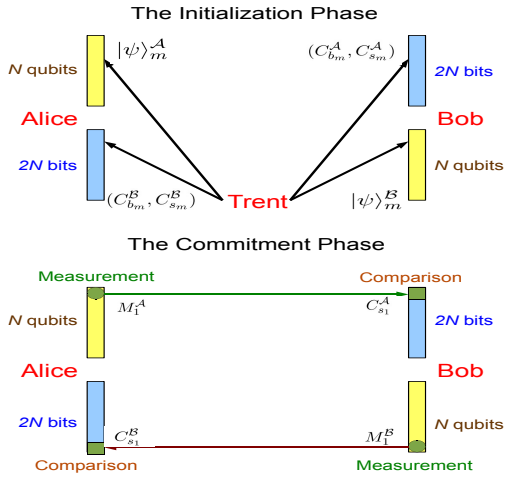

FIG. 1: (color online) The Initialization and The Commitment Phase.

$|\psi\rangle_m^{\mathcal{A}/\mathcal{B}} \in \mathcal{B}_A$, while $C_{b_m}^{\mathcal{A}/\mathcal{B}} = 0$ otherwise; $C_{s_m}^{\mathcal{A}/\mathcal{B}} = 1$ if $|\psi\rangle_m^{\mathcal{A}/\mathcal{B}} \in \{|1\rangle, |+\rangle\}$, while $C_{s_m}^{\mathcal{A}/\mathcal{B}} = 0$ otherwise. Each qubit state is randomly chosen from the set $\{|0\rangle, |1\rangle, |-\rangle, |+\rangle\}$. Trent distributes to Alice N qubits $|\psi\rangle_m^{\mathcal{A}}$ and $2N$ classical bits $C_m^{\mathcal{B}}$, and analogously for Bob, keeping the copy of the classical data to himself.

The Commitment Phase: Alice and Bob perform measurements on their qubits and exchange the measurements results with each other. The exchange is supposed to be finished until some previously arranged moment in time t_0. Without the loss of generality, we assume Alice is the first to start communication. She measures an observable of her choice ($\hat{A}$ or $\hat{R}$) on the state $|\psi\rangle_1^{\mathcal{A}}$, obtaining the result $M_1^{\mathcal{A}} \in \{0, 1\}$ and sends it to Bob. Bob compares $M_1^{\mathcal{A}}$ with $C_{s_1}^{\mathcal{A}}$. If the values are different, Alice measured her qubit in the basis corresponding to $(1+C_{b_1}^{\mathcal{A}})$mod2. Otherwise, the comparison is inconclusive. Next, Bob repeats the procedure described for Alice. The rest of the exchange consists in repeating the above procedure for the states $(|\psi\rangle_m^{\mathcal{A}}, |\psi\rangle_m^{\mathcal{B}})$ with $m \in \{2, \ldots N\}$.

The Binding Phase: Without the loss of generality, we assume that Alice requests for Trent to bind the contract. Trent announces the value α sampled from a known probability distribution $p(\alpha)$. In order for a contract to be binding two requirements have to be satisfied. Alice has to present at least $\alpha N_A^{\mathcal{A}}$ results, obtained by measuring her qubits from the Accept basis, whose values are the same as the corresponding classical data: if $C_{b_m}^{\mathcal{A}} = 1$ then $M_m^{\mathcal{A}} = C_{s_m}^{\mathcal{A}}$, for at least $\alpha N_A^{\mathcal{A}}$ values (note that in general Alice and Bob have different numbers of the Accept qubits, $N_A^{\mathcal{A}} \neq N_A^{\mathcal{B}}$). Secondly, Bob should not be able to present satisfactory correlations between his results obtained by measuring his qubits prepared in the Reject basis with the corresponding classical data: if $C_{s_m}^{\mathcal{B}} = 0$ then $M_m^{\mathcal{B}} = C_{s_m}^{\mathcal{B}}$ for less than $\alpha N_R^{\mathcal{B}}$ qubits. To bind the contract, Alice has to show that she accepted it, while Bob did not reject it.

In the following, we show that there exists a strategy for an honest side (say, Alice) that would always, with high probability, leave her with the option to reject the contract in case Bob attempts to cheat, unless both sides have already accepted the contract and are unable to reject it. First, we assume that only $\hat{A}$ or $\hat{R}$ are measured, and that no measurement errors or qubit state corruption occur. At the end, we discuss general observables and the real-life scenario of imperfect measurements and noisy channels.

First, note that it is impossible for Bob to reproduce *all* classical data corresponding to his qubit states, even when general measurements are allowed, unless with negligible probability (which secures the BB84 protocol [6, 7] as well). The probability to guess the classical data is continuous in α, thus Bob cannot pass *both* the commit and the reject test during the binding phase, for a suitable range of α. Therefore, he must trick Alice by playing a strategy such that after a certain step m in the results' exchange, with high probability Alice is no longer able to reject the contract while Bob can. Since only $\hat{A}$ or $\hat{R}$ are measured, Bob starts the information exchange by measuring his qubits in the Accept basis, pretending to be an honest side.

After m steps, Bob's probability to cheat is $P_{ch}^{\mathcal{B}}(m) = P_{bind}^{\mathcal{B}}(m)(1 - P_{bind}^{\mathcal{A}}(m))$, where Bob's/Alice's probability to bind the contract $P_{bind}^{\mathcal{B}/\mathcal{A}}(m) = P_A^{\mathcal{B}/\mathcal{A}}(m)(1 - P_R(m)^{\mathcal{A}/\mathcal{B}})$ is given in terms of probability to accept $P_A^{\mathcal{B}/\mathcal{A}}(m)$ and reject $P_R^{\mathcal{B}/\mathcal{A}}(m)$ the contract (to bind it, Bob has to accept, while Alice must not be able to reject the contract). If out of m steps Bob measures the Reject observable δm times, the probability to obtain wrong results on states from the Accept basis, and thus being detected cheating, is exponentially fast approaching to one, $p_w(\delta m) \propto 1 - 2^{-\delta m/2}$. Therefore, for $1/2 < \alpha < 1$ and large enough N, $\delta m << (1-\alpha)N$ and we can assume $P_A^{\mathcal{B}}(m)\ 1 = P_A^{\mathcal{A}}(m)$ (Alice is honest and measures only $\hat{A}$), while $P_R^{\mathcal{B}}(m) = P_R^{\mathcal{A}}(m - \delta m)$. The expected δm is small and for large enough N the probability to reject the contract is a slow function of m, $P_R^{\mathcal{A}}(m)\ P_R^{\mathcal{A}}(m - \delta m)$. Therefore, we can assume $P_R^{\mathcal{A}}(m)\ P_R^{\mathcal{B}}(m)$.

We will first evaluate the probability to (be able to) reject the contract $P_R(m; \alpha, N_R)$ (obtain less than $(1-\alpha)N_R$ wrong results on qubits from the Reject basis, measuring the Accept observable on the first m qubits), for a given acceptance ratio α and the number of qubits prepared in the Reject basis N_R, keeping for simplicity the N dependence implicit. Then $P_R(m; \alpha) = \sum_{N_R=0}^{N} q(N_R) P_R(m; \alpha, N_R)$, with $q(N_R) = 2^{-N} \begin{pmatrix} N \\ N_R \end{pmatrix}$ being the probability to have exactly N_R states from the Reject basis, and $P_{ch}(m; \alpha) = P_R(m; \alpha)(1 - P_R(m; \alpha))$. Finally, the *expected* probability to cheat, with respect to a given probability distribution $p(\alpha)$ on the segment I_α, is $\bar{P}_{ch}(m) = \int_{I_\alpha} p(\alpha) P_{ch}(m; \alpha) d\alpha$.

For $m < (1-\alpha)N_R$ there is always a chance to reject the contract and $P_R(m; \alpha, N_R) = 1$. Otherwise, $P_R(m; \alpha, N_R) = \sum_{n=n'}^{m'} P(n \text{ in R}; m, N_R) P_R(n \text{ in R}; \alpha, N_R)$. Here,

$P(n \text{ in R}; m, N_R) = \binom{m}{n}\binom{N-m}{N_R-n}\binom{N}{N_R}^{-1}$ is the probability that exactly n out of m qubit states are from the Reject basis, while $P_R(n \text{ in Reject}; \alpha, N_R) = 2^{-n}\sum_{i=0}^{T}\binom{n}{i}$ is the probability of being able to reject the contract if n qubits are from the Reject basis, where $T = (1-\alpha)N_R - 1$ if $n \geq (1-\alpha)N_R$ and $T = n$ otherwise. Due to the constraint of having exactly $N_{A/R}$ qubits from the Accept/Reject basis, the range of the summation for n is given by $n' = 0$ for $m \leq N_A$ while $n' = m - N_A$ otherwise, and $m' = m$ for $m \leq N_R$ while $m' = N_R$ otherwise.

Using the simplest uniform probability $p(\alpha) = 1/I_\alpha$ on the segment $I_\alpha = [0.9, 0.99]$, we numerically evaluated the expected probability to cheat $\bar{P}_{ch}(m)$ for up to $N = 600$, while for the "typical" case of $N_A = N_R$ we managed to evaluate it up to $N = 8000$, see Fig. 2. We see that the *fairness condition* $\sup_m \bar{P}_{ch}(m) << 1$ is satisfied (for $N = 600$ we got $\sup_m \bar{P}_{ch}(m) = \bar{P}_{ch}(92) = 0.0811$, while for $N_A = N_R$ we have $\sup_m \bar{P}_{ch}(m) = \bar{P}_{ch}(1455) = 0.0247$ for $N = 8000$), which is explicitly shown on Fig. 2. Moreover, the numerical fit gives $\sup_m \bar{P}_{ch}(m) \propto N^{-1/2}$ behavior.

Now, let us assume that Alice performs m measurements of $\hat{A}$ while Bob measures $m - k$ times $\hat{A}$ and k times $\hat{K} = 0 \cdot |m\rangle\langle m| + 1 \cdot |m^\perp\rangle\langle m^\perp|$, where $|m\rangle = \cos\frac{\theta}{2}|0\rangle + e^{\varphi}\sin\frac{\theta}{2}|1\rangle = \cos\frac{\theta'}{2}|-\rangle + e^{\varphi'}\sin\frac{\theta'}{2}|+\rangle$. Bob's measurements are equivalent to (for simplicity, we omit writing the α and N_R dependences): (i) $q_a \cdot k$ measurements of $\hat{A}$ and $\delta m = [1-q_a]\cdot k$ measurements of $\hat{R}$ on qubits from the Accept basis, where $q_a = \cos\theta$, and her probability to notice cheating is $p_w(\delta m)$; (ii) $q_r \cdot k$ measurements of $\hat{A}$ and $[1-q_r]\cdot k$ measurements of $\hat{R}$ on qubits from the Reject basis, where $q_r = \cos\theta'$. Thus, Alice's probability to reject is $P_R(m)$, while Bob's is $P_R(m - [1-q_r]k)$. The corrected probability to cheat is then $P_{ch}(m) = P_R(m - [1-q_r]k)[1 - P_R(m)]$. Since $p_w(\delta m) = 1 - 2^{-[1-q_a]k/2}$, either k is small, in which case $m - [1-q_r]k \approx m$, or $q_a \approx 1$, in which case $\hat{K} \approx \hat{A}$ and $q_r \approx 1$. Therefore, the corrected probability to cheat will not be considerably altered and the protocol would still be fair, even if arbitrary number of observables $\hat{K}_i$ is allowed.

The above argument could be generalized for joint L-qubit measurements, if $L \propto N^t$ and $t < 1$: for every joint observable $\hat{O}_L \neq \hat{A}^{\otimes L}$ there is a non-zero probability q_L that at least one wrong result will be obtained on the accept qubits, which scales as q_L^k, k being the number of $\hat{O}_L$ measurements (note that for ideal measurements, Alice will notice cheating as soon as she receives the *first* wrong result from Bob). In case $L \propto N$ the fairness of our protocol could be seen as a consequence of the security of the BB84 protocol [7]: Bob has to be correct on αN qubits from *both* the Accept and the Reject bases, which is, due to continuity in α of the probability to guess the classical data, for a suitable range of α impossible unless with negligible probability.

In the case of measurement errors 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 η gives the ratio of unavoidably produced wrong results. Therefore, for $\eta < \alpha$ and big enough N, our protocol would still be fair. Note that in this case, to notice cheating, Alice could use Bob's statistics for qubits from the Reject basis as well.

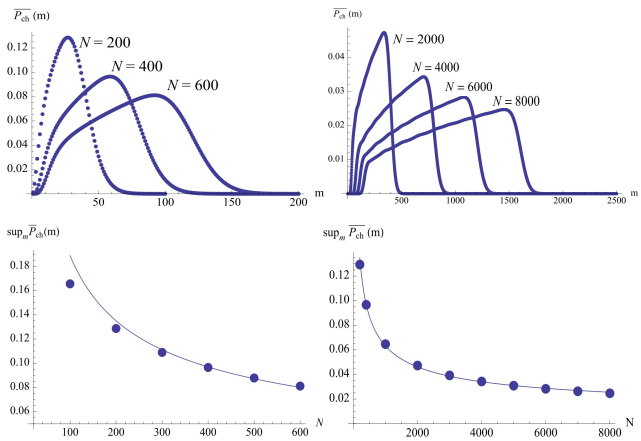

FIG. 2: (color online) The expected probability to cheat $\bar{P}_{ch}(m)$ (upper row) and the maximal expected probability to cheat $\sup_m \bar{P}_{ch}(m)$ (lower row) for the uniform $p(\alpha)$ on $I_\alpha = [0.9, 0.99]$. The plots from the left column represents present results for our protocol, while the right ones are for the restricted "typical" case of $N_A = N_R$. Note the scaling behavior $\sup_m \bar{P}_{ch}(m) \propto N^{-1/2}$.

We have presented a fair probabilistic quantum protocol for contract signing that not require the exchange of information with the trusted party during the commitment phase. Our fairness condition is stronger than the one satisfied by the classical protocol proposed by Ben-Or *et. al.* [4]. Analogously to the previous proposal of a quantum contract signing protocol [11], the present one could also be easily performed using entangled pairs instead of single qubits and classical information, but it does not require tamper-proof devices nor is based on the effects of decoherence. Our protocol can also be easily generalized to many clients, while still being fair in the stronger sense. Finally, our protocol could be easily performed with the current technology used in quantum cryptography.

The authors thank EU FEDER and FCT projects QSec PTDC/EIA/67661/2006 and QuantPrivTel PTDC/EEA-TEL/103402/2008. NP thanks the support from EU FEDER and FCT grants SFRH/BPD/31807/2006 and Ciência 2008. The authors acknowledge discussions with V. Božin and Č. Brukner.

[1] S. Even and Y. Yacobi, Technical Report 175, Technicon (1980).

[2] Asokan, N., Shoup V., and Waidner, M. Optimistic fair exchange of digital signatures. IEEE J. Sel. Areas Commun., 18,

4 (2000), 593–610.
[3] M. J. Fischer, N. A. Lynch and M. Paterson, J. ACM **32**, 374 (1985).
[4] M. Ben-Or, O. Goldreich, S. Micali and R. L. Rivest, *IEEE Transactions on Information Theory*, **36**, 40 (1990).
[5] N. Asokan, M. Schunter and M. Waidner, *ACM Conference on Computer and Communications Security*, 7 (1997).
[6] C. H. Bennett and G. Brassard, *IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India,* 175 (1984).
[7] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000); D. Mayers, J. ACM **48**, 351 (2001); V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[8] P. W. Shor, *Proc. 35nd Annual Symposium on Foundations of Computer Science*, IEEE Press, 124 (1994).
[9] Č. Brukner, M. Zukowski, J.-W. Pan and A. Zeilinger, Phys. Rev. Lett. **92**, 127901 (2004), H. Buhrman, R. Cleve, S. Massar, R. de Wolf, arXiv:0907.3584 (2001).
[10] I. D. Ivanović, J. Phys. A **14**, 3241 (1981).
[11] J. Bouda, P. Mateus, N. Paunkovic, and J. Rasga, Int. J. Quant. Inf. **6**, 219 (2008).