MATEMATIČKI VESNIK
МАТЕМАТИЧКИ ВЕСНИК
69, 1 (2017), 65–74
March 2017

research paper
оригинални научни рад

NECESSITY OF PARAMETER RANDOMIZATION IN QUANTUM CONTRACT SIGNING

Hana Almoner Louka

Abstract. We present a proof that randomization is necessary in quantum contract signing protocol of Paunković, Bauda and Mateus. We prove that for any fixed value of the protocol parameter α, for large N the probability of cheating can be as high as 25%, where N is the number of messages exchanged between the parties, and thus without randomization the protocol is not fair.

1. Introduction

In this section we give background and short review of the content of the paper.

A contract is a written or spoken agreement between two or more parties that specifies the obligations and duties of the signed parties.

Traditionally, signing a contract is done by the transacting parties who need to be present at the same place and the same time. Each party signs a copy of the contract and exchange signed papers, therefore every party gets a copy of the signed contract. In case the parties are not at the same place the parties can communicate using technical means, like e-mail, internet, etc.

Signing contract between two parties (Alice and Bob) using technical means posses new challenges, e.g. Bob may be cheating: Bob could get a copy of the contract with Alice's signature on it without signing the contract himself, which is an *unfair situation*.

Contract signing protocols, first formally introduced in [3], cannot be fair without involving a trusted third party, shortly: "TTP" (usually referred as Trent), as shown in [4].

Quantum information theory is based on Quantum mechanics, and the basic concept is that of a *qubit*. A qubit is a vector from a two dimensional Hilbert space. Quantum signing protocols are considered in this context.

2010 Mathematics Subject Classification: 81P94, 94A60
Keywords and phrases: contract signing protocol; parameter randomization; qubit

A quantum contract signing protocol was proposed by Paunković, Bouda and Mateus in [7]. It is based on concepts from quantum information theory (see for instance [6]). In this protocol, in *initialization phase* Trent produces N qubits each with corresponding classical data about the qubits received by the other party. In the next phase, the *exchange phase* Trent is not involved except in the case of interrupted exchange or when there is a proof of cheating. Such contract signing protocols are called *optimistic*, see [1]. Other than that, process consists of Alice and Bob making measurements of their choice on their qubits and exchanging the measurement results with each other. In the final phase, called the *binding phase* Trent will decide if the contract is valid based on the results of measurements of Alice and Bob. This resolves possible disputes: for instance, if Alice is honest, she can accept or reject contract as she wishes, and if Bob is a cheater Trent's judgment will be hugely in favour of an honest Alice.

In the Paunković-Bauda-Mateus protocol (see [7]), a parameter α is chosen according to some probability distribution. This parameter is a threshold, used by Trent to determine if the contract is binding or not, as explained in more detail in the next section. In the protocol from [7], this parameter is chosen randomly, in what we call a *randomization*. In other words, instead of using just one value of α, Trent's choice of α is not determined in advance. In the paper [7] a uniform distribution on the interval $[0.9, 0.99]$ was considered for choosing α, but any other probability distribution on the interval $(0.5, 1)$ can be considered. One may compare different probability distributions to see which are best suited for the purpose of quantum contract signing. However, in this paper we consider the question if this randomization can be skipped in the protocol. We show that the randomization is necessary for protocol to be fair, and that we cannot rely on a single value of the parameter α.

2. Protocol without randomization

Denote by $\{|0\rangle, |1\rangle\}$ the standard basis of a qubit, i.e. two dimensional Hilbert space.

Let

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \qquad \text{and} \qquad |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

We will call the states $\{|-\rangle, |+\rangle\}$ the "reject basis", and $\{|0\rangle, |1\rangle\}$ the "accept basis". Define

$$\widehat{A} = 1 \cdot |1\rangle \langle 1| + 0 \cdot |0\rangle \langle 0| \qquad \text{(reject observable)}$$

$$\widehat{R} = 1 \cdot |+\rangle \langle +| + 0 \cdot |-\rangle \langle -| \qquad \text{(accept observable)}$$

Steps of Paunković-Bauda-Mateus protocol of contract signing between Alice and Bob are as follows:

1. In the initialization phase, Trent chooses at random N qubits from the set $\{|-\rangle, |+\rangle, |1\rangle, |0\rangle\}$ and sends them to Alice, and other N to Bob. In addition,

Trent lets Alice know the states of qubits sent to Bob, and analogously for Bob. Therefore, Alice has N qubits, but does not know their states, whilst Bob knows the states of qubits sent to her, and vice versa.

2. In the exchange phase, Trent is not involved. If Alice wants to reject the contract, she will measure her first qubit in the reject basis (i.e. measure observable $\widehat{R}$ on her first qubit), end send result to Bob. If she wants to accept contract, she will measure $\widehat{A}$ instead and Bob will do the same, sending the result to Alice. The process continues until all N qubits are measured.

Note that almost half of the qubits sent to each Alice and Bob are in accept, and half in reject basis. Thus, Alice can note what the Bob is measuring and vice versa, by comparing the results sent to them on the qubits prepared in the states from the corresponding measurement observable/basis, when there should be a perfect agreement with the classical information sent by Trent. Thus, if Alice and Bob are honest and want to accept the contract, they will note this and do not need to invoke Trent (i.e. the protocol is viable). But, if Alice or Bob note that there is evidence of cheating, they have an option to stop communication, and proceed to binding. In this case, they will have an option to try to accept the contract, by measuring all the remaining qubits in the accept basis, or reject the contract, by measuring all the remaining qubits in the reject basis. After that they send all of their results to Trent, together with information about which $\widehat{A}$, or $\widehat{R}$ they measured.

3. In the binding phase, Trent makes the final decision if the contract is binding: accepted/valid, or rejected/void. In order to do that, Trent will get results of the measurement on all of their qubits by Alice and Bob. Then Trent chooses α randomly according to some probability distribution, so that it is between 0.5 and 1. Let N_R^B, N_A^B and N_R^A, N_A^A denote the number of of Bob's and Alice's qubits prepared in Reject (Accept) basis. The contract is binding to Alice and Bob, if Bob presents at least αN_A^B accept results and Alice presents less than αN_R^A reject results, or vice versa. If there is proof that Bob cheated, only Alice's results will count, and similarly if Alice cheated, only Bob's results will count. In all other cases, contract is declared invalid.

Paunković, Bouda and Mateus have shown that protocol is viable[1] and probabilistically fair[2], and the probability for a dishonest client to successfully cheat can be made arbitrarily small, i.e. as N goes to infinity, the probability of success at cheating goes to zero. Fair probabilistic contract signing (see [2] and [8]) protocols rely on concept of probabilistic fairness, which requires that, in case Trent is called upon, no agent has a significant (probabilistically) advantage over the other.

We will consider the case of fixed α and show that in this case, probability of cheating does not go to zero. We base our considerations on equations from [7], and will use them in our proof.

[1] Viable protocol is one where, if both parties behave honestly, they will both get each other's commitments.

[2] Fair protocol means that either both parties get each others' commitment or none gets.

Throughout this paper, in all formulas, where a non-integer parameter appears in binomial coefficients, we may understand its value when integer part is computed and omit it for brevity (in particular, we take integer part of m in formula (4)). The next equations are taken from [7].

The probability of cheating is given by (see formula (12) from [7]):

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

for a given m between 0 and N, and $\alpha \in (0.5, 1)$, where $P_R(m;\alpha)$, the expected probability to reject the contract is

$$P_R(m;\alpha) = \sum_{N_R=0}^{N} q(N_R) P_1(m;\alpha,N_R). \tag{2}$$

Here $q(N_R)$ is the probability to have exactly N_R states from the reject basis:

$$q(N_R) = 2^{-N}\binom{N}{N_R}, \sum_{N_R=0}^{N} q(N_R) = \sum_{N_R=0}^{N} 2^{-N}\binom{N}{N_R} = 1$$

and $P_1(m;\alpha,N_R)$ is the probability to (be able to) reject the contract:

$$P_1(m;\alpha,N_R) = \sum_{n=n'}^{m'} P_2(n;m,N_R) P_3(n;\alpha,N_R). \tag{3}$$

Here

$$n' = \begin{cases} m - N + N_R, & \text{if } m \geq N - N_R \\ 0, & \text{otherwise,} \end{cases} \qquad m' = \begin{cases} N_R, & \text{if } m \geq N_R \\ m, & \text{;otherwise,} \end{cases}$$

$$P_2(n;m,N_R) = \binom{m}{n}\binom{N-m}{N_R-n}\binom{N}{N_R}^{-1}, \tag{4}$$

$$P_3(n;\alpha,N_R) = 2^{-n}\sum_{i=0}^{T}\binom{n}{i}, \tag{5}$$

$$T = \begin{cases} n, & \text{if } n < (1-\alpha)N_R \\ (1-\alpha)N_R, & \text{otherwise.} \end{cases}$$

Note that these values are of various probabilities, and between 0 and 1.

Example 1. Consider the case $\alpha = 0.7$, $N = 3$, $m = 1$, and let us show how one computes $P_{ch}(m;\alpha)$. For that, we need to find $P_R(m;\alpha)$.

$$P_R(m;\alpha) = \sum_{N_R=0}^{N} q(N_R) P_1(m;\alpha,N_R)$$
$$= q(0)P_1(1;0.7,0) + q(1)P_1(1;0.7,1) + q(2)P_1(1;0.7,2) + q(3)P_1(1;0.7,3),$$

where $q(0) = 2^{-3}\binom{3}{0} = \dfrac{3}{(3-0)!\times 3!} = 0.125$, $q(1) = 2^{-3}\binom{3}{1} = \dfrac{3}{(3-1)!\times 3!} = 0.375$, $q(2) = 2^{-3}\binom{3}{2} = \dfrac{3}{(3-2)!\times 3!} = 0.375$, $q(3) = 2^{-3}\binom{3}{3} = \dfrac{3}{(3-3)!\times 3!} = 0.125$. We have $P_1(m;\alpha,N_R) = \sum_{n=n'}^{m'} P_2(n;m,N_R)P_3(n;\alpha,N_R)$.

Here. for $N_R = 0$ we have $n' = 0$, $m' = 0$, for $N_R = 3$ we have $n' = 1$, $m' = 1$ and in all other cases $n' = 0$, $m' = 1$. Then

$$P_1(1; 0.7, 0) = P_2(0; 1, 0)P_3(0; 0.7, 0) = 1,$$
$$P_1(1; 0.7, 1) = P_2(0; 1, 1)P_3(0; 0.7, 1) + P_2(1; 1, 1)P_3(1; 0.7, 1) = 0.833333,$$
$$P_1(1; 0.7, 2) = P_2(0; 1, 2)P_3(0; 0.7, 2) + P_2(1; 1, 2)P_3(1; 0.7, 2) = 0.666667,$$
$$P_1(1; 0.7, 3) = P_2(1; 1, 3)P_3(1; 0.7, 3) = 0.5.$$

So, we have

$$P_R(m; \alpha) = \sum_{N_R=0}^{N} q(N_R)P_1(m; \alpha, N_R)$$
$$= 0.125 \times 1 + 0.375 \times 0.833333 + 0.375 \times 0.666667 + 0.125 \times 0.5 = 0.75$$

and

$$P_{ch}(m; \alpha) = P_R(m; \alpha)(1 - P_R(m; \alpha)) = 0.75(1 - 0.75) = 0.1875.$$

We now proceed to our main result:

THEOREM 1. *For any fixed $\alpha \in (0.5, 1)$ and $\varepsilon < 0.25$, maximum over all m between 0 and N of $P_{ch}(m; \alpha)$ will be greater than ε if N is large enough. Moreover, $P_{ch}(2(1 - \alpha)N; \alpha)$ tends to $1/4$ as N goes to infinity.*

Proof. We will set $m = 2(1 - \alpha)N$ in equation (1), or integer part of that (we shall omit the integer part according to our notation convention, for brevity). Subsequently the probability to cheat is given by:

$$P_{ch}(2(1 - \alpha)N; \alpha) = P_R(2(1 - \alpha)N; \alpha)(1 - P_R(2(1 - \alpha)N; \alpha)) \tag{1'}$$

We will show that $P_R(2(1 - \alpha)N; \alpha)$ tends to $1/2$ as N goes to infinity, and this will prove our result, as the maximum of the function $x(1 - x)$ is $1/4$, achieved at $x = 1/2$. For convenience of the estimates, we will introduce a number c, and assume $N \gg c^2$, and prove that the limit is $1/2$ when both c and N tend to infinity; we may think of this limit as a repeated limit of P_R, $\lim_{c\to\infty} \lim_{N\to\infty} P_R$, or of its estimates (which may in fact depend on c).

The expected probability to reject the contract, $P_R(2(1 - \alpha)N; \alpha)$, is:

$$P_R(2(1 - \alpha)N; \alpha) = \sum_{\frac{N}{2} - c\sqrt{N} < N_R < \frac{N}{2} + c\sqrt{N}} q(N_R)P_1(2(1 - \alpha)N; \alpha, N_R)$$
$$+ \sum_{N_R=0}^{\frac{N}{2} - c\sqrt{N}} q(N_R)P_1(2(1 - \alpha)N; \alpha, N_R)$$
$$+ \sum_{N_R \geq \frac{N}{2} + c\sqrt{N}}^{N} q(N_R)P_1(2(1 - \alpha)N; \alpha, N_R). \tag{2'}$$

Here, $0 \leq P_R(2(1-\alpha)N; \alpha) \leq 1$, $q(N_R)$ is the probability to have exactly N_R states from the reject basis: $q(N_R) = 2^{-N}\binom{N}{N_R}$, $\sum_{N_R=0}^{N} q(N_R) = \sum_{N_R=0}^{N} 2^{-N}\binom{N}{N_R} = 1$.

We can use Hoeffding's inequality (see [5]) for binomial distribution[3] to estimate the last two sums:

$$\sum_{N_R=0}^{\frac{N}{2}-c\sqrt{N}} q(N_R)P_1(2(1-\alpha)N;\alpha,N_R) \le \sum_{N_R=0}^{\frac{N}{2}-c\sqrt{N}} q(N_R),$$

$$\sum_{N_R=0}^{\frac{N}{2}-c\sqrt{N}} q(N_R) = 2^{-N} \sum_{N_R=0}^{N(\frac{1}{2}-\frac{c}{\sqrt{N}})} \binom{N}{N_R} \le e^{-2\frac{c^2}{N}N} = e^{-2c^2},$$

$$\sum_{N_R\ge\frac{N}{2}+c\sqrt{N}}^{N} q(N_R)P_1(2(1-\alpha)N;\alpha,N_R) \le \sum_{N_R\ge\frac{N}{2}+c\sqrt{N}}^{N} q(N_R),$$

$$\sum_{N_R\ge\frac{N}{2}+c\sqrt{N}}^{N} q(N_R) = 1 - \Big(\sum_{N_R=0}^{\frac{N}{2}+c\sqrt{N}} q(N_R)\Big),$$

$$\sum_{N_R=0}^{\frac{N}{2}+c\sqrt{N}} q(N_R) = 2^{-N} \sum_{N_R=0}^{\frac{N}{2}+c\sqrt{N}} \binom{N}{N_R} = 2^{-N} \sum_{N_R=0}^{N(\frac{1}{2}+\frac{c}{\sqrt{N}})} \binom{N}{N_R} \ge 1 - e^{-2c^2}.$$

Thus,

$$\sum_{N_R\ge\frac{N}{2}+c\sqrt{N}}^{N} q(N_R) = 1 - \Big(\sum_{N_R=0}^{\frac{N}{2}+c\sqrt{N}} q(N_R)\Big) \ge 1 - (1-e^{-2c^2}) = e^{-2c^2}.$$

Then,

$$\sum_{N_R=0}^{\frac{N}{2}-c\sqrt{N}} q(N_R)P_1(2(1-\alpha)N;\alpha,N_R) + \sum_{N_R\ge\frac{N}{2}+c\sqrt{N}}^{N} q(N_R)P_1(2(1-\alpha)N;\alpha,N_R) \le 2e^{-2c^2}.$$

So, we can rewrite $P_R(2(1-\alpha)N;\alpha)$ using the last inequality to get, as c goes to infinity:

$$P_R(2(1-\alpha)N;\alpha) = \sum_{\frac{N}{2}-c\sqrt{N}<N_R<\frac{N}{2}+c\sqrt{N}} q(N_R)P_1(2(1-\alpha)N;\alpha,N_R) + o(1).$$

Note that in the formula (3), for our chosen value of $m = 2(1-\alpha)N$, value $m/2$ will be between n' and m', when $\frac{N}{2} - c\sqrt{N} < N_R < \frac{N}{2} + c\sqrt{N}$, for fixed c if N is large enough.

Note also that if $\frac{m}{2} - 3c\sqrt{N} < n < \frac{m}{2} + 3c\sqrt{N}$, we can substitute $\sqrt{N}$ with $\sqrt{\frac{m}{2(1-\alpha)}}$ to obtain $\frac{m}{2} - q\sqrt{m} < n < \frac{m}{2} + q\sqrt{m}$, where $q = 3c/\sqrt{2(1-\alpha)}$, and the

[3] $2^{-n} \sum_{i=0}^{n(1/2-\epsilon)} \binom{n}{i} \le e^{-2\epsilon^2 n}$, $2^{-n} \sum_{i=0}^{n(1/2+\epsilon)} \binom{n}{i} \ge 1 - e^{-2\epsilon^2 n}$

whole interval will be between n' and m' for fixed c if N is large enough, so

$$P_1(m;\alpha,N_R) = \sum_{\frac{m}{2}-q\sqrt{m}<n<\frac{m}{2}+q\sqrt{m}} P_2(n;m,N_R)P_3(n;\alpha,N_R)$$
$$+ \sum_{n=n'}^{\frac{m}{2}-q\sqrt{m}} P_2(n;m,N_R)P_3(n;\alpha,N_R)$$
$$+ \sum_{n\geq\frac{m}{2}+q\sqrt{m}}^{m'} P_2(n;m,N_R)P_3(n;\alpha,N_R). \qquad (3')$$

We will again prove that the last two sums are $o(1)$, assuming $|N_R - N/2| < c\sqrt{(}N)$. Recall that

$$P_2(n;m,N_R) = \binom{m}{n}\binom{N-m}{N_R-n}\binom{N}{N_R}^{-1}. \qquad (4')$$

Hence, $\sum_{n=0}^{m} P_2(n;m,N_R) = 1$, as a probability distribution, corresponding to probabilities that among the N_R uniformly chosen different natural numbers from 1 to N there are exactly n no larger than m. Also P_3 is between 0 and 1, so we will estimate tails of the distribution P_2.

We will use the following version of normal approximation to the binomial distribution (see for instance [9]):

$$\binom{k}{k/2-l}\frac{1}{2^{k+1}} = \frac{e^{-2l^2/k}}{\sqrt{2\pi k}} + O(\frac{1}{k^{3/2}}).$$

Note that in the last two sums of (3′), $|n - m/2| \geq 3c\sqrt{N}$, and moreover, since other values of N_R are part of $o(1)$ terms in (2′), $\frac{N}{2} - c\sqrt{N} < N_R < \frac{N}{2} + c\sqrt{N}$.

From this, it follows that

$$\binom{m}{n}\binom{N}{N_R}^{-1} \leq \binom{m}{m/2}\binom{N}{N/2-c\sqrt{N}}^{-1}$$
$$= (2^m/\sqrt{m})/(2^N(e^{-2c^2}/\sqrt{N}))(1+O(\frac{1}{N}))$$
$$= 2^{m-N}(e^{2c^2}\sqrt{\frac{N}{m}}))(1+O(\frac{1}{N}))$$
$$= 2^{m-N}e^{2c^2}/\sqrt{2(1-\alpha)}(1+O(\frac{1}{N})).$$

Using this, we get

$$\sum_{n=\frac{m}{2}+q\sqrt{m}}^{m'} P_2(n;m,N_R)P_3(n;\alpha,N_R) \leq \sum_{n=\frac{m}{2}+q\sqrt{m}}^{m'} P_2(n;m,N_R)$$
$$\leq e^{2c^2}/\sqrt{2(1-\alpha)}(1+O(\frac{1}{N}))\cdot 2^{-(N-m)} \sum_{n=\frac{m}{2}+3c\sqrt{N}}^{m'} \binom{N-m}{N_R-n}$$

$$\leq e^{2c^2}/\sqrt{2(1-\alpha)}(1+O(\frac{1}{N}))\cdot 2^{-(N-m)}\sum_{k=0}^{\frac{N-m}{2}-2c\sqrt{N}}\binom{N-m}{k}$$
$$\leq e^{2c^2}/\sqrt{2(1-\alpha)}(1+O(\frac{1}{N}))\cdot e^{-8c^2\frac{N}{N-m}}$$
$$\leq e^{-6c^2}/\sqrt{2(1-\alpha)}(1+O(\frac{1}{N}))=o(1),$$

as c goes to infinity, where we applied the Hoeffding's inequality to get the last line.

Similarly, we get

$$\sum_{n=n'}^{\frac{m}{2}-q\sqrt{m}}P_2(n;m,N_R)P_3(n;\alpha,N_R)\leq\sum_{n=n'}^{\frac{m}{2}-q\sqrt{m}}P_2(n;m,N_R)$$
$$\leq e^{2c^2}/\sqrt{2(1-\alpha)}(1+O(\frac{1}{N}))\cdot 2^{-(N-m)}\sum_{n=n'}^{\frac{m}{2}-3c\sqrt{N}}\binom{N-m}{N_R-n}$$
$$\leq e^{2c^2}/\sqrt{2(1-\alpha)}(1+O(\frac{1}{N}))\cdot 2^{-(N-m)}\sum_{k\geq\frac{N-m}{2}+2c\sqrt{N}}^{N-m}\binom{N-m}{k}$$
$$\leq e^{2c^2}/\sqrt{2(1-\alpha)}(1+O(\frac{1}{N}))\cdot e^{-8c^2\frac{N}{N-m}}$$
$$\leq e^{-6c^2}/\sqrt{2(1-\alpha)}(1+O(\frac{1}{N}))=o(1).$$

Moreover, from these calculations we see that, when $|N_R-N/2|<c\sqrt(N)$,

$$\sum_{\frac{m}{2}-q\sqrt{m}<n<\frac{m}{2}+q\sqrt{m}}P_2(n;m,N_R)=1+o(1).$$

Note that $\binom{m}{n}=\binom{m}{m-n}$, $\binom{N-m}{N_R-n}=\binom{N-m}{(N-N_R)-(m-n)}$ and $\binom{N}{N_R}=\binom{N}{N-N_R}$ from symmetry of binomial coefficients, so

$$P_2(n;m,N_R)=P_2((m-n);m,N-N_R).$$

Similarly, $q(N_R)=q(N-N_R)$.

We want to show that $P_3(n;\alpha,N_R)+P_3((m-n);\alpha,N-N_R)=1+o(1)$, for fixed c but as N goes to infinity, under restrictions on N_R and n, namely, $\frac{N}{2}-c\sqrt{N}<N_R<\frac{N}{2}+c\sqrt{N}$ and $\frac{m}{2}-q\sqrt{m}<n<\frac{m}{2}+q\sqrt{m}$, as we only consider first sums in $(2')$ and $(3')$. Such pairing will then help us prove that limit of P_R is indeed $1/2$.

We will again use the normal approximation to binomial distribution, i.e. as N goes to infinity (c, on which restrictions depend, is fixed), we have:

$$P_3(n;m,N_R)=2^{-n}\sum_{i=0}^{T_1}\binom{n}{i}=\frac{1}{2}\big(1+\operatorname{erf}(y_1)\big)+o(1),$$
$$P_3((m-n);m,(N-N_R))=2^{-(m-n)}\sum_{i=0}^{T_2}\binom{m-n}{i}=\frac{1}{2}\big(1+\operatorname{erf}(y_2)\big)+o(1)$$

where, under our restrictions on N_R and n, $T_1 = (1-\alpha)N_R$, $T_2 = (1-\alpha)(N-N_R)$, with the corresponding values

$$y_1 = \frac{\frac{T_1}{n} - \frac{1}{2}}{\frac{1}{2\sqrt{n}}\sqrt{2}} \quad \text{and} \quad y_2 = \frac{\frac{T_2}{m-n} - \frac{1}{2}}{\frac{1}{2\sqrt{m-n}}\sqrt{2}}.$$

Thus, to prove $P_3(n;\alpha,N_R)+P_3(m-n;\alpha,N-N_R) = 1+o(1)$ it is enough to show $y_1 + y_2 = o(1)$ as N goes to infinity, as the function erf is odd and smooth with bounded derivative in $\mathbb{R}$.

$$\begin{aligned} y_1 + y_2 &= \left(\frac{\frac{T_1}{n} - \frac{1}{2}}{\frac{1}{2\sqrt{n}}\sqrt{2}}\right) + \left(\frac{\frac{T_2}{m-n} - \frac{1}{2}}{\frac{1}{2\sqrt{m-n}}\sqrt{2}}\right) \\ &= \Big(\frac{T_1}{n} - \frac{1}{2}\Big)\sqrt{2}\sqrt{n} + \Big(\frac{T_2}{m-n} - \frac{1}{2}\Big)\sqrt{2}\sqrt{m-n}. \end{aligned}$$

Set $n = \frac{m}{2} + k$, $-q\sqrt{m} < k < q\sqrt{m}$ and $N_R = \frac{N}{2} + A$, $-c\sqrt{N} < A < c\sqrt{N}$. After some algebraic manipulations, we get

$$\begin{aligned} y_1 + y_2 &= \sqrt{2}\Big(\frac{(1-\alpha)(\frac{N}{2}+A) - \frac{1}{2}((1-\alpha)N+k)}{\sqrt{(1-\alpha)N+k}} \\ &\qquad + \frac{(1-\alpha)(\frac{N}{2}-A) - \frac{1}{2}((1-\alpha)N-k)}{\sqrt{(1-\alpha)N-k}}\Big) \\ &= \sqrt{2}\Big(\frac{(1-\alpha)A-k}{\sqrt{(1-\alpha)N+k}} + \frac{-(1-\alpha)A+k}{\sqrt{(1-\alpha)N-k}}\Big) \\ &= \sqrt{2}((1-\alpha)A-k)\Big(\frac{1}{\sqrt{(1-\alpha)N+k}} - \frac{1}{\sqrt{(1-\alpha)N-k}}\Big) \\ &= \sqrt{2}((1-\alpha)A-k)\Big(\frac{\sqrt{(1-\alpha)N-k} - \sqrt{(1-\alpha)N+k}}{\sqrt{(1-\alpha)^2N^2-k^2}}\Big) \\ &= \sqrt{2}((1-\alpha)A-k)\Big(\frac{\sqrt{(1-\alpha)N}(\sqrt{1-\frac{k}{(1-\alpha)N}} - \sqrt{1+\frac{k}{(1-\alpha)N}})}{\sqrt{(1-\alpha)^2N^2-k^2}}\Big). \end{aligned}$$

Using Taylor series expansion for $\sqrt{1-\frac{k}{(1-\alpha)N}}$ and $\sqrt{1+\frac{k}{(1-\alpha)N}}$ we get

$$\begin{aligned} y_1 + y_2 &= \sqrt{2}\sqrt{(1-\alpha)N}((1-\alpha)A-k) \\ &\qquad \times \left(\frac{\big(1 - \frac{1}{2}\frac{k}{(1-\alpha)N} + O(\frac{k^2}{N^2})\big) - \big(1 + \frac{1}{2}\frac{k}{(1-\alpha)N} + O(\frac{k^2}{N^2})\big)}{\sqrt{(1-\alpha)^2N^2-k^2}}\right) \\ &= \sqrt{2}\sqrt{(1-\alpha)N}((1-\alpha)A-k)\Big(\frac{\frac{-k}{(1-\alpha)N}(1+o(1))}{\sqrt{(1-\alpha)^2N^2-k^2}}\Big). \end{aligned}$$

Using that both A and k are $O(\sqrt{N})$, we finally get $y_1 + y_2 = O(1/\sqrt{N}) = o(1)$.

So in this case we have $P_3(n;\alpha,N_R)+P_3((m-n);\alpha,N-N_R)=1+o(1)$, and for fixed c, convergence is uniform on the interval of restriction for N_R and n, as N goes to infinity.

Using our pairing, and considering the first, main sum of $(2')$, and of $(3')$, we see that indeed P_R is $1/2+o(1)$ as both c and N tend to infinity. Namely, if we expand the main part of the sum in $(2')$ and $(3')$, and double the whole sum, and then rearrange the terms so that corresponding pairs with (n,m,N_R) and $(m-n,m,N-N_R)$ come together, we end up with a sum of the form $\sum q(N_R)P_2(n,m,N_R)(1+o(1))$, which sums to $1+o(1)$ since both q in N_R and P_2 in n are probability distributions. ■

Thus, as we have seen, the randomization is necessary in order for protocol to be fair. If the protocol does not use randomization, but relies on a single value of parameter α, then there is possibility for parties to cheat with significant probability.

Acknowledgement. I would like to thank my advisor, Vladimir Božin, for useful comments and suggestions. Also thanks to all who gave me a helping hand, especially prof. Aleksandar Lipkovski and the referees of this paper.

REFERENCES

[**1**] N. Asokan, M. Schunter, M. Waidner, *Optimistic protocols for fair exchange*, Proceedings of the 4th ACM Conference on Computer and Communications Security, CCS 97, pp. 7–17, New York, NY, USA, 1997.

[**2**] M. Ben-Or, O. Goldreich, S. Micali, R. L. Rivest, *A fair protocol for signing contracts (extended abstract)*, In: W. Brauer Ed., ICALP, Vol. 194, Lecture Notes Comp. Sci., pp. 43–52. Springer, 1985.

[**3**] S. Even, Y. Yacobi, *Relations among public key signature systems*, Technical report, Technicon, 1980.

[**4**] M. J. Fischer, N. A. Lynch, M. S. Paterson, *Impossibility of distributed consensus with one faulty process*, J. ACM, **32**(2) (1985), 374–382.

[**5**] W. Hoeffding, *Probability inequalities for the sum of bounded random variables*. J Amer. Stat. Assoc. **58** (1963), 13–30.

[**6**] M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, (2000).

[**7**] N. Paunković, J. Bouda, P. Mateus, *Fair and optimistic quantum contract signing*, Physical Review A, **84** (6) (2011).

[**8**] M. Rabin, *Transaction protection by beacons*, J. Computer & System Sci. **27** (1983), 256-267.

[**9**] R. Sedgewick, Ph. Flajolet, *An Introduction to the Analysis of Algorithms*, 2nd Ed., Addison-Wesley Professional, 2013.

(received 05.08.2016; in revised form 02.09.2016; available online 29.11.2016)

Faculty of Mathematics, University of Belgrade, Studentski trg 16, Beograd, Serbia
E-mail: hanaalmoner@yahoo.com