PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 101(115) (2017), 37–45 https://doi.org/10.2298/PIM1715037B

ASYMPTOTICS OF QUANTUM CONTRACT SIGNING

Vladimir Božin and Hana Louka

ABSTRACT. We prove that maximal probability of cheating in quantum signing protocol of Paunković, Bouda and Matheus behaves as $O\left(1/\sqrt{N}\right)$ for large number of qubits N. This confirms a conjecture that was based on numerical evidence.

1. Introduction

Distance contract signing has been an important topic in cryptography, relevant to numerous applications, including stock market [**1**]. It involves two parties, called Alice and Bob, who want to exchange their commitment to a contract. The fundamental problem is that one party has to go first in sending their commitment, which gives the other an advantage, and one would like to design a protocol which is both *fair* and *viable*.

A protocol is *fair* if neither party can get a commitment if it does not give it at the same time. An unfair protocol would, for instance, give a trader a right to trade future or option if it is favorable to him, without having to pay if things do not turn advantageously. A protocol is *viable* if it enables signing parties to get each other commitments provided they both act honestly.

It can be shown (see [**3**]) that it is impossible to design a fair and viable contract signing protocol, without involving a third, trusted party (called Trent in cryptography). If the third party is involved, then Alice and Bob could, for instance, send their commitments to Trent, who would send them back in a way that ensures fairness and viability. However, it is desirable to involve Trent only if necessary. A protocol is called *optimistic*, if the third, trusted party, is involved only when one party is cheating or the communication is interrupted.

In optimistic protocols, Alice and Bob *exchange* messages, so that in the end both parties will end up with signed contract. However, if there is a disruption or evidence of cheating, the parties have an option to invoke Trent, who would then *bind* the contract, assuring fairness.

2010 *Mathematics Subject Classification:* 81P68; 41A60.
Key words and phrases: quantum information theory, asymptotic behaviour.
Communicated by Žarko Mijajlović.

Some protocols are only probabilistically fair, i.e., there is a small probability of advantage to one party. Such protocols have been designed using classical cryptography, which are both optimistic and probabilistically fair by Rabin in [**4**] and Ben-Or, Goldreich, Micali, and Rivest in [**5**].

However, they rely heavily on digital signatures. In [**2**], a protocol was proposed in the context of quantum information theory [**6**], which does not.

2. Paunković–Bouda–Mateus Protocol

The idea of quantum contract signing is to use a pair of non-commuting observables (quantum complementarity), and inherent properties of quantum mechanics, to achieve a probabilistically fair, viable and optimistic protocol, without reliance on the digital signatures.

In [**2**], the following protocol is proposed for that purpose. Trent, a trusted third party, sends to Alice and Bob in *initialisation phase*, N qubits each, and classical data about the qubits received by the other party. In *exchange phase*, Alice and Bob make measurements of their choice on their qubits, and send the results to the other party in alternating turns. This phase does not involve Trent (protocol is optimistic). However, if the exchange is interrupted or there is evidence of cheating, they have an option to invoke Trent again. In this case *binding phase* occurs. They present to Trent their results of measurements and claims about which observables they measured. Trent then decides if the contract is a void, or if it is bound by the presented results. The idea is, that the party which was honest, has a way to enforce the contract (i.e., bind it) or reject it, the moment it notices a problem (i.e., evidence of cheating by the other party).

Let

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

Thus, $\{|+\rangle, |-\rangle\}$ is an alternative orthonormal qubit frame. We will call this frame the "reject basis", while $\{|0\rangle, |1\rangle\}$ will be the "accept basis". Define

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

to be the corresponding accept and reject observables.

In the initialization phase, Trent chooses, at random, N qubits, out of the set $\{|+\rangle, |-\rangle, |0\rangle, |1\rangle\}$, and sends them to Alice, and similarly, randomly chosen N qubits from the same set to Bob. In addition, Trent lets Alice know which qubits are sent to Bob, and lets Bob know which qubits are sent to Alice. Thus, Alice has N qubits but does not know (without performing measurement) which ones she has, while Bob knows which qubits are sent to her, and vice versa.

In the exchange phase, Trent is not involved. If Alice wants to accept the contract, she will measure her first qubit in the accept basis (i.e., measure obserable $\hat{A}$ on her first qubit), end send result to Bob. If she wants to reject the contract, she will measure $\hat{R}$ instead. Then Bob reciprociates, by measuring either accept or reject observable on his first qubit, and sends the result to Alice. The process continues until all N qubits are measured.

Note that roughly half of the qubits sent to each Alice and Bob are in reject, and half in accept bases. Thus, parties can note what the other party is measuring, by comparing the results sent to them on the qubits which are in the corresponding basis, when there should be a perfect agreement with the classical information sent by Trent. Thus, if both parties are honest and want to accept the contract, they will note this and do not need to invoke Trent (i.e., protocol is viable). However, if they notice that there is evidence of cheating (for instance, change in basis being measured), they have an option to stop communication, and proceed to binding. In this case, they will have an option to try to bind contract, by measuring all the remaining qubits in the accept basis, or refuse 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 observables they measured.

In the binding phase, when it occurs, Trent makes the ultimate decision if the contract is binding, or rejected/void. In order to do that, Trent will get results of the measurement on all of their qubits by both Alice and Bob. Then he chooses, according to a pre-defined (by the protocol, this is something defined in advance) probability distribution a number α between 1/2 and 1. The contract is binding to both parties, if at least a fraction α of Alice's qubits from accept basis are measured correctly, and also less that α fraction of his reject qubits are measured correctly by Bob, or vice versa. If there is evidence that Alice cheated (did not measure the basis she reported she had done), only Bob's results will count, and similarly if Bob cheated, only Alice will be taken into account. In all other cases, contract is declared invalid.

Paunković, Bouda and Mateus have shown that a protocol is viable and probabilistically fair, and that the probability of cheating can be made arbitrarily small. They have hypothesized that as N goes to infinity, probability of cheating goes to zero as $N^{-1/2}$, but have shown this only by numerical evidence.

The probability of cheating, computed in [**2**], depends on the strategy of the cheating party. Namely, out of N qubits, a number of them, say m, can be measured in the attempt to cheat, and thus strategies of cheating that they considered are indexed by a number m. For given m, and α chosen by Trent, probability of successful cheating is then given by (note that N as a parameter is suppressed in notation from [**2**])

$$P_{\mathrm{ch}}(m,\alpha) = P_{\mathrm{ch}}(m,\alpha;N) = P_R(m;\alpha)(1 - P_R(m;\alpha)),$$

where $P_R(m;\alpha)$, the expected probability to reject contract for a given α, is

$$P_R(m;\alpha) = \sum_{N_R=0}^{N} q(N_R) P_1(m,\alpha;N_R), \tag{2.1}$$

where $q(N_R)$ is the probability to have exactly N_R states from the reject basis, equal to $2^{-N}\binom{N}{N_R}$

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

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

$$\begin{aligned} P_1(m;\alpha,N_R) &= \sum_{n=n'}^{m'} P_2(n;m,N_R)P_3(n;\alpha,N_R) \\ P_2(n;m,N_R) &= \binom{m}{n}\binom{N-m}{N_R-n}\binom{N}{N_R}^{-1} \\ P_3(n;\alpha,N_R) &= 2^{-n}\sum_{i=0}^{T}\binom{n}{i}, \end{aligned}$$

where

$$T = \min\{n, \lceil(1-\alpha)N_R\rceil\} \tag{2.2}$$

and $m' = \min\{m, N_R\}$, $n' = \max\{0, m+N_R-N\}$.

Note that P_R, P_1, P_2, P_3 are all numbers between 0 and 1.

Finally, if $p(\alpha)$ is Trent's probability distribution for choosing α, probability of cheating for cheater strategy indexed by m is given by

$$P_{\text{ch}}(m) = \int_{1/2}^{1} p(\alpha)\, P_{\text{ch}}(m;\alpha)\, d\alpha$$

and one wants to estimate maximum of this over all m between 0 and N, which represents the maximal probability of cheating.

3. Asymptotic Behavior

To assess the asymptotic behavior, the following formulas, coming from the normal approximation to the binomial distribution, will be useful:

$$\binom{n}{\lfloor n/2-l\rfloor}\frac{1}{2^{n+1}} = \frac{e^{-2l^2/n}}{\sqrt{2\pi n}} + O\Big(\frac{1}{n^{3/2}}\Big),\quad \binom{n}{\lceil n/2-l\rceil}\frac{1}{2^{n+1}} = \frac{e^{-2l^2/n}}{\sqrt{2\pi n}} + O\Big(\frac{1}{n^{3/2}}\Big)$$

In particular, we get estimate for the maximal binomial coefficient

$$\binom{n}{\lceil n/2\rceil} = \frac{2^{n+1}}{\sqrt{2\pi n}}(1+O(1/n)). \tag{3.1}$$

These estimates can be obtained from the Stirling expansion formula, and the following inequalities (see [**8**])

$$\sqrt{2\pi n}\Big(\frac{n}{e}\Big)^n e^{\frac{1}{12n+1}} < n! < \sqrt{2\pi n}\Big(\frac{n}{e}\Big)^n e^{\frac{1}{12n}}. \tag{3.2}$$

From this, by using elementary inequality (rough, as coefficient 3/2 on right-hand side is not optimal), valid for all $x, |x| < 1$,

$$(1-x)\ln(1-x) + (1+x)\ln(1+x) \leqslant \tfrac{3}{2}x^2, \tag{3.3}$$

we can obtain the following (rough) estimates:

LEMMA 3.1. *Let n be a positive integer and suppose l is an arbitrary real number between $-n/2$ and $n/2$. Then*

$$\binom{n}{\lfloor n/2-l\rfloor} \geqslant 2^{n+1}\frac{e^{-3l^2/n}}{\sqrt{2\pi n}}, \quad \binom{n}{\lceil n/2-l\rceil} \geqslant 2^{n+1}\frac{e^{-3l^2/n}}{\sqrt{2\pi n}}.$$

PROOF. Suppose first that $n/2-l$ is an integer different from 0 and n. Then, using

$$\binom{n}{n/2-l} = \frac{n!}{(n/2-l)!(n/2+l)!}$$

and inequalities (3.2), we get

$$\binom{n}{n/2-l} \geqslant \frac{\sqrt{2\pi n}\exp\left(\frac{1}{12n+1}-\frac{1}{12(n/2+l)}-\frac{1}{12(n/2-l)}\right)}{\sqrt{2\pi(n/2-l)}\sqrt{2\pi(n/2+l)}}e^C$$

where

$$C = n(\ln n-1)-(n/2-l)(\ln(n/2-l)-1)-(n/2+l)(\ln(n/2+l)-1).$$

Then

$$\binom{n}{n/2-l} \geqslant \frac{2e^{-1/6}}{\sqrt{2\pi n}}e^C.$$

Also, if $x = 2l/n$, we have

$$C = n\ln 2-\tfrac{n}{2}\big((1-x)\ln(1-x)+(1+x)\ln(1+x)\big).$$

So, by (3.3), we have

$$C \geqslant n\ln 2-\frac{n}{2}\Big(\frac{3x^2}{2}\Big) = n\ln 2-\frac{3l^2}{n}, \quad \binom{n}{n/2-l} \geqslant \frac{2^{n+1}e^{-1/6}}{\sqrt{2\pi n}}e^{-3l^2/n}.$$

Now assume that $n/2 \geqslant l \geqslant 0$. We get

$$\binom{n}{\lfloor n/2-l\rfloor} \geqslant \frac{2^{n+1}e^{-1/6}}{\sqrt{2\pi n}}e^{-3(l+1)^2/n} \geqslant \frac{2^{n+1}e^{-1/6}}{\sqrt{2\pi n}}e^{-3l^2/n}e^{-6} \geqslant \frac{2^{n+1}}{500\sqrt{2\pi n}}e^{-3l^2/n}.$$

The case $-n/2 \leqslant l \leqslant 0$ and $\binom{n}{\lceil n/2-l\rceil}$ is analogous. □

We also recall Hoeffding's inequalities (see [**7**]):

$$2^{-n}\sum_{i=0}^{n(1/2-\varepsilon)}\binom{n}{i} \leqslant e^{-2\varepsilon^2 n}, \quad 2^{-n}\sum_{i=0}^{n(1/2+\varepsilon)}\binom{n}{i} \geqslant 1-e^{-2\varepsilon^2 n}$$

We now state our main result, using notation introduced in the previous chapter (also used in [**2**]).

THEOREM 3.1. *If the probability density is bounded, i.e., $p(\alpha) < B$ for some constant B, then there is a constant A such that $P_{\mathrm{ch}}(m;N) \leqslant A/\sqrt{N}$, where $P_{\mathrm{ch}}(m;N) = \int_{1/2}^{1} p(\alpha)\,P_{\mathrm{ch}}(m,\alpha;N)\,d\alpha$.*

To prove this main result, we will need the following lemma.

LEMMA 3.2. *There is a constant C such that if $|m-2(1-\alpha)N| > x\sqrt{N}$, then $P_{\mathrm{ch}}(m,\alpha;N) < Ce^{-x^2/128}$, where $\alpha \in (1/2,1)$, $0 \leqslant m \leqslant N$, $x \geqslant 0$.*

PROOF. Note first that from $|m-2(1-\alpha)N| > x\sqrt{N}$ it follows that $x < \sqrt{N}$. Next, note that when $|N_R - N/2| \geqslant x\sqrt{N}/16$, we have, by Hoeffding's inequality,

$$\sum_{N_R, |N_R - N/2| \geqslant x\sqrt{N}/16} 2^{-N}\binom{N}{N_R} \leqslant 2e^{-x^2/128} \tag{3.4}$$

and in particular, contribution of such N_R to $P_R(m,\alpha)$ in (2.1) is bounded by $2e^{-x^2/128}$.

Now, assume

$$N/2 - x\sqrt{N}/16 < N_R < N/2 + x\sqrt{N}/16. \tag{3.5}$$

Let us estimate in this case the sum

$$\sum_{n, |n-m/2| \geqslant x\sqrt{N}/4} P_2(n; m, N_R).$$

Recall that

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

Using (3.5), it follows that if $|n - m/2| \geqslant x\sqrt{N}/4$, then we have

$$\begin{aligned} |(N/2 - m/2) - (N_R - n)| &= |(N/2 - N_R) - (m/2 - n)| \\ &\geqslant |(m/2 - n)| - |(N_R - N/2)| \\ &\geqslant (1/4 - 1/16)x\sqrt{N} = 3x\sqrt{N}/16. \end{aligned} \tag{3.6}$$

Using (3.1) and Lemma 3.1, we get

$$\begin{aligned} \binom{N-m}{N_R - n}\binom{N}{N_R}^{-1} &\leqslant \binom{N-m}{\lceil (N-m)/2 \rceil}\binom{N}{\lfloor N/2 - x\sqrt{N}/16 \rfloor}^{-1} \\ &\leqslant 500\frac{2^{N-m}/\sqrt{N-m}}{2^N(e^{-3x^2/256}/\sqrt{N})}(1+O(1/N)) \\ &= 2^{-m}\big(e^{3x^2/256}500\sqrt{N/(N-m)}\,\big)(1+O(1/N)), \\ \binom{m}{n}\binom{N}{N_R}^{-1} &\leqslant \binom{m}{\lceil m/2 \rceil}\binom{N}{\lfloor N/2 - x\sqrt{N}/16 \rfloor}^{-1} \\ &\leqslant 500\frac{2^m/\sqrt{m}}{2^N\big(e^{-3x^2/256}/\sqrt{N}\,\big)}(1+O(1/N)) \\ &= 2^{m-N}\big(e^{3x^2/256}500\sqrt{N/m}\,\big)(1+O(1/N)). \end{aligned}$$

Note that, by Hoeffding's inequality, and using $m \leqslant N$, we have

$$\sum_{n, |n-m/2| \geqslant x\sqrt{N}/4} \binom{m}{n} \leqslant \sum_{n, |n-m/2| \geqslant x\sqrt{m}/4} \binom{m}{n} \leqslant 2e^{-x^2/8}2^m$$

and, using (3.6)

$$\sum_{n,|n-m/2|\geqslant x\sqrt{N}/4} \binom{N-m}{N_R-n} \leqslant \sum_{n,|(N/2-m/2)-(N_R-n)|\geqslant 3x\sqrt{N}/16} \binom{N-m}{N_R-n}$$
$$\leqslant \sum_{n,|(N/2-m/2)-(N_R-n)|\geqslant 3x\sqrt{N-m}/16} \binom{N-m}{N_R-n} \leqslant 2e^{-9x^2/128}2^{N-m}.$$

Now, either $m \leqslant N/2$, when $N/(N-m) \leqslant 2$, in which case we use the first of each pair of the inequalities above, to get

$$\sum_{n,|n-m/2|\geqslant x\sqrt{N}/4} P_2(n;m,N_R) \leqslant 1000\sqrt{2}e^{-14.5x^2/128}(1+O(1/N)),$$
$$\sum_{n,|n-m/2|\geqslant x\sqrt{N}/4} P_2(n;m,N_R) = O(e^{-x^2/128}),$$

or when $m > N/2$, so $N/m \leqslant 2$, when we get from the second inequalities

$$\sum_{n,|n-m/2|\geqslant x\sqrt{N}/4} P_2(n;m,N_R) \leqslant 1000\sqrt{2}e^{-7.5x^2/128}(1+O(1/N))$$
$$\sum_{n,|n-m/2|\geqslant x\sqrt{N}/4} P_2(n;m,N_R) = O(e^{-x^2/128}).$$

So, when (3.5) holds, we have

$$\sum_{n,|n-m/2|\geqslant x\sqrt{N}/4} P_2(n;m,N_R) = O(e^{-x^2/128}). \tag{3.7}$$

Now assume that that $m - 2(1-\alpha)N > x\sqrt{N}$, or $m > 2(1-\alpha)N + x\sqrt{N}$. Suppose that (3.5) holds and that

$$m/2 - x\sqrt{N}/4 < n < m/2 + x\sqrt{N}/4 \tag{3.8}$$

and also $n, m \leqslant N$. We have then $(1-\alpha)N + x\sqrt{N}/4 < n$ and from (3.5) it follows $n > N_R(1-\alpha)$. So we have that, in formula (2.2), $T = \lceil N_R(1-\alpha)\rceil$. However, we have then that

$$T < (1-\alpha)N/2 + x\sqrt{N}(1-\alpha)/16 + 1 < n/2 - x\sqrt{N}/16 + 1$$
$$\leqslant n/2 - (x - 16/\sqrt{N})\sqrt{N}/16 \leqslant n/2 - (x-16/\sqrt{N})\sqrt{n}/16.$$

So, by Hoeffding's inequality, and using $|x| < \sqrt{N}$, we have that, in this case $P_3(n,\alpha;N_R) = O(e^{-x^2/128})$.

Now we can estimate $P_R(m,\alpha)$. For $|N_R - N/2| \geqslant x\sqrt{N}/16$, the contribution to the sum is bounded by $2e^{-x^2/128}$ by (3.4). When (3.5) holds, using $q(N_R)$ as probability distribution, we can estimate P_1. Again, we have two cases. In the first case, when $|n - m/2| \geqslant x\sqrt{N}/4$, we see that the contribution of such n to P_1 is $O(e^{-x^2/128})$ by (3.7). Finally, using P_2 as a probability distribution in n (probability that out of N_R chosen elements out of N, specified n chosen elements will be among the first m), when (3.8) holds, it is enough to bound P_3. But we have demonstrated that in that case $P_3(n,\alpha;N_R) = O(e^{-x^2/128})$. Thus,

$$P_R(m,\alpha) \leqslant 2e^{-x^2/128} + O(e^{-x^2/128}) + O(e^{-x^2/128}) = O(e^{-x^2/128}),$$

and consequently, $P_{\mathrm{ch}}(m;\alpha,N) = O(e^{-x^2/128})$.

The case $m < 2(1-\alpha)N - x\sqrt{N}$ is analogous. Namely, from

$$N/2 - x\sqrt{N}/16 < N_R < N/2 + x\sqrt{N}/16,$$
$$m/2 - x\sqrt{N}/4 < n < m/2 + x\sqrt{N}/4$$

it follows $n < (1-\alpha)N - x\sqrt{N}/4$. If in (2.2), $T = n$, then $P_3 = 1$; otherwise $T = \lceil N_R(1-\alpha)\rceil$ and

$$T > (1-\alpha)N/2 - x\sqrt{N}(1-\alpha)/16 > n/2 + x\sqrt{N}/16 \geqslant n/2 + x\sqrt{n}/16,$$

So, by Hoeffding's inequality, we have that $P_3(n,\alpha;N_R) \geqslant 1 - e^{-x^2/128}$.

Now we can estimate $P_R(m,\alpha)$. Recall that P_R, P_1, P_2 and P_3 take values between 0 and 1, and that P_2 is probability distribution in n and $q(N_R) = 2^{-N}\binom{N}{N_R}$ is probability distribution in N_R. Note that from (3.4) it follows

$$\sum_{N_R, |N_R - N/2| \leqslant x\sqrt{N}/16} 2^{-N}\binom{N}{N_R} \geqslant 1 - 2e^{-x^2/128},$$

and that from (3.7) it follows that, if $|N_R - N/2| \leqslant x\sqrt{N}/16$, then

$$\sum_{n, |n - m/2| \leqslant x\sqrt{N}/4} P_2(n;m,N_R) = 1 - O(e^{-x^2/128}).$$

Now summing just contributions from N_R with $|N_R - N/2| \leqslant x\sqrt{N}/16$ to P_R, and from n with $|n - m/2| \leqslant x\sqrt{N}/4$ to P_1, and using $P_3(n,\alpha;N_R) \geqslant 1 - e^{-x^2/128}$, we get

$$P_R(m,\alpha) \geqslant (1 - 2e^{-x^2/128})(1 - O(e^{-x^2/128}))(1 - e^{-x^2/128}),$$
$$P_R(m,\alpha) \geqslant 1 - 2e^{-x^2/128} - O(e^{-x^2/128}) - e^{-x^2/128},$$
$$P_R(m,\alpha) = 1 - O(e^{-x^2/128}),$$

and consequently, in the case $m < 2(1-\alpha)N - x\sqrt{N}$, we also get

$$P_{\mathrm{ch}}(m;\alpha,N) = O(e^{-x^2/128}). \qquad \square$$

Now we are ready to prove our main result, Theorem 3.1.

Proof of Theorem 3.1. Note that $\alpha = 1 - m/2N + c/\sqrt{N}$ is the relationship between c and α, then $d\alpha = dc/\sqrt{N}$ and hence, assuming $p(\alpha) < B$, we get

$$P_{\mathrm{ch}}(m;N) = \int_{1/2}^{1} p(\alpha)\, P_{\mathrm{ch}}(m,\alpha;N)\, d\alpha$$

$$\leqslant \int_{1-m/2N-1/\sqrt{N}}^{1-m/2N+1/\sqrt{N}} BP_{\mathrm{ch}}(m,\alpha;N)\,d\alpha + \int_1^\infty 2BCe^{-c^2/128}dc/\sqrt{N}$$
$$\leqslant 2BC/\sqrt{N} + 2BC/\sqrt{N}\int_0^\infty e^{-c^2/128}dc \leqslant 2BC/\sqrt{N}\big(1+\sqrt{32\pi}\,\big). \ \square$$

This proves the conjecture from [**2**].

References

1. N. Asokan, V. Shoup, M. Waidner, *Optimistic fair exchange of digital signatures*, IEEE J. Sel. Areas Commun. **18**(4) (2000), 593–610.
2. N. Paunković, J. Bouda, P. Mateus, *Fair and optimistic quantum contract signing*, Physical Review A **84**(6) (2011), 062331, 11p.
3. M. J. Fischer, N. A. Lynch, M. Paterson, *Impossibility of distributed consensus with one faulty process*, J. Assoc. Comput. Mach. **32** (1985), 374–382.
4. M. O. Rabin, *Transactions protected by beacons*, J. Comput. Syst. Sci. **27** (1983), 256–267.
5. M. Ben-Or, O. Goldreich, S. Micali, R. L. Rivest, *A fair protocol for signing contracts*, IEEE Trans. Inf. Theory **36**(1) (1990), 40–46.
6. M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.
7. W. Hoeffding, *Probability inequalities for the sum of bounded random variables*, J. Am. Stat. Assoc. **58** (1963), 13–30.
8. H. Robbins, *A remark on Stirling's formula*, Am. Math. Month. **62**(1) (1955), 26–29.

Department of Mathematics
University of Belgrade
Belgrade
Serbia
bozin@matf.bg.ac.rs

(Received 01 09 2016)
(Revised 15 11 2016)