Filomat 38:6 (2024), 1915–1922
https://doi.org/10.2298/FIL2406915B

Published by Faculty of Sciences and Mathematics,
University of Niš, Serbia
Available at: http://www.pmf.ni.ac.rs/filomat

On quantum contract signing protocol

Vladimir Božin[a,*], Hana Louka[a]

[a] *Matematički fakultet, Univerzitet u Beogradu*

Abstract.
In this paper, we examine quantum contract signing protocol of Paunković, Bouda and Matheus. We show that there is a limit function for modified probability of cheating, substantially improving results previously obtained by the authors.

1. Introduction

Contract signing is an important topic in cryptography, which involves two parties, called Alice and Bob, who want to exchange the commitments to a contract. But one party has to go first in sending their commitment, giving an advantage to the other party, and hence one wants a protocol which is both *fair* and *viable*.

A protocol is *fair* if either both parties get each other commitments, or none does. A protocol is *viable* if it enables signing parties to get each other commitments provided they both act honestly. It can be shown (see [2]) that it is impossible to design a fair and viable contract signing protocol, without involving a third, trusted party (called Trent). 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.

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 M.O.Rabin in [3] and Ben-Or, O. Goldreich, Silvio Micali, and R.L. Rivest in [4].

However, they rely heavily on digital signatures. In [1], a protocol was proposed in the context of quantum information theory [5]. 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. Let us first describe this protocol.

2020 *Mathematics Subject Classification*. Primary 81P68; Secondary 41A60
Keywords. quantum information theory, asymptotic behaviour, cryptography
Received: 24 September 2016; Accepted: 27 February 2017
Communicated by Dragan S. Djordjević
* Corresponding author: Vladimir Božin
Email address: Vladimir.Bozin@matf.bg.ac.rs (Vladimir Božin)

Let

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

and

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Define

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

to be the corresponding accept and reject observables.

The protocol consists of three phases, initialization, exchange, and binding.

- 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, sends 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), and send result to Bob. If she wants to reject the contract, she will measure $\hat{R}$ instead. Then Bob reciprocates, by measuring either accept or reject observable on his first qubit, and sends 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 basis. 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 predefined (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 than α fraction of Bob's 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 did), 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 protocol is viable and proabilistically fair, and that 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 [1], 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 fixed N and given m, and α chosen by Trent, probability of successful cheating is then given by:

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

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

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

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

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

Note that these values are of various probabilities, 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

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

In [8] it was shown that parameter randomization is necessary in order for probability of cheating to go to zero for large N. Otherwise, the cheating party can pick a value of m such that the probability of cheating stays bounded away from zero:

Theorem 1.1. *(see [8]) 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.*

On the other side, when the probability density function p is bounded, i.e. when the probability of choosing α from any interval does not exceed some fixed constant times length of that interval, the authors have shown in [9] that probability of cheating goes to zero as $1/\sqrt{N}$, confirming the conjecture from [1]. Namely,

Theorem 1.2. *(see [9]) If the probability density function p is bounded, then there is a constant A such that $P_{ch}(m,N) \leq A/\sqrt{N}$, where*

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

This result was based on the following estimating lemma:

Lemma 1.3. *(see [9]) There is a constant C such that if $|m - 2(1-\alpha)N| > x\sqrt{N}$, then $P_{ch}(m,\alpha;N) < Ce^{-x^2/128}$, where $\alpha \in (1/2,1)$, $0 \leq m \leq N$.*

In this paper we obtain a more precise estimate, in effect substantially improving on these previous results. Define for $0 \leq x \leq 1$ and a natural number N,

$$Q_{ch}(x,N) = P_{ch}(\lfloor xN \rfloor, N)\sqrt{N}. \tag{6}$$

Note that these functions also depend on the probability distribution according to which a parameter α is chosen in the binding phase - we treat this probability distribution as a fixed part of the protocol, and study how probabilities of cheating depend on number of qubits exchanged and measured.

Then we get in particular the following result:

Theorem 1.4. *Suppose $p : (1/2,1) \to \mathbb{R}$ is a non-negative, bounded probability density function, which has only discontinuities of first kind. Then the corresponding functions $Q_{ch}(\cdot,N)$ have a point-wise limit*

$$Q(x) = \lim_{N\to\infty} Q_{ch}(x,N),$$

$$Q(x) = \frac{1}{\sqrt{4\pi}} \bar{p}(1-x/2)\sqrt{x(2+x(1-x)(2-x))} \tag{7}$$

where $\bar{p}(\alpha) = p(\alpha)$ at points of continuity, otherwise $\bar{p}(\alpha)$ is mean of one-sided limits of p at α.

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

$$\binom{n}{\lfloor n/2 - l \rfloor} \frac{1}{2^{n+1}} = \frac{e^{-2l^2/n}}{\sqrt{2\pi n}} + O(n^{-3/2}) \tag{8}$$

and

$$\binom{n}{\lceil n/2 - l \rceil} \frac{1}{2^{n+1}} = \frac{e^{-2l^2/n}}{\sqrt{2\pi n}} + O(n^{-3/2}) \tag{9}$$

These well known estimates can be also be obtained from the Stirling expansion formula (see, for instance [7]).

We also recall the Hoeffding's inequalities (see [6]):

$$2^{-n} \sum_{0 \leq i \leq n(1/2-\varepsilon)} \binom{n}{i} \leq e^{-2\varepsilon^2 n} \tag{10}$$

and

$$2^{-n} \sum_{0 \leq i \leq n(1/2+\varepsilon)} \binom{n}{i} \geq 1 - e^{-2\varepsilon^2 n} \tag{11}$$

2. Limit Function

In this section, we will give a proof of Theorem 1.4.

Proof. Suppose that p is a bounded probability density function with discontinuities only of first kind, and let $d > 0$ be some number. Using Lemma 1.3, we have (extending p to be 0 to define it on all real numbers, if necessary):

$$\begin{aligned} P_{ch}(m;N)\sqrt{N} &= \sqrt{N}\int_{1/2}^{1} p(\alpha)P_{ch}(m,\alpha;N)d\alpha \\ &= \sqrt{N}\int_{1-m/2N-d/\sqrt{N}}^{1-m/2N+d/\sqrt{N}} p(\alpha)P_{ch}(m,\alpha;N)d\alpha + O\Big(\int_{d}^{\infty} e^{-y^2/128}dy\Big) \\ &= \sqrt{N}\int_{1-m/2N-d/\sqrt{N}}^{1-m/2N+d/\sqrt{N}} p(\alpha)P_{ch}(m,\alpha;N)d\alpha + o(1) \end{aligned}$$

where the the error terms are uniform as d goes to infinity by Lemma 1.3.

Suppose $x = m/N$, and use change of variables so that $\alpha(t) = 1-x/2+t/\sqrt{N}$, which gives that $d\alpha = dt/\sqrt{N}$, we get

$$P_{ch}(m;N)\sqrt{N} = \int_{-d}^{d} p(\alpha(t))P_{ch}(m,\alpha(t);N)dt + o(1)$$

To compute our limit, we will let d be large, and then compute limit as N goes to infinity, treating our limit essentially as a repeated limit.

Set $\alpha = \alpha(t)$. The probability to cheat is given by:

$$P_{ch}(m;\alpha) = P_R(m;\alpha)(1 - P_R(m;\alpha)) \tag{12}$$

Thus we are interested in $P_R(xN; 1 - x/2 + t/\sqrt{N}) = Q_R(x,t,N)$. We will compute limit of this function as N goes to infinity. Note that estimates we will use do not change if we change x by θ/N with $|\theta| < 1$, so when evaluating $Q_R(x,t,N)$ we will take $m = \lfloor xN \rfloor$ without loss of generality.

For convenience of the estimates, we will introduce a number c, and assume $N \gg c^2$; we may think of our 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) .

From Hoeffding inequalities (10, 11) we see, regardless of m, that as c goes to infinity:

$$P_R(m;\alpha) = \sum_{\frac{N}{2}-c\sqrt{N}<N_R<\frac{N}{2}+c\sqrt{N}} q(N_R)P_1\Big(m;\alpha,N_R\Big) + o(1) \tag{13}$$

Note that in the formula (3), for our chosen value of $m = xN$, 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 $\frac{m}{2} - q\sqrt{m} < n < \frac{m}{2} + q\sqrt{m}$, with q proportional to$c$ as N goes to infinity, and the whole interval will be between n' and m' for fixed c if N is large enough, so

$$P_1(m;\alpha,N_R) = \sum_{\frac{m}{2}-q\sqrt{m}<n<\frac{m}{2}+q\sqrt{m}} P_2(n;m,N_R)P_3(n;\alpha,N_R) \tag{14}$$

$$+ \sum_{n'\le n\le\frac{m}{2}-q\sqrt{m}} P_2(n;m,N_R)P_3(n;\alpha,N_R) \tag{15}$$

$$+ \sum_{\frac{m}{2}+q\sqrt{m}\le n\le m'} P_2(n;m,N_R)P_3(n;\alpha,N_R) \tag{16}$$

We will again prove that the last two sums are $o(1)$. Recall that

$$P_2(n;m,N_R)=\binom{m}{n}\binom{N-m}{N_R-n}\binom{N}{N_R}^{-1} \tag{17}$$

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.

Note that in the last two sums of (16), $|n-m/2|\geq 3c\sqrt{N}$, and moreover, since other values of N_R are part of $o(1)$ terms in (13), $\frac{N}{2}-c\sqrt{N}<N_R<\frac{N}{2}+c\sqrt{N}$.

From this it follows that

$$\begin{aligned}\binom{m}{n}\binom{N}{N_R}^{-1} &\leq \binom{m}{m/2}\binom{N}{N/2-c\sqrt{N}}^{-1}\\ &= (2^m/\sqrt{m})\Big(2^N(e^{-2c^2}/\sqrt{N})\Big)^{-1}\Big(1+O(1/N)\Big)\\ &= 2^{m-N}\Big(e^{2c^2}\sqrt{\frac{N}{m}}\Big)\Big(1+O(1/N)\Big)=2^{m-N}O(e^{2c^2})\end{aligned}$$

Using (8) and (10), we get

$$\begin{aligned}\sum_{n=\frac{m}{2}+q\sqrt{m}}^{m'} P_2(n;m,N_R)P_3(n;\alpha,N_R) &\leq \sum_{n=\frac{m}{2}+q\sqrt{m}}^{m'} P_2(n;m,N_R)\\ &= O(e^{2c^2})\cdot 2^{-(N-m)}\sum_{n=\frac{m}{2}+3c\sqrt{N}}^{m'}\binom{N-m}{N_R-n}\\ &= O(e^{2c^2})\cdot 2^{-(N-m)}\sum_{k=0}^{\frac{N-m}{2}-2c\sqrt{N}}\binom{N-m}{k}\\ &= O(e^{2c^2})\cdot e^{-8c^2\frac{N}{N-m}}=o(1)\end{aligned}$$

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

Similarly, we get

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

Moreover, from these calculations we see that

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

Let us estimate $P_3(n;\alpha,N_R)$, 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 (13) and (16). Let $N_R=\frac{N}{2}+r\sqrt{N}$ and $n=\frac{m}{2}+s\sqrt{m}=\frac{m}{2}+s\sqrt{x}\sqrt{N}$

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

$$P_3(n;m,N_R)=2^{-n}\sum_{i=0}^{T}\binom{n}{i}=\frac{1}{2}\Big(1+\mathrm{erf}(y)\Big)+o(1),$$

where $\mathrm{erf}(y)=\frac{2}{\sqrt{\pi}}\int_0^y e^{-u^2}du$, and under our restrictions on N_R and n, $T=\lceil(1-\alpha)N_R\rceil$, with the corresponding value $y=\frac{\frac{T}{n}-\frac{1}{2}}{\frac{1}{2\sqrt{n}}\sqrt{2}}=\frac{2T-n}{\sqrt{2n}}=r\sqrt{x}-t/\sqrt{x}-s+o(1)$.

Thus, we get as N goes to infinity,

$$P_3(n;m,N_R)=2^{-n}\sum_{i=0}^{T}\binom{n}{i}=\frac{1}{2}\Big(1+\mathrm{erf}(r\sqrt{x}-t/\sqrt{x}-s)\Big)+o(1).$$

Similarly, using (8) we get

$$P_2(n;m,N_R)=\frac{\sqrt{2}e^{-2s^2/x}e^{-2(r-s\sqrt{x})^2/(1-x)}}{\sqrt{x(1-x)\pi N}e^{-2r^2}}(1+o(1))$$

and

$$q(N_R)=\frac{2e^{-2r^2}(1+o(1))}{\sqrt{2\pi N}}.$$

Now, passing from sums to integrals, and taking limit as N tends to infinity, we see that there is

$$\lim_{N\to\infty}Q_R(x,t,N)=Q_R(x,t),$$

where

$$Q_R(x,t)=\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}drds\frac{1}{\pi}\frac{e^{-2s^2/x}e^{-2(r-s\sqrt{x})^2/(1-x)}}{\sqrt{x(1-x)}}\Big(1+\mathrm{erf}(r\sqrt{x}-t/\sqrt{x}-s)\Big),$$

$$Q_R(x,t)=1/2+\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}drds\frac{1}{\pi}\frac{e^{-2s^2/x}e^{-2(r-s\sqrt{x})^2/(1-x)}}{\sqrt{x(1-x)}}\mathrm{erf}(r\sqrt{x}-t/\sqrt{x}-s).$$

Using a table integral

$$\int_{-\infty}^{\infty}e^{-x^2/c}\mathrm{erf}(ax+b)dx=\sqrt{c\pi}\,\mathrm{erf}(b/\sqrt{1+ca^2})$$

(which can be obtained for instance using Fourier transform), we compute

$$\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}drds\frac{1}{\pi}\frac{e^{-2s^2/x}e^{-2(r-s\sqrt{x})^2/(1-x)}}{\sqrt{x(1-x)}}\mathrm{erf}\,(r\sqrt{x}-t/\sqrt{x}-s)$$

$$=\int_{-\infty}^{\infty}ds\frac{e^{-2s^2/x}}{\sqrt{2\pi x}}\mathrm{erf}\Big(\frac{-t/\sqrt{x}-s(1-x)}{\sqrt{1+x(1-x)/2}}\Big)=\frac{1}{2}\mathrm{erf}\Big(\frac{-t}{\sqrt{x(1+x(1-x)(2-x)/2)}}\Big)$$

Finally, we get, using that erf is odd, and $\int_0^\infty (1-\mathrm{erf}^2(x))dx = \sqrt{2/\pi}$

$$Q(x) = p^+ \int_0^\infty Q_R(x,t)(1-Q_R(x,t))dt + p^- \int_{-\infty}^0 Q_R(x,t)(1-Q_R(x,t))dt$$
$$= \frac{\bar{p}}{2}\int_0^\infty dt\Big(1-\mathrm{erf}^{\,2}\Big(\frac{t}{\sqrt{x(1+x(1-x)(2-x)/2)}}\Big)\Big) = \bar{p}\,\frac{\sqrt{x(2+x(1-x)(2-x))}}{2\sqrt{\pi}}$$

where $p^+ = \lim_{\alpha\to(1-x/2)^+} p(\alpha)$ and $p^- = \lim_{\alpha\to(1-x/2)^-} p(\alpha)$, and $\bar{p} = (p^+ + p^-)/2$. So we have obtained

$$Q(x) = \frac{1}{\sqrt{4\pi}}\bar{p}(1-x/2)\sqrt{x(2+x(1-x)(2-x))} \tag{18}$$

as claimed. □

Now note that if we set $x = 2(1-\alpha)$ then

$$\sqrt{x(2+x(1-x)(2-x))} = 2\sqrt{1-3\alpha+8\alpha^2-10\alpha^3+4\alpha^4},$$

so if we set $C = \int_{1/2}^1 d\alpha/(2\sqrt{1-3\alpha+8\alpha^2-10\alpha^3+4\alpha^4})$, $C = 0.673673\ldots$, then the optimal probability distribution on interval $(1/2,1)$ is obtained with the following probability density function:

$$p_0(\alpha) = \frac{1}{2C\sqrt{1-3\alpha+8\alpha^2-10\alpha^3+4\alpha^4}},$$

for which

$$Q_0 = 1/(2C\sqrt{\pi}) = 0.41874\ldots$$

is the optimal (sharp) lower bound for supremum of $Q(x)$ over $x \in (0,1)$. The bound is attained if Trent uses p_0, and on the other hand we have

Corollary 2.1. *For any bounded probability density function p on $(1/2,1)$ with discontinuities only of first kind, there is $x \in (0,1)$ such that*

$$Q(x) \geq Q_0,$$

where $Q(x)$ is given by expression (18).

From this it follows that no strategy of Trent for choosing α in the binding phase can beat the choice according to p_0, namely

Corollary 2.2. *For any constant $C < Q_0$ and sufficiently large N,*

$$\max_m P_{ch}(m,N) > \frac{C}{\sqrt{N}}.$$

References

[1] N. Paunković, J. Bouda, and P. Mateus, *Fair and optimistic quantum contract signing*, Physical Review A **84 (6)** (2011), 62331–62331.
[2] M. J. Fischer, N. A. Lynch and M. Paterson, *Impossibility of distributed consensus with one faulty process* J. ACM **32 (2)** (1985), 374—382.
[3] M. O. Rabin, *Transactions protected by beacons*, Journal of Computer and System Sciences **27** (1983), 256–267.
[4] M. Ben-Or, O. Goldreich, S. Micali, R. L. Rivest, *A fair protocol for signing contracts*, IEEE Transactions on Information Theory **36 (1)** (1990), 40—46.
[5] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press (2000).
[6] W. Hoeffding, *Probability inequalities for the sum of bounded random variables*, Journal of the American Statisitcal Association **58** (1963), 13—30.
[7] H. Robbins, *A Remark on Stirling's Formula*, The American Mathematical Monthly **62 (1)** (1955), 26–29.
[8] H. Louka, *Necessity of parameter randomization in quantum contract signing*, Matematički Vesnik, **69 (1)** (2017), 65–74.
[9] V. Božin and H. Louka, *Asymptotics of quantum contract signing*, Publications de l'Institut Mathématique, **101 (115)** (2017), 37–45.