Semi-loss-tolerant strong quantum coin-flipping protocol using quantum non-demolition measurement

Article *in* Quantum Information Processing · July 2014

DOI: 10.1007/s11128-014-0747-5 · Source: arXiv

Jiajun Ma
Tsinghua University
12 PUBLICATIONS **119** CITATIONS

N-party semi-loss-tolerant strong quantum dice rolling protocol using quantum non-demolition measurement

Qian Yang[1,2,3], Jia-Jun Ma[1], Fen-Zhuo Guo[2*] and Qiao-Yan Wen[1]
[1] State Key Laboratory of Networking and Switching Technology,
Beijing University of Posts and Telecommunications, Beijing, 100876, China
[2] School of Science, Beijing University of Posts and Telecommunications, Beijing, 100876, China
[3] Center for Quantum Information, IIIS, Tsinghua University, Beijing, China

(Dated: January 9, 2014)

In this paper, we present a semi-loss-tolerant strong quantum coin-flipping protocol using quantum non-demolition (QND) measurement, obtaining the recent best bias of 0.3536. Furthermore, we make use of the single photon as a single qubit avoiding the difficult implement of EPR resources, so that it is of great simplicity to construct three-party, four-party and a more normal N-party dice rolling protocol, including the parallel and serial ones different in time complexity. The protocol is fair in the sense that every player has the same probability of success in cheating attempts at biasing the outcome of the dice rolling. We also analyze explicit and optimal cheating strategies and get the best result among dice rolling protocols considering loss.

PACS numbers: 03.67.Mn, 03.65.Ta

I. INTRODUCTION

Dice rolling (DR) in classical settings was extensively introduced in 1999 by Feige U[1]. It is a cryptographic problem firstly proposed by N Aharon and J Silman[2], describing N remote distrustful parties must decide on a random string between 0 and $N-1$. There are two types of QDR protocol defined by [2]. Weak N-sided QDR is the problem that N remote distrustful parties having to decide on a number between 0 and $N-1$, such that: (i) each party is aware of any other party's preferred outcome. In particular, no two or more parties may share the same preference. (ii) If all parties are honest the probability of each outcome is equal to $1/N$. While M-party strong N-sided QDR is defined as the problem of M remote distrustful parties having to decide on a number between 1 and N, such that: (i) no party is aware of any other party's preferred outcome. In particular, any number of parties may share the same preference. (ii) If all parties are honest the probability of each outcome is equal to $1/N$.

Obviously QDR is a generalization of Quantum Coin Flipping (QCF) which is also a cryptographic task firstly introduced by Blum in 1981[3]. The goal of QCF is to enable two distrustful and spatially separated parties, usually referred as Alice and Bob, to generate a random bit whose value cannot be controlled by anyone of them. There are also two variants of QCF: "strong" CF (SCF)[5–9] and "weak" CF (WCF)[10–12]. In SCF each party is not aware of the other's preference for the coin's outcome, while in WCF the parties have opposite and known preferences. Obviously, every strong CF protocol can also be used to implement a weak CF protocol, but the converse statement is generally not true. The security of a CF protocol is quantified by the biases $\epsilon_A^{(i)}$and $\epsilon_B^{(i)}(i\epsilon 0,1)$; if $P_A^{(i)^*}$ and $P_B^{(i)^*}$ are the maximal probabilities that a dishonest Alice or Bob can force the outcome i, then

$$\epsilon_j^{(i)} = P_j^{(i)^*} - 1/2, i \in 0,1, j = A, B. \qquad (1)$$

In classical settings, given unlimited computational power, a dishonest party can always fully bias the outcome as he or she chooses, i.e., $\epsilon = 1/2$[4]. In contrast, this is not the case in the quantum world. Unconditional secure coin flipping is possible to some extent. Although the results of Mayers[13] and Lo Chau[14] implied the impossibility of perfect quantum coin flipping(the possibilities of both 0 and 1 are all 1/2 no matter what strategies a cheater uses), it can help guarantee neither of the two parties can totally control the outcome(which is impossible by classical means). The first strong coin flipping protocol was provided by Aharanov et al.[5] with a bias of 0.414. Subsequently Ambainis[6] as well as Spekkens and Rudolph[7] independently improved this bound to 0.25. Unfortunately it was proven by Kitaev[15] that any quantum strong coin flipping protocols can not enjoy a bias less than 0.207 and this bound has been saturated by Chailloux and Kerenidis's protocol[9]. Compared with quantum SCF, quantum WCF is less studied, Spekkens and Rudolph[11] firstly introduced a family of protocols with a bias of 0.207 and Mochon then improved it to 0.192 and finally to any $\epsilon \geq 0$[12].

Although a lot of progresses have been made along the way of exploring the least bias protocols, there is a common limit of previous results: practical issues were not taken into consideration. On imperfect practical conditions such as losses and noise in the quantum channel as well as in the quantum memory storage, many protocols will totally fail. As the most common practical imperfection in the long distance communication, losses were firstly analyzed in devising new practical protocols.

[*] Email: gfenzhuo@bupt.edu.cn

In 2008, Berlín *et al*[16](see also Ref.[17]) introduced a loss-tolerant SCF protocol with a relatively poor bias 0.4. Before long Aharon et al.[18] presented a family of loss-tolerant quantum coin flipping protocols which achieve a smaller bias than Berlin *et al* but at a small rate. Very recently, Andre Chailloux[19] presented an improved loss-tolerant quantum coin flipping with bias 0.359, by extending Berlín *et al*'s protocol by adding an encryption step. This result was slightly improved by Ma *et al*'s protocol[20] to 0.3536.

Compared with all loss-tolerant SCF mentioned above, our protocol presented here obtains the recent best bias of 0.3536, reproducing the result of the protocol in [20] using a single state with QND measurement which is easier to prepare in practice than EPR pairs used in [20]. After detailed analysis, we get the bias under fair condition as a function of p, where p is the probability that the qubit in the Bob's quantum memory storage is lost. When p approaches 0, the bias $\epsilon(p) \approx 0.3525$, which is equal to the protocol in [20] and also a best result over all the earlier loss-tolerant protocols[1–3]. We also show the bias will monotonously increase with a decreasing p. To achieve more flexibility and practical value, three-party DR protocol, four-party DR protocol and their extended form N-party DR protocol are given.

After this introduction, the structure of the paper is organized as follows. We begin our protocol in Sec. 2 with a contrast to the protocol in [20]. In Sec. 3, We propose an impressive three-party DR protocol, four-party DR protocol and extend them into the parallel and serial N-party DR protocol which are different in time complexity and all loss-tolerant. And the most normal attack that may exist to get the bias when those protocols are fair are analyzed. Conclusions and open problems are presented in Sec. 4.

II. QND-BASED SEMI-LOSS-TOLERANT COIN-FLIPPING PROTOCOL

The least bias among all SCF protocols considering the loss in practice is 0.3536 in ref. [1] showed as follows.

1. Bob prepares a singlet $|\varphi\rangle = \frac{|0_A 1_B\rangle - |1_A 0_B\rangle}{\sqrt{2}}$ and sends particle A to Alice, where the subscripts A and B denote the two entangled particles.

2. Alice randomly selects classical bit a, where $a = 0$ represents that she chooses basis $|0\rangle, |1\rangle$ and $a = 1$ represents that she chooses basis $cos|0\rangle + sin|1\rangle, sin|0\rangle - cos|1\rangle$, then she measures particle A along the basis she chooses.

3. If Alice successfully detects the particle, whose outcome is denoted as r_A, she asks Bob to proceed the protocol, otherwise, she asks Bob to restart the protocol.

4. Bob sends Alice a randomly selected classical bit b.

5. Alice informs Bob of her selected a and outcome r_A.

6. Bob measures particle B along the basis that a represents. If he successfully detects it, whose outcome is recorded as r_B, and $r_B = r_A$, he will abort and claim Alice is cheating. In all other cases the outcome of the coin flipping is given by $b \oplus r_A$.

However, the protocol in [20] utilizes EPR pairs to make the semi-loss-tolerant come true. Considering the difficulty of preparing entangled states, we give some impressive improvements to get the same result and efficiency using Quantum nondemolition (QND) measurements[21].

Replacing the preparation of EPR pairs with QND measurements, we make the implementation more accessible with current technology.

1. We say of $\varphi(a, x)\rangle$ that a is the basis and r_A is the bit which could be showed as follows.

$$a = 0 \begin{cases} |\varphi_{(0,0)}\rangle = |0\rangle \\ |\varphi_{(0,1)}\rangle = |1\rangle \end{cases}, a = 1 \begin{cases} |\varphi_{(1,0)}\rangle = \cos\alpha|0\rangle + \sin\alpha|1\rangle \\ |\varphi_{(1,1)}\rangle = \sin\alpha|0\rangle - \cos\alpha|1\rangle \end{cases}.$$

Alice prepares one state $|\varphi_{(a,r_A)}\rangle$ from $|\varphi_{(0,0)}\rangle = |0\rangle, |\varphi_{(0,1)}\rangle = |1\rangle, |\varphi_{(1,0)}\rangle = \cos\alpha|0\rangle + \sin\alpha|1\rangle, |\varphi_{(1,1)}\rangle = \sin\alpha|0\rangle - \cos\alpha|1\rangle$ with basis $a(0,1)$ and bit $r_A(0,1)$ chosen independently at random, then she sends the single photon to Bob.

2. Bob makes sure that he received this photon using QND measurements, keep the received qubit in his quantum memory storage, and notice Alice about it. Otherwise, he will restart the protocol.

3. Bob sends Alice a randomly selected classical bit b.

4. Alice informs Bob of her selected single photon $|\varphi_{(a,r_A)}\rangle$.

5. Bob measures the qubit in the quantum memory according to Alice's announcing a. If he detects it, whose outcome is denoted as r_B, and finds that $r_A \neq r_B$, he aborts the protocol, calling Alice a cheater. If $r_A = r_B$ or even he doesn't detect the qubit due to the probability p that the qubit in the Bobs quantum memory storage is lost, the outcome of the coin flipping is $b \oplus r_A$.

III. N-PARTY LOSS-TOLERANT DICE ROLLING PROTOCOL

Three-party loss-tolerant dice rolling protocol is given as follows:

The first round: Alice and Bob roll the dice according to QND-BASED SEMI-LOSS-TOLERANT PROTOCOL described above. In the final step, if Bob detects the qubit, whose outcome is denoted as r_B, and finds that $r_A \neq r_B$, he aborts the protocol, calling Alice a cheater. If $r_A = r_B$ or even he doesn't detect the qubit, the outcome of the coin flipping is $b \oplus r_A$. Here we can suppose that Alice will win the first round if $b \oplus r_A$ is 0, and Bob will win the first round if $b \oplus r_A$ is 1. The winner, who can be supposed to be Alice, without losing the normality, will join the next competition.

The second round: Alice and Charlie roll the dice based on QND-BASED SEMI-LOSS-TOLERANT PROTOCOL described above. If Charlie detects it, whose outcome is denoted as r_C, and finds that $r_A \neq r_C$, he aborts the protocol, calling Alice a cheater. If $r_A = r_C$ or even he doesn't detect the qubit, the outcome of the coin flipping is $c \oplus r_A$. Here we can suppose that Alice will win the first round if $c \oplus r_A$ is 0, and Charlie will win the first round if $C \oplus r_A$ is 1. The winner is the final winner of the three parties.

The key difference between the protocol in [20] and ours is that we choose two different methods to better solve the problem that the qubit-receiver(Bob in our protocol) may receive no qubit so that the qubit-sender(Alice in our protocol) could announce any result she wants to bias the result to what she wants. The protocol in [20] chooses to utilize EPR pairs and ours' intention is to make it more practical by using one single state with QND measurement. The remaining steps of the two protocols are equivalent. Consequently our security analysis follows directly from the analysis of the protocol in [20].

We will show security analysis of three-party loss-tolerant dice rolling protocol below.

DR protocol is fair if and only if

$$\overline{P_A^*} = \overline{P_B^*} = \overline{P_C^*}, \tag{2}$$

according to the definition in [2], with $\overline{P_A^*}(\overline{P_B^*}, \overline{P_C^*})$is the maximum probability that party A (B, C) loses. Consequently, we analyze the following context based on the maximum probability of lose.

What's more, we will be interested in the N "worst case" scenarios to maximize the bias, where all but one of the parties are dishonest and moreover, are cooperating with one another, using the classical and quantum communication channels.

Then we get the bias of three-party loss-tolerant protocol:

It would be relatively easy to realize that our result would be the same as Ma's conclusion because except the key step of using resources, our protocol could change into Ma's model in an equivalent transformation point of view. Consequently, Alice would win (or lose) the game with the probability of $\frac{1+\cos\alpha}{2} \cdot (1 - \frac{1+\cos\alpha}{2})$, and Bob would win (or lose) the game with $\frac{1+p+(1-p)\sin\alpha}{2} \cdot (1 - \frac{1+p+(1-p)\sin\alpha}{2})$. So the maximum probability that party Bob loses is

$$\overline{P_B^*} = \frac{1+\cos\alpha}{2} + (1 - \frac{1+\cos\alpha}{2}) \cdot \frac{1+p+(1-p)\sin\beta}{2}. \tag{3}$$

Using the same method, the maximum probability that party Charlie loses is

$$\overline{P_C^*} = 1 - \frac{1+p+(1-p)\sin\alpha}{2}. \tag{4}$$

and the maximum probability that party Alice loses is

$$\overline{P_A^*} = \frac{1+p+(1-p)\sin\alpha}{2} + [1 - \frac{1+p+(1-p)\sin\alpha}{2}] \cdot \frac{1+p+(1-p)\sin\beta}{2}. \tag{5}$$

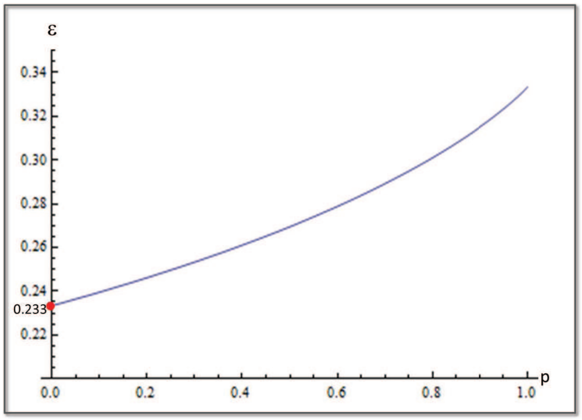

FIG. 1: Maximal fair bias is a function of p, it decreases with decreasing p, and our optimal bias reproduces the best result.

On the whole, considering $\overline{P_A^*} = \overline{P_B^*} = \overline{P_C^*}$, this protocol is fair iff

$$\alpha = \arcsin\frac{p^2 - p + \sqrt{2-2p}}{p^2 - 2p + 2}. \tag{6}$$

$$\beta = \arcsin\frac{p^2 - 1 + 4\sqrt{1-p}}{5 - 2p + p^2}. \tag{7}$$

Finally, we can get the bias of this protocol is $\overline{P_C^*} - \frac{2}{3} = \frac{1+\sqrt{1-(\frac{p^2-1+4\sqrt{1-p}}{5-2p+p^2})^2}}{2} - 2/3 (0 \leqslant p \leqslant 1)$.We can see it clearly in Curve Simulation(Fig 1).

A six-round weak three-sided DR protocol is constructed in [2] using three-round weak imbalanced CF protocol twice. However, it cannot be loss-tolerant and therefore has less practical usage because of the kernel CF protocol it uses. Our protocol could be more practical and at the same time, safer with a lower bias.

Assuming that one round of CF in our N-party protocol has the time consumption of t, where t is a constant. Obviously, the parallel and serial three-party DR protocol have the same time consumption $2t$. When it comes to N-party, where N is more than three, the DR protocol can be divided into parallel and serial ones. We find the difference between the parallel and serial DR protocol by analyzing the four-party ones then we extend it to N-party in a normal model.

According to the construction steps introduced in three-party, we can get four-party loss-tolerant dice rolling protocol which described in Fig 2 and Fig 3.

Obviously, the parallel and serial three-party DR protocol have the same time complexity. We find the difference between the serial and parallel DR protocol by analyzing the four-party ones so that N-party DR protocol is constructed directly. Serial four-party DR protocol showed in Fig 2 has the time complexity $3t$ while parallel one in Fig 3 has the time complexity $2t$ because two rounds of DR are executed simultaneously in the parallel one. By construction, we can get N-party DR protocol

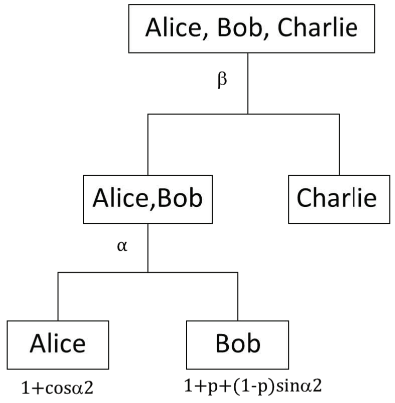

FIG. 2: The model of serial four-party DR protocol.

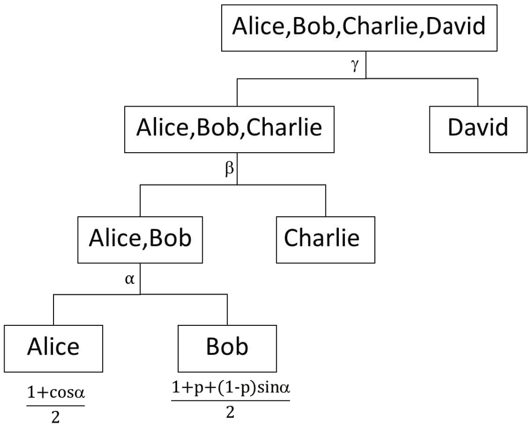

FIG. 3: The model of parallel four-party DR protocol.

both in the term of serial and parallel one. For N-party, the time complexity of parallel one approximately approachs $\Omega(logN)t$ which is smaller than serial one $\Omega(N)t$.

IV. CONCLUSION

To sum up, we get a semi-loss-tolerant strong quantum coin-flipping protocol using quantum non-demolition (QND) measurement, and obtain the recent best bias of 0.3536, reproducing the result in [20]. Our protocol is advantageous in that, we avoid the difficult implement of EPR resources by using the single photon, which could be an improvement for the design of coin-flipping protocol.

To inherited this simplicity, we can easily construct more practical three-party and four-party dice rolling protocols and drive them into any N-party dice rolling protocol, including the parallel and serial ones different in time complexity which is demonstrated clearly. We analyzed explicit and optimal cheating strategies and proved that our protocol is fair, especially when two parties, both Alice and Bob have an optimal cheating strategy capable of producing their desired outcome with 0.8536 probability of success (assuming the other player is honest). When it comes to three parties, the probability becomes 0.23+0.67=0.9 which is also the best result among dice rolling protocols considering loss.

It is necessarily important that we go on to find a safer loss-tolerant quantum coin-flipping protocol with a smaller bias.

Acknowledgments

This work is supported by NSFC (Grant Nos. 61272057, 61202434, 61170270, 61100203, 61003286, 61121061), NCET (Grant No. NCET-10-0260), Beijing Natural Science Foundation (Grant Nos. 4112040, 4122054), the Fundamental Research Funds for the Central Universities (Grant No. 2012RC0612, 2011YB01). It is also supported in part by the National Basic Research Program of China Grant 2011CBA00300, 2011CBA00302, the National Natural Science Foundation of China Grant 61073174, 61033001, 61061130540.

[1] Feige U, 1999 Proc. 40th Annual IEEE Symp. on the Foundations of Computer Science (Los Alamitos, CA: IEEE Computer Society Press) p 142.

[2] N Aharon and J Silman, 2010 New J. Phys. 12 033027.

[3] M. Blum, in Advances in Cryptology: A Report on CRYPTO '81(Santa-Barbara, CA, 1981), p. 11.

[4] J. Kilian, in Proceedings of the 20th Annual ACM Symposium on Theory of Computing (ACM Press, New York, 1988), p. 20.

[5] D. Aharonov, A. Ta-Shma, U. Vazirani, and A. C. Yao (2000), Quantum Bit Escrow, Proceedings of the 32nd Annual Symposium on Theory of Computing (New York), pp. 705.

[6] A. Ambainis (2001), A new protocol and lower bounds for quantum coin-flipping, Proceedings of the 33rd Annual Symposium on Theory of Computing (New York), pp. 134.

[7] R.W. Spekkens and T. Rudolph (2001), Degrees of concealment and bindingness in quantum bit commitment protocols, Phys. Rev. A, Vol. 65, pp. 012310.

[8] Roger Colbeck (2007), An Entanglement-Based Protocol For Strong Coin Tossing With Bias 1/4, Phys. Lett. A, Vol. 362, pp. 390-392.

[9] A. Chailloux and I. Kerenidis (2009), Optimal quantum strong coin-flipping, Proceedings of the 50th Annual IEEE Symposium on the Foundations of Computer Science (Atlanta, GA), pp. 527.

[10] C. Mochon (2004), Quantum weak coin-flipping with bias

of 0.192, quant-ph/0403193.

[11] R. W. Spekkens and T. Rudolph (2002), Quantum Protocol for Cheat-Sensitive Weak Coin Flipping, Phys. Rev. Lett., Vol. 89, pp. 227901.

[12] C. Mochon (2007), Quantum weak coin-flipping with arbitrarily small bias, quant-ph/0711.4114.

[13] Dominic Mayers (1997), Unconditionally secure quantum bit commitment is impossible, Phys. Rev. Lett., Vol. 78, pp. 3414-3417.

[14] Hoi-Kwong Lo and H. F. Chau (1997), Is quantum bit commitment really possible?, Phys. Rev. Lett., Vol. 78, pp. 3410-3413.

[15] A. Kitaev (unpublished). The proof is reproduced in Ref. [14].

[16] G. Berlín, G. Brassard, F. BussiReres, and N. Godbout (2009), Fair loss-tolerant quantum coin flipping, Phys. Rev. A, Vol. 80, pp. 062321.

[17] A. T. Nguyen, J. Frison, K. Phan Huy, and S. Massar (2008), Experimental quantum tossing of a single coin, New J. Phys., Vol. 10, pp. 083037.

[18] N. Aharon, S. Massar, and J. Silman (2010), A family of loss-tolerant quantum coin flipping protocols, Phys. Rev. A, Vol. 82, pp. 052307.

[19] A. Chailloux (2011), Improved Loss-Tolerant Quantum Coin Flipping, quant-ph/1009.0044.

[20] Jia-Jun Ma, Fen-Zhuo Guo, Qian Yang, Yan-Bing Li, Qiao-Yan Wen, Quantum Inf. Comput. 12 pp.0489-0500 (2012).

[21] V. B. Braginsky and F. Ya. Khalili, Quantum nondemolition measurements: the route from toys to tools, Reviews of Modern Physics, Vol. 68, No. 1, January 1996.