Measurement-Device-Independent Quantum Coin Tossing

Liangyuan Zhao, Zhenqiang Yin,* Shuang Wang, Wei Chen,† Hua Chen, Guangcan Guo, and Zhengfu Han
Key Laboratory of Quantum Information, University of Science and Technology of China, CAS, Hefei, Anhui 230026, China
Synergetic Innovation Center of Quantum Information & Quantum Physics,
University of Science and Technology of China, Hefei, Anhui 230026, China

Coin tossing (CT) allows two spatially separated mistrustful parties, e.g., Alice and Bob, to generate a common random bit. CT is an important cryptographic primitive and can be used in many applications, such as the secure two-party computation. The first classical coin tossing was introduced by Blum [1] in 1981. Its quantum counterpart, namely quantum coin tossing (QCT), was investigated by Bennett and Brassard in their 1984 paper for the first time[2], henceforth referred to as BB84 QCT. Unfortunately, as argued in [2] and the following Mayers-Lo-Chau (MLC) [3–5] no-go theorem, an unconditionally secure *ideal* QCT is impossible. However, based on the laws of quantum mechanics, QCT can achieve a maximal cheating probability lower than 1, which is impossible for any non-relativistic classical coin tossing unless unproven computational assumptions are made [6–12].

There is an assumption in the above protocols that the practical implementation is perfect. The security may be completely broken if the imperfections of practical systems are taken into account. One of the notorious problem is losses, which makes the early two QCT experiments [13, 14] completely insecure. A breakthrough method was made by Berlin *et al.* [15], who proposed a loss-tolerant QCT protocol (BBBG09 protocol) that is completely impervious to loss of quantum states with single-photon source. BBBG09 has been implemented with an entangled source [16] and modified for the weak coherent state source (the modified protocol is referred as PCDK11 protocol) [17]. The PCDK11 was implemented based on a commercial plug-and-play scheme designed for quantum key distribution (QKD) with several modifications [18], considering all the standard realistic imperfections.

However, there are side channel loopholes, especially the detector side channels, in practical QKD that could affect the security of practical QCT. Take the detector-blinding attack for example. The principle of the detector-blinding attack on the practical QCT is as follows. First, a malicious Alice transmits bright light into Bob's detectors to convert them into classical linear model [19], and then sends a honest state to Bob. Bob has a successful click only if his basis is consistent with the sent state. Consequently, Alice can correlate her basis choice with Bob's successful detections. Note that only the first successful detection is used for the post-processing. Thus, Alice can declare special state she has sent to Bob according to Bob's announced random bit and her desired coin's outcome. In this way, Alice has complete control over the coin's outcome without being detected as cheating.

To remove all the known and unknown detector-side channel attacks launched by Alice in practical QCT systems, we propose a measurement-device-independent QCT (MDI-QCT) protocol [20] based on BBBG09, which benefits from the idea of MDI-QKD [21, 22]. The advantage of MDI-QKD is that the legitimate parties only need to characterize their state preparations and they do not need to hold a measurement device anymore. Thus, the measurement device can be viewed as a black box and it naturally removes all the detector side-channels. The concept of MDI-QCT is similar to MDI-QKD in that Alice and Bob only need to know their state preparation processes and Bob does not have to trust his measurement device. That is to say, Bob can treat his measurement device as a black box and just obtain a Bell state outcome from it. Combining the outcome with his and Alice's announced states, Bob can estimate whether Alice is cheating with a non-vanishing (but non-unit) probability. Adapting MDI paradigm in QCT is not quite an easy issue, for Alice and Bob in QCT are mistrustful, while they are trustworthy in QKD. Note that the untrusted measurement device now is in Bob's laboratory, which is also different from MDI-QKD. Considering these differences, we emphasize that Bob should shield his source for preventing both Alice and the untrusted measurement device from knowing the classical information about his state preparation.

Our protocol is based on the BBBG09 and we assume that each party uses a single-photon source for the aim of completely tolerating losses.

Protocol: MDI-QCT—

1. Alice picks, uniformly at random, a basis $\alpha \in \{0,1\}$ and a bit $a \in \{0,1\}$. She then prepares the polarization state $|\phi_{\alpha,a}\rangle$, i.e.,

$$\begin{aligned} |\phi_{\alpha,0}\rangle &= \sqrt{y}|H\rangle + (-1)^{\alpha}\sqrt{1-y}|V\rangle, \\ |\phi_{\alpha,1}\rangle &= \sqrt{1-y}|H\rangle - (-1)^{\alpha}\sqrt{y}|V\rangle, \end{aligned} \tag{1}$$

where $y \in (\frac{1}{2}, 1)$, which will be adjusted to make the protocol *fair*, $|H\rangle$ and $|V\rangle$ represent the horizontal and vertical polarization states, respectively. Alice sends the state to Bob.

2. Bob prepares the state $|\phi_{\beta,b}\rangle$ ($\beta \in \{0,1\}, b \in \{0,1\}$) randomly and independently of Alice. Then, he inputs Alice's and his states into a black box to perform a Bell state measurement (BSM) that projects $|\phi_{\alpha,a}\rangle$ and $|\phi_{\beta,b}\rangle$

* yinzheqi@mail.ustc.edu.cn
† kooky@mail.ustc.edu.cn

into a Bell state (see Fig. 1). If the BSM does not obtain a Bell state, then the black box outputs a "failure" click. Bob now will ask Alice to restart step 1. Otherwise, Bob records the corresponding result. Bob needs only to identify Bell states $|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$, implying the black box can only use linear optical elements. Theoretical probabilities of the outcomes $|\Psi^{\pm}\rangle$ for different combinations of $|\phi_{\alpha,a}\rangle$ and $|\phi_{\beta,b}\rangle$ are shown in Table I.

3. Bob sends Alice a random bit $b' \in \{0, 1\}$.

4. Alice reveals $\{\alpha, a\}$.

5. Bob compares $\{\alpha, a\}$ and $\{\beta, b\}$ with the cells in Table I. If the combination of $\{\alpha, a\}$ and $\{\beta, b\}$ corresponds to the cell with probability 0, then Bob detects Alice cheating and aborts the protocol. Otherwise, the outcome of the coin value is $x = a \oplus b'$.

One feature of MDI-QCT is its loss tolerant property with single-photon sources. The main reason that MDI-QCT retains this key property is that neither Bob nor Alice could use the unambiguous discrimination or the maximal-confidence discrimination to obtain a higher *bias* than the minimum-error discrimination. The concrete proof is given in the attached full paper [20].

The security of MDI-QCT is analyzed in two aspects [20]. First, we discuss the correctness of the protocol in noisy environment, which is modeled by the abort probability when both parties are honest. We find that the coincidence detections of the BSM make our protocol more robust against the noise in practical system. Then, we calculate each all powerful dishonest party's maximal cheating probability given that the other party is honest.

The optimal cheating strategy of a malicious Bob is to perform an optimal measurement to discriminate the received states sent by honest Alice, i.e., to obtain a. As the honest states sent by Alice are no different in form from those in BBBG09 [15], dishonest Bob's optimal cheating strategy is the same as theirs. For the case where honest Alice uses a single-photon source, Bob's maximal cheating probability is $Pr_B[x] = y$ [15]. In the above cheating strategy, a dishonest Bob will deviate the MDI-protocol to obtain a maximal cheating probability. However, our protocol is designed only to protect an honest Bob, thus it is no matter that the advantage of the MDI paradigm does not exists for a dishonest Bob.

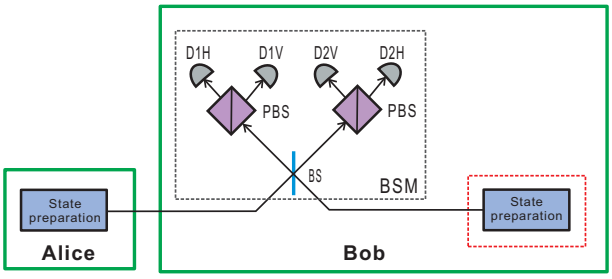

FIG. 1. (Color online) Schematic diagram of MDI-QCT when both parties are honest. Here, BS stands for 50:50 beam splitter and PBS stands for polarization beam splitter. Alice and Bob prepare polarization states as Eq. (1) randomly using single-photon sources. Bob performs the BSM and records the results for the verification of Alice's honesty. A joint click on $D1H$ and $D2V$, or $D1V$ and $D2H$, represents a projection into Bell state $|\Psi^{-}\rangle$. And a joint click on $D1H$ and $D1V$, or $D2H$ and $D2V$, represents a projection into Bell state $|\Psi^{+}\rangle$. The red dotted box means that the classical information of Bob's state preparation is not leaked to the BSM and Alice. The grey dotted box represents that Bob does not need to trust the BSM device.

When Alice is dishonest, one important assume is that Alice builds the measurement device which contains her cheating device, and gives it to Bob. Bob only needs to protect the classical information of his state preparation from leakage to the untrusted measurement device and Alice. On the other hand, the outcome of the BSM cannot reveal Bob's quantum state with certainty. Therefore, we can let the black box send classical information to Alice. These are equivalent to that the measurement device is placed in Bob's side and Bob announces the measurement results. Thus, all the detector side channels are removed. We first introduce an individual attack where Alice places a cheating device to discriminate Bob's state in the black box. In this attack, she can bias the coin with probability $Pr_A^{ind}[x] = \frac{3}{4}$. Then, we discuss a coherent attack with the assumption that Alice always let the black box do BSM. The coherent attack is derived from the pioneering work of Spekkens and Rudolph [8]. In the coherent attack, Alice can bias the coin with probability $Pr_A^{coh}[x] = \frac{3+2\sqrt{y(1-y)}}{4}$, which is the same as with BBBG09 [15].

To make the protocol *fair*, we can let $Pr_A^{coh}[x] = Pr_B[x]$. Thus, we have $y = 0.9$ for the state preparation and basis choice processes of the protocol. The *bias* of the protocol is 0.4 under this coherent attack.

From this work we can see that some side channel attacks presented in practical QKD can also arise in other practical quantum cryptographic tasks with mistrustful parties. The MDI-QCT protocol suggests that the method in MDI-QKD can also be modified to be applied to mistrustful quantum cryptography. Thus we extend the scope of the skill of MDI-QKD into a very rich field. Furthermore, our protocol can increase the transmission distance if we permit an agent of Bob to perform the BSM in the middle of Alice and Bob.

We have already proven the security of MDI-QCT against a dishonest Alice under a coherent attack. It is interesting to have a more general security analysis in the future. Another theoretic research needed is to combine the source flaws into security analysis. Because we have assumed that Alice's and Bob's states are perfect. It should examine this condition carefully in practice.

In the experiments, MDI-QCT can be modified in a way like the PCDK11 to be implemented with a weak coherent state source. Thus, the platforms for the implementation of MDI-QKD [24–29] is useable, which implies MDI-QCT can be utilized in practical QCT systems soon.

TABLE I. Theoretical probabilities of Bell states $|\Psi^{\pm}\rangle$ for different combinations of $|\phi_{\alpha,a}\rangle$ and $|\phi_{\beta,b}\rangle$. These can be calculated by the interferences of the honest states at the beam splitter.

			$\|\Psi^+\rangle$					$\|\Psi^-\rangle$	
(a)	$\|\phi_{0,0}\rangle$	$\|\phi_{0,1}\rangle$	$\|\phi_{1,0}\rangle$	$\|\phi_{1,1}\rangle$	(b)	$\|\phi_{0,0}\rangle$	$\|\phi_{0,1}\rangle$	$\|\phi_{1,0}\rangle$	$\|\phi_{1,1}\rangle$
$\|\phi_{0,0}\rangle$	$2y(1-y)$	$\frac{1}{2}(1-2y)^2$	0	$\frac{1}{2}$	$\|\phi_{0,0}\rangle$	0	$\frac{1}{2}$	$2y(1-y)$	$\frac{1}{2}(2y-1)^2$
$\|\phi_{0,1}\rangle$	$\frac{1}{2}(1-2y)^2$	$2y(1-y)$	$\frac{1}{2}$	0	$\|\phi_{0,1}\rangle$	$\frac{1}{2}$	0	$\frac{1}{2}(2y-1)^2$	$2y(1-y)$
$\|\phi_{1,0}\rangle$	0	$\frac{1}{2}$	$2y(1-y)$	$\frac{1}{2}(2y-1)^2$	$\|\phi_{1,0}\rangle$	$2y(1-y)$	$\frac{1}{2}(1-2y)^2$	0	$\frac{1}{2}$
$\|\phi_{1,1}\rangle$	$\frac{1}{2}$	0	$\frac{1}{2}(2y-1)^2$	$2y(1-y)$	$\|\phi_{1,1}\rangle$	$\frac{1}{2}(1-2y)^2$	$2y(1-y)$	$\frac{1}{2}$	0

[1] M. Blum, in *Advances in Cryptology: A Report on CRYPTO'81* (Santa-Barbara, California, 1981) pp. 11–15.

[2] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, p. 175.

[3] H.-K. Lo and H. F. Chau, Physica D: Nonlinear Phenomena **120**, 177 (1998).

[4] D. Mayers, Physical review letters **78**, 3414 (1997).

[5] H.-K. Lo and H. F. Chau, Physical Review Letters **78**, 3410 (1997).

[6] D. Aharonov, A. Ta-Shma, U. V. Vazirani, and A. C. Yao, in *Proceedings of the thirty-second annual ACM symposium on Theory of computing* (ACM, 2000) pp. 705–714.

[7] A. Ambainis, in *Proceedings of the thirty-third annual ACM symposium on Theory of computing* (ACM, 2001) pp. 134–142.

[8] R. W. Spekkens and T. Rudolph, Quantum Information & Computation **2**, 66 (2002).

[9] R. W. Spekkens and T. Rudolph, Physical Review A **65**, 012310 (2001).

[10] A. Nayak and P. Shor, Physical Review A **67**, 012304 (2003).

[11] R. Colbeck, Physics Letters A **362**, 390 (2007).

[12] A. Kitaev, Talk at QIP (2003).

[13] G. Molina-Terriza, A. Vaziri, R. Ursin, and A. Zeilinger, Physical review letters **94**, 040501 (2005).

[14] A. T. Nguyen, J. Frison, K. P. Huy, and S. Massar, New Journal of Physics **10**, 083037 (2008).

[15] G. Berlin, G. Brassard, F. Bussieres, and N. Godbout, Physical Review A **80**, 062321 (2009).

[16] G. Berlín, G. Brassard, F. Bussières, N. Godbout, J. A. Slater, and W. Tittel, Nature communications **2**, 561 (2011).

[17] A. Pappa, A. Chailloux, E. Diamanti, and I. Kerenidis, Physical Review A **84**, 052305 (2011).

[18] A. Pappa, P. Jouguet, T. Lawson, A. Chailloux, M. Legré, P. Trinkler, I. Kerenidis, and E. Diamanti, Nature communications **5** (2014).

[19] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nature photonics **4**, 686 (2010).

[20] L. Zhao, Z. Yin, S. Wang, W. Chen, H. Chen, G. Guo, and Z. Han, Physical Review A **92**, 062327 (2015).

[21] H.-K. Lo, M. Curty, and B. Qi, Physical review letters **108**, 130503 (2012).

[22] F. Xu, M. Curty, B. Qi, and H.-K. Lo, Selected Topics in Quantum Electronics, IEEE Journal of **21**, 1 (2015).

[23] S. Sajeed, I. Radchenko, S. Kaiser, J.-P. Bourgoin, A. Pappa, L. Monat, M. Legré, and V. Makarov, Phys. Rev. A **91**, 032326 (2015).

[24] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Physical review letters **111**, 130501 (2013).

[25] T. F. da Silva, D. Vitoreti, G. Xavier, G. do Amaral, G. Temporão, and J. von der Weid, Physical Review A **88**, 052303 (2013).

[26] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, *et al.*, Physical review letters **111**, 130502 (2013).

[27] F. Xu, B. Qi, Z. Liao, and H.-K. Lo, Applied Physics Letters **103**, 061101 (2013).

[28] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, Physical review letters **112**, 190503 (2014).

[29] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, *et al.*, Physical review letters **113**, 190501 (2014).