Experimental preparation and verification of quantum money

Experimental preparation and verification of quantum money

Jian-Yu Guan,[1,2] Juan Miguel Arrazola,[3] Ryan Amiri,[4] Weijun Zhang,[5] Hao Li,[5] Lixing You,[5] Zhen Wang,[5] Qiang Zhang,[1,2] and Jian-Wei Pan[1,2]

[1]*Shanghai Branch, Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, P. R. China*

[2]*CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, Shanghai Branch, University of Science and Technology of China, Hefei, Anhui 230026, China*

[3]*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543*

[4]*SUPA, Institute of Photonics and Quantum Sciences, Heriot-Watt University, Edinburgh EH14 4AS, United Kingdom*

[5]*State Key Laboratory of Functional Materials for Informatics, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 200050, P. R. China*

(Received 21 September 2017; published 27 March 2018)

A quantum money scheme enables a trusted bank to provide untrusted users with verifiable quantum banknotes that cannot be forged. In this work, we report a proof-of-principle experimental demonstration of the preparation and verification of unforgeable quantum banknotes. We employ a security analysis that takes experimental imperfections fully into account. We measure a total of 3.6×10^6 states in one verification round, limiting the forging probability to 10^{-7} based on the security analysis. Our results demonstrate the feasibility of preparing and verifying quantum banknotes using currently available experimental techniques.

DOI: 10.1103/PhysRevA.97.032338

I. INTRODUCTION

Remarkable progress has been made in quantum cryptography since its inception several decades ago. Quantum key distribution is widely considered to be one of the first practical quantum technologies [1–3], while many other protocols are beginning to shift from theoretical proposals to experimental demonstrations. Examples of these are developments in quantum signature schemes [4–9], quantum fingerprinting [10–12], secure quantum computation [13–16], covert communication [17–20], and bit commitment [21–24]. Despite these advances, quantum money [25] (the first quantum cryptography protocol to be proposed) has only recently started to enter the realm of possible experimental implementations.

Quantum money was first introduced in a seminal paper by Wiesner in 1970. The goal of any quantum money scheme is to enable a trusted authority, the bank, to provide untrusted users with verifiable banknotes that cannot be forged. Many variants of Wiesner's original scheme were found to be vulnerable to so-called "adaptive attacks" [26–28], which motivated the formulation of new quantum money protocols which are provably secure against unbounded quantum adversaries. Similarly, progress was made in developing simpler protocols that take into account experimental limitations. In Ref. [29], a secure quantum money protocol was proposed requiring only classical communication between a verifier and the bank. The issue of tolerance to experimental errors was first addressed in Ref. [30], with further developments in Ref. [31]. Recently, a practical protocol with nearly optimal noise tolerance was proposed in Ref. [32]. These developments have led to the first quantum money experiment, with a demonstration of forging in Wiesner's original scheme [33]. An unforgeable demonstration of quantum money remains experimentally challenging.

In this work, we present an experimental implementation of the quantum money scheme of Ref. [32], demonstrating the entire life-cycle of the quantum states contained in a quantum banknote: from preparation using a laser source and phase modulation, to verification using passive linear optics. We perform a security analysis of the protocol that takes experimental imperfections fully into account. The setup allows for fast and efficient verification of quantum banknotes, compatible with on-chip realizations and storage in quantum memories [34], which may be performed in the future.

In the remainder of this paper, we give a detailed description of the quantum money protocol, including the bank's algorithm for preparing the quantum banknotes and the verification procedure of the holders. We then describe the experimental setup for state preparation and verification, and finally give the results of calibration of the protocol as well as the verification of the banknotes.

II. QUANTUM MONEY PROTOCOL

Any scheme for producing unforgeable quantum banknotes consists of a procedure from the bank to prepare the banknotes and a method to verify their authenticity. In this work, we implement the practical quantum money scheme of Ref. [32], which is based on hidden matching quantum retrieval games (QRGs) [29,35]. In these QRGs, the bank encodes a four-bit classical string $x = x_1x_2x_3x_4$ into a sequence of coherent states with amplitude α of the form

$$|\alpha,x\rangle := |(-1)^{x_1}\alpha\rangle|(-1)^{x_2}\alpha\rangle|(-1)^{x_3}\alpha\rangle|(-1)^{x_4}\alpha\rangle. \quad (1)$$

The verifier's goal is to perform a measurement on $|\alpha,x\rangle$ that allows her to retrieve the value of the parity bit $b = x_i \oplus x_j$, where the possible (i,j) pairs are specified by the

matchings $M_1 = \{(1,2),(3,4)\}$, $M_2 = \{(1,3),(2,4)\}$, and $M_3 = \{(1,4),(2,3)\}$. This measurement can be done by employing unbalanced Mach-Zehnder interferometers, as explained in detail later in this paper. These hidden matching QRGs form the building block of the quantum money protocol, as described below.

A. Banknote preparation

1. The bank independently and randomly chooses N strings of four bits which we call $x^1, \ldots, x^N$.

2. The bank creates N quantum states $|\alpha, x^1\rangle$, $|\alpha, x^2\rangle, \ldots, |\alpha, x^N\rangle$, which constitute the quantum banknote. The bank assigns a unique serial number to the banknote for identification.

3. The bank creates a classical binary register r and initializes it to 0^N. This register keeps a record of the states that have been previously used in the verification.

4. The bank creates a counter variable s and initializes it to 0. This counter keeps a record of the number of verification attempts for the banknote. The bank also has a pre-defined maximum number of allowed verifications T. The banknote should be returned to the bank if $s \geqslant T$.

B. Banknote verification

Before the verification step, the protocol must be calibrated with respect to the total efficiency η and the base error rate β of the measurement setup. The details of this calibration are explained in Appendix A. The verification procedure is specified below.

1. The holder randomly chooses a subset of indices $L \subset [N]$ of size $l = |L|$ such that $r_k = 0$ for each $k \in L$. For each $k \in L$, the holder sets the corresponding bit of r to 1, indicating that these states will be measured.

2. For each $k \in L$, the holder picks a matching M^k at random from M_1, M_2, M_3 and applies the corresponding measurement to obtain outcome $b_k = x_i \oplus x_j$. If there is no outcome, we set $b_i = \emptyset$. The number of successful outcomes is defined as l'.

3. The bank sets the efficiency threshold to be $\eta - \epsilon$, where $\epsilon > 0$ is a small positive security parameter. If $l' < l_{\min} := (\eta - \epsilon)l$, the verifier aborts the protocol.

4. The holder sends all triplets $[k,(i,j),b_k]$ to the bank, who checks that $s < T$.

5. For each k, the bank checks whether the answer is correct by comparing $[k,(i,j),b_k]$ to the secret x^k values. The bank sets an error threshold to be $\beta + \delta$, where δ is a small positive constant. The bank accepts the banknote as valid only if fewer than $l'(\beta + \delta)$ of the answers are incorrect.

6. The bank updates s to $s + 1$.

The complete protocol is illustrated in Fig. 1. The security and correctness of this protocol was proven in Ref. [32], where it was shown that an honest verifier will fail to verify a valid banknote with probability

$$\Pr(\text{Ver fails}) \leqslant e^{-2l_{\min}\delta^2} + e^{-2l\epsilon^2}, \tag{2}$$

and the probability that an adversary can forge a banknote is bounded by

$$\Pr(\text{Forge}) \leqslant e^{-2\frac{\epsilon^2}{\eta^2}l} + e^{-2l\epsilon^2} + e^{-2l_{\min}\delta^2}. \tag{3}$$

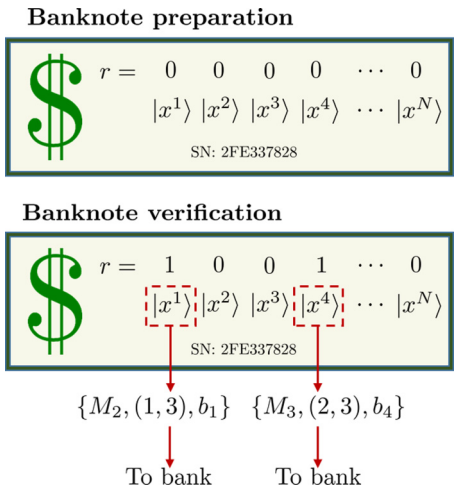

FIG. 1. Schematic illustration of the quantum money protocol. The bank produces N quantum states $|x^1\rangle, |x^2\rangle, \ldots, |x^N\rangle$ according to a random secret string $x = x^1x^2\cdots x^N$. The bank also assigns a unique serial number to the banknote and creates a register r that records whether each state has been used previously for verification. To verify the banknote, a holder randomly selects l quantum states. For each state, the holder randomly selects one of the three matchings M_1, M_2, M_3 and performs the corresponding measurement. The outcomes consist of a matching pair (i,j) and a parity bit b, which are recorded and sent for comparison with the bank's secret string x. The banknote is accepted as valid if the error rate observed by the bank is sufficiently low.

Both of these probabilities decrease exponentially in the protocol parameter l. The parameters ϵ and δ are chosen to minimize the value of l necessary to achieve a given security level. We use $e_{\min}$ to represent the minimum average error rate introduced by an adversary attempting to forge a banknote. Here, $e_{\min}$ comes from forging action totally. Even the adversary forges from a perfect coin and using a perfect measurement device, he cannot get an average error rate smaller than $e_{\min}$. A natural choice for δ is then $\delta = (e_{\min} - \beta)/2$, i.e., half of the gap between the average error rate for a genuine coin and a forged coin. This is a compromise between high security against forging (which increases with δ) and correctness of verification for honest users (which increases with small δ). Security can always be obtained as long as $\beta < e_{\min}$. For the protocol, it was proven in Ref. [32] that $e_{\min}$ is bounded by

$$e_{\min} \geqslant \left(\frac{\frac{1}{6} - \frac{3\epsilon}{2\eta}}{1 - \frac{3\epsilon}{\eta}}\right)\frac{4|\alpha|^2 e^{-4|\alpha|^2}}{1 - e^{-4|\alpha|^2}}. \tag{4}$$

The optimal choice of ϵ depends on the system parameters and is calculated numerically. In what follows, we outline the experimental procedure to implement the quantum money protocol.

III. EXPERIMENTAL IMPLEMENTATION

To prepare the banknotes, we employ a continuous-wave (CW) laser with a wavelength of 1550.12 nm and a linewidth of 50 kHz. The laser's amplitude is modulated to generate a block of four continuous pulses using an intensity modulator. Every block is 96-ns long while each individual pulse has a width of

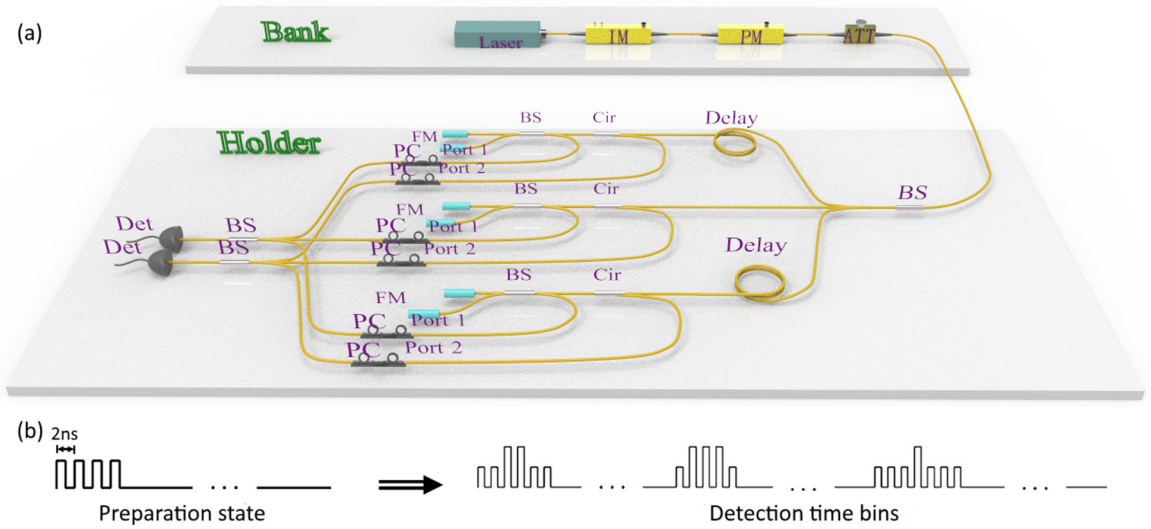

FIG. 2. (a) Experimental setup for generating and verifying quantum banknotes. A laser source produces sequences of coherent states which are modulated in phase according to a secret string x and attenuated to an amplitude of $|\alpha|^2 = 0.25$. The signals are passively split into three arms using a 1×3 beam-splitter and routed to three Mach-Zehnder interferometers. The interferometers, which, respectively, have delays of 2, 4, and 6 ns, are standard fiber Michelson interferometers. Each of them consists of a single beam-splitter and two Faraday mirrors. The delays are depicted in the figure in terms of the varying length of the lower arm of the interferometer connected to the mirror. Delays of lengths 5 and 10 m are placed to distinguish the outputs of each interferometer, which are recombined using a 1×3 beam-splitter and measured using superconducting nanowire single-photon detectors. IM: Intensity Modulator. PM: Phase Modulator. ATT: Attenuator. BS: beam-splitter (2×2 and 1×3). Cir: Circulator. FM: Faraday Mirror. PC: Polarization Controller. (b) The block structure scheme. The graph in the left side shows the initial state, consisting of a total of four pulses. The graph in the right side shows the detection time-bins in one cycle, which consist of three parts corresponding to a 4, a 2, and a 6 ns MZI, respectively. The delay of the three parts are mainly decided by the length of delay lines.

2 ns so that the blocks of four pulses occupy a total of 8 ns, see Fig. 2(b). This resulting low duty ratio is chosen to allow for time multiplexing while still allowing a large repetition rate of 10 MHz. The block's length is much shorter than laser's coherent time, so all the pulses in a block have the same global phase. The phase information, which depends on the bank's secret key x, is encoded on each pulse via a phase modulator to create the states as in Eq. (1). The secret key x is generated using a quantum random number generator and stored in a pulse pattern generator (PPG) with amplifiers. The key data are then used to modulate the phase of the pulses. Finally, an attenuator adjusts the average photon number to $|\alpha|^2 = 0.25$. Each block is now a quantum state of the banknote, which is transmitted to the holder.

For verification of the banknote, the holder randomly selects a subset of all pulses and measures them. In this proof-of-principle experiment, this is done by measuring all states and selecting a random subset of all outcomes. Verification requires the holder to choose randomly between three different measurements, each corresponding to a different matching. This is achieved using a 1×3 beam-splitter (BS) to passively select between three Mach-Zehnder interferometers with delays of 2, 4, and 6 ns. The interferometers employ Faraday mirrors and a single beam-splitter to combine all possible pairings in the matchings. Due to interference in the beam-splitter, the holder can retrieve information about the parity of the secret bits encoded in the phase of the pulses.

Since the pulses in each block are separated by 2 ns, the 2-ns interferometer performs interference of the pairs (1,2),(2,3),(3,4); the 4 ns interferes pairs (1,3),(2,4); and the last interferometer interferes the pairing (1,4). This covers all six pairs in the matchings, allowing the holder to perform the banknote verification. At the output of the beam-splitter, delays of lengths 0, 5, and 10 m are introduced to distinguish the outputs of the interferometers by their arrival time. Two 1×3 beam-splitters are used to recombine the output light of the interferometers. We use two superconducting nanowire single-photon detectors (SNSPDs) for detection. The SNSPDs have a desired polarization which corresponds to its maximum detection efficiency of 70%. At each output port of the interferometers, we use a polarization controller to adjust the polarization. Finally, the detection events are recorded by a time-digital converter (TDC) for analysis. The experimental setup is shown in Fig. 2(a). The timing jitter of SNSPD is about 50 ps. The TDC's timing jitter is 25 ps, the same as its bin time. It is sufficient to distinguish each pulse. The TDC's data were transmitted and stored in a computer and we processed data after all experiments rounds finished.

IV. EXPERIMENTAL RESULTS

As seen in Eqs. (2) and (3), the security levels of the protocol depend partly on two parameters: the overall efficiency η and the expected error rate β. The parameters α and ϵ are optimized to achieve the lowest number of measurement states l. The detailed method for optimization can be referred to Appendix B. Before verification, we perform calibration to determine the error rate of a genuine banknote in our setup, as well as the final system efficiency after balancing each measurement basis, allowing an optimal choice of protocol

TABLE I. Calibration data for the quantum money protocol. A total of 10^8 states are prepared and measured using our experimental setup, obtaining a total of 3,543,143 detection events, unevenly distributed among all matching pairs due to imperfections in the experiment. The third column shows the fraction of measurement outcomes that will be kept for each pairing. The last column shows the error rate of each matching pair.

Matching pair	Total counts	Percentage kept	Error rate
(1,2)	602,341	93%	0.0268
(1,3)	619,482	90%	0.0260
(1,4)	559,590	100%	0.0368
(2,3)	578,825	97%	0.0332
(2,4)	613,475	91%	0.0311
(3,4)	569,430	98%	0.0303

parameters. The calibration result is shown in Table I. We obtain $\eta = 3.36\%$ and $\beta = 0.033$, leads to an optimal value of $\epsilon = 0.002$, and the value of $e_{\min} = 0.055$. The details of the calibration step can be found in Appendix A. In Fig. 3, we estimate the experimental error rate for different block sizes. The shaded area corresponds to accepting the banknote in our protocol. The genuine banknote leads to an error rate near β, thus all the genuine banknotes pass the verification.

The security of the quantum money protocol is quantified by the forging probability, which we set to 10^{-7} for definiteness, although other values could be chosen depending on the security requirements. The forging probability of our protocol is shown in Fig. 4. At most $l = 2.16 \times 10^6$ states need to be measured in one verification round to ensure the desired security level, which decreases exponentially with l. This verification takes less than 210 ms in our experiment. We also compare it to the ideal case, where there is no base error. It is seen that to get the same security level, the number of verification states used are only roughly twice the value of the ideal case.

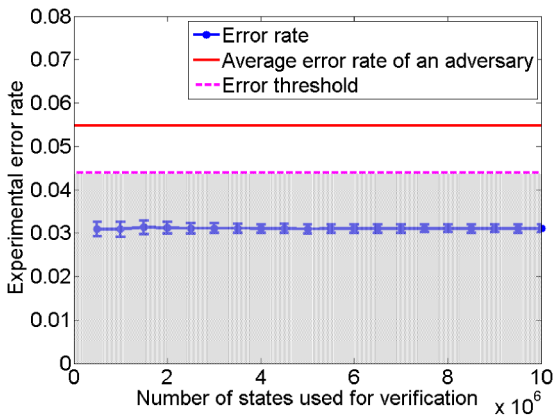

FIG. 3. Experimental error rate for different values of the number of states l used in the verification. The standard error is calculated from ten rounds of experiments. The red solid line shows $e_{\min}$, the minimum average error rate caused by an adversary, the magenta dashed line shows the acceptance threshold, and the shaded area corresponds to values of the error rate where the banknote is accepted. The genuine banknotes generated in the experiment can pass the verification, and coincide with the calibration results $\beta = 0.033$.

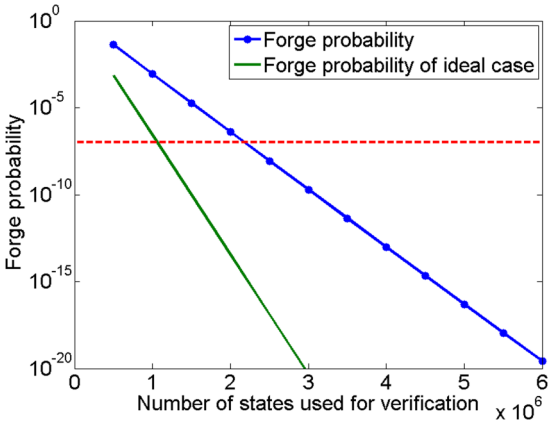

FIG. 4. Forging probability for different values of the number of states used in verification l. The blue line corresponds to our experimental parameters while the green line corresponds to the ideal case. The dashed line represents the 10^{-7} target security level.

V. DISCUSSION

We report an experimental implementation of the preparation and verification of unforgeable quantum banknotes. As a proof-of-principle demonstration, our results show that these ingredients of quantum money protocols are technologically viable. To reach full applicability of quantum money schemes, it is crucial to be able to store the quantum states constituting the banknote in quantum memories. This remains a daunting challenge, but progress has been made rapidly in developing memories capable of storing the quantum states of optical modes as required by this money protocol [36–38]. Additionally, the interferometers used for verification are suitable for an implementation using integrated optics, which would allow a convenient method for verifying quantum banknotes. Beyond their application to quantum money, our results demonstrate an implementation of QRGs, which have the potential to be used as building blocks in other cryptographic protocols. This is an area worth exploring further. For example, it is intriguing to note the similarity between hidden matching QRGs and round-robin differential phase-shift QKD [39], a connection that may lead to new insights into these protocols.

Note added. Recently we became aware of a relevant work [40]. Their work is based on the theoretical proposal of Ref. [30] using polarization qubits while we utilize high-dimensional time-bin qudits based on the protocol of Ref. [32].

ACKNOWLEDGMENTS

This work has been supported by the National Basic Research Program of China (under Grant No. 2013CB336800), the National Natural Science Foundation of China, the Chinese Academy of Science, and the 1000 Youth Fellowship program in China.

APPENDIX A: CALIBRATION OF THE QUANTUM MONEY PROTOCOL

The protocol requires calibration of the total efficiency η and the base error rate β of the measurement device. Security can be guaranteed as long as $\beta < e_{\min}$, but an optimal value of the parameter δ requires knowledge of the average error rate.

There is another requirement in the calibration and verification steps. The security proof requires that all three measurements are selected with equal probability. This, in turn, leads to an equal average number of outcomes for each of the six pairs (1,2),(1,3),(1,4),(2,3),(2,4),(3,4). In an ideal implementation, this condition is ensured because all pulses have equal amplitude when they interfere, leading to an equal probability of obtaining a click. However, due to imperfections, there will be a difference between the average number of outcomes obtained for each of the three interferometers. This is addressed in the protocol by introducing additional loss for the more frequently occurring pairings, so that the same average number of outcomes is obtained for all pairs.

In the calibration step, we prepared 10^8 blocks and measured them using the interferometers. We recorded a total of 3,543,143 detection events, leading to a detection efficiency of 3.54%. From the statistics, it is possible to determine the fraction of outcomes that should be kept for each pair. The result is shown in Table I in the main text, leading to a final efficiency of $\eta = 3.36\%$. The expected error rate β is calculated from the number of errors in these measurements, yielding a value of $\beta = 0.033$. In a verification round, the raw outcomes should be postprocessed according to the percentage kept in Table I in the main text, then sent to the bank for verification.

APPENDIX B: OPTIMIZATION OF PROTOCOL PARAMETERS

The parameters ϵ and α must be optimized in the protocol to achieve the lowest possible value of l, the number of states used in each verification. For now, we consider α to be fixed and we perform an optimization over ϵ. The optimization procedure can then be repeated for different values of α to arrive at optimal parameters. First, we rewrite the expression of Pr(Forge) as follows:

$$\Pr(\text{Forge}) \leqslant \exp[-2T_1 l] + \exp[-2T_2 l] + \exp[-2T_3 l], \tag{B1}$$

$$T_1 = \frac{\epsilon^2}{\eta^2}, \tag{B2}$$

$$T_2 = \epsilon^2, \tag{B3}$$

$$T_3 = (\eta - \epsilon)\delta^2. \tag{B4}$$

Note that Pr(Forge) depends implicitly on α through the parameter δ. Because l is very large, Pr(Forge) is dominated by the value of $\min\{T_1, T_2, T_3\}$, with the other terms being exponentially smaller in comparison. In our setup, it holds that $T_1 \gg T_2$ so we have $\exp[-2T_1 l] \ll \exp[-2T_2 l]$ and the first term in Eq. (B1) can be omitted. We recall that

$$e_{\min} \geqslant \left(\frac{\frac{1}{6} - \frac{3\epsilon}{2\eta}}{1 - \frac{3\epsilon}{\eta}}\right) \frac{4|\alpha|^2 e^{-4|\alpha|^2}}{1 - e^{-4|\alpha|^2}}. \tag{B5}$$

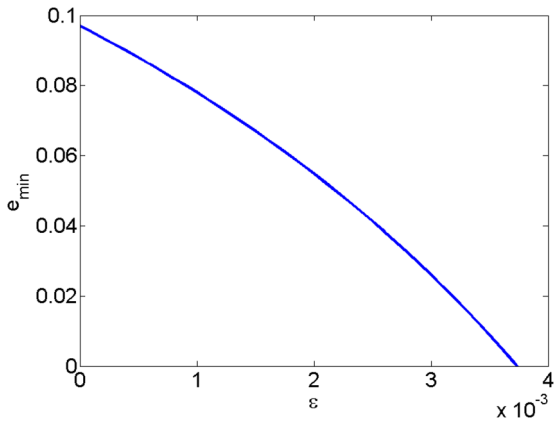

FIG. 5. The relationship between $e_{\min}$ and ϵ.

The parameter $e_{\min}$ is a decreasing function of ϵ (see Fig. 5). Thus, T_3 will decrease with ϵ while T_2 increases. The goal of the optimization is then to find $\max_\epsilon \min\{T_2, T_3\}$. For a given α, based on the calibration result for η and β, we can numerically compute the optimal value of ϵ as illustrated in Fig. 6.

To find an optimal value of α, we try several different values and find a best one. The optimal value of $|\alpha|^2$ should be 0.32. However, our detectors have a maximum counting rate of 450 k events every second. When input photons exceed this value, the detector will shutdown. Even when input photons are slightly lower than this value, there is still some chance for the detector shutdowns after working a while. We turn down the $|\alpha|^2$ to 0.25, seeing the detectors work stablly during the entire experiment. In that case, the optimal ϵ is 0.002, and we require $l = 2.02 \times 10^6$ states in one verification round to achieve a forging probability of 9.6×10^{-8}. Here, enlarging the block time can also reduce the average light intensity, but the amplitude modulator will not work as well and therefore create more errors.

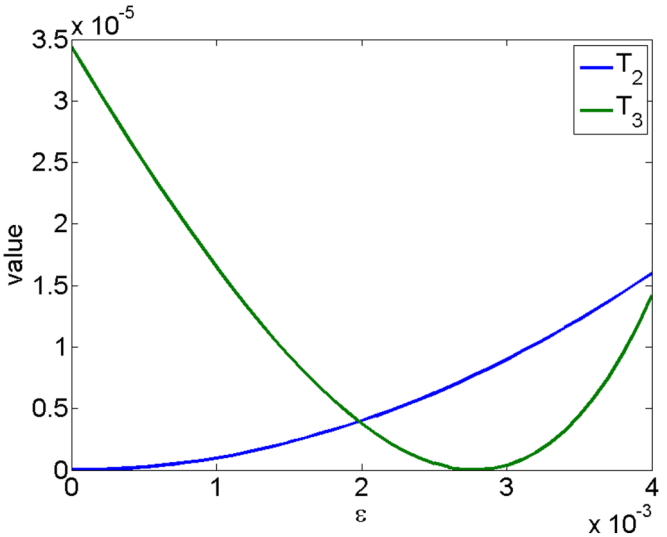

FIG. 6. Optimization curves for computing $\max_\epsilon \min T_2, T_3$.

[1] C. H. Bennett and G. Brassard, Theor. Comput. Sci. **560**, 7 (2014).

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[3] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, Quantum Information **2**, 16025 (2016).

[4] R. Amiri, P. Wallden, A. Kent, and E. Andersson, Phys. Rev. A **93**, 032325 (2016).

[5] J. M. Arrazola, P. Wallden, and E. Andersson, Quantum Inf. Comput. **16**, 0435 (2016).

[6] R. Amiri and E. Andersson, Entropy **17**, 5635 (2015).

[7] R. J. Collins, R. Amiri, M. Fujiwara, T. Honjo, K. Shimizu, K. Tamaki, M. Takeoka, M. Sasaki, E. Andersson, and G. S. Buller, Sci. Rep. **7**, 3235 (2017).

[8] R. J. Collins, R. Amiri, M. Fujiwara, T. Honjo, K. Shimizu, K. Tamaki, M. Takeoka, E. Andersson, G. S. Buller, and M. Sasaki, Opt. Lett. **41**, 4883 (2016).

[9] H.-L. Yin *et al.*, Phys. Rev. A **95**, 042338 (2017).

[10] J. M. Arrazola and N. Lütkenhaus, Phys. Rev. A **89**, 062305 (2014).

[11] F. Xu, J. M. Arrazola, K. Wei, W. Wang, P. Palacios-Avila, C. Feng, S. Sajeed, N. Lütkenhaus, and H.-K. Lo, Nat. Commun. **6**, 8735 (2015).

[12] J.-Y. Guan, F. Xu, H.-L. Yin, Y. Li, W.-J. Zhang, S.-J. Chen, X.-Y. Yang, L. Li, L.-X. You, T.-Y. Chen, Z. Wang, Q. Zhang, and J.-W. Pan, Phys. Rev. Lett. **116**, 240502 (2016).

[13] A. Broadbent, J. Fitzsimons, and E. Kashefi, in *FOCS'09. 50th Annual IEEE Symposium on Foundations of Computer Science, 2009,* (IEEE, New York, 2009), pp. 517–526.

[14] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, Science **335**, 303 (2012).

[15] S. Barz, J. F. Fitzsimons, E. Kashefi, and P. Walther, Nat. Phys. **9**, 727 (2013).

[16] C. Greganti, M.-C. Roehsner, S. Barz, T. Morimae, and P. Walther, New J. Phys. **18**, 013020 (2016).

[17] B. Sanguinetti, G. Traverso, J. Lavoie, A. Martin, and H. Zbinden, Phys. Rev. A **93**, 012336 (2016).

[18] B. A. Bash, A. H. Gheorghe, M. Patel, J. L. Habif, D. Goeckel, D. Towsley, and S. Guha, Nat. Commun. **6**, 8626 (2015).

[19] J. M. Arrazola and V. Scarani, Phys. Rev. Lett. **117**, 250503 (2016).

[20] K. Bradler, T. Kalajdzievski, G. Siopsis, and C. Weedbrook, arXiv:1607.05916.

[21] N. H. Y. Ng, S. K. Joshi, C. C. Ming, C. Kurtsiefer, and S. Wehner, Nat. Commun. **3**, 1326 (2012).

[22] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner, and H. Zbinden, Phys. Rev. Lett. **111**, 180504 (2013).

[23] Y. Liu *et al.*, Phys. Rev. Lett. **112**, 010504 (2014).

[24] E. Verbanis, A. Martin, R. Houlmann, G. Boso, F. Bussières, and H. Zbinden, Phys. Rev. Lett. **117**, 140506 (2016).

[25] S. Wiesner, ACM Sigact News **15**, 78 (1983).

[26] S. Aaronson, in *Computational Complexity, 2009. CCC'09. 24th Annual IEEE Conference on* (IEEE, New York, 2009), pp. 229–242.

[27] A. Lutomirski, arXiv:1010.0256.

[28] A. Brodutch, D. Nagaj, O. Sattath, and D. Unruh, Quantum Inf. Comput. **16**, 1048 (2016).

[29] D. Gavinsky, in *Computational Complexity (CCC), 2012 IEEE 27th Annual Conference* (IEEE, New York, 2012), pp. 42–52.

[30] F. Pastawski, N. Y. Yao, L. Jiang, M. D. Lukin, and J. I. Cirac, Proc. Natl. Acad. Sci. USA **109**, 16079 (2012).

[31] M. Georgiou and I. Kerenidis, in *LIPIcs-Leibniz International Proceedings in Informatics*, Vol. 44, (Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, Wadern, Gemany, 2015).

[32] R. Amiri and J. M. Arrazola, Phys. Rev. A **95**, 062334 (2017).

[33] K. Bartkiewicz, A. Černoch, G. Chimczak, K. Lemr, A. Miranowicz, and F. Nori, Quantum Information **3**, 7 (2017).

[34] S.-J. Yang, X.-J. Wang, X.-H. Bao, and J.-W. Pan, Nat. Photon. **10**, 381 (2016).

[35] J. M. Arrazola, M. Karasamanis, and N. Lütkenhaus, Phys. Rev. A **93**, 062311 (2016).

[36] N. Sinclair *et al.*, Phys. Rev. Lett. **113**, 053603 (2014).

[37] M. Gündoğan, P. M. Ledingham, K. Kutluer, M. Mazzera, and H. de Riedmatten, Phys. Rev. Lett. **114**, 230501 (2015).

[38] A. I. Lvovsky, B. C. Sanders, and W. Tittel, Nat. Photonics **3**, 706 (2009).

[39] T. Sasaki, Y. Yamamoto, and M. Koashi, Nature **509**, 475 (2014).

[40] M. Bozzio, A. Orieux, L. T. Vidarte, I. Zaquine, I. Kerenidis, and E. Diamanti, Quantum Information **4**, 5 (2018).