Experimental quantum money

Jian-Yu Guan,[1, 2] Juan Miguel Arrazola,[3] Ryan Amiri,[4] Qiang Zhang,[1, 2, 5] Norbert Lütkenhaus,[6] and Jian-Wei Pan[1, 2]

[1]*Department of Modern Physics and National Laboratory for Physical Sciences at Microscale,*
Shanghai Branch, University of Science and Technology of China, Hefei, Anhui 230026, 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]*Jinan Institute of Quantum Technology, Jinan, Shandong, 250101, China*
[6]*Institute for Quantum Computing and Department of Physics and Astronomy,*
University of Waterloo, 200 University Avenue West, Waterloo, Ontario, N2L 3G1, Canada

We present the first experimental implementation of a quantum money scheme. We demonstrate the entire life-cycle of the states contained in a quantum coin – preparation, transmission, and verification. We are able to achieve this by implementing the practical protocol described in Ref. [2]. The scheme has three main features which, compared to previous schemes c.f. [3–5], make it particularly suited to practical use.

1. The quantum states embedded into the coins can be implemented by sequences of coherent states.
2. The scheme is able to tolerate much higher system losses than previous protocols by allowing verifiers to post-select on successful measurement outcomes.
3. The scheme can tolerate 16.7% of errors, which is higher than all previous protocols, which could tolerate an error rate of at most 14.6%.

Quantum money schemes contain a trusted party, the bank, and an unlimited number of potential recipients. The trusted party creates coins, which they can distribute to the recipients. The schemes we consider must satisfy the following main requirements:

- Verification – all coin holders should be able to verify that the coin they hold is genuine i.e. it will be accepted by the bank. The verification consists of a local measurement by the holder followed by classical communication with the bank. The coins should be verifiable a finite number of times before needing to be refreshed.
- Unforgeability – coins should be unforgeable with information-theoretic security. This means that any quantum adversary in possession of n genuine coins cannot create $n+1$ coins, such that all coins will pass the verification test performed by an honest party.

A quantum coin is a collection of quantum states together with a classical register tracking whether each state in the coin has been measured or not. Each state contained in the coin is chosen uniformly at random by the bank from the set $\{|\psi_x\rangle\}$, where each $|\psi_x\rangle$ is a sequence of coherent states

$$|(-1)^{x_1}\alpha\rangle\,|(-1)^{x_2}\alpha\rangle\cdots|(-1)^{x_n}\alpha\rangle \tag{1}$$

that depend on the n-bit string x and the amplitude α [2]. The bank's secret key is the classical record of the x-strings specifying the states contained in the coin.

Upon receiving a coin, the holder verifies the coin's authenticity by choosing a random selection of the unused states within the coin and performing a randomly chosen measurement. These possible measurements are specified by a perfect matching on the set $[n] = 1, 2, \ldots, n$ and the outcomes reveal the parity $x_i \oplus x_j$, where (i, j) is an edge of the matching. Once the measurement has been performed, the state contains no further information on x and should not be used in future verifications. The measurement that was made and its outcome are sent to the bank which checks each outcome against their secret key. If more than a threshold number of outcomes are correct, the bank declares the coin as valid, otherwise, it is declared invalid.

Quantum money schemes such as this are widely applicable to a host of practical scenarios. The most prominent application is, of course, the creation of unforgeable quantum money, but the coins could also be used in any application involving restriction of access, such as secure ticketing systems.

A. Experimental implementation

The coin verification procedure contains two distinct challenges: coin preparation and measurement. In this experiment, we focus on the case $n = 4$, which sets an error tolerance of 16.7%. The coin states are generated using a laser source to create a block of coherent state pulses of the form

$$|\alpha, x\rangle = |(-1)^{x_1}\alpha\rangle\,|(-1)^{x_2}\alpha\rangle\,|(-1)^{x_3}\alpha\rangle\,|(-1)^{x_4}\alpha\rangle\,, \tag{2}$$

where α is optimised to $\alpha = 0.45$. The states are transmitted to the designated holder, who will use all

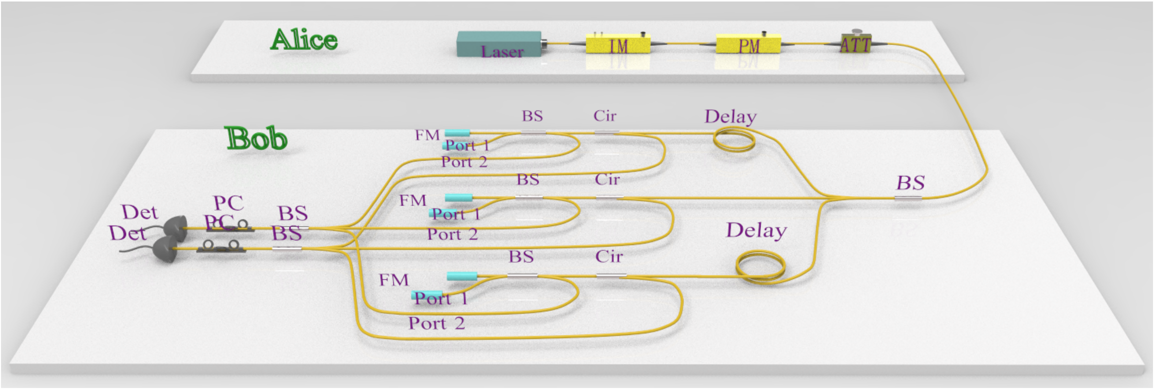

FIG. 1: Experimental setup for generating, transmitting, and verifying quantum coins. A laser source produces sequences of coherent states, which are modulated in phase according to a secret string x and attenuated to an amplitude of $\alpha = 0.44$. The signals are passively split into three arms using a 1×3 beam-splitter, with delays introduced in two of them to allow us to distinguish the outputs of each interferometer using only two detectors. The Mach-Zehnder interferometers – which respectively have delays of 2ns, 4ns, and 6ns – are implemented using a single beam-splitter and Faraday mirrors. The delays are depicted in the figure in terms of the varying length of the lower arm. The output ports of the interferometers are finally recombined using 1×3 beam-splitter and measured using single-photon detectors. IM: Intensity Modulator. PM: Phase Modulator. ATT: Attenuator. BS: Beam Splitter (2X2 and 1X3). Cir: Circulator. FM: Faraday Mirror. PC: Polariser Controller.

states received to perform the verification process.

The aim of the verifier's measurement is to determine the value of the parity $x_i \oplus x_j$, where the possible (i, j) pairs are specified by the measurement choice. For $n = 4$, the possible measurements are described by the matchings

$$\begin{aligned} M_1 &= \{(1,2),(3,4)\} \\ M_2 &= \{(1,3),(2,4)\} \\ M_3 &= \{(1,4),(2,3)\}. \end{aligned} \tag{3}$$

To implement the measurements, we employ three Mach-Zehnder interferometers of different delays, which interfere pairs of pulses according to a fixed separation. In the experiment, subsequent pulses are separated in time by 2 nanoseconds, and the interferometers have delays of 2, 4, and 6 nanoseconds respectively. The choice of interferometer is performed passively by a 1×3 beam-splitter and a fixed delay is introduced in each arm in order to later distinguish the outputs of each interferometer using just two detectors. The Mach-Zehnder interferometers are implemented using a single 50:50 beam-splitter and Faraday mirrors. Through the use of circulators, the outputs of the interferometers are recombined in two different ports using 1×3 beam-splitters where the signals are then measured using superconducting single-photon detectors. The experimental setup is illustrated in Fig. 1.

In order to have security in the scheme, one must be careful to ensure that all possible pairings (i, j) are equally likely to occur as a measurement outcome. As shown in Ref. [2], this can be enforced simply by introducing a post-processing stage that randomly discards a proportion of successful measurement outcomes so that all are equally likely. The discarded outcomes can be considered artificial loss and included within the overall system loss. In our scheme, the 2ns interferometer interferes pairs $(1, 2), (2, 3), (3, 4)$, the 4ns one interferes $(1, 3), (2, 4)$ and the 6ns one interferes $(1, 4)$, which are all the pairs we need for verification.

The protocol analysis performed in Ref. [2] shows that even large system losses can be tolerated. Indeed, the coin is accepted or rejected based only on the error rate seen in successful measurement outcomes. With system loss removed as a limiting factor, the implementation is significantly simpler and can be performed using only passive linear optics and post-processing, as we have done in this experiment.

We performed preliminary testing on three interferometers with delays of 2ns, 4ns and 6ns, and achieved visibilities of 93%, 95% and 97%, respectively. The resulting error rates are all well below the 16.7% threshold which is required for security, showing that our setup is apt for verifying the quantum coins. The overall system loss, including limited detector efficiency, is approximately 12 dB. Given these experimental parameters, approximately $60,000$ successful measurement outcomes are necessary to verify a coins authenticity to a security level of 10^{-6}. This requires approximately $960,000$ states to be transmitted, which in our setup running at 10 MHz, i.e. we send four pulses every 100 nanoseconds, can be done in ~ 0.1 seconds.

B. Significance of our results

We have presented the first experimental demonstration of a quantum money scheme, involving state preparation and verification. For applications where coins are created, transmitted, and immediately verified, our results indicate that quantum money can indeed be a practical technology. More generally, our experiment also shows the viability of using laser sources and passive linear optics to perform complex protocols that go beyond simple operations on qubits.

We believe that our results will be of great interest to the quantum cryptography community: quantum money was the first protocol ever conceived in the field and we are now reaching the point where it has become a topic of experimental relevance. Moreover, with quantum key distribution having reached the point of great maturity, a large interest has grown in exploring new quantum cryptographic protocols that are experimentally relevant. Our work indicates that quantum money is one of such protocols, which we hope will be an exciting result for everyone working in this field.

A full manuscript reporting our results is currently in preparation.

[1] Wiesner, Stephen. “Conjugate coding.” ACM Sigact News 15.1 (1983): 78-88.

[2] Amiri, Ryan, and Juan Miguel Arrazola. “Quantum money with nearly optimal error tolerance.” arXiv preprint arXiv:1610.06345 (2016).

[3] Gavinsky, Dmitry. “Quantum money with classical verification.” Computational Complexity (CCC), 2012 IEEE 27th Annual Conference on. IEEE, 2012.

[4] Pastawski, Fernando, Norman Y. Yao, Liang Jiang, Mikhail D. Lukin, and J. Ignacio Cirac. “Unforgeable noise-tolerant quantum tokens.” Proceedings of the National Academy of Sciences 109, no. 40 (2012): 16079-16082.

[5] Georgiou, Marios, and Iordanis Kerenidis. “New constructions for quantum money.” LIPIcs-Leibniz International Proceedings in Informatics. Vol. 44. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2015.