Experimental demonstration of practical unforgeable quantum money

Mathieu Bozzio,[1,2] Adeline Orieux,[1,3] Luis Trigo Vidarte,[1,4]
Isabelle Zaquine,[2] Iordanis Kerenidis,[3,5] and Eleni Diamanti[1]

[1]*LIP6, CNRS, Université Pierre et Marie Curie, Sorbonne Universités, 75005 Paris, France*
[2]*LTCI, Télécom ParisTech, Université Paris-Saclay, 75013 Paris, France*
[3]*IRIF, Université Paris Diderot, Sorbonne Paris Cité, 75013 Paris, France*
[4]*LCF, Institut d'Optique Graduate School, CNRS, Université Paris-Saclay, 91127 Palaiseau, France*
[5]*Center for Quantum Technologies, National University of Singapore, Singapore*

Wiesner's unforgeable quantum money scheme is widely celebrated as the first quantum information application. Nevertheless, despite its central role in quantum cryptography, its experimental implementation has remained elusive because of the lack of realistic protocols adapted to practical quantum storage devices and verification techniques. Here, we experimentally demonstrate a quantum money protocol that rigorously satisfies the security condition for unforgeability, using a practical system exploiting single-photon polarization encoding of highly attenuated coherent states of light for on-the-fly credit card state generation and readout. Our implementation includes classical verification and is designed to be compatible with state-of-the-art quantum memories, which have been taken into account in the security analysis, together with all system imperfections. Our results constitute a major step towards a real-world realization of this milestone quantum information protocol.

Introduction. The principle behind quantum money is to ensure unforgeability of tokens, banknotes or credit cards by encoding them with qubit states prepared in one of two possible conjugate bases [1]. The no-cloning theorem then ensures that a malicious party willing to duplicate the money cannot copy the unknown qubit state perfectly. Several schemes for unforgeable quantum credit cards have been proposed, usually involving verification procedures that require quantum communication with an honest bank as in Wiesner's original work [1]. A scheme involving classical communication during the verification process has also been proposed [2], making use of hidden-matching quantum retrieval games [3, 4], as well as a more practical scheme making use of simple BB84-type states [5]. Recently, quantum banknotes have been implemented "on-the-fly" but also shown to be forgeable [6]. Unforgeable quantum credit cards, on the other hand, have not been implemented to date.

Protocol. The quantum money protocol that we have analyzed and implemented is based on [5, 7] and has a number of desirable features, including single-round classical verification, credit card re-usability, and information-theoretic security with exponentially good parameters. In our protocol, the bank stores an amount of money into a credit card using a unique secret string and gives the card to the client. When a transaction is to be made, the following interactions occur: first, the client gives the credit card to a vendor, who chooses at random one out of two challenge questions and accesses the credit card (*i.e.*, performs a measurement on the stored qubits) in order to get an answer to the challenge; second, the vendor sends to the bank the challenge and the answer and the bank, using its initial secret string, verifies the authenticity of the credit card and responds with a yes or no. If the bank's answer is yes then the transaction may occur, otherwise the card is rejected and declared as a counterfeit.

The basic unit of the credit card state consists of a qubit pair, chosen by a secret classical string s from the set $S_{\text{pair}} = \{|0+\rangle, |0-\rangle, |1+\rangle, |1-\rangle, |+0\rangle, |+1\rangle, |-0\rangle, |-1\rangle\}$, where $|0\rangle$, $|1\rangle$ and $|+\rangle$, $|-\rangle$ are the Pauli σ_z and σ_x basis eigenstates, respectively. The string s consists of three bits, indicating the basis of the first qubit in the pair and the selected states of the two qubits.

During the verification procedure, the vendor chooses one of the two challenges, Q_{zz} or Q_{xx}, which for a single qubit pair read, respectively : *"Provide two outcomes for the measurement of each qubit in the pair in the σ_z (resp. σ_x) basis, such that the outcome corresponding to the qubit prepared in the σ_z (resp. σ_x) basis is correct"*. Then, he performs a measurement on the credit card, namely he measures each qubit in the pair in the σ_z (resp. σ_x) basis and sends the outcomes to the bank, which uses the secret information s to verify if the credit card is valid or not. In principle a valid credit card can always be verified. We denote by c the probability of successfully answering Q_{zz} or Q_{xx} (correctness parameter), which in the ideal case is 1 for the above challenges (measuring both qubits in the

σ_z basis always answers correctly the challenge Q_{zz} and similarly for Q_{xx}). In a realistic implementation c might not be equal to 1 due to the system imperfections.

Let us now see what happens when a malicious client tries to duplicate the credit card. Since the quantum state is unknown, there is no way that the two copies of the credit card can pass both challenges with high probability. More precisely, let us define the challenge Q_ϵ as the conjunction of challenges Q_{zz} and Q_{xx}. We denote by ϵ the probability of successfully answering the conjunction challenge Q_ϵ, *i.e.*, the probability of successfully cheating (security parameter). For the above challenges, one can prove that $\epsilon \leq 3/4$ [2, 5, 7].

For a (c,ϵ)-game G as the one above, and given that the parameters c and ϵ satisfy some inequality, one can easily extend the game to another one that uses n qubit pairs and new challenges, so that for the new game the parameter c' is exponentially close to 1, and the parameter ϵ' is exponentially close to zero. For this, we need that the parameter c exceeds a specific ϵ-dependent theoretical bound, which for the above case is $B(\epsilon) = 7/8$ for ideal qubits. As regards to weak coherent states, which we also use as qubits in our proof-of-principle experiment, a new security threshold $B(\epsilon, \mu)$, dependent on the average photon number per pulse μ, must be derived in order to counter photon-splitting attacks. These two bounds may be tested experimentally, and correspond in practice to two types of quantum storage devices: a single-emitter-type quantum memory will always yield a one photon output, and in that case $c > B(\epsilon)$ is sufficient to demonstrate unforgeability. For other quantum memories consisting of cold atom clouds, the output state remains a coherent state and the more stringent $c > B(\epsilon, \mu)$ condition must be fulfilled to achieve information-theoretic security.

Experimental Principle. In order to test in practice the security conditions that pertain to a single game G, it is necessary to generate blocks of photon pairs randomly chosen from the set S_{pair} and estimate the probability of successfully answering the challenge questions Q_{zz} or Q_{xx}, namely estimate the parameter c. Note that in the protocol description we have assumed that the probabilities corresponding to the two challenges, c_{zz} and c_{xx}, are the same and equal to c. However, in reality this may not be the case. In our experiment, we estimate these parameters separately, measuring a block in the $\sigma_z \otimes \sigma_z$ basis and another in the $\sigma_x \otimes \sigma_x$ basis, to estimate c_{zz} and c_{xx}, respectively. The correctness parameter is then calculated as $c = (c_{zz} + c_{xx})/2$. This does not compromise the security of the implementation as it is always possible to symmetrize the data by relabeling the bases such that in practice the two parameters become effectively the same. The experimental setup is displayed in Fig. 1.

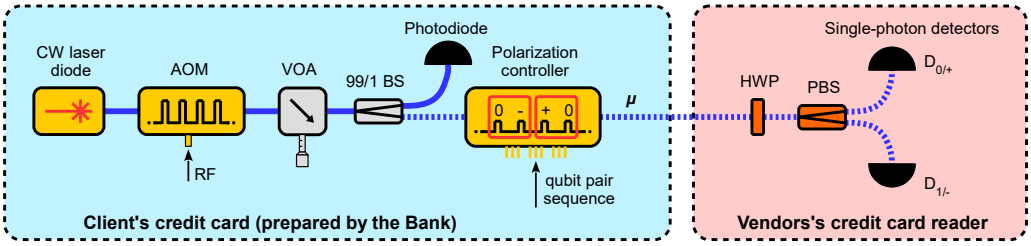

Figure 1. **Experimental setup of the quantum money scheme.** The credit card state preparation is performed using pulses carved from light emitted by a telecommunication wavelength laser diode using an acousto-optic modulator (AOM). A multi-stage polarization controller (EOSPACE) is then used to select the polarization states according to the protocol by applying suitable voltages. The average photon number of pulse μ is set by a variable optical attenuator (VOA) and is calibrated with a 99/1 beam splitter (BS) and a photodiode. The credit card reader is materialized by a standard polarization analysis setup including a half-wave plate (HWP), a polarization beam splitter (PBS) and two InGaAs single-photon avalanche photodiodes (IDQ201). The entire setup is synchronized using a multi-channel delay generator and is controlled by software incorporating the random state generation and data acquisition and processing.

Results. Regarding the ideal qubit case, where the security threshold is constant at $B(\epsilon) = 7/8$, our measured c parameter with $\mu = 1$ reaches $c = 0.9726\ (\pm 0.0002) >> B(\epsilon)$, which ensures unforgeability for over an hour of continuous system operation. Regarding the weak coherent state case, the security threshold increases to practically 1 as μ increases above 0.5 and this is because a malicious client can use pulses with more than one photon to perfectly cheat with photon-splitting attacks. Our results are presented as a function of μ in Fig. 2.

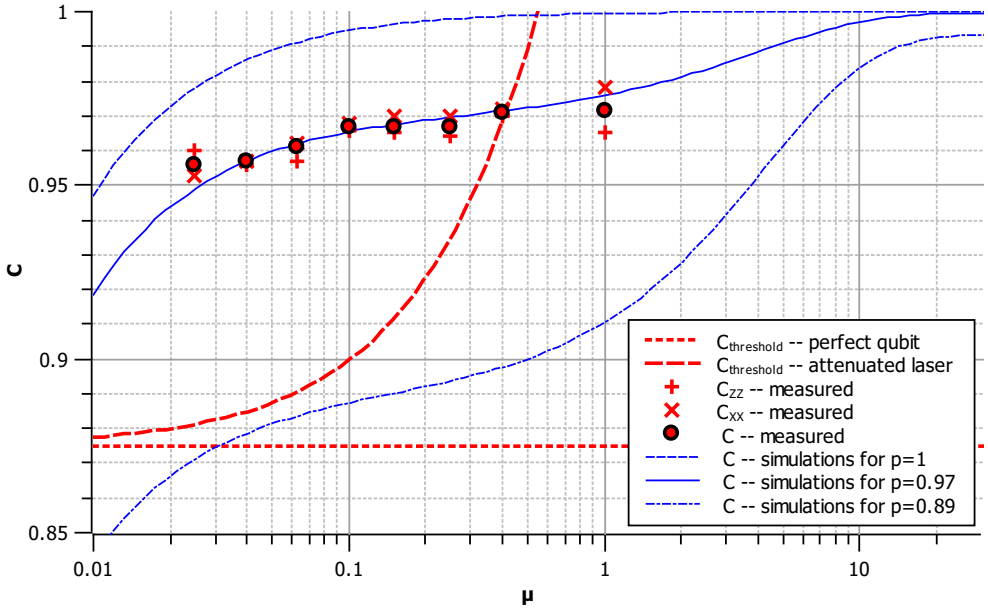

Figure 2. **Experimental quantum money results.** Measured c values are plotted as a function of the average photon number per pulse μ. The red dotted line corresponds to the security threshold $B(\epsilon)$ while the red dashed line corresponds to the security threshold for weak coherent states $B(\epsilon, \mu)$. The blue curves correspond to theoretical simulations assuling a dark count probability of 7×10^{-5}, detection efficiency of 25%, state purity values of $p = 0.89, 0.97, 1$ and post-selection of pulses with one and only one detector clicking. We also show the experimental result obtained for the ideal qubit case.

Our results allow us to determine the optimal μ that satisfies the security condition of our protocol. The highest value for c, obtained for $\mu = 0.40$, lies on the threshold curve, and therefore compromises the scheme's security. All values of μ included in the range 0.02 through to 0.25, on the other hand, lie above the required threshold, ensuring credit card unforgeability. To optimize the performance of the setup, it is in general preferable to keep μ as high as possible in order to maximize the number of useful detected pulses; hence, we can conclude that our proof-of-principle experiment works optimally for $\mu \in [0.25, 0.40]$.

Fig. 2 also shows simulations of the evolution of c with μ according to a theoretical model that takes into account Poisson photon statistics, dark count probability, detection efficiency, state purity and post-selection of pulses where one and only one detector clicks. The best fit of our data points corresponds to a state purity of 97%. The simulation allows us to determine the critical purity under which the protocol cannot be secure regardless of the μ parameter. This critical value is 89%, as the corresponding curve in Fig. 2 does not have any intersection with the security threshold curve.

Our quantum money experiment is based on a practical setup and anticipates the use of quantum memories for real-world realization of quantum credit cards. It therefore provides an important benchmark for unforgeability of quantum money.

[1] S. Wiesner, ACM Sigact News **15**, 78 (1983).
[2] D. Gavinski, in *Proc. IEEE 27th Annual Conference on Computational Complexity (CCC)* (2012), pp. 42–52.
[3] Z. Bar-Yossef, T. S. Jayram, and I. Kerenidis, in *Proc. 36th Annual ACM Symposium on Theory of Computing (STOC)* (2004), pp. 128–137.
[4] J. M. Arrazola, M. Karasamanis, and N. Lütkenhaus, Phys. Rev. A **93**, 062311 (2016).
[5] F. Pastawski, N. Y. Yao, L. Jiang, M. D. Lukin, and J. I. Cirac, PNAS **109**, 16079 (2012).
[6] K. Bartkiewicz, A. Cernoch, G. Chimczak, K. Lemr, A. Miranowicz, and F. Nori, npj Quantum Information **3**, 7 (2017).
[7] M. Georgiou and I. Kerenidis, in *Proc. 10th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC)* (2015), vol. 44, pp. 92–110.