Implementation 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], Eleni Diamanti[1]

[1] LIP6, CNRS, Sorbonne Université, 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. The principle 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. Despite quantum money's 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.

Schemes involving classical communication during the verification process have already been proposed in [2] and [3]. Recently, quantum banknotes have been implemented "on-the-fly" but also shown to be forgeable [4]. Unforgeable quantum credit cards, on the other hand, have not been implemented to date, and no protocol has ever been fully demonstrated taking into account the effect of a quantum memory.

Our protocol is based on [3] and [5], and has a number of desirable features, including single-round classical verification, credit card re-usability, and information-theoretic security with exponentially good parameters. Ideally, 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.

In order to test in practice the security conditions that pertain to our protocol, it is necessary to generate blocks of photon pairs randomly chosen 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, and estimate the probability c of successfully answering some challenge questions. We do so by chopping a continuous 1564nm laser into pulses with an acousto-optic modulator, encoding the polarization information with a polarization controller, and measuring a block of pairs either in the $\sigma_z \otimes \sigma_z$ or $\sigma_x \otimes \sigma_x$ basis with a 50/50 beamsplitter, a half-wave plate, and two Id201 single photon avalanche detectors.

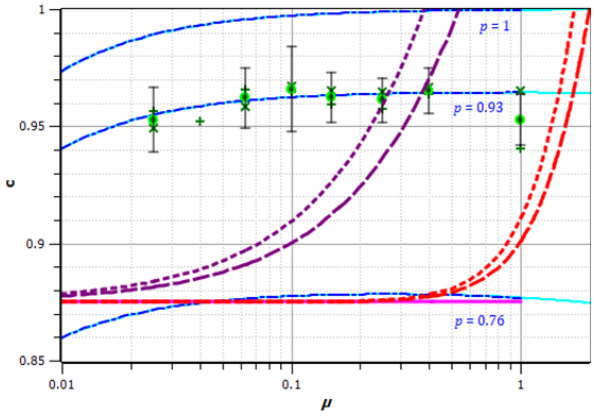

Figure 1: Average measured c values (green symbols) are plotted as a function of average photon number per pulse μ. Red lines correspond to a weak security threshold including only one type of attack (unambiguous state discrimination), while purple lines correspond to the general security threshold. The pink line displays the security threshold assuming perfect single photon states. Blue lines result from simulations for dark count probability $7 \times 10^{-}5$, detection efficiency 25%, and various values of state purity p.

Our results, described in detail in [6], allow us to determine the range of average photon number per pulse μ that satisfy the practical security condition of our on-the-fly protocol, anticipating the use of either a single-emitter type quantum memory or an atomic ensemble type quantum memory (see Figure 1). Our data points satisfy the strictest and most general theoretical security threshold provided that $\mu = 0.025$ to 0.200. We are now currently running the protocol and testing such conditions including a highly-efficient cold cesium cloud quantum memory [7] in our setup.

[1] S. Wiesner, ACM Sigact News15, 78 (1983).

[2] D. Gavinski, inProc. IEEE 27th Annual Conference on Computational Complexity (CCC)(2012), pp. 4252.

[3] F. Pastawski et al., PNAS109, 16079 (2012).

[4] K. Bartkiewicz et al., npj Quantum Information3, 7 (2017).

[5] M. Georgiou and I. Kerenidis (2015), vol. 44, pp. 92110.

[6] M. Bozzio et al., preprint at arXiv:1705.01428.

[7] P. Vernaz-Gris et al., preprint at arXiv:1707.09372.