Experimental investigation of practical unforgeable quantum money

Mathieu Bozzio1,2, Adeline Orieux1,3, Luis Trigo Vidarte1,4, Isabelle Zaquine2, Iordanis Kerenidis3,5 and Eleni Diamanti6

Wiesner’s unforgeable quantum money scheme is widely celebrated as the first quantum information application. Based on the no-cloning property of quantum mechanics, this scheme allows for the creation of credit cards used in authenticated transactions offering security guarantees impossible to achieve by classical means. However, despite its central role in quantum cryptography, its experimental implementation has remained elusive because of the lack of quantum memories and of practical verification techniques. Here, we experimentally implement a quantum money protocol relying on classical verification that rigorously satisfies the security condition for unforgeability. Our system exploits polarization encoding of weak coherent states of light and operates under conditions that ensure compatibility with state-of-the-art quantum memories. We derive working regimes for our system using a security analysis taking into account all practical imperfections. Our results constitute a major step towards a real-world realization of this milestone protocol.

npj Quantum Information (2018) 4:5 ; doi:10.1038/s41534-018-0058-2

INTRODUCTION

The fundamental property of quantum mechanics at the heart of quantum cryptography is the no-cloning theorem,1 which states that it is physically impossible to clone an unknown quantum system, that is, to generate two identical copies of the system starting from a single copy. This property in essence prevents a malicious party from recovering information about the system without disturbing it, something that is always possible in the classical world. In his seminal work,2 Wiesner used this property to show that by encoding classical information into conjugate quantum bases it is possible to protect the encoded information from forgery. For instance, classical bits can be encoded using the bases \{0, 1\} and \{+, -\}, with \(|±\rangle = (|0\rangle ± |1\rangle)/\sqrt{2}\), where the first qubit state in each basis encodes the bit 0 and the second the bit 1. Then, Heisenberg’s uncertainty principle ensures that measuring the encoded qubit in one of the two bases destroys any information about the encoding in the other, while the no-cloning theorem ensures that only a party knowing the basis used for the encoding can unambiguously recover the encoded information upon measurement of the qubit. This idea was subsequently extensively used in many quantum cryptographic schemes,3 and in particular in the BB84 quantum key distribution protocol,4 which has since thrived as one of the most studied and successfully implemented quantum information applications.5,6

The application that Wiesner’s original work was interested in was unforgeable quantum money. The goal of a quantum money scheme is to perform an authenticated and efficient transaction between a client, a vendor and a bank via the use of a prepaid credit card (private-key money scheme) or between a client and a vendor via the use of banknotes (public-key money scheme), with maximal security guarantees. More precisely, in a quantum credit card system, a trusted bank uses a secret to preload a certain amount of money on a credit card, namely a device that contains encoded quantum information, and gives it to a client who can make payments to a vendor who has in his possession a credit card reader, namely a device that can access the card and communicate with the bank, which can then verify using the initial secret if the credit card is valid and can be used for the payment. The security guarantee is that the client cannot duplicate the credit card or increase the amount of money associated with it. In quantum banknotes, the difference is that the verification must be done without the help of the bank, hence there is no private key involved in the process.

In the classical world, money schemes are impossible with information-theoretic security and are therefore based on computational assumptions. In the quantum world, schemes for unforgeable quantum credit cards typically involve verification procedures with quantum communication with the bank.2 A simpler information-theoretically secure credit card scheme using classical communication during verification was proposed,7 and is based on hidden matching quantum retrieval games;8,9 these typically involve several rounds of communication between the vendor and the bank and the use of specific entangled states, although these requirements have been improved recently.10 This classical verification scheme has also been further simplified to use again the so-called BB84 states as in the original Wiesner scheme, additionally taking into account realistic conditions.11

As regards to quantum banknotes, it is known that even in the quantum world such schemes cannot base their security solely on the no-cloning theorem but must also use some computational assumptions, such as knot problems or quantum obfuscation.12–17 This computational security is still interesting since in the classical world there can be no notion of mathematical security for banknotes; their security is based only on the fact that it is difficult...
for a counterfeiter to copy a banknote due to its intricate coloring and hologram design. Recent experimental work has shown how such quantum banknotes can be constructed on-the-fly but also forged. On the other hand, unforgeable quantum credit card schemes have never been implemented until now.

Here we develop and implement an on-the-fly version of a practical unforgeable quantum money scheme for credit card transactions (independent work implementing a hidden matching version of quantum money has appeared in ref. 19). Our protocol builds upon the work in 11 in conjunction with the techniques developed in 16 and uses only BB84 states and a single round of classical communication for the verification. Our construction allows us to formulate conditions for correctness and security that can be experimentally tested. In particular, we derive conditions in scenarios of practical interest, corresponding to quantum memories based on single emitters or on atomic ensembles, and to implementations with weak coherent states. In all cases, we demonstrate that these conditions are rigorously satisfied experimentally using a practical photonic setup based on polarization encoding of weak coherent states of light, and we analyze operational regimes where unforgeability is guaranteed. Our experiment includes the full procedure of credit card state generation, readout and verification and is compatible with the future use of quantum storage devices, hence paving the way for the realization of quantum money transactions with information-theoretic security impossible to achieve in the classical world.

RESULTS

The quantum money protocol

To describe the protocol that we have analyzed, we first define a reduced scheme that guarantees a weak security condition, before extending it to a larger scheme with exponentially good security parameters. The reduced scheme is schematically shown in Fig. 1.

Let us assume that the bank prepares a prepaid credit card state, which for now consists of a single pair of qubits only, chosen from the following set using a random secret classical string $s$:

$$S_{\text{pair}} = \{ |0\rangle, |1\rangle, |+\rangle, |-\rangle \}.$$

When a transaction is to be made, the following interactions occur: first, the client hands the credit card to the 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 for the selected challenge. As a second step, the vendor sends the classical bits corresponding to the chosen challenge, along with the answer obtained upon measurement, to the bank. Finally, the bank verifies the authenticity of the credit card using the secret string $s$ and responds with a yes or no. If the answer of the bank is yes then the transaction may occur, otherwise the card is rejected and declared as a counterfeit.

The two challenge questions, $Q_{zz}$ and $Q_{xx}$, read:

- $Q_{zz} = \text{Guess the two bits } c_0, c_1$, such that the guess corresponding to the qubit prepared in the $\sigma_z$ basis is correct.
- $Q_{xx} = \text{Guess the two bits } c_0, c_1$, such that the guess corresponding to the qubit prepared in the $\sigma_x$ basis is correct.

We may also define the conjunction of both challenges:

$$Q_e = \text{Guess the two bits } c_0, c_1.$$

The main idea here is that a valid credit card can always be verified in the ideal case: the vendor performs a measurement in the $\sigma_z \otimes \sigma_z$ basis in order to verify the $Q_{zz}$ challenge, and in the $\sigma_x \otimes \sigma_x$ basis in order to verify the $Q_{xx}$ challenge. In general, we denote by $c$ the probability of successfully answering $Q_{zz}$ or $Q_{xx}$, and we call this the correctness parameter. In the ideal case, $c$ is equal to 1 for the above challenges: measuring both qubits in the $\sigma_z$ basis always answers the $Q_{zz}$ challenge correctly, and similarly for $Q_{xx}$. In a realistic implementation, however, $c$ might not be equal to 1 due to system imperfections. It might also take different values, $c_{zz}$ and $c_{xx}$, for $Q_{zz}$ and $Q_{xx}$, respectively. In this case, $c$ can be calculated as the average of $c_{zz}$ and $c_{xx}$ as we describe later.

Let us now see what happens if a dishonest client tries to duplicate the credit card. Since the 2-qubit state is unknown, there is no way that the two copies of the credit card can pass both challenges with high probability. The upper bound on this cheating probability has been derived in 7 and shown to be 3/4. A crucial property of the game is that if one plays in parallel such games, then one can upper bound the probability $c$ of cheating to the composite Hilbert space of all qubit pairs in the card cannot yield a higher cheating probability than performing an optimal attack on each individual pair. In general, we denote by $c$ the probability of successfully answering the conjunction challenge $Q_e$, i.e., the probability of successfully cheating, and we call this the security parameter materializing the non-clonability of the quantum state. We refer to such a challenge game as a $(c, e)$-game $G$.

Starting from a $(c, e)$-game $G$ that consists of a single pair of qubits and for which the following relation between the correctness and the security parameter holds,

$$c > \frac{e + 1}{2},$$

we can construct a different game $G'$ that consists of $n$ such pairs of qubits, where we denote by $|S_n\rangle$ the 2$n$-qubit state chosen by a randomly generated secret classical string $s$ of length $3n$. Here again, the vendor chooses at random one out of two challenge questions and performs a measurement on all 2$n$ qubits accordingly (either $\sigma_z \otimes \sigma_z$ on all $n$ pairs or $\sigma_x \otimes \sigma_x$ on all $n$ pairs). If we now define the two challenges as: (i) answering the challenge $Q_{zz}$ correctly for at least a fraction $\delta - 6$ of the $n$ pairs,
and (ii) answering the challenge $Q_{\text{ch}}$ for at least a fraction $c - \delta$ of the $n$ pairs, where we define (see Methods)

$$\delta = \frac{2c - \epsilon - 1}{3} > 0,$$

(3)
then we can use the analysis in,16 based on a Chernoff bound argument,23 and have that the correctness $c'$ and security $\epsilon'$ of the game $G'$ satisfy

$$c' = 1 - e^{-\frac{2\delta}{3}}$$

and $\epsilon' = e^{-\frac{2\delta}{3}}$.

(4)

This means that, for the game $G'$, the correctness parameter $c'$ is exponentially close to 1 and the security parameter $\epsilon'$ exponentially close to zero.

Since in our initial game G we have $\epsilon = 3/4$, then we can see from Eq. (2) that in any secure implementation of the game G we need to achieve $c > 7/8 = 0.875$. The more $c$ exceeds this bound, the better security (i.e., the lower $\epsilon'$) we will get for a game $G'$ of size $n$.

The above description provides a game with exponentially good security parameters. By including quantum states that correspond to many such games in the same credit card as well as a unique classical serial number, one can use theorems from7,14,16 to extend the above scheme into a quantum prepaid credit card scheme, where the quantum credit card may be re-used multiple times and a dishonest client cannot create a copy of the credit card even if he has in his possession multiple credit cards. Hence, satisfying Eq. (2) experimentally is enough to implement a full quantum money scheme with information-theoretic security given by correctness and security parameters from Eq. (4).

Security analysis for weak coherent states

In our discussion up till now, we have assumed that the bank creates single-qubit states and stores them in the credit card. In practice, this assumption would be compatible with an implementation using either a quantum memory based on single emitters,24,25 which are expected to emit true single photons to be measured by the vendor for verification regardless of the input state used by the bank in the card preparation stage, or a quantum memory based on atomic ensembles26,27 when the input state is a true single-photon state. In the following, we shall refer to this case as the “single-photon state” protocol. The correctness and security parameters defined above apply to this case.

In other cases of practical interest, however, we would like to use atomic-ensemble quantum memories and also weak coherent states as an input, as is typically the case, for instance, in quantum cryptographic applications.3 In this case, the memory preserves the Poisson photon statistics in the output state and simply introduces attenuation, hence reducing the average photon number per pulse $\mu$ that characterizes such states. The security threshold therefore has to be modified. More specifically, the bound that $c$ must exceed has to be a function of $\mu$. In the following, we shall refer to this case as the “weak coherent state” protocol. Our security analysis first considers specific attacks that may take place in an experimental implementation where the phase of each state is not randomized, namely unambiguous state discrimination (USD) attacks. As a second step, we derive a rigorous bound that applies to all attacks in the phase randomized case.

Starting with the non phase-randomized case, USD attacks are possible only for sets of linearly independent states,28–30 which is the case for the set of states used in our protocol when physically realized with weak coherent state encoding. A dishonest client willing to copy the credit card can perform specific positive operator valued measurements to perfectly discriminate and identify a fraction of the states in the card. Successfully identifying one state in a pair allows the successful cloning of the whole pair, since the adversary knows that the other state is prepared in the conjugate basis. Following the analysis in refs. 29,30 for our set of states, for $\mu \leq 2$, and assuming that no phase randomization is performed on our states, gives a probability for successful USD

$$p_D = 2e^{-\frac{\mu}{2}} \left( \sinh \frac{\mu}{2} - \sin \frac{\mu}{2} \right).$$

(5)

By a Chernoff bound argument,23 we then have that for $n$ pulses (in the 2n-qubit sequence) that are created according to the Poisson distribution with a mean photon number $\mu$, with very high probability the number of pulses among these $n$ pulses for which the USD is successful is very close to its expectation. In other words, if $L_1, \ldots, L_n$, are random variables that take the value 1 if the pulse leads to a successful USD, then we have for the sum $L = \sum L_i$

$$\Pr[L \geq (1 + \eta)\mu] \leq e^{-\frac{\mu \eta^2}{2}},$$

where $\eta > 0$ is a parameter accounting for finite number statistics that can be optimized as discussed further on.

We can now define a new parameter $\delta$ as

$$\delta = \frac{2c - \epsilon - (1 + \eta)\mu}{3} > 0,$$

(7)

and restate the condition of Eq. (2) as

$$c > \frac{\epsilon + (1 + \eta)\mu + 1}{2},$$

(8)
leading to the following correctness and security parameters that take into account possible USD attacks:

$$c' = 1 - e^{-\frac{2\delta}{3}}$$

and $\epsilon' = e^{-\frac{2\delta}{3}} + e^{-\frac{2\delta}{3} - \frac{\mu \eta^2}{2}}$.

(9)

Note that the second term in the expression of $\epsilon'$ comes from the fact that, in case $L$ is bigger than its expectation, then the dishonest client can perfectly cheat on a larger number of pairs.

A dishonest client may further boost his cheating probability by exploiting the losses present in a realistic implementation. In the presence of losses, the client having used USD to copy the card may indeed replace the states that he has successfully identified with states containing a higher average photon number $\mu$ at the input of the card reader, in order to increase the probability of detection by the vendor, and replace the ones that he failed to identify with vacuum states. Such a strategy will not be detected when a state is measured in the correct basis but it will induce an increase in the number of total clicks on the detectors registered by the card reader when a state is measured in the conjugate basis. As was shown in ref. 29, in order for this cheating strategy to be detected and thus for the protocol to be secure, the total efficiency must fulfill the condition

$$\eta_{\text{qm}} \eta_{\text{det}} > \frac{-\ln(1 - \eta_{\text{det}})}{\mu},$$

(10)
where $\eta_{\text{qm}}$ is the retrieval efficiency of the quantum memory in the original valid card and $\eta_{\text{det}}$ is the detection efficiency of the card reader.

Thus, for the "weak coherent state" protocol, as long as it is possible to satisfy Eqs. (8) and (10) experimentally, then a quantum credit card scheme secure against USD attacks, characterized by correctness and security parameters given in Eq. (9), can be implemented.

In the case where phase randomization is performed, then each weak coherent state appears to the adversary as a Poisson distributed mixture of Fock states:31

$$\frac{1}{2^n} \int_0^{2\pi} |\sqrt{\mu} e^{i\phi}\rangle \langle \sqrt{\mu} e^{i\phi}| d\phi = e^{-\frac{\mu}{2}} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} |n\rangle \langle n|$$

(11)

This allows us to derive a general security bound considering three distinct cases. If the state is a vacuum state, then there is no information content. If the state is a single-photon state, then the
Experimental investigation of practical unforgeable quantum money
M Bozzio et al.

The cyan curves correspond to theoretical simulations for weak coherent states assuming a dark count probability of $7 \times 10^{-4}$. The red lines correspond to the security threshold for the quantum credit card scheme with information-theoretic security. The purple line corresponds to the threshold for general attacks on phase-randomized weak coherent states, for the same values of $\lambda$. The full pink line corresponds to the security threshold for the “single-photon state” protocol. The cyan curves correspond to the experimental results for different values of $\mu$. Measured $c_{zz}$, $c_{xx}$, and $c$ values (green symbols) are plotted as a function of the average photon number per pulse $\mu$. Each measured block consists of a number of post-selected pairs ranging from $1.3 \times 10^5$ for $\mu = 0.025$ to $2.6 \times 10^5$ for $\mu = 1$. The red lines correspond to the security threshold for the “weak coherent state” protocol encompassing USD attacks for values of $\eta = 0.020$ and $\eta = 0.402$, while the purple line corresponds to the threshold for general attacks on phase-randomized weak coherent states, for the same values of $\eta$. The full pink line corresponds to the security threshold for the “single-photon state” protocol.

Experimental results for different values of $\mu$. Measured $c_{zz}$, $c_{xx}$, and $c$ values (green symbols) are plotted as a function of the average photon number per pulse $\mu$. Each measured block consists of a number of post-selected pairs ranging from $1.3 \times 10^5$ for $\mu = 0.025$ to $2.6 \times 10^5$ for $\mu = 1$. The red lines correspond to the security threshold for the “weak coherent state” protocol encompassing USD attacks for values of $\eta = 0.020$ and $\eta = 0.402$, while the purple line corresponds to the threshold for general attacks on phase-randomized weak coherent states, for the same values of $\eta$. The full pink line corresponds to the security threshold for the “single-photon state” protocol.

As long as it is possible to satisfy Eq. (12) experimentally, then a quantum credit card scheme with information-theoretic security against all attacks performed on uniformly phase randomized weak coherent states, characterized by correctness and security parameters given in Eq. (13), can be implemented.

Experimental principle and setup
In order to test in practice the security conditions from Eqs. (2), (8) and (10) and identify suitable operation regimes, we have implemented an on-the-fly version of our quantum money protocol in which the qubit pairs of the credit card are sent directly to the vendor’s card reader, without intermediate storage in a quantum memory. In our experiment we have not performed phase randomization (this can be implemented subsequently in the same manner as ref. 32), hence the security bound of Eq. (12) has not been explicitly considered. The verification test consists in measuring the correctness parameters $c_{zz}$ for the challenge question $Q_{zz}$ and $c_{xx}$ for $Q_{xx}$ on blocks of $n$ qubit pairs, each of which is randomly chosen from the set of Eq. (1). This is done by measuring each block in the $\sigma_z \otimes \sigma_z$ basis or in the $\sigma_x \otimes \sigma_x$ basis, respectively. As noted earlier, the correctness parameter is calculated as $c = (c_{zz} + c_{xx})/2$, and must exceed the thresholds from Eqs. (2) and (8) in order for the credit card to be validated by the bank. 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. Once $c$ has been measured, the correctness and security of the full protocol can be estimated for the different scenarios from Eqs. (4) and (9).

The experimental setup is shown in Fig. 2. The qubit pairs of the credit card state are encoded in the polarization of weak coherent states of light produced with standard optical communication components. The light emitted at 1564 nm by a continuous-wave laser diode is first modulated using an acousto-optic modulator to produce pulses with a duration of 20 $\mu$s and a repetition rate of 20 kHz. A variable optical attenuator is used to reduce the intensity of the pulses and set the average photon number per pulse $\mu$. Then, the light pulses go through a multi-stage polarization controller consisting of an electro-optic modulator, which sets the
The experimental results for the values of μ, the protocol is insecure against USD attacks. Note that for the threshold of Eq. (12) which ensures security against any attack (for phase-randomized states), it can be seen that μ must not exceed 0.40. The simulations in Fig. 3 also show that the protocol is insecure when the state purity ρ drops below 76%, since the value of c then falls below the USD attack security threshold. However, for 0.01 ≤ μ ≤ 1 and for p ≥ 0.76, there is a wide region of parameters for which the protocol is secure against such attacks. Indeed, for our experimental results with p = 0.93, the protocol is secure against USD attacks for values of μ up to 1. In Fig. 4, we show the security regions corresponding to Eq. (10) as a function of μ and ηtot = ηqm/ηdet: our experiments, with ηqm = 1 and ηdet = 0.25, are situated in the secure region for all values of μ ≤ 2.

For the “single-photon state” protocol, the security threshold of Eq. (2) is constant and equal to 7/8 = 0.875 for all values of μ. Our experimental data, interpreted as if resulting from single-photon states with a polarization purity p = 0.93 and an efficiency 0.02 ≤ μ ≤ 1, are secure and show a value of c well above the security threshold. We also notice that the protocol can tolerate large attenuations even for relatively low values of purity.

The measured values for c allow us to estimate the number n of qubit pairs required for our prepaid quantum credit card scheme (corresponding to the game G′) to reach a high level of security. In Fig. 5, we show values for the correctness and security parameters c′ and c′ defined in Eq. (4) for the “single-photon state” protocol, using the experimental values c = 0.953 ± 0.011 for μ = 1 (full red line), c = 0.966 ± 0.018 for μ = 0.10 (dashed red line) and c = 0.953 ± 0.014 for μ = 0.025 (dotted red line). We see that, as c′ drops quickly with the number of qubit pairs n, a measured credit card state consisting of a number of pairs comprised between 102 and 106 is sufficient to reach an arbitrarily small cheating probability in this case, for a wide range of efficiencies μ ∈ [0.025,1]. Note that when estimating c′ and c′, we use the lowest value for the experimental value of c taking into account error bars of 5%. In this way, there is a probability no higher than 10−6 that the true c value actually lies beneath this point.

In Fig. 5, we also display values for the correctness and security parameters c′ and c′ defined in Eq. (9) for the “weak coherent state” protocol, using the experimental values c = 0.953 ± 0.011 for μ = 1 (full blue line), c = 0.965 ± 0.010 for μ = 0.40 (mixed blue line), c = 0.966 ± 0.018 for μ = 0.10 (dashed blue line) and c = 0.953 ± 0.014 for μ = 0.025 (dotted blue line). The parameter η has an opposite effect in the two terms in the expression of c′ and we find that these two terms must be roughly balanced. Values for η have therefore been chosen accordingly, and we see that the optimal values strongly depend on μ: they must be increased as μ decreases. We also notice that, in general, states with large values of μ require a higher number of detected pairs than states with small values of μ in order to reach the same security level. However, as long as μ is not too big, the minimal number of pairs remains of the order of 106, and this effect is counter-balanced by the fact that a higher value of μ increases the number of useful detected pulses and hence the number n of detected pairs. Thus, despite this trade-off, in order 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 detected pairs. We may
that our implementation has minimal channel losses as the transaction is performed locally, while detection losses are processed through our post-selection procedure and taken into account in our security analysis when practical weak coherent states are used in the implementation.

Our work sets a complete theoretical and operational framework for quantum money, and is fully compatible with presently existing quantum memories. In this sense, we provide a crucial experimental benchmark for unforgeability of quantum money, and for any other application where our transaction framework may be relevant.

**METHODS**

Derivation of $\delta$

For the completeness of game $G$, we have that the honest client must ensure at least $C - \delta$ of the $Q_x$ challenges, or at least $C - \delta$ of the $Q_z$ challenges, are answered correctly. The correctness $c'$ in the first half of Eq. (4) comes from a simple Chernoff bound, since the client succeeds with probability $c$ in the challenge. In order to prove that the security parameter $c'$ is the one given in the second part of Eq. (4), it suffices to show that the cheating client has to ensure the challenge $Q_z$ is answered correctly for a fraction of at least $C + \delta$ of the games $G$ in order to cheat in $G'$. Note that the client must be able to ensure the correct answer for at least a fraction of $C - \delta$ of each of the two challenges and hence the fraction of games where both challenges must be answered is at least $2C - \delta - 1$, as illustrated below:

\[
\begin{align*}
\text{Correctness} & : c' + \frac{2C - \delta - 1}{3} \\
\text{Security} & : \delta \\
\end{align*}
\]

Making this equal to $\epsilon + \delta$ provides the value of $\delta$ for the "single-photon state" protocol:

\[
\delta = \frac{2C - \epsilon - (1 + \eta)P_{\text{success}} - 1}{3}.
\]

Setting of $\mu$

The value of $\mu$ in our experiment is defined as the average photon number per single-photon-detector gate at the output of the polarization controller. It can be expressed as follows:

\[
\mu = \frac{\lambda}{h} \frac{T_{\text{pulse}}}{T_{\text{rep}}} \frac{P_{\text{success}}}{P_{\text{loss}}},
\]

where $\lambda = 1564$ nm is the wavelength, $h$ is Planck's constant, $c$ is the speed of light in vacuum, $T_{\text{gate}} = 500$ ps is the duration of the detection gate of the single-photon detectors, $T_{\text{pulse}} = 20$ $\mu$s is the duration of the light pulses, $P_{\text{loss}} = 20$ kHz is the repetition rate of these pulses, $r_{\text{split}}$ is the exact splitting ratio of the 99/1 beam splitter, $P_{\text{loss}} = 0.50$ is the transmission coefficient of the polarization controller and $P_{\text{success}}$ is the mean power measured at the 99 output of the 99/1 beam splitter.

**DISCUSSION**

The results that we have presented constitute the first on-the-fly implementation of provably unforgeable quantum money. Our implementation is based on a practical photonic setup with requirements close to those of standard quantum key distribution systems, which is used for quantum credit card on-the-fly generation and readout. The validation of our quantum money protocol and the chosen experimental conditions anticipate the future use of state-of-the-art quantum storage devices, based on single emitters or atomic ensembles, for real-world realization of credit card states.

The integration of our system with a quantum memory requires further developments, in particular to ensure wavelength matching and synchronization, and the full system will be mainly limited by the performance of the quantum storage device, in particular with respect to timing and losses. Regarding losses, we remark

\[
\begin{align*}
\text{Extraction of } c_{xz} & : \\
& = \frac{1}{2} (c_{x} + c_{z}) \\
& = \frac{1}{2} \frac{N_{0} (D_{x, \text{ only}})}{N_{0} (D_{x, \text{ or } D_{z}})} \\
& + \frac{1}{2} \frac{N_{0} (D_{z, \text{ only}})}{N_{0} (U_{x, \text{ or } D_{z}})},
\end{align*}
\]

Experimental investigation of practical unforgeable quantum money, which is used for quantum credit card on-the-fly implementation is based on a practical photonic setup with requirements close to those of standard quantum key distribution systems, which is used for quantum credit card on-the-fly generation and readout. The validation of our quantum money protocol and the chosen experimental conditions anticipate the future use of state-of-the-art quantum storage devices, based on single emitters or atomic ensembles, for real-world realization of credit card states.

The results that we have presented constitute the first on-the-fly implementation of provably unforgeable quantum money. Our implementation is based on a practical photonic setup with requirements close to those of standard quantum key distribution systems, which is used for quantum credit card on-the-fly generation and readout. The validation of our quantum money protocol and the chosen experimental conditions anticipate the future use of state-of-the-art quantum storage devices, based on single emitters or atomic ensembles, for real-world realization of credit card states.
and
\[ c_{\alpha} = \frac{1}{2} (c_+ + c_-) \]
\[ = \left\{ \begin{array}{ll}
N_+ (D_0, \text{only}) \\
\frac{1}{2} N_+ (D_0, \text{or} \ D_1, \text{...})
\end{array} \right. \]
\[ + \left\{ \begin{array}{ll}
N_+ (D_1, \text{only}) \\
\frac{1}{2} N_+ (D_0, \text{or} \ D_1, \text{...})
\end{array} \right. \]

where \( c_\alpha \) is the fidelity of the state \( |\alpha\rangle \), \( N_+ (D_0, \text{only}) \) and \( N_+ (D_1, \text{only}) \) are the number of pulses corresponding to the state \( |\alpha\rangle \) that generated a click on at least one of the detectors, \( N_0 (D_0, \text{only}) \) and \( N_0 (D_1, \text{only}) \) are the number of pulses corresponding to the state \( |\alpha\rangle \) that generated a click on the detector \( D_{0\alpha} \) but not on the detector \( D_{1\alpha} \) or on \( D_{1\beta} \) but not on \( D_{0\beta} \), respectively, with \( s = 0, 1, +, - \).

The parameter \( c_{\alpha} \) is estimated from measurements performed in the \( \alpha \) basis for the entire block, i.e., with the half-wave plate rotated to 0°, while \( c_\beta \) is estimated from measurements performed in the \( \beta \) basis for the entire block, i.e., with the half-wave plate rotated to 22.5°.

Statistical errors

The pulse sequences used for measuring \( c_{\alpha} \) and \( c_\beta \) for each value of \( \mu < 1 \) consisted of \( 3 \times 10^4 \) pulses (i.e., \( 1.5 \times 10^5 \) pairs) before post-selection. Each of the four polarization states was generated with probability 0.25, that is, \( c_{\alpha} \) is estimated from measurements performed in the \( \alpha \) basis for the entire block, i.e., with the half-wave plate rotated to 0°, while \( c_\beta \) is estimated from measurements performed in the \( \beta \) basis for the entire block.

Theoretical models for \( c \)

The correctness parameter and its evolution with \( \mu \) can be simulated with a simple theoretical model taking into account experimental parameters. This model was used to plot the simulation curves in Fig. 3. We model the polarization state generated by the polarization controller as a density matrix \( \rho \) for each value of \( \mu \) and for a detection efficiency of 25%. Errors on the correctness parameters were estimated by propagating the Poisson errors of the click counting.

ACKNOWLEDGEMENTS

We thank Julien Laurat and Frederic Grosshans for useful discussions. This research was supported by the European Research Council projects QCC and QUSCO, the French National Research Agency project qUBIC and the BPI France project RIQ.

AUTHOR CONTRIBUTIONS

M.B., A.O., I.K., and E.D. performed the theoretical analysis. M.B. and L.T.V. developed the software and system control tools. M.B. built and operated the experimental system and collected the data. M.B., A.O., I.Z., and E.D. analyzed the data. I.K. and E.D. conceived and supervised the project. M.B., A.O., I.K., and E.D. wrote the manuscript, with contributions from all the authors.

ADDITIONAL INFORMATION

Competing interests: The authors declare no competing financial interests.

REFERENCES

1. Wooters, W. K. & Zurek, W. H. A single quantum cannot be cloned. Nature 299, 802 (1982).
2. Wiezer, S. Conjugate coding. ACM SIGACT News 15, 78 (1983).
3. Broadbent, A. & Schaffner, C. Quantum cryptography beyond quantum key distribution. Des. Codes Cryptogr 78, 351 (2016).
4. Bennett, C. H. & Brassard. Quantum cryptography: public key distribution and coin tossing. G. Proc. IEEE Int. Conf. Comput. Syst. Signal Process 175, 8 (1984).
5. Scarani, V. et al. The security of practical quantum key distribution. Rev. Mod. Phys. 81, 1301 (2009).
6. Diamanti, E., Lo, H.-K., Qi, B. & Yuan, Z. Practical challenges in quantum key distribution. npj Quantum Inf. 2, 16025 (2016).
7. Gavinski, D. Quantum money with classical verification, In Proc. 27th Annual Conference on Computational Complexity (CCC), Porto, Portugal, IEEE, 42–52 (2012).
8. Bar-Yossef, Z., Jayram, T. S. & Kerendis, I. Exponential separation of quantum and classical one-way communication complexity, In Proc. 36th Annual ACM Symposium on Theory of Computing, Chicago, Illinois, USA, ACM, 128–137 (2004).
9. Arzazola, J. M., Karasamian, M. & Lütkenhaus Practical quantum retrieval games. N. Phys. Rev. A 93, 062311 (2011).
10. Amiri, R. & Arzazola, J. M. Quantum money with nearly optimal error tolerance. Phys. Rev. A 95, 062334 (2017).
11. Pastawski, F., Yao, N., Ji, J., Ljubnik, M. D. & Girac, J. I. Unforgeable noise-tolerant quantum tokens. Proc. Natl. Acad. Sci. USA 109, 16079 (2012).
12. Lutomirski, A. et al. Breaking and making quantum money: toward a new quantum cryptographic protocol, In Proc. Innovations in Computer Science (ICS), Tsinghua University, Beijing, China, 20–31 (2010).
13. Mosca, M. & Stebila, D. Error-correcting codes. Finite Geom. Cryptogr. 523, 35 (2010).
14. Aaronson, S. & Christiano, P. Quantum money from hidden subspaces, Theory of Computing 9, 349 (2013).
15. Fehr, E., Gotsos, D., Hassidim, A., Lutominerski, A. & Shor, P. Quantum money from knots, In Proc. 3rd Innovations in Theoretical Computer Science Conference, ITCS'12, ACM, 276–289 (New York, NY, 2012).
16. Geogu, M. & Kerendis, I. New constructions for quantum money, In Proc. 10th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC), vol. 44, 92–110 (Brussels, Belgium, 2015).
17. Alagic, G. & Fefferman, B. On quantum obfuscation, Preprint at http://arxiv.org/abs/1602.01771 (2016).
18. Bartkiewicz, K. et al. Experimental quantum forgery of quantum optical money. npj Quantum Inf. 3, 7 (2017).
19. Guan, J.-Y., Jia, X. & Wang, W. Experimental preparation and verification of quantum money, Preprint at https://arxiv.org/abs/1709.05882 (2017).
20. Lvovsky, A. I., Sanders, B. C. & Tittel, W. Optical quantum memory. Nat. Photonics 3, 706 (2009).
21. Brennen, G., Giacobino, E. & Simon, C. Focus on quantum memory. New. J. Phys. 17, 050201 (2015).
22. Heshami, K. et al. Quantum memories: emerging applications and recent advances. J. Mod. Opt. 63, 20 (2016).
23. Mierzyniak, M. & Upfal, E. Probability and Computing: Randomized Algorithms and Probabilistic Analysis (Cambridge University Press, 2005).
24. Specht, H. P. et al. A single atom quantum memory. Nature 473, 190 (2011).
25. Maurer, P. C. et al. Room-temperature quantum bit memory exceeding one second. Science 336, 1283 (2012).
26. Nicolás, A. et al. Quantum memory for orbital angular momentum photonic qubits. Nat. Photon. 8, 234 (2014).
27. Rui, J. & al. Operating spin echo in the quantum regime for an atomic ensemble quantum memory. Phys. Rev. Lett. 115, 133002 (2015).
28. Cheffes, A. Unambiguous discrimination between linearly-independent quantum states. Phys. Lett. A 239, 339 (1998).
29. Cheffes, A. & Barnett, S. M. Optimum unambiguous discrimination between linearly independent symmetric states. Phys. Lett. A 223, 223 (1998).
30. Dusek, M., Jha, M. & Lütkenhaus, Unambiguous state discrimination in quantum cryptography with weak coherent states, N. Phys. Rev. A 62, 022306 (2000).
31. Lo, H.-K. & Preskill, J. Phase randomization improves the security of quantum key distribution, Preprint at https://arxiv.org/abs/quant-ph/0504209 (2005).
32. Zhao, Y., Qi, B. & Lo, H.-K. Experimental quantum key distribution with active phase randomization. Appl. Phys. Lett. 90, 044106 (2007).
