npj | Quantum Information

www.nature.com/npjqi

ARTICLE OPEN

Experimental quantum forgery of quantum optical money

Karol Bartkiewicz[1,2,3], Antonín Černoch[4], Grzegorz Chimczak[1], Karel Lemr[2], Adam Miranowicz[1,3] and Franco Nori[3,5]

Unknown quantum information cannot be perfectly copied (cloned). This statement is the bedrock of quantum technologies and quantum cryptography, including the seminal scheme of Wiesner's quantum money, which was the first quantum-cryptographic proposal. Surprisingly, to our knowledge, quantum money has not been tested experimentally yet. Here, we experimentally revisit the Wiesner idea, assuming a banknote to be an image encoded in the polarization states of single photons. We demonstrate that it is possible to use quantum states to prepare a banknote that cannot be ideally copied without making the owner aware of only unauthorized actions. We provide the security conditions for quantum money by investigating the physically-achievable limits on the fidelity of 1-to-2 copying of arbitrary sequences of qubits. These results can be applied as a security measure in quantum digital right management.

npj Quantum Information (2017)3:7 ; doi:10.1038/s41534-017-0010-x

INTRODUCTION

The seminal proposal of quantum money by Wiesner[1] (see also ref. 2), followed by the introduction of quantum key distribution (QKD) protocols by Bennet and Brassard[3] and by Ekert,[4] have triggered a breathtaking interest and progress not only in quantum cryptography but, in general, in quantum information over the last three decades. It is not surprising that refs 3, 4 on QKD are among the most often cited works in quantum information, and both quantum and classical cryptography. Moreover, various commercial implementations of QKD protocols (for a recent review see ref. 5), together with quantum random-number generators and the D-Wave machine (see, e.g., 6) are probably the only commercial applications of quantum information and quantum optics up to now.[7] Although, various protocols of quantum money have already been proposed (see, e.g., refs 8–17), this interest cannot be compared with the immense popularity and applicability of QKD (see refs 18–20 as an example of recent and fundamental achievements). This is partially because there have not been, to our knowledge, any experimental realizations of quantum money performed yet. Here, we report not only an experimental implementation of quantum money but also an experimental attempt to its forgery using optimal cloning machines.

Our experimental work basically describes one-by-one attacks on each single qubit. In the quantum money scheme, however, eavesdroppers, in principle, can access every qubit at once. So, they can globally access multiple qubits and can seek superior attacks using such global access. This could be a reason why there has not been a known representative work for the experiment of attacking quantum money, because this would need to treat numerous qubits and difficult global controls of their quantum states. The attacks presented in this work are less distinguished from quantum cloning itself or the attack for BB84 quantum key distribution. Thus, collective or coherent attacks on multiple qubits simultaneously can, in principle, optimize the attacker's strategy. This is, nevertheless, considerably more demanding if not impossible with the current state of experimental quantum information processing. In this paper, we investigate a more accessible form of attack based on individual cloning which, in our view, represents a realistic threat for near-future quantum communications, including quantum money schemes.

Any information can be encoded as a sequence of zeros and ones. This sequence can also be represented using a set of single photons prepared in the horizontal and vertical polarization states. The polarization states of a photon can be described as a superposition of the two orthogonal polarization states, i.e.,

$$|\psi\rangle = \cos\frac{\theta}{2}\,|\leftrightarrow\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|\updownarrow\rangle, \qquad (1)$$

where the angles θ and ϕ are the spherical coordinates of this qubit on the Bloch sphere, while $\leftrightarrow$ and $\updownarrow$ denote horizontal and vertical polarizations, respectively. For each such state there exists an orthogonal state

$$|\psi_{\perp}\rangle = \sin\frac{\theta}{2}\,|\leftrightarrow\rangle - e^{i\phi}\cos\frac{\theta}{2}\,|\updownarrow\rangle. \qquad (2)$$

Any pair of such orthogonal states can be used to encode logical values 0 and 1. Without knowing what particular states have been used (i.e., without knowing θ and ϕ), there is no way of telling (with certainty) what logical value is associated with the photon.

Any attempt of gaining this information from the photon will disturb its polarization state and damage the information. Therefore, using photons to transmit sensitive information appears to be a promising idea. In the simplest scenario, the sequence of polarized photons is associated with a set of numbers indicating the correct measurement bases. These latter sequence needs to be confidential. If this sequence would be intercepted together with the sequence of photons, the quantum information could be read and reproduced at will. First, by deterministically

[1]Faculty of Physics, Adam Mickiewicz University, Poznań PL-61-614, Poland; [2]RCPTM, Joint Laboratory of Optics of Palacký University and Institute of Physics of Academy of Sciences of the Czech Republic, 17. listopadu 12, Olomouc 772 07, Czech Republic; [3]CEMS, RIKEN, Wakoshi 351-0198, Japan; [4]Institute of Physics of Czech Academy of Sciences, Joint Laboratory of Optics of PU and IP AS CR, 17. listopadu 50A, Olomouc 772 07, Czech Republic and [5]Department of Physics, The University of Michigan, Ann Arbor, MI 48109-1040, USA
Correspondence: Karol Bartkiewicz (bark@amu.edu.pl)

Received: 18 July 2016 Revised: 16 January 2017 Accepted: 25 January 2017
Published online: 01 March 2017

distinguishing between $|\psi\rangle$ and $|\psi_{\perp}\rangle$ associated with the bit values 0 and 1, respectively. Next, by reproducing the detected state.

Therefore, the advantages provided by this kind of quantum communication are limited to protocols, where a trusted arbiter checks the validity of a given sequence of qubits. Thus, the sequence of qubits can be used, e.g., as one-time passwords (tokens)[15] or arbitrated quantum currency.[1] However, some research has been conducted in order to eliminate the need for an arbiter in the quantum currency schemes.[12, 16]

Currently, tokens are widely applied as an extra layer of security, e.g., in a two-step authentication protocols used in social media services or Internet banking etc. While the classical tokens are sensitive to being copied, the quantum tokens cannot be delivered to two or more users at the same time without disturbing a given quantum dataset.[1, 15, 17]

It is claimed today that the security of our data is as good as its passwords. In the following text we discuss how to generate and check the security of the best tokens allowed by the laws of nature. The quantum passwords cannot be copied nor viewed without damaging them. However, quantum data are prone to noise and some level of noise has to be tolerated in order to harness the benefits of quantum technologies.

The quantum tokens can also be used as quantum money. The idea of quantum money goes back to Wiesner[1] who proposed to embed a sequence of qubits into banknotes that would be verified by banks. This was the first idea of quantum cryptography introduced already in the early 1970s and eventually published in 1983.[1, 21]

In order to be able to verify the money, a bank would attach information about the banknote serial number as classical information. This pioneering idea evolved over the last decades to more practical protocols, which are shown to be more secure and less demanding on the participating parties of a quantum currency system.[12, 16] However, all the protocols face the problem of decoherence that makes the quantum banknotes to be usable for a limited amount of time, even if the currency is represented as a sequence of photons,[15] which can have exceptionally-long coherence times.

Photons are robust to decoherence, because they do not usually interact with each other. Moreover, if the string of photons is handled properly it can last in a coherent state long enough to be useful in some financial transactions. Let us consider a transaction, where quantum money is withdrawn at the speed of light from a bank by an authorized user as a sequence of photons that arrives at a payment terminal, which allows its user to redirect the money to any other payment terminal. The final user sends the sequence to the bank together with an account number, where the money is to be stored. Lossless transmission of photons is impossible. Therefore, banks would have to accept large enough parts of incomplete quantum banknotes and issue new ones. The same is done nowadays if a banknote is damaged or a small part of it is missing. The communication between the payment terminals cannot be wiretapped without damaging this quantum money. Thus, this quantum money scheme (QMS) allows for some anonymity if the addresses of the terminals are not assigned to a specific person and there is at least one terminal used between the initial and final users. However, the money could be signed without damaging it using, e.g., the approach discussed in ref. 22.

Perfect copying of quantum information is impossible,[16, 23, 24] but as it was shown in various works, we can copy partially-known quantum information with very high fidelity. If we are going to clone some qubits more often than others, we can use a generic distribution function $g(\theta, \phi)$ to describe this intent. The higher the value of g, the more frequent cloning of the specific qubit is. This distribution function satisfies the following normalization condition

$$\int_{\Omega} g(\theta, \phi)\, \mathrm{d}\Omega = 1, \tag{3}$$

where $\mathrm{d}\Omega \equiv \sin\theta\, \mathrm{d}\phi\, \mathrm{d}\theta$ and Ω is the full solid angle. The distribution g can be arbitrary, but until now only highly-symmetric distributions have been analyzed (see, e.g., refs 25–27 and references therein). Therefore, one can be under the impression that this optimal cloning problem can be solved only for a highly-symmetric class of distributions. However, as we show below, we are in principle able to always find an optimal cloning machine corresponding to any randomly generated quantum tokens or banknotes. Note that the most secure tokens are the ones with the highest entropy. The same applies here, because the lowest average cloning fidelity, corresponding to the case most resistant to cloning attacks, is achieved for a uniform distribution g, which has the highest possible entropy. However, while generating quantum money of a finite size at random, it is hard to ensure each time the perfect entropy. Therefore, in practice, we could deal with any qubit distribution function g that could be potentially known to the counterfeiter. In particular, there exist qubit distributions g made of a weighted sum of two Dirac's delta functions at any antipodes of the Bloch sphere. In this special case, the problem is reduced to the classical case of standard digital tokens. This is because these particular functions tell us that there are only two states sent that could be discriminated deterministically. Quantum money of this kind should obviously be avoided.

Let us briefly review the main possible attack scenarios. Without any knowledge about the token, the counterfeiter can use the universal quantum cloner (UC).[28] If the states, appearing in the qubit sequence, are known but their order is unknown, the attacker can apply a specialized optimal quantum cloning machine. This is equivalent to the situation in which the attacker has some information about the money statistics, but does not know the sequence of qubits itself. The results of such an attack can be seen in Fig. 1. Unfortunately, if the attacker knows the sequence of bases, the quantum money (tokens) can be perfectly copied.

RESULTS

Noise tolerance vs. security

Let us estimate the level of noise tolerance needed for a quantum token to be validated in realistic conditions and compare it to the level of noise introduced by a given optimal quantum cloning. By doing so, we will limit the class of distributions associated with acceptable tokens. We assume that a counterfeiter can replace the noisy communication channel with a less noisy one and perform a quantum man-in-the-middle attack with an optimal quantum cloning machine. An equivalent assumption is that the counterfeiter is a party in the QMS. Finding the optimal cloning transformation for a given g is a semi-definite programming problem.[29, 30] Such problem can be described as a task of finding a semi-definite operator $\hat{\chi}$ (a cloning map) describing the copying process that maximizes the average single-copy fidelity F. Such operator is isomorphic to a completely positive trace-preserving map.[31] The average single-copy fidelity for an arbitrary distribution (for symmetric 1→2 cloning) can be expressed refs 26, 27 as

$$F = \frac{1}{2} \int_{\Omega} g(\theta, \phi)(F_0 + F_1)\, \mathrm{d}\Omega, \tag{4}$$

where the fidelities of copying a particular qubit for the first and second clones are

$$F_0 = \mathrm{Tr}\,[(\hat{\rho}^{\mathrm{T}} \otimes \hat{\rho} \otimes \hat{\mathbb{1}})\,\hat{\chi}] \text{ and } F_1 = \mathrm{Tr}\,[(\hat{\rho}^{\mathrm{T}} \otimes \hat{\mathbb{1}} \otimes \hat{\rho})\,\hat{\chi}]\,, \tag{5}$$

where $\hat{\rho} = |\psi\rangle\langle\psi|$, T stands for transposition, and $\hat{\mathbb{1}}$ is the single-

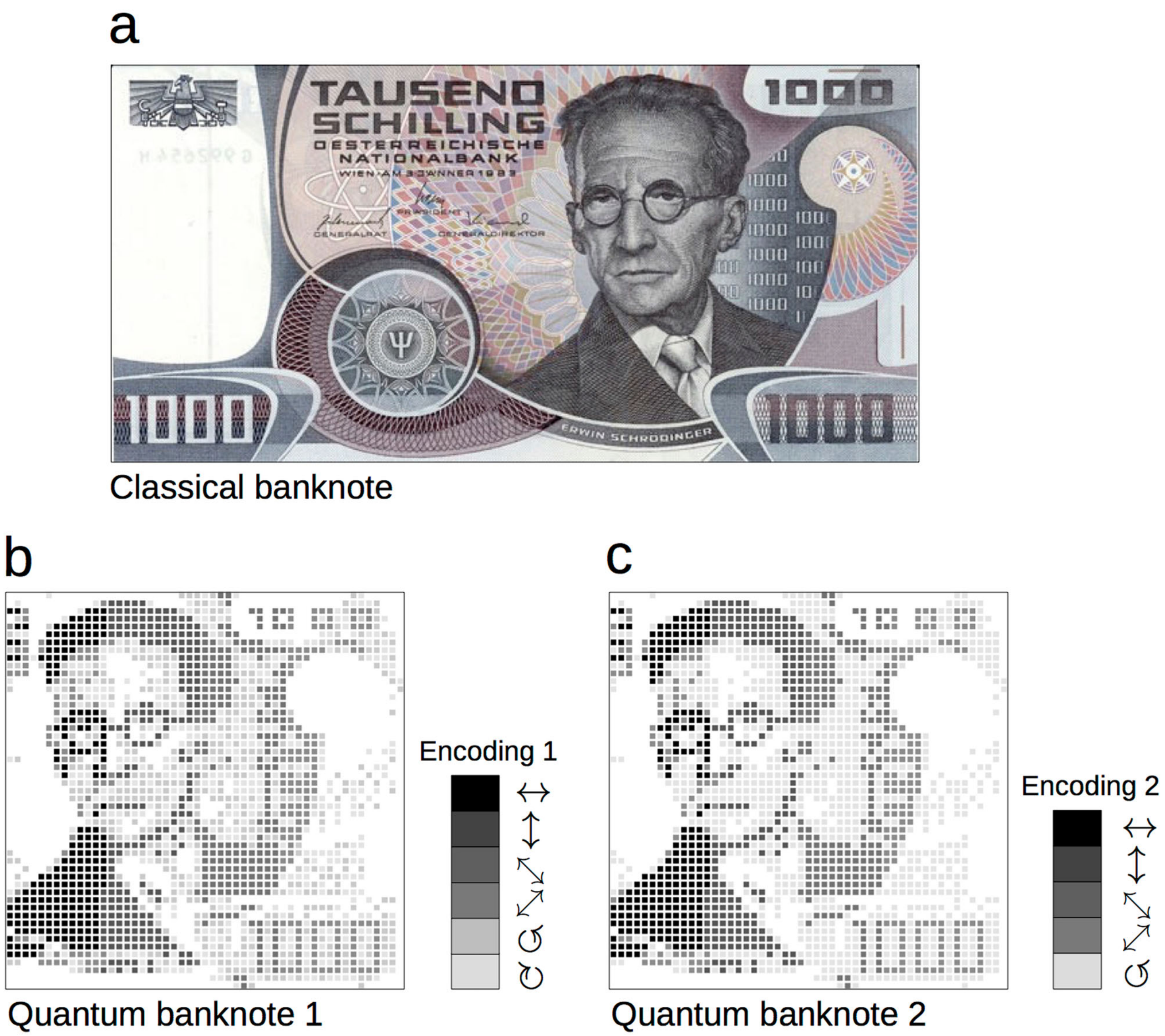

Fig. 1 An illustrative example of **a** a classical banknote. In panels **b** and **c**, the simplified banknote from panel **a** with the decreased number of colors and resolution is encoded experimentally in two ways to form two examples of quantum banknotes. The symbols used here correspond to different linear (↔, ↕, …) and circular (↺ and ↻) photon polarizations (as explained in the main text). Note that the white regions in **b** and **c** correspond to the lack of photons

qubit identity operator. The density matrices of both clones are identical and they read $\rho_i = \mathrm{Tr}_{\mathrm{in},i\oplus 1}[(\hat{\rho}^{\mathrm{T}} \otimes \mathbb{1}^{\otimes 2})\hat{\chi}]$, where we calculate the partial trace over the input qubit and one of the two clones (⊕ stands for sum modulo 2).

The average single-copy fidelity written in a compact form reads

$$F = \mathrm{Tr}\,(\hat{R}\hat{\chi}). \tag{6}$$

In order to find the optimal cloning map $\hat{\chi}$, one needs to compute the $\hat{R}$ operator defined as

$$\hat{R} = \frac{1}{2}\int_{\Omega} g(\theta,\phi)\,\hat{\rho}^{\mathrm{T}} \otimes (\hat{\mathbb{1}} \otimes \hat{\rho} + \hat{\rho} \otimes \hat{\mathbb{1}})\,\mathrm{d}\Omega. \tag{7}$$

Remarkably, we show in the Methods that this operator depends only on its five expansion coefficients of g in the basis of spherical harmonics, regardless of the exact form of g. The optimal map $\hat{\chi}$ is found by maximizing F in Eq. (6) for a given $\hat{R}$ with the optimization algorithm described in ref. 29 (see also refs 18, 25–27, 32).

The output distribution g_{out} of the cloned qubits will differ from g, because perfect cloning is impossible. Each cloning machine prepares a perfect clone (1), with probability equal to the fidelity F_i, and an orthogonal state (2), with probability $1-F_i$. Thus, the distribution $g_{\mathrm{out}}(\theta,\phi)$ of the cloned qubit states can be expressed as

$$g_{\mathrm{out}}(\theta,\phi) = F_i(\theta,\phi)g(\theta,\phi) + [1 - F_i(\theta+\pi,\phi+\pi)]g(\theta+\pi,\phi+\pi). \tag{8}$$

There is no difference between g and g_{out}, if the function is symmetric with respect to inverting the directions of the Bloch sphere. This includes the scenarios both for the best case (a uniform qubit distribution) and the worst case (a sequence of distinguishable states). The class of such distributions defines the so-called mirror phase-covariant cloner (or cloning) (MPCC).[26] Note that the MPCC is a generalization of the phase-covariant cloners (PCCs), which enable optimal copying of a qubit state from the equator of the Bloch sphere[33] or other states on the Bloch sphere with a definite angle θ (see refs 25, 34) (see the Supplementary Information for more theoretical details on optimal axially-symmetric quantum cloners together with some additional experimental data, and about the MPCC and PCC). The output distribution cannot be used directly to quantify the quality of the clones, because it does not carry the information about the order of states in a given sequence.

The analyzed sequence would usually contain some additional noise due to small random polarization rotations caused by various imperfections. These include state preparation, distribution, storage, and finally delivery and analysis. In practice, all these imperfections lead to the average sequence fidelity $F_{\text{pass}} < 1$ with respect to the ideally-performed qubit preparation, storage, and detection steps.

For simplicity, we assume that all the enlisted protocol elements are perfect, except the final step of our state analysis. If this final step is the polarization analysis of single photons with standard detectors and a polarization beam splitter, we have $F_{\text{pass}} \approx 98\%$. Here, we model the joint dispersion of the transmission channel and the state verification with respect to the target polarization by the spherical dispersion model on a sphere given by the von Mises-Fisher distribution[35] (i.e., the Gaussian distribution on a sphere)

$$f(\kappa, \alpha) = \frac{\exp(\kappa \cos \alpha)}{2\pi I_0(\kappa)}, \tag{9}$$

which is the probability density function of any qubit prepared in a target state given by its Bloch vector being rotated by an angle α. The level of concentration of the density function around the state vector $|\psi\rangle$ is given by the parameter κ. The density function is normalized with the modified Bessel function $I_0(\kappa)$.[36] From this model it follows that the probability of detecting a qubit described by the density matrix $\rho = |\psi\rangle\langle\psi|$ is equivalent to the average fidelity (6) and is given by

$$F_{\text{proc}}(\rho, \kappa) = \int_0^{\pi} \int_0^{2\pi} f(\kappa, \alpha) \langle \mu|\rho|\mu\rangle \, \mathrm{d}\delta \, \mathrm{d}\alpha, \tag{10}$$

where $|\mu\rangle = \cos(\frac{\theta-\alpha}{2})|\psi\rangle + \exp(i\delta)\sin(\frac{\theta-\alpha}{2})|\psi_\perp\rangle$. For example, our direct calculations for $\alpha = 0$ lead to $F_{\text{proc}}(\theta, \kappa) = [2\kappa \cos\theta \cosh\kappa + \pi\kappa I_1(\kappa)\sin\theta + 2(\kappa - \cos\theta)\sinh\kappa)]/(4\kappa \sinh\kappa)$, where I_1 is the modified Bessel function.[36] Thus, for the QMS to be feasible, we need to accept those sequences with fidelity $F_{\text{pass}} = F_{\text{proc}}(|\psi\rangle\langle\psi|, \kappa_0)$. Hence, κ_0 describes the minimum resolution required to reveal an attack using a cloner with a given value of F_{pass}. The value of κ_0 can be derived numerically from the fixed value of F_{pass} corresponding to the fidelity of polarization analysis. For a single qubit, we can use the following security condition $F_{\text{proc}}(\rho_i, \kappa) < F_{\text{pass}}$, where now κ describes the dispersion of the channel used by the counterfeiter to deliver the copied sequence. If this condition is satisfied, the counterfeiter cannot cheat the verification process. The verification process is performed on the full sequence of qubits. Therefore, any verification process that allows for some implementation imperfections should depend on the average verification fidelity. For a long sequence of cloned qubits this average fidelity is

$$\overline{F}_i(\kappa) = \int_\Omega g(\theta, \phi) F_{\text{proc}}(\rho_i, \kappa) \, \mathrm{d}\Omega, \tag{11}$$

whereas for the verification threshold reads as

$$\overline{F}_{\text{pass}}(\kappa_0) = \int_\Omega g(\theta, \phi) F_{\text{pass}}(\theta, \phi) \, \mathrm{d}\Omega. \tag{12}$$

These values can be obtained by projecting the delivered quantum banknote on the associated sequence of bases. These can be approximated as the ratios of the number of the correctly projected states to the number of the conclusive state projections. A quantum banknote passes the verification process if $\overline{F}_i > \overline{F}_{\text{pass}}$. These quantities (used in this inequality) depend implicitly on the choice of g as the quality of the optimally-counterfeited state depends on g, specifically on its five expansion coefficients in terms of spherical harmonics, i.e., five real numbers that could be estimated by the counterfeiter after measuring some random parts of the banknote. Thus, in the following text, we assume that g is publicly known. We demonstrate experimentally that this weakness could be exploited by a counterfeiter.

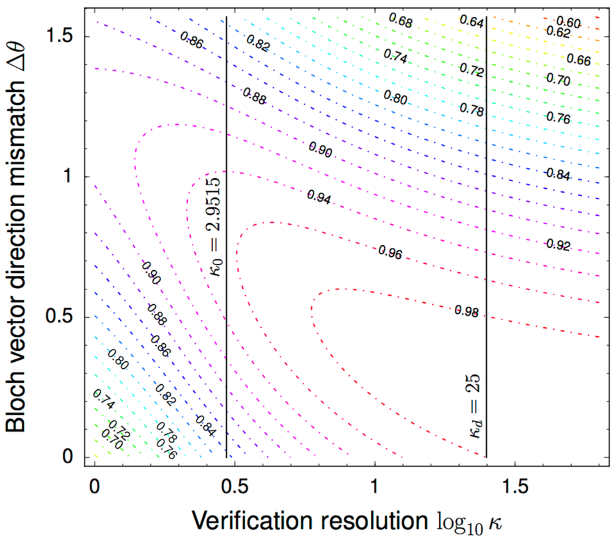

Fig. 2 Contour plot showing how the probability of detecting a qubit of an unknown state $|\psi(\theta, \phi)\rangle$ for money verification depends on the imperfect choice of the measurement direction $\Delta\theta$ and the photon verification (or discrimination) resolution κ. Specifically, this probability is equivalent to the fidelity $F_{\text{proc}}(\Delta\theta, \kappa)$ for which the Bloch vector is rotated with respect to its correct orientation by $\Delta\theta$ for a given value of κ. Note that the probability does not depend on θ or ϕ, but only on $\Delta\theta$, which measures the angle between the original and rotated Bloch vectors. The *solid black lines* mark two specific values of κ: $\kappa_0 = 2.9515$ describes the minimal resolution needed to detect an attack with an optimal universal cloning machine and $\kappa_d = 25$ corresponds to the resolution reached in our experiment. Note that the shape of the depicted relation depends on the dispersion function of the detector. Here, this function is chosen as the von Mises-Fisher distribution

Let us consider the situation where the security threshold is given by a theoretical value of $\overline{F}_i$, where $\kappa \to \infty$, which does not take into account the threat of the counterfeiter using the knowledge about g. In this case, one would naively assume that the forgery cannot lead to the fidelity $\overline{F}_i$ exceeding 5/6, corresponding to the fidelity of the universal cloning machine.[28] It would appear that using the security threshold of $\overline{F}_{\text{pass}} = 5/6$ might be a good idea, as it makes the QMS more robust against errors. This means that one could naively allow the resolution of the verification process κ_0 to be as small as $\kappa_0 = 2.9515$. This value is obtained from $F_{\text{proc}}(0, \kappa_0) = 5/6$. To illustrate that this could be a problem, let us imagine that we verify qubits described by the Bloch vectors rotated by an angle $\Delta\theta$ from the Bloch vectors of the expected states. In Fig. 2, we see that the measured fidelity $F_{\text{proc}}(\Delta\theta, \kappa_0)$ would be seemingly above the security threshold even for $\Delta\theta \approx \pi/2$, which means that the verification process would recognize a large volume of pure states as valid. However, it would not accept the states for which the Bloch vectors are rotated by more that 90° from the target Bloch vectors. In this regime, we are approaching the situation where any state prepared in a basis, which is unbiased with respect to the verification basis, would pass the verification process. The counterfeiter can guess the conjugate basis correctly with probability 2/3 and choose the correct state in the matching basis with probability 1/6. This means that 83% of an arbitrary banknote prepared by the counterfeiter is accepted and the QMS is broken. Fortunately, this is not exactly the case as

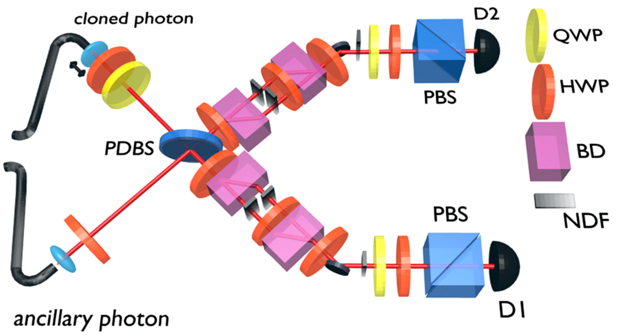

Fig. 3 Experimental setup for cloning quantum bankotes. Components are labeled as follows: HWP is half-wave plate, QWP is quarter wave-plate, PDBS is polarization dependent-beam splitter, PBS is polarizing beam splitter, BD is beam divider, NDF is neutral density filter, and D is single photon detector. A successful cloning and verification of a qubit from a given sequence is registered as a simultaneous detection event at the two detectors

$F_{\text{proc}}(\pi/2, 2.9515) = 0.8115 < 5/6$. Note that this could be dangerous if the dispersion of the state verification would not be described with the von Mises-Fisher distribution, but with some similar function. Thus, for the low resolution regime of $\kappa_0 \approx 2.9515$ the full characterization of the verification setup is required in order to exclude this classical attack.

The detection resolution κ_d of a given experimental setup should be as large as possible. In our experiment we achieved $\kappa_d = 25$, which is obtained from $F_{\text{proc}}(0, \kappa_d) = 0.98$. Even if the detection resolution is perfect $\kappa_0 \to \infty$, the quantum money can be counterfeited using a specialized quantum cloner optimized for g. In the following section we illustrate this with an experiment.

Experimental quantum forgery

Let us consider cloning the quantum banknote 1 from Fig. 1, where single-photon polarization states appear approximately with the following probabilities: $p(⤡) = 0.125$, $p(⤢) = 0.125$, $p(\updownarrow) = 0.125$, $p(\leftrightarrow) = 0.125$, $p(↺) = 0.25$, $p(↻) = 0.25$, where the poles of the Bloch sphere correspond to the left-circular (↺) and right-circular (↻) polarization states, while the equatorial plane is spanned by the horizontal (↔), vertical (↕), diagonal (⤡), and anti-diagonal (⤢) polarization states. In this case the optimal cloning machine is an axially-symmetric PCC [27] corresponding to the MPCC.[26] The probability distribution is described here with only one nonzero number, i.e., $c_{2,0} = 0.25(5\pi)^{1/2}$ (using the notation from ref. 27: $a_2 = c_{2,0}/(5\pi)^{1/2}$ and $|\Gamma| = 0$). The fidelity of copying the equatorial states is then equal to $F(\leftrightarrow) = F(\updownarrow) = F(⤡) = F(⤢)=0.789$ and $F(↺) = F(↻) = 0.894$ for the pole states. This results in the theoretical value of $\overline{F}_i(\kappa \to \infty) = 0.842$, which is a bit above the security threshold of $\overline{F}_i = 0.833$. Using our experimental setup shown in Fig. 3, we achieve $\overline{F}_{i,\text{experiment}} = (81.9 \pm 2.0)\%$. This experimental value is close to the universal cloning limit, i.e., $\overline{F}_i = 0.833$. In this case, only $(14.0 \pm 2.9)\%$ of the sequence was successfully copied. Alternatively, when we attack this banknote with our implementation of the optimal universal cloner, we obtain $\overline{F}_{i,\text{experiment}} = (81.5 \pm 1.2)\%$; and $(19.6 \pm 1.2)\%$ of qubits are copied. This makes the forgery unsuccessful for two reasons: (i) the quality of the delivered qubits is lower than allowed, (ii) we delivered less than 50% of the sequence to each recipient. More than 50% of the qubits have to be delivered to exclude the possibility of duplicating the money by cutting it into pieces. However, the forgery becomes successful if one uses the optimal quantum cloning process, with high fidelity but low success rate, interchangeably with a classical cloning process, with high success rate but low fidelity.

Let us consider another case, where we can crack the QMS and the quantum banknote 2 from Fig. 1 is described with the following probabilities: $p(⤡) = 0.125$, $p(⤢) = 0.125$, $p(\updownarrow) = 0.125$, $p(\leftrightarrow) = 0.125$, $p(↺) = 0.50$, and $p(↻) = 0$. In this case the optimal cloning machine is also an axially-symmetric (phase-covariant) cloner[27] (ASC), where $c_{1,0} = 0.5(3\pi)^{1/2}$, $c_{2,0} = 0.25(5\pi)^{1/2}$, which corresponds to $a_1 = 0.5$, $a_2 = 0.25$, and $|\Gamma| = \infty$, using the notation from ref. 27. We have falsified this banknote by applying interchangeably both the optimal classical and the best quantum copying strategies (see ref. 32). The optimal classical copying can be viewed as measuring a fraction ε of the original photons from the sequence in a random basis (selected according to g) and preparing two photons in the detected state. We implemented this strategy by randomly swapping a fraction of photons from the original sequence with the circularly-polarized photons selected in accord with g (for details see the Methods). The fidelity of this strategy is $(3 + \langle \cos\theta \rangle^2)/4 = (3 + a_1^2)/4$. We used this optimal classical strategy with probability $\varepsilon = 0.4$. Using this method, we implemented a cloning attack, which copies circa $(54.9 \pm 0.1)\%$ of the sequence (this means that we could sacrifice about 4% of the sequence to estimate g). Our implementation of the optimal quantum copying strategy allows us to copy $24.8 \pm 0.1\%$ of the sequence with a fidelity of $(92.4 \pm 0.4)\%$ (the theoretical value is 92.6%). The optimal classical copying strategy[32] operated with fidelity circa 81.3%. This provides us with the experimental average cloning fidelity of $\overline{F}_{i,\text{experiment}} = 0.842 \pm 0.002$. Thus, we demonstrated that it is possible to crack the Wiesner QMS with currently available technology. However, this was possible only because the incoming sequence of photons was synchronized with the probing photons allowing them to interact on a beam splitter. The counterfeiter would face some additional technical challenges when applying the discussed copying method in real life (see the discussion in ref. 18). This cloning regime, where the cloning process happens with a fidelity larger than the fidelity of the best classical copying process, and the transmitted qubits are successfully copied with a probability larger than 50%, can also be applied constructively to increase the classical product capacity of a quantum channel.[32]

The experimental results of the above-discussed copying strategies for the two experimental quantum banknotes are summarized in Fig. 4. Moreover, in Figs 5, 6 we demonstrate how the measured success probability of the cloning process and the corresponding single-copy fidelity depend on the value of the hybridization parameter ε. The selected values of this parameter correspond to optimal classical ($\varepsilon = 1$), hybrid ($\varepsilon = 0.4$), and optimal quantum cloning ($\varepsilon = 0$). The significant reduction of variance in these figures with respect to purely quantum cloning ($\varepsilon = 0$) is caused by using a robust classical copying process interchangeably with a more delicate optimal quantum cloning strategy (for details see the Methods).

DISCUSSION

We demonstrated that using currently available technology we are able to both implement and crack the original QMS of Wiesner.[1] given that (i) a sequence of qubits, representing the quantum banknote is not sampled uniformly over the Bloch sphere, (ii) the banknote is considered valid if more than 50% of the sequence is delivered and its average fidelity is above the fidelity of the universal cloner.[28] i.e., 83.3%. From our results it follows that to make the Wiesner QMS secure against copying, one should apply a g-dependent verification threshold, which corresponds to the average single-copy fidelity of the relevant optimal quantum cloner. We have shown that a specialized optimal cloner for an arbitrary qubit distribution g can easily be found by computing only its five parameters and subsequently applying the optimization procedure described in ref. 29. We believe that our results will

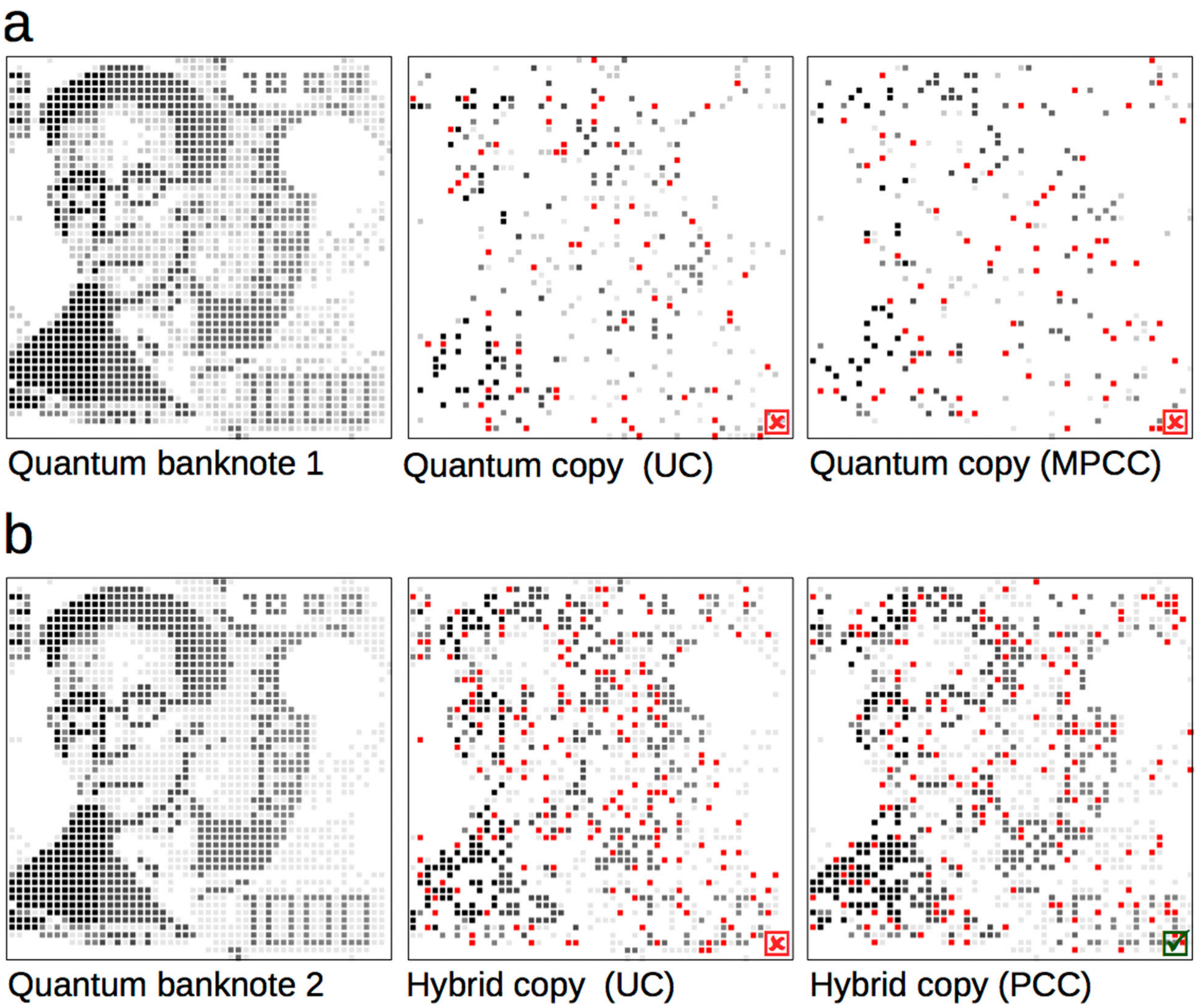

Fig. 4 Experimental quantum banknotes 1**a** and 2**b** are copied probabilistically with an optimal 1-to-2 linear optical cloning machine shown in Fig. 3 and subsequently verified. This device can be tuned to implement, in special cases, the UC, the PCC, and the MPCC. Note that the white regions in quantum banknotes, or their copies, correspond to either a lack of photons or the cases where the cloning process failed to deliver one photon per banknote. One observes that the copies, which are provided with the best possible cloning machines, are noisy and, thus, the sequences of qubits are damaged (shown in red). The performance of a given cloning process depends on the statistics of photon polarizations. Thus, the copies of quantum banknote 1**a** obtained by an optimal purely-quantum cloner (the UC and MPCC) fail the verification. The copies of banknote 2**b** obtained by an optimal hybrid (i.e., quantum-classical) cloner fail the verification if the UC is used, but pass the verification if the PCC is applied

stimulate further research on secure quantum communication and quantum technologies.

METHODS

Theory

In our theoretical considerations we apply the spherical harmonics[36] Y_l^m for $l=0,1,2$ and $m=0,1,...,l$. The spherical harmonics for $m<0$ are simply related to these for $m>0$, because

$$Y_l^m=(-1)^m\overline{Y}_l^{-m}. \tag{13}$$

The operator $\hat{R}$, in terms of the spherical harmonics $Y_{l,m}$, can be expressed as

$$\hat{R}=\sum_{l=0}^{2}\sum_{m=-l}^{l}\hat{K}_{l,m}c_{l,m}\,, \tag{14}$$

where

$$\hat{K}_{l,m}=\frac{1}{2}\int_\Omega\hat{\rho}^{\mathrm{T}}\otimes(\widehat{\mathbb{1}}\otimes\hat{\rho}+\hat{\rho}\otimes\widehat{\mathbb{1}})\overline{Y}_l^m(\theta,\phi)\,\mathrm{d}\Omega\,, \tag{15}$$

the bar denotes complex conjugation, and

$$c_{l,m}=\int_\Omega g(\theta,\phi)Y_l^m(\theta,\phi)\,\mathrm{d}\Omega. \tag{16}$$

It can be directly shown that

$$\hat{\rho}^{\mathrm{T}}\otimes(\widehat{\mathbb{1}}\otimes\hat{\rho}+\hat{\rho}\otimes\widehat{\mathbb{1}})=2\sum_{l=0}^{2}\sum_{m=-l}^{l}\hat{K}_{l,m}Y_l^m(\theta,\phi)\,, \tag{17}$$

hence, we do not need terms with $l>2$. For a real-valued distribution g we obtain

$$c_{l,m}=(-1)^m\overline{c}_{l,-m}. \tag{18}$$

This property follows from the definition of the spherical harmonics. Thus, for the normalized g distributions one computes $c_{l,m}$ only for $l=1,2$ and $m=0,1,...,l$, which results in five integrals in total. Depending on the symmetry of the distribution g, some of the integrals vanish, which simplifies further calculations. The expansion coefficients $\hat{K}_{l,m}$ can be written in the form of block matrices as given in the Supplementary Information. (see Supplementary Information for more theoretical details on optimal axially-symmetric quantum cloners together with some additional experimental data).

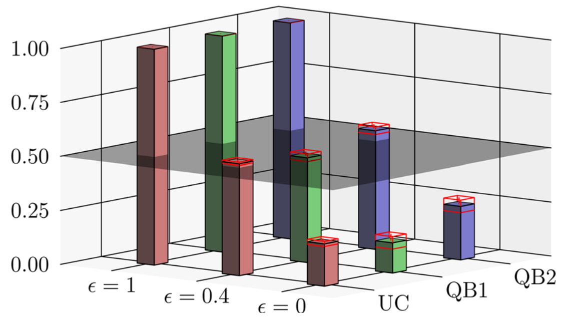

Fig. 5 Success probabilities of the cloning processes for quantum banknotes 1 and 2 (QB1 and QB2), and optimal universal cloning (UC). The red frames show the error bars of the measured probabilities. The gray surface shows the minimum cloning efficiency needed to output on average more cloned photons than the input photons

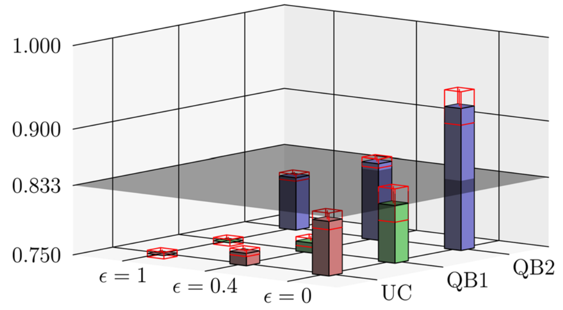

Fig. 6 Experimentally measured average cloning fidelity $\overline{F}_i$ for quantum banknotes 1 and 2 (QB1 and QB2), and optimal universal cloning (UC). The red frames show the error bars of the measured probabilities. The verification threshold (gray surface) is set at 0.833, which is the fidelity of the optimal universal cloning process, i.e., the process that ignores any information about g

Experiment

The experimental setup is depicted in Fig. 3. Pairs of photons were generated in the process of spontaneous parametric down-conversion using a LiIO$_3$ crystal pumped by 200 mW of cw Kr$^+$ laser beam at 413 nm. Hundreds of photon pairs were collected using single-mode fibers and transferred to the input of the cloner setup. One photon of each pair (i.e., a cloned photon) was used to encode a bit of quantum information into its polarization state, while the other photon served as an ancilla being either horizontally or vertically polarized. In the next step, the cloned and ancillary photon interfere on a polarization-dependent beam splitter (PDBS). Ideally, this beam splitter should transmit the horizontally-polarized light with intensity transmissivity of 0.789 and the vertically-polarized light with intensity transmissivity of 0.211. Due to manufacturing errors, the real intensity transmissivities of our PDBS are 0.76 and 0.18 for horizontal and vertical polarizations, respectively. To correct for this deviation between the real and ideal PDBS parameters, a beam divider assembly (BDA) is inserted into each output mode of the PDBS. This BDA consists of two beam displacers separating and subsequently rejoining horizontal and vertical polarization components of photons wave packets. By inserting a neutral-density filter (NDF) into either a horizontal or vertical polarization mode inside the BDA, one can achieve polarization sensitive losses and, thus, compensate for incorrect parameters of the PDBS. Note that this compensation can restore an ideal operation of the PDBS at the expense of a lower success rate. To balance the rate of the cloned and ancillary photons, some additional NDFs can be placed behind the BDAs. Finally, both the cloned and ancillary photons are subjected to our polarization analysis consisting of a set of quarter-wave (QWP) and half-wave (HWP) plates followed by a polarizing prism.[37] The coincident photon detections are counted for each combination of the polarization projection onto the horizontal, vertical, diagonal, anti-diagonal, and both circular polarizations. The density matrices of the corresponding two-photon states are then estimated using a maximum-likelihood algorithm.[38] A more detailed account on the experimental procedure is available in our technical paper.[39] The swapping procedure used for the optimal classical copying strategy was implemented with the setup shown in Fig. 3 by removing the PDBS and filters used in the BDAs. We applied the following hybrid quantum-classical cloning procedure: Initially, we prepared the best classical replacement for $\rho = |\psi\rangle\langle\psi|$, i.e., $\hat{\sigma} = \int_\Omega g|\psi\rangle\langle\psi|\, d\Omega$ in the ancillary mode and randomly swapped it with the input state $\hat{\rho}$ for a fraction ε of the input photons. For the remaining $1 - \varepsilon$ photons we performed the relevant optimal quantum cloning. When properly tuned, this procedure is far less noisy than the implementation of pure quantum cloning and, thus, the quality (described by, e.g., the dispersion of the fidelity) of this hybrid cloning procedure depends mostly on the quality of the quantum cloning process (see Figs 5, 6).

ACKNOWLEDGEMENTS

We gratefully acknowledge the financial support of the Polish National Science Centre under grant DEC-2013/11/D/ST2/02638 (K.B., K.L.) and the support by the GAČR grants No. 16-10042Y (K.B., K.L.) and No. P205/12/0382 (AČ). F.N. is partially supported by the RIKEN iTHES Project, MURI Center for Dynamic Magneto-Optics, JSPS-RFBR contract no. 12-02-92100, JST-IMPACT, CREST, and a Grant-in-Aid for Scientific Research (A). AM and FN acknowledge the support of a grant from the John Templeton Foundation.

AUTHOR CONTRIBUTIONS

K.B. developed the theoretical framework, planned the experiment, processed the experimental results, and wrote the paper together with A.M. A.Č. and K.L. designed and built the experimental setup, and performed the measurements. Figures were prepared by G.C. and A.Č. The idea of this paper was proposed by K.B. and A.M. All authors discussed the results and participated in the manuscript preparation. Theoretical aspects corresponding author is K.B. (email: bark@amu.edu.pl). Experimental aspects corresponding authors are A.Č (email: acernoch@fzu.cz) and K.L (email: k.lemr@upol.cz).

COMPETING INTERESTS

The authors declare that they have no competing interests.

REFERENCES

1. Wiesner, S. Conjugate coding. *ACM SIGACT News* **15**, 78–88 (1983). Original manuscript written circa 1970.
2. Bennett, C. H., Brassard, G., Breidbart, S. & Wiesner, S. Quantum cryptography, or unforgeable subway tokens. In *Advances in Cryptology: Proc. Crypto 82.* (eds David Chaum, Ronald, L. Rivest & Alan T. Sherman), 267–275 (Springer, 1983).
3. Bennett Ch, H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 175–179 (IEEE, New York, 1984).
4. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).
5. Lo, H.-K., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nat. Photonics* **8**, 595–604 (2014).
6. Jones, N. Computing: the quantum company. *Nature* **498**, 286–288 (2013).
7. Georgescu, I. & Nori, F. Quantum technologies: an old new story. *Physics World* **25**, 16 (2012).
8. Buhrman, H., Cleve, R., Watrous, J. & de Wolf, R. Quantum fingerprinting. *Phys. Rev. Lett.* **87**, 167902 (2001).
9. Barnum, H., Crépeau, C., Gottesman, D., Smith, A. & Tapp, A. Authentication of quantum messages. In *43th Annual IEEE Symposium on Foundations of Computer Science*, (ed. Danielle, C.) 449–458 (IEEE, 2002).
10. Tokunaga, Y., Okamoto, T. & Imoto, N. Anonymous quantum cash. In *ERATO Conference on Quantum Information Science—EQIS' 03* (2003).
11. Mosca, M. & Stebila, D. In *Error-Correcting Codes, Finite Geometries and Cryptography* Vol. 523 of *Contemp. Math.*, 35–47 (Amer. Math. Soc., 2010).
12. Farhi, E., Gosset, D., Hassidim, A., Lutomirski, A. & Shor, P. Quantum money from knots. In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference, ITCS '12*, 276–289 (ACM, 2012).
13. Lutomirski, A. *et al.* Breaking and making quantum money: toward a new quantum cryptographic protocol. In *Proc. Innovations in Computer Science, ICS 2010*, (ed. Andrew Chi-Chih Yao) 20–31 (Tsinghua, 2010).
14. Lutomirski, A. An online attack against Wiesner's quantum money. *arXiv:1010.0256* (2010).

15. Pastawski, F., Yao, N. Y., Jiang, L., Lukin, M. D. & Cirac, J. I. Unforgeable noise-tolerant quantum tokens. *Proc. Natl. Acad. Sci. USA* **109**, 16079–16082 (2012).
16. Aaronson, S. & Christiano, P. Quantum money from hidden subspaces. *Theory Comput.* **9**, 349–401 (2013).
17. Molina, A., Vidick, T. & Watrous, J. Optimal counterfeiting attacks and generalizations for Wiesner's quantum money. In *Theory of Quantum Computation, Communication, and Cryptography: 7th Conference, TQC 2012*, 45–64 (Springer, 2013).
18. Bartkiewicz, K., Lemr, K., Černoch, A., Soubusta, J. & Miranowicz, A. Experimental eavesdropping based on optimal quantum cloning. *Phys. Rev. Lett.* **110**, 173601 (2013).
19. Sasaki, T., Yamamoto, Y. & Koashi, M. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature* **509**, 475–478 (2014).
20. Takesue, H., Sasaki, T., Tamaki, K. & Koashi, M. Experimental quantum key distribution without monitoring signal disturbance. *Nat. Photonics* **9**, 827–831 (2015).
21. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145–195 (2002).
22. Bartkiewicz, K., Černoch, A. & Lemr, K. Using quantum routers to implement quantum message authentication and Bell-state manipulation. *Phys. Rev. A* **90**, 022335 (2014).
23. Wootters, W. K. & Zurek, W. H. A single quantum cannot be cloned. *Nature* **299**, 802–803 (1982).
24. Dieks, D. Communication by EPR devices. *Phys. Lett. A* **92**, 271–272 (1982).
25. Fiurášek, J. Optical implementations of the optimal phase-covariant quantum cloning machine. *Phys. Rev. A* **67**, 052314 (2003).
26. Bartkiewicz, K., Miranowicz, A. & Özdemir, Ş. K. Optimal mirror phase-covariant cloning. *Phys. Rev. A* **80**, 032306 (2009).
27. Bartkiewicz, K. & Miranowicz, A. Optimal cloning of qubits given by an arbitrary axisymmetric distribution on the Bloch sphere. *Phys. Rev. A* **82**, 042330 (2010).
28. Bužek, V. & Hillery, M. Quantum copying: beyond the no-cloning theorem. *Phys. Rev. A* **54**, 1844–1852 (1996).
29. Fiurášek, J. Extremal equation for optimal completely positive maps. *Phys. Rev. A* **64**, 062310 (2001).
30. Audenaert, K. & De Moor, B. Optimizing completely positive maps using semi-definite programming. *Phys. Rev. A* **65**, 030302 (2002).
31. Jamiołkowski, A. Linear transformations which preserve trace and positive semidefiniteness of operators. *Rep. Math. Phys.* **3**, 275–278 (1972).
32. Bartkiewicz, K., Černoch, A., Lemr, K., Soubusta, J. & Stobińska, M. Efficient amplification of photonic qubits by optimal quantum cloning. *Phys. Rev. A* **89**, 062322 (2014).
33. Bruß, D., Cinchetti, M., D'Ariano, M. G. & Macchiavello, C. Phase-covariant quantum cloning. *Phys. Rev. A* **62**, 012302 (2000).
34. Karimipour, V. & Rezakhani, A. T. Generation of phase-covariant quantum cloning. *Phys. Rev. A* **66**, 052111 (2002).
35. Fisher, R. Dispersion on a sphere. *Proc. R. Soc. A* **217**, 295–305 (1953).
36. Arfken, G. *Mathematical Methods for Physicists* 3rd edn, Ch. 11.5, 12.6 and 12.9 (Academic Press, 1985).
37. Halenková, E., Černoch, A., Lemr, K., Soubusta, J. & Drusová, S. Experimental implementation of the multifunctional compact two-photon state analyzer. *Appl. Opt.* **51**, 474–478 (2012).
38. Ježek, M., Fiurášek, J. & Hradil, Z. Quantum inference of states and processes. *Phys. Rev. A.* **68**, 012305 (2003).
39. Lemr, K., Bartkiewicz, K., Černoch, A., Soubusta, J. & Miranowicz, A. Experimental linear-optical implementation of a multifunctional optimal qubit cloner. *Phys. Rev. A* **85**, 050307 (2012).

Supplementary Information accompanies the paper on the *npj Quantum Information* website (doi:10.1038/s41534-017-0010-x).