Free-Space Quantum Signatures Using Heterodyne Measurements

Free-Space Quantum Signatures Using Heterodyne Measurements

Callum Croal,[1] Christian Peuntinger,[2,3,4] Bettina Heim,[2,3] Imran Khan,[2,3] Christoph Marquardt,[2,3] Gerd Leuchs,[2,3] Petros Wallden,[5] Erika Andersson,[6] and Natalia Korolkova[1]

[1]*School of Physics and Astronomy, University of St. Andrews, North Haugh, St. Andrews, Fife KY16 9SS, Scotland*
[2]*Max Planck Institute for the Science of Light, Günther-Scharowsky-Str. 1/Building 24, 91058 Erlangen, Germany*
[3]*Institute of Optics, Information and Photonics, University of Erlangen-Nuremberg, Staudtstraße 7/B2, 91058 Erlangen, Germany*
[4]*Department of Physics, University of Otago, 730 Cumberland Street, Dunedin 9016, New Zealand*
[5]*School of Informatics, University of Edinburgh, 10 Crichton Street, Edinburgh EH8 9AB, United Kingdom*
[6]*SUPA, Institute of Photonics and Quantum Sciences, School of Engineering and Physical Sciences, Heriot-Watt Universiity, David Brewster Building, Edinburgh EH14 4AS, United Kingdom*

(Received 13 April 2016; published 2 September 2016)

Digital signatures guarantee the authorship of electronic communications. Currently used "classical" signature schemes rely on unproven computational assumptions for security, while quantum signatures rely only on the laws of quantum mechanics to sign a classical message. Previous quantum signature schemes have used unambiguous quantum measurements. Such measurements, however, sometimes give no result, reducing the efficiency of the protocol. Here, we instead use heterodyne detection, which always gives a result, although there is always some uncertainty. We experimentally demonstrate feasibility in a real environment by distributing signature states through a noisy 1.6 km free-space channel. Our results show that continuous-variable heterodyne detection improves the signature rate for this type of scheme and therefore represents an interesting direction in the search for practical quantum signature schemes. For transmission values ranging from 100% to 10%, but otherwise assuming an ideal implementation with no other imperfections, the signature length is shorter by a factor of 2 to 10. As compared with previous relevant experimental realizations, the signature length in this implementation is several orders of magnitude shorter.

DOI: 10.1103/PhysRevLett.117.100503

Digital signatures [1] are ubiquitous in electronic communication, used in, for example, Email and digital banking. They guarantee the provenance, integrity, and transferability of messages. Currently used classical digital signature schemes, however, rely on unproven computational assumptions [2], and may become insecure especially if quantum computers can be built [3]. Quantum digital signatures (QDSs) [4–10], on the other hand, give information-theoretic security [7], loosely speaking based on the fact that nonorthogonal quantum states cannot be perfectly distinguished from each other.

The first quantum signature schemes assumed tamper-proof, "authenticated" quantum communication links. Intuitively, this could be accomplished using parameter estimation techniques similar to those used in quantum key distribution (QKD). How to achieve this was explicitly shown only recently [10,11]. In addition, recent quantum signature schemes [6,9], including our protocol, do not require long-term quantum memory. Importantly, this means that quantum signatures can be implemented with current technology, essentially similar to QKD setups. "Classical" signature schemes with information-theoretic security also exist [12–14], but rely on secret shared keys, which could be accomplished using QKD. Quantum signature schemes may have some advantages over schemes relying on shared keys generated using QKD. In particular, the quantum bit error threshold for a signature scheme is in practice less strict than for distilling a secret shared key [11]. In addition, the required postprocessing is less demanding. Exactly what signature schemes are the most efficient, however, remains an open problem.

Note that most QDS protocols, including this one, use quantum states to sign a *classical message*. In fact, it is impossible to sign a quantum message [15] using a non-arbitrated scheme [16]. Arbitrated signing of quantum messages has previously been investigated [17–20].

Since messages may be forwarded between recipients, a signature protocol has at least three parties, a sender Alice and two recipients, Bob and Charlie. In QKD, the communicating parties Alice and Bob are assumed to be honest. In signature protocols, however, any of the involved parties could be dishonest. Signature schemes should be secure against forging (with high probability, only messages sent by Alice should be accepted) and against repudiation (it is unlikely that Alice could successfully deny having sent a message that she did send). Repudiation is closely related to message transferability. Transferability means that it is unlikely that one recipient accepts a message as genuine, but that this message then is rejected if it is forwarded to another recipient. If there is no trusted third party, one way to settle disputes is by majority voting. For three parties, which is the case we will consider, nonrepudiation and message transferability then become equivalent.

In principle, quantum signature schemes are based on a "quantum one-way function" which maps classical information (a "private key") to nonorthogonal quantum states (a "public key") [7]. In the simplest case, Alice wants to be able to, later on, send a one-bit message "0" or "1". For longer messages, the scheme could be suitably iterated. Generically, signature schemes have a *distribution stage*, where the scheme is set up, and a *messaging stage*, when messages are sent and received. The distribution stage could be compared to leaving a sample of a handwritten signature, e.g., when first opening a bank account. The messaging stage typically takes place much later. In our quantum signature scheme, the messaging stage is entirely classical.

In the distribution stage, Alice selects sequences of quantum states, one sequence for each possible future message 0 and 1. The states in the sequences are selected from some set of nonorthogonal quantum states. The classical information about what states Alice has selected forms her private keys for the possible messages 0 or 1. The quantum state sequences are the corresponding public keys. Alice then sends copies of the public key sequences to Bob and Charlie, who measure the states they receive. Since it is impossible to perfectly discriminate nonorthogonal quantum states, Bob and Charlie, or any other party, can never obtain full information about Alice's private keys.

Later on, in the messaging stage, when Alice wants to send a message to Bob or Charlie, she sends the message together with the corresponding private key. The recipient of a message checks that the appended private key sufficiently well matches the measurement results he obtained in the distribution stage for the respective message. In a real implementation, there will be mismatches even for a private key sent by an honest Alice. However, if imperfections are not too high, then anyone other than Alice would cause a higher level of mismatches than Alice. This guarantees security against message forging.

Similarly, to forward a message, a recipient forwards the message together with its private key, received from Alice, and the new recipient checks for mismatches with his measurement record. Related to this, Bob and Charlie also need to ensure that Alice cannot cheat, which would mean that she could make them disagree about the validity of a message. They achieve this by some kind of symmetrization procedure, done in the distribution stage [7,8,21]. In our protocol, as in Ref. [21], Bob and Charlie randomly forward half of their obtained measurement results to each other using a classical communication channel, secret from Alice. This channel could be realized using standard quantum key distribution. To ensure that Alice is unlikely to make Bob and Charlie disagree about the validity of a signature, the threshold for accepting a message directly from Alice should be stricter than for accepting a forwarded message. For more details see Ref. [22].

In this Letter, we implement a quantum signature scheme using continuous variable (CV) heterodyne quantum measurements. Previous quantum signature schemes [5,6,23] have instead used unambiguous quantum measurements. We demonstrate that our scheme is viable in a noisy environment using a free-space urban optical communication link. Finally, we show that, even when experimental imperfections are taken into account, this scheme outperforms a recent scheme that uses unambiguous state elimination measurements [23].

Our QDS scheme is represented in Fig. 1, with the protocol described below. The stages in the text correspond to the respective numbers in the figure. We use a discrete set of CV states, four phase-encoded coherent states $|\alpha\rangle$, $|i\alpha\rangle$, $|-\alpha\rangle$, $|-i\alpha\rangle$, and heterodyne CV measurements [24]. The same states were also used in previous QDS schemes [5,6,23] and are similar to those used in some types of CV QKDs [25,26]. In Refs. [5,6,23], however, recipients made "discrete" quantum measurements with error-free (unambiguous) results, at the expense of sometimes obtaining no result. Here we instead perform heterodyne measurements, which always give a result, at the expense of increased errors in the results. In many cases, unambiguous results are required for a protocol to perform efficiently [27,28]. Surprisingly, we find that for this particular QDS protocol, heterodyne measurements provide an advantage.

Distribution stages 1–4.—(1) For each possible future one-bit message $k = 0, 1$, Alice generates two identical copies of sequences of phase-encoded coherent states, $\mathrm{QuantSig}_k = \otimes_{l=1}^{L} |\psi_l^k\rangle\langle\psi_l^k|$, where $|\psi_l^k\rangle$ is a randomly chosen phase-encoded coherent state, $|\psi_l^k\rangle = |\alpha e^{i\phi_l^k}\rangle$, $\phi_l^k \in \{0, \pi/2, \pi, 3\pi/2\}$, and L is a suitably chosen integer. The state $\mathrm{QuantSig}_k$ is called the quantum signature, and the sequence of phases $\mathrm{PrivKey}_k = (\phi_1^k, \ldots, \phi_L^k)$ is called the private key.

(2) Alice sends one copy of $\mathrm{QuantSig}_k$ to Bob and one to Charlie, for each possible message $k = 0$ and $k = 1$.

(3) Bob (Charlie) measures the states received from Alice by performing a heterodyne detection [24,29] of the $\hat{x}$ and $\hat{p}$ quadrature. He records the result of the measurement and the associated position in the sequence l. For each quadrature, the sign of the measured result determines

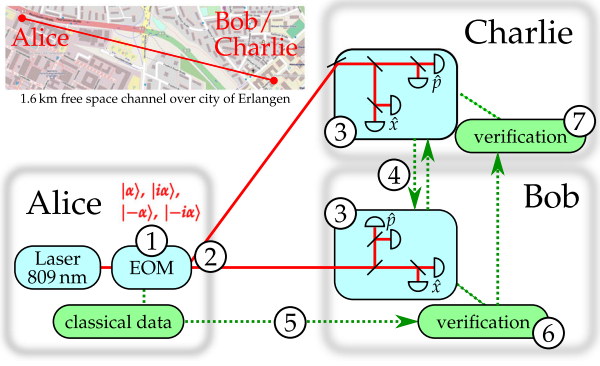

FIG. 1. Depiction of the scheme. The numbered parts relate to the corresponding stages in the main text. Green dashed lines indicate classical communication. Red lines indicate communication with quantum states.

which state is eliminated. For example, if a positive result is measured, then the state $|-\alpha\rangle$ or $|-i\alpha\rangle$ is eliminated, depending on the measured quadrature. In this way, Bob (Charlie) eliminates two states, one for each quadrature, for each signature element.

(4) Symmetrization: Bob (Charlie), for each element l of $\mathrm{QuantSig}_k$, randomly chooses with equal probability to either forward the measurement results and position to Charlie (Bob) or not, secret from Alice, who should not learn the positions of the forwarded results. The resulting sequences of measurement outcomes, after the forwarding procedure, form Bob's and Charlie's "eliminated signatures." Bob (Charlie) keeps the results obtained directly from Alice, and the results forwarded to him by Charlie (Bob) separate. Therefore, he has an eliminated signature in two parts, each of length $L/2$.

Heterodyne measurements will, even in the ideal case, sometimes eliminate the sent state. If everybody follows the protocol, the probability for this depends on the overlap of the coherent states, and would be equal to $\frac{1}{2}\mathrm{erfc}(\alpha/\sqrt{2})$ in the ideal case with no loss or experimental imperfections, where $\mathrm{erfc}(x)$ is the complementary error function. For $\alpha = 0$, this probability equals one half, and quickly approaches zero as α increases. Because of the unavoidable errors, this measurement protocol is an example of "ambiguous state elimination." Since measurements are performed immediately on receipt of the states, no quantum memory is required, just as in Refs. [6,9].

Messaging stages 5–7.—(5) To send a signed one-bit message m, Alice sends $(m, \mathrm{PrivKey}_m)$ to Bob.

(6) Bob checks whether $(m, \mathrm{PrivKey}_m)$ matches both parts of his stored eliminated signature by counting how many elements of Alice's private key were eliminated during the distribution stage. If there are fewer than $s_a L/2$ mismatches in each of the two parts of his eliminated signature, where s_a is the authentication threshold, Bob accepts the message.

(7) If Bob wishes to forward a message, he forwards the message and its corresponding private key. Charlie tests for mismatches in the same way as Bob, but with a higher verification threshold s_v, to protect against repudiation. Charlie accepts the message if there are fewer than $s_v L/2$ mismatches in each of the two parts of his eliminated signature, with $p_{\mathrm{err}} < s_a < s_v < \frac{1}{2}$.

In essence, the security of this scheme comes from two sources. First, it is impossible for a forger to perfectly determine the private key, since the used quantum states are nonorthogonal. If noise is sufficiently low, the distributor Alice has an advantage over any other party. Second, the forwarding of measurement results ensures that, from Alice's point of view, Bob's and Charlie's measurement records follow the same statistics. This means that if Charlie uses a higher verification threshold s_v than Bob's authentication threshold s_a, then Alice's probability to repudiate can be made arbitrarily small by choosing the signature length L large enough. An upper bound on the repudiation probability is calculated using the Hoeffding inequality [30] in the Supplemental Material [22].

Security against collective attacks follows from the fact that different signature states are completely uncorrelated, meaning that the optimal collective attack is an individual attack on each signature element [6]. Security against coherent attacks is left for future work, noting that due to the forwarding of measurement results amongst other things [31], methods from the security of QKDs cannot be directly carried over. Security against coherent attacks has nevertheless been analyzed for a related quantum signature protocol [11,21]. We also assume that there are authenticated quantum channels between Alice, Bob, and Charlie. Some kind of parameter estimation procedure should be used to replace this assumption, analogous to Refs. [10,11].

To successfully forge, Bob must guess a sequence of states that meets Charlie's verification threshold. For individual and collective forging, the optimal forging attack is to perform a minimum-cost measurement on the individual signature states [31]. The minimum cost C_{min} is the minimum probability that an honest party will detect an error in an individual signature element coming from the forger, and is calculated in the Supplemental Material [22]. As long as C_{min} is larger than p_{err}, which denotes the probability of a mismatch with the sent signature when all parties are honest, the signature scheme can be made secure by appropriately choosing other protocol parameters such as the length L. Note that p_{err} is determined from experimental data. A final condition for a useful QDS scheme is that it must be robust; i.e., it must succeed with a high probability if all parties are honest.

The exact security definitions can vary and depend on whether one party is more likely to be dishonest than the others. As detailed in the Supplemental Material [22], we set protocol parameters so that the repudiation probability, the forging probability, and the failure probability are all approximately equal. In this way, the probability that the scheme will fail in any one of these ways is bounded by

$$P(\mathrm{failure}) \leq 2\exp\left(-\frac{g^2}{16}L\right), \tag{1}$$

where $g = C_{\mathrm{min}} - p_{\mathrm{err}}$ is the advantage that the legitimate sender Alice has over a forger for a single position of the signature sequence [22,23]. Since the failure probability decays exponentially with the signature length L, the scheme is secure, and any required security level can be achieved with sufficiently large L. The figure of merit we use to characterize the quality of our QDS schemes is the length $2L$ required to sign a one-bit message with a failure probability of 0.01%.

To show the robustness of the protocol, the experiment was carried out over a real free-space urban link [32,33]. The signal states $|\pm\alpha\rangle$, $|\pm i\alpha\rangle$ were then repeatedly transmitted, polarization multiplexed with the local oscillator, which is needed for later detection, through a free-space channel between the buildings of the Max Planck

Institute and the University of Erlangen-Nürnberg [32–34]. The length of the channel is approximately 1.6 km. The channel transmission fluctuated between 50% and 85% due to beam wandering and scintillation. At the receiver the signal was split on a balanced beam splitter to measure both the $\hat{x}$ and $\hat{p}$ quadratures. Simultaneously, the transmission was recorded for each state (for more details see Ref. [22]). The experiment was implemented for three different signal amplitudes, $\alpha = 0.48$, $\alpha = 0.93$, and $\alpha = 1.63$, and we attribute the first (second) half of the measurement time to Bob (Charlie). To remedy the channel fading, Bob's (Charlie's) measurement data are then sorted into 32 subchannels according to the measured transmission [32,33]. Depending on the sign of the quadrature measurement values, for each signal state, two of the possible sent states were eliminated.

For each set of data, the sequence of eliminated states was used to produce a cost matrix [31] that gives the probability that each state was eliminated for a particular signal state. For each cost matrix, we calculate the minimum difference between an off-diagonal element of the cost matrix (probability of eliminating a state that was not sent) and the diagonal element of that row (probability of eliminating the sent state). This difference was multiplied by the appropriate $p_{\min}$ to obtain the parameter g from Eq. (1) for that cost matrix. The minimum probability that a forger will incorrectly identify the state is $p_{\min}$ (see Ref. [22]). For each g, the signature length $2L$ to sign a one-bit message with a failure probability of 0.01% was calculated. In Fig. 2, the length L is plotted against transmission T with $T + R = 1$ for $\alpha = 0.48$.

To account for experimental imperfections, a theoretical model was developed, using only experimental data, with

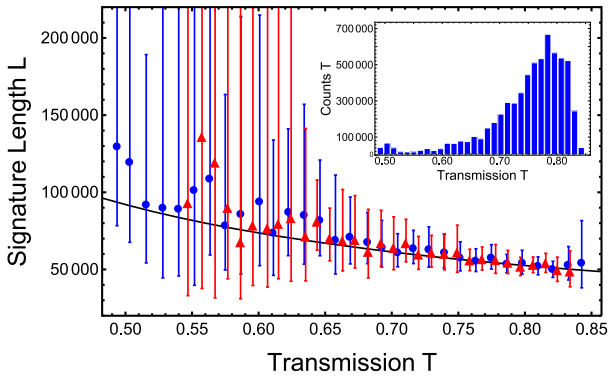

FIG. 2. Signature length for $\alpha = 0.48$. Blue curve: theoretical model. Blue dots and bars: results from the data attributed to Bob. Red triangles and bars: results from the data attributed to Charlie. The error bars calculated are derived by investigating the standard deviation of ten subsets of the entire data set. The errors naturally increase with decreasing transmission since g from Eq. (1) decreases. In addition, less data was available at lower transmission values (see histogram of signals received by Bob per transmission subchannel as inset). The data used for each point comes from a small range of transmissions, but horizontal error bars are omitted for clarity.

no free parameters (for details see the Supplemental Material [22]). The larger errors bars in Fig. 2 are mostly due to the statistical error of the smaller amount of data available at lower transmission. The experiment has a clock rate of about 2.2 MHz and the required signature length of about 10^5 is easily manageable in the subchannels; thus this demonstrates a viable QDS scheme.

The experiment was also carried out at $\alpha = 0.93$ and $\alpha = 1.63$ (results given in Ref. [22]). Increasing α improves the cost matrix but also decreases $p_{\min}$, which makes the guess of the forger easier. There is a trade-off between these two effects, with the optimal α predicted to be $\alpha \approx 0.5$, supported by the experimental results.

The main purpose of this experiment is as a test of the measurement procedure used. A calculation of the cost matrix provides all the information relevant for implementing a full scheme. In the experiment, all the quantum steps were carried out; the rest is classical communication and information processing. The experiment is also the first to demonstrate a signature scheme in a free-space setting, in contrast to previous experiments using optical fibers.

It is important to compare the performance of this scheme to previous results. In Ref. [23], a similar scheme is presented, but with unambiguous state elimination rather than the "continuous-variable ambiguous state elimination" used here. There, the signature length required was about 10^9, for 500 m of optical fiber and a total loss level of 35%. Comparing this to our results, the signature length was about 7×10^4 with a similar loss level and a 1.6 km free-space channel. In Ref. [23], the experiment ran at a clock rate of 100 MHz, whereas the clock rate of this experiment was 2.2 MHz. Increasing the clock rate into the GHz range is straightforward with available technology and the authors have recently demonstrated a continuous-variable system, capable of distributing quantum states at GHz rates [35].

Figure 3 shows the dependence of signature lengths from transmission for the two schemes (details of the models given in Ref. [22]). Even including experimental errors, our

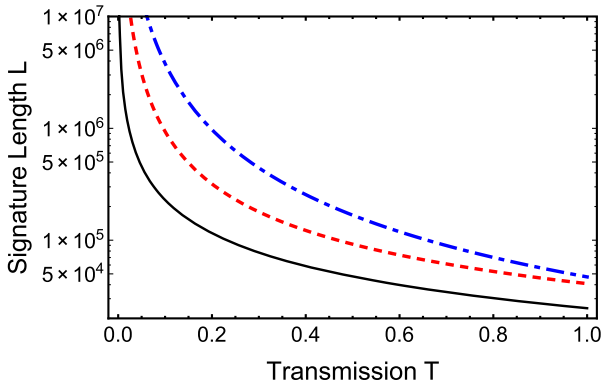

FIG. 3. Black (solid) curve: Signature length for an ideal ambiguous measurement scheme. Red (dotted) curve: Signature length for an ambiguous measurement scheme with realistic imperfections. Blue (dot-dashed) curve: Signature length for an ideal unambiguous measurement scheme.

scheme requires a shorter signature than the ideal result for Ref. [23]. That is, the QDS protocol based on ambiguous state elimination has a fundamental advantage over unambiguous state elimination. This advantage is even more pronounced when experimental inefficiencies are taken into account. Approximately 1 order of magnitude of the advantage comes purely from the chosen measurement, as shown in Fig. 3. The rest comes from the improved technical performance of heterodyne measurements compared to single-photon detectors. Notably, heterodyne detection is more compatible with modern telecommunication networks, than single photon detection, furthering its appeal and holding promise to move to GHz rates and higher transmission ranges. The improvement in signature length is the greatest, a factor of 10 shorter, for a transmission of 10%. This indicates that heterodyne measurements may be more robust against losses.

In conclusion, we have presented a QDS scheme that uses heterodyne measurements. We have experimentally demonstrated that the scheme works over a fluctuating free-space channel, which is the first free-space realization for quantum signatures. In addition, the signature rate per quantum state sent is orders of magnitude better than in previous comparable work. Heterodyne detection used for ambiguous state elimination gives a result for each sent state. Interestingly, this overcompensates the increased error probability and leads to an overall better performance compared to unambiguous measurements.

C. C. and N. K. acknowledge the support from the Scottish Universities Physics Alliance (SUPA) and the Engineering and Physical Sciences Research Council (EPSRC). The project was supported within the framework of the International Max Planck Partnership (IMPP) with Scottish Universities. C. P. and B. H. thank their colleagues at the FAU computer science building for hosting the receiver. E. A. acknowledges the support of EPSRC EP/M013472/1.

[1] W. Diffie and M. E. Helman, IEEE Trans. Inf. Theory **22**, 644 (1976).
[2] D. E. Knuth, *The Art of Computer Programming: Seminumerical Algorithms* (Addison-Wesley, Reading, MA, 1969).
[3] P. W. Shor, SIAM J. Comput. **26**, 1484 (1997).
[4] R. Amiri and E. Andersson, Entropy **17**, 5635 (2015).
[5] P. J. Clarke, R. J. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G. S. Buller, Nat. Commun. **3**, 1174 (2012).
[6] R. J. Collins, R. J. Donaldson, V. Dunjko, P. Wallden, P. J. Clarke, E. Andersson, J. Jeffers, and G. S. Buller, Phys. Rev. Lett. **113**, 040502 (2014).
[7] D. Gottesman and I. Chuang, arXiv:quant-ph/0105032v2.
[8] E. Andersson, M. Curty, and I. Jex, Phys. Rev. A **74**, 022304 (2006).
[9] V. Dunjko, P. Wallden, and E. Andersson, Phys. Rev. Lett. **112**, 040502 (2014).
[10] H. Yin, Y. Fu, and Z. Chen, Phys. Rev. A **93**, 032316 (2016).
[11] R. Amiri, P. Wallden, A. Kent, and E. Andersson, Phys. Rev. A **93**, 032325 (2016).
[12] D. Chaum and S. Roijakkers, *Advances in Cryptology-CRYPTO'90, LNCS, Santa Barbara, USA, 1990* (Springer-Verlag, Berlin Heidelberg, 1991), Vol. 537, pp. 206.
[13] G. Hanaoka, J. Shikata, Y. Zheng, and H. Imai, *Advances in Cryptology-ASIACRYPT 2000, LNCS, Kyoto, Japan, 2000* (Springer, Berlin Heidelberg, 2000), Vol. 1976, pp. 130–142.
[14] C. M. Swanson and D. R. Stinson, *Information Theoretic Security, Proceedings of ICITS 2011, LNCS, Amsterdam* (Springer, Berlin Heidelberg, 2011), Vol. 6673, pp. 100–116.
[15] H Barnum *et al.*, *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science, Vancouver, 2002* (IEEE, Los Alamitos, 2002).
[16] Q. Li, W. H. Chan, C. Wu, and Z. Wen, Int. J. Theor. Phys. **52**, 4335 (2013).
[17] M. Curty, D. J. Santos, E. Pérez, and P. García-Fernández, Phys. Rev. A **66**, 022301 (2002).
[18] F. Gao, S.-J. Qin, F.-Z. Guo, and Q.-Y. Wen, Phys. Rev. A **84**, 022344 (2011).
[19] K. Bartkiewicz, A. Černoch, and K. Lemr, Phys. Rev. A **90**, 022335 (2014).
[20] G. Zeng and C. H. Keitel, Phys. Rev. A **65**, 042312 (2002).
[21] P. Wallden, V. Dunjko, A. Kent, and E. Andersson, Phys. Rev. A **91**, 042304 (2015).
[22] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.117.100503 for the details of security proof and experimental realization.
[23] R. J. Donaldson, R. J. Collins, K. Kleczkowska, R. Amiri, P. Wallden, V. Dunjko, J. Jeffers, E. Andersson, and G. S. Buller, Phys. Rev. A **93**, 012329 (2016).
[24] U. Leonhardt, *Essential Quantum Optics* (Cambridge University Press, Cambridge, England, 2010).
[25] A. Leverrier and P. Grangier, Phys. Rev. Lett. **102**, 180504 (2009).
[26] S. Lorenz, N. Korolkova, and G. Leuchs, Appl. Phys. B **79**, 273 (2004).
[27] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[28] J. A. Bergou, U. Herzog, and M. Hillery, Phys. Rev. Lett. **90**, 257901 (2003).
[29] U. Leonhardt and H. Paul, Prog. Quantum Electron. **19**, 89 (1995).
[30] W. Hoeffding, J. Am. Stat. Assoc. **58**, 13 (1963).
[31] P. Wallden, V. Dunjko, and E. Andersson, J. Phys. A **47**, 125303 (2014).
[32] C. Peuntinger, B. Heim, C. R. Müller, C. Gabriel, C. Marquardt, and G. Leuchs, Phys. Rev. Lett. **113**, 060502 (2014).
[33] B. Heim, C. Peuntinger, N. Killoran, I. Khan, C. Wittmann, Ch. Marquardt, and G. Leuchs, New J. Phys. **16**, 113018 (2014).
[34] N. Korolkova, G. Leuchs, R. Loudon, T. C. Ralph, and C. Silberhorn, Phys. Rev. A **65**, 052306 (2002).
[35] I. Khan, B. Stiller, K. Jaksch, N. Jain, C. Peuntinger, K. Günthner, T. Röthlingsöfer, D. Elser, Ch. Marquardt, and G. Leuchs, *5th International Conference on Quantum Cryptography QCRYPT, Tokyo, Japan, 2015*, http://2015.qcrypt.net/wp-content/uploads/2015/09/Poster69_Imran-Khan.pdf.