Heriot-Watt University
Research Gateway

Experimental demonstration of kilometer-range quantum digital signatures

Citation for published version:
Donaldson, RJ, Collins, RJ, Kleczkowska, K, Amiri, R, Wallden, P, Dunjko, V, Jeffers, J, Andersson, AEE & Buller, GS 2016, 'Experimental demonstration of kilometer-range quantum digital signatures', *Physical Review A*, vol. 93, no. 1, 012329. https://doi.org/10.1103/PhysRevA.93.012329

Digital Object Identifier (DOI):
10.1103/PhysRevA.93.012329

Link:
Link to publication record in Heriot-Watt Research Portal

Document Version:
Publisher's PDF, also known as Version of record

Published In:
Physical Review A

General rights
Copyright for the publications made accessible via Heriot-Watt Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
Heriot-Watt University has made every reasonable effort to ensure that the content in Heriot-Watt Research Portal complies with UK legislation. If you believe that the public display of this file breaches copyright please contact open.access@hw.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 24. Aug. 2022

PHYSICAL REVIEW A **93**, 012329 (2016)

Experimental demonstration of kilometer-range quantum digital signatures

Ross J. Donaldson,[1] Robert J. Collins,[1] Klaudia Kleczkowska,[1] Ryan Amiri,[1] Petros Wallden,[2] Vedran Dunjko,[3,4] John Jeffers,[5] Erika Andersson,[1] and Gerald S. Buller[1]

[1]*SUPA, Institute of Photonics and Quantum Sciences, School of Engineering and Physical Sciences, David Brewster Building, Heriot-Watt University, Edinburgh, EH14 4AS, United Kingdom*

[2]*School of Informatics, Informatics Forum, University of Edinburgh, 10 Crichton Street, Edinburgh, EH8 9AB, United Kingdom*

[3]*Institute for Theoretical Physics, University of Innsbruck, Technikerstrasse 25, A-6020 Innsbruck, Austria*

[4]*Division of Molecular Biology, Ruder Bošković Institute, Bijenička cesta 54, 10002 Zagreb, Croatia*

[5]*SUPA, Department of Physics, John Anderson Building, University of Strathclyde, 107 Rottenrow, Glasgow, G4 0NG, United Kingdom*

(Received 17 August 2015; revised manuscript received 5 November 2015; published 19 January 2016)

We present an experimental realization of a quantum digital signature protocol which, together with a standard quantum key distribution link, increases transmission distance to kilometer ranges, three orders of magnitude larger than in previous realizations. The bit rate is also significantly increased compared with previous quantum signature demonstrations. This work illustrates that quantum digital signatures can be realized with optical components similar to those used for quantum key distribution and could be implemented in existing quantum optical fiber networks.

DOI: 10.1103/PhysRevA.93.012329

I. INTRODUCTION

Signature schemes are widely used in electronic communication to guarantee the authenticity and transferability of messages. Transferability means that a signed message is unlikely to be accepted by one recipient and, if forwarded, subsequently rejected by another recipient [1]. This property distinguishes signature schemes from message authentication schemes, which do not guarantee transferability. Transferability is closely related to nonrepudiation; message repudiation would mean that a sender can successfully deny having sent a message they really did send. The most widespread signature schemes are the public-key protocols Rivest, Shamir and Aldeman [2], Digital Signature Algorithm [3] and Elliptic Curve Digital Signature Algorithm [4], where security depends on the computational difficulty of factorizing large numbers or finding discrete logarithms. Since the security of public-key schemes is not information theoretic but relies on computational assumptions, it can be retrospectively affected by future advances in technology or the discovery of efficient algorithms. In fact, all of the above schemes are known to be insecure against an adversary with a quantum computer [5].

The security of quantum digital signatures (QDS) [6,7], on the other hand, is information theoretic, guaranteed by the laws of quantum mechanics to be secure against an adversary with unrestricted computational capabilities. This is a potentially significant advantage. There also exist unconditionally secure so-called classical digital signature schemes [8]. In addition to requiring pairwise secret classical communication channels (which could be achieved using quantum key distribution, QKD), the scheme by Chaum and Roijakkers [9] requires an authenticated broadcast channel (which is a challenging requirement), and the one by Hanaoka *et al.* [10] is phrased in terms of a third party, trusted by all participants. Such assumptions are not straightforward. Also, while pairwise message authentication can be efficiently implemented with information-theoretic security using short preshared keys, [11] this does not enable the implementation of an authenticated broadcast channel. Quantum signature protocols need neither an authenticated broadcast channel, nor a trusted third party. Further, information-theoretically secure secret classical channels can be generated using QKD. Therefore, even in terms of required resources, if the secret shared keys are generated using QKD, QDS schemes are in this sense no more demanding than the classical unconditionally secure signature schemes.

Although QDS has been successfully realized in the laboratory between three parties, a sender Alice and two receivers Bob and Charlie [12,13], the transmission distance for these realizations was limited to the order of meters due to the inherent design of these earlier protocols. The earliest versions of QDS protocols [6,12] also required long-term quantum memory [14–17] to store the signature states at the receivers, making full implementation impossible with currently available technology. Quantum memory is no longer needed if the recipients directly measure the quantum states sent by Alice, for example, using unambiguous state elimination (USE) [18,19], and then store only the classical measurement outcomes [13,18]. However, these QDS schemes still relied on a multiport to guarantee nonrepudiation, comprising two intertwined interferometers controlled locally by Bob and Charlie. The multiport design required internal delays equal to the link length between Bob and Charlie, as well as introducing unavoidable additional high optical loss, restricting the practical transmission distance to approximately 5 m [12,13].

For QDS to be useful in real-world applications, protocols which allow for higher transmission rate and greater distance between parties must be developed and demonstrated experimentally. In this paper we present an experimental realization of a key part of such a protocol, along the lines of QDS protocols proposed in Ref. [20]. The paper is organized as follows. Section II is divided into two subsections, the first of

Published by the American Physical Society under the terms of the Creative Commons Attribution 3.0 License. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

which outlines the protocol (which is covered in more detail in Appendix A), while the second provides an overview of the experimental system. In Sec. III we present and analyze the experimental results. Only an outline of the analysis is given here, with more details given in Appendix B. Section IV concludes the paper.

II. METHODS

A. Overview of protocol

Signature protocols have two stages, a distribution stage and a messaging stage. The scheme is established in the distribution stage, to enable signed messages to be sent and received in the messaging stage, which is entirely classical and could occur at any future date. An outline of the protocol will be presented here with a more complete description in Appendix A. We will describe how to sign a 1-bit message m; longer messages may be sent by suitably iterating this procedure. In the distribution stage, Alice chooses two random sequences of L phase-encoded coherent states, one sequence for each possible message, 0 or 1. Increasing the length L of the sequence will increase the security of the scheme. The security also depends on other parameters, such as the mean photon number per pulse $|\alpha|^2$ and imperfections in the setup [20]. Alice chooses her quantum states randomly from a known alphabet of nonorthogonal quantum states, in our case the four phase-encoded states $|\alpha\rangle$, $|\alpha e^{i\pi/2}\rangle$, $|\alpha e^{i\pi}\rangle$, and $|\alpha e^{3i\pi/2}\rangle$, relative to a common phase reference. She keeps the complete classical description of the two sequences secret; this constitutes her so-called private key. Nonorthogonal quantum states cannot be perfectly distinguished from each other, so only Alice can know her full private key. The phase reference pulse in our implementation is strong, so that tampering with it could in principle be detected by performing state tomography.

Alice sends one copy of each sequence of coherent quantum states to both Bob and Charlie, through separate quantum channels. Bob and Charlie measure the received coherent states, in our case using quantum USE [13,19,20], ruling out zero, one or more of the four possible phases for each position in each sequence of states. Bob and Charlie perform the measurements by combining the suitably adjusted reference pulses with the signal pulses using two beam splitters, one for each nonorthogonal phase pair in the four-state alphabet. Each detection event eliminates one of the four possible states sent by Alice. In Fig. 1, the phase of the reference state entering beam splitter 2 at Bob is set so that he can eliminate the 0 and π phases, and the phase at beam splitter 3 is set to eliminate the $\pi/2$ and $3\pi/2$ phases. From the detection statistics, one obtains the conditional probabilities for Bob to eliminate each of the four states, given that Alice sent a particular state. An example of this so-called cost matrix is illustrated in Fig. 2(a) for $|\alpha|^2 = 0.5$.

Bob and Charlie now each have a measurement record for the sequences sent by Alice. They then both randomly and independently choose half of their measurement outcomes to forward to the other recipient. They keep secret from Alice which measurement outcomes are forwarded and which are kept. This last step is not implemented in our present setup, but could be achieved using a standard QKD link. Employing a

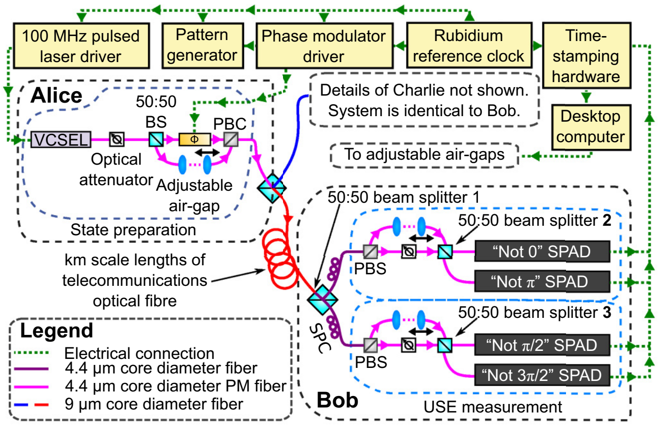

FIG. 1. Experimental setup for kilometer-range quantum digital signatures. Alice uses a pulsed 850-nm-wavelength vertical cavity surface-emitting laser (VCSEL) diode to generate coherent states which are phase encoded using a lithium niobate ($LiNbO_3$) phase modulator. Alice sends the coherent states through standard telecommunications optical fiber to the receivers, who then perform a phase measurement. Sender and receivers are constructed from polarization-maintaining optical fiber to improve the interferometric visibility. Polarization routing of modulated signal and unmodulated reference was carried out using polarization-dependent beam splitters (PBS) while static polarization controllers (SPCs) corrected for polarization shift induced in the telecommunications fiber.

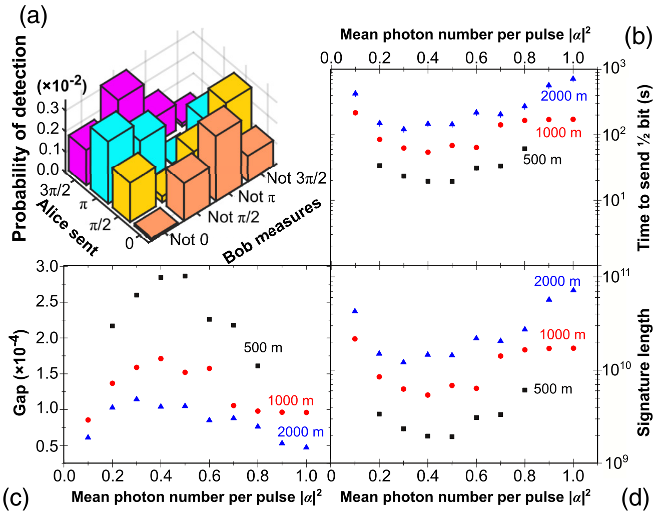

FIG. 2. Experimental results and calculated parameters. In our experiment, measurement statistics for Bob and Charlie were similar. (a) Conditional probabilities for unambiguous state elimination by Bob, with $|\alpha|^2 = 0.5$. These probabilities are used to calculate the gap g and the required signature length per half-bit. (b) Time required for Alice to send a half-bit to Bob. (c) The gap achieved in the experiments is a calculated from both receivers' cost matrices. (d) The length L required to prevent forging and repudiation, per half-bit of message, for a security level of 0.01%. For all subfigures at 500 m, mean photon number points of 0.1, 0.9, and 1 have been removed. Here, the combination of count rate and the dead time of the detector led to nonlinearity in the detection.

standard QKD link does not affect the maximum transmission distance or security level of the system, and does not further complicate the security analysis. This is because it is only used to secure the classical processing after the coherent states have been transmitted and measured.

The random forwarding procedure replaces the symmetrising multiport in earlier implementations and ensures that Bob and Charlie obtain the same final measurement statistics irrespective of what states Alice sends them. This is true even for the most general cheating strategies by Alice, which could involve entangled states. A dishonest Alice could attempt repudiation, that is, deny having sent a message that she actually did send. If the whole signature scheme is to have information-theoretic security, then a secret classical communication channel with information-theoretic security is needed for forwarding the measurement results, since otherwise security against repudiation would not be information theoretic. At the end of the distribution stage, Bob and Charlie should each be left with different and incomplete descriptions of the signature sent by Alice, which are kept until the messaging stage.

In the messaging stage, Alice chooses a message m and sends it together with her corresponding private key, that is, the classical description of the corresponding sequence of quantum states, to the intended recipient, say, Bob. All communication during the messaging stage takes place over pairwise authenticated classical communication channels; quantum communication is needed only in the distribution stage. To accept the message, Bob checks Alice's private key against his measurement record for the message m. He accepts the message if he finds fewer than Ls_a mismatches, where s_a is an authentication threshold and L is the length of the sequences chosen by Alice.

If Bob wishes to forward the message, he sends the message together with Alice's private key to Charlie. Charlie then checks for mismatches in the same way as before, but applies a different verification threshold s_v, which is larger than s_a. The message is only accepted if there are fewer than Ls_v mismatches. It is important that the threshold for accepting a message directly from Alice is different from the threshold for accepting a forwarded message. Otherwise Alice could repudiate with high probability [6]. Signing a message uses up the distributed signatures, which cannot be reused.

Here, as for all existing QDS protocols, we assume that none of the participants are tampering with or eavesdropping on the quantum channels between other participants. It is expected this assumption could be removed by using a parameter estimation procedure analogous to that used in QKD, as has been shown for a quantum signature protocol using Bennett and Brassard 1984 states [21]. By declaring (sacrificing) some of the states in the distribution stage, participants should be able to estimate the level of eavesdropping, aborting if it is too high. When considering security against forging by either Bob or Charlie, one assumes that the other recipient and Alice are honest, since no protocol can guarantee security if two of the three parties are dishonest and collude. Similarly, when considering security against repudiation by Alice, one assumes that Bob and Charlie are honest.

All pairwise classical communication in the present protocol, just as for QKD, must be authenticated. Pairwise message authentication can in modern cryptography be efficiently implemented using short preshared keys [22]. It is not, even in principle, possible to prevent man-in-the-middle attacks in QKD or QDS schemes unless there has been some prior interaction between parties. If information-theoretic security is required, one needs to use an appropriate authentication scheme for all classical communication [23]. The security analysis for the QDS protocol implemented here proceeds much as in Collins *et al.* [13] and is detailed in Appendix B.

B. Experimental method

The experimental system shown in Fig. 1 shares many similarities with QKD experiments [24–29]. The sender and receivers are constructed from 4.4-μm-core-diameter so-called panda-eye polarization-maintaining fiber [30] that can support two orthogonal linear polarization modes. Alice generates 850.17-nm-wavelength coherent-state pulses at a repetition rate of 100 MHz by means of a vertical cavity surface-emitting laser and an optical attenuator [13]. A lithium niobate phase modulator is used to encode the phases on weak pulses, while a strong reference pulse is delayed by half a period from the encoded states. The signal and reference pulses have orthogonal linear polarizations and are recombined using a polarization beam combiner [31] before transmission through the 9-μm-core-diameter optical fiber quantum channel. The quantum channel is composed of Corning SMF-28e optical fiber [32], which is retained within the same laboratory as Alice, Bob, and Charlie. Short lengths of 4.4-μm-core-diameter fiber [33] are fusion spliced onto the quantum channel to eliminate higher order spatial modes [34].

Stresses induced on the quantum channel will introduce a time-evolving birefringence which reduces the linearity of the polarizations as they propagate. Bob and Charlie employ paddle-type static polarization controllers to apply an opposing birefringence over a short (≈1 m) length of 4.4-μm-core-diameter fiber, returning the states to linear prior to the measurement step. Future revisions of this system will employ automatic correction by monitoring the delayed bright reference pulse.

A polarization beam splitter in each receiver ensures that the weak signal pulse traverses the delaying path while the bright reference pulse traverses the short path. The polarization and intensity of the reference pulses are altered to match the signal pulse before recombination on a 50:50 beam combiner where interfere occurs. Commercially available free-running photon-triggering [35] silicon single-photon avalanche diodes [36] (Si-SPADs) are employed as detectors, due to their high single-photon detection efficiency (≈40%) for photons with a wavelength of 850 nm, a low dark count rate (≈300 counts per second), and a low afterpulsing probability (≈0.5%) when compared to semiconductor detectors used at the telecommunications wavelengths [37,38]. Conveniently these detectors operate near room temperature, although it should be noted that superconducting detectors have exhibited much higher single-photon-detection efficiencies, e.g., 93% [39], albeit at temperatures of 4 K or less [40], while semiconductor technologies usually operate near room temperature [36,38]. There have been recent advances in semiconductor detector technologies for wavelengths around 1550 nm [38], and future

QDS experiments will likely employ these technologies to further enhance the transmission range.

The air gaps in each receiver consist of an immobile launching collimating lens and a collection lens attached to a linear piezoelectric actuator. The receivers adjust the relative lengths of their measurement setup to ensure optimum interferometric visibility (typically greater than 93%). The receivers' demodulation systems have a mean attenuation of 6.96 dB.

Detector trigger events are time stamped with a resolution of 1 ps [41] before analysis of the raw time-stamp information is carried out by custom software written in MATLAB [42], which filters events to discard those that occur outside of a window of ±2 ns centered on the expected arrival time of a pulse, a process that retains 80% on average of the raw counts and performs USE. The measurement records are then retained to allow forwarding of results from Bob to Charlie and vice versa. This must be done in secret from Alice and could be accomplished using a channel secured using a one-time pad with a prestored key which may come from a standard QKD link between Bob and Charlie.

III. RESULTS AND DISCUSSION

In Fig. 2, we plot experimental data and parameters for a range of mean photon numbers $|\alpha|^2$ sent by Alice. When $|\alpha|^2$ increases, the probability that a forger will be able to select the correct declaration increases but likewise so does an honest recipient's ability to detect mismatches in a fake declaration. It is therefore nontrivial to determine the optimal value of $|\alpha|^2$. The gap, g, between the probability for a forger's fake declaration to be rejected and the probability for Alice's true declaration to be rejected, $g = C_{\min} - p_h$ (see Appendix B), depends on $|\alpha|^2$. Other experimental parameters, such as system loss and interferometric visibility, are automatically taken into account in the cost matrices that are used to obtain $C_{\min}$ and the gap g. It can be seen from Fig. 2(c) that the maximum gap occurs around $|\alpha|^2 = 0.4$ for transmission distances of 500, 1000, and 2000 m, showing that this value of $|\alpha|^2$ is the best choice for the sender in this particular experimental implementation.

For the desired security level, the length required to sign one half-bit can then be calculated using $P(\text{protocol failure}) = 2e^{-(g/4)^2 L}$ (see Appendix B). In this paper, we use a security level of 0.01%. The resulting signature length for each half-bit is graphed in Fig. 2(d) for varying $|\alpha|^2$. As $|\alpha|^2$ increases, the length per half-bit dips to a minimum and increases again. For our experimental data, the maximum value for the gap and the minimum values for the length are around $|\alpha|^2 = 0.4$.

To further illustrate the measurements by the recipients, state elimination success rates are shown in Fig. 3. A successful USE measurement means eliminating any state except the state Alice sent. On average, the USE success rate is 80% of the raw count rate. Only a single detection event is required to eliminate a state, and therefore the success rate is higher than for unambiguous state discrimination (USD), where one has to eliminate all possible states except the one sent. The success rate for USD is typically many orders of magnitude lower than the time-gated detector count rate [13]. The failure rate of USE (eliminating the state that was actually sent) depends on the visibility of the interferometers formed by Alice's state preparation and the receiver's detection setup. In the security proof we assume that Alice has full control over the failure rate and so can generate any number of mismatches she likes. For these experiments, the USE failure rate was on average 1.7% of the pulse repetition rate. Knowing Alice's repetition rate and the signature length L required to sign a half-bit message allows us to calculate the time it would take for Alice to distribute a signature state sequence for signing one half-bit using the current system.

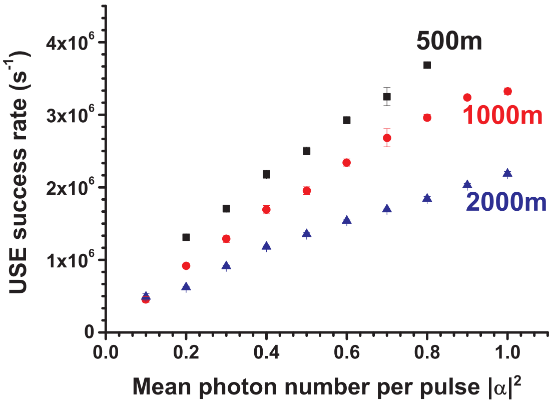

FIG. 3. Unambiguous state elimination (USE) success rate at different transmission distances for Bob. Results for Bob and Charlie are again very similar so only results for Bob are shown. The failure rate of USE is on average only 1.7% of the pulse-repetition frequency and is not plotted. For transmission distance 500 m, points for mean photon number 0.1, 0.9, and 1 have been removed, since here the combination of count rate and the dead time of the detector led to nonlinearity in the detection of events.

In a previous QDS experiment using a mulitport [13], with a transmission distance of 5 m, the largest gap was found to be 1.20×10^{-6}, which occurred for $|\alpha|^2 = 1$. The USE success rate was 2×10^5 counts per second. For a security level of 0.01%, the length L required to securely sign a half-bit was found to be 5.0×10^{13}, and the estimated time it would take to securely sign a half-bit was over eight years. In contrast, for the present setup and a transmission distance of 500 m, the maximum gap, $g = 2.86 \times 10^{-4}$, occurs at a $|\alpha|^2 = 0.5$, with a USE success rate of 2.48×10^6. This gap is two orders of magnitude greater than for the previous short-range system. The length L per half-bit for this new realization is 1.93×10^9 for a security level of 0.01%, and the estimated time it would take to securely sign a half-bit is less than 20 s. As the transmission distance increases, the time taken to sign one half-bit naturally increases, but even at 2000 m the time taken to sign one half-bit is four orders of magnitude smaller than in the previous experimental demonstrations of QDS.

IV. CONCLUSIONS

We have presented a QDS test bed that employs technologies similar to common phase-basis set QKD systems to overcome the previous limitations on maximum transmission length and demonstrate signature generation over transmission lengths up to 2 km—a significant improvement over previous demonstrations that were limited to a few meters [12,13].

Removing the cumbersome multiport of previous QDS hardware iterations means that this test bed exhibits significantly enhanced robustness against environmental disturbances while simultaneously highlighting a pathway to implementation of QDS with QKD hardware. Furthermore, compared to previous implementations of USE-USD QDS [13] this improved design requires significantly fewer coherent states to sign an individual half-bit.

The system reported here operates over relatively short distances when compared to the current maximum transmission distances achieved for QKD experiments [43]. This is because quantum signatures are different from QKD both in functionality, protocol and security analysis. We also note the increased losses of 2.2 dB km^{-1} in standard telecommunications fiber at the wavelength of 850 nm, selected for these experiments, as opposed to 0.2 dB km^{-1} at 1550 nm, typically used in QKD experiments. Although the protocol demonstrated in this paper shows a significant enhancement in transmission distance and message signing rate compared with previous QDS demonstrations, further improvements in signature transmission rate, in particular, will be necessary to fully exploit the potential of QDS.

The recently proposed signature protocol P2 in Ref. [20] uses standard QKD systems to first generate pairwise shared keys between all parties. The secret keys are then used to sign messages. Currently, such schemes seem more efficient than any proposed quantum protocol that directly signs a message without first distilling a secret key. Nevertheless, direct quantum signature protocols, such as the one discussed in this paper, are still worth investigating, as they may eventually prove better than signature protocols based on secret shared keys. For example, direct quantum protocols can remain secure even if the available quantum channels are too noisy for practical QKD [21]. Also, the most efficient direct quantum protocol should intuitively be at least as efficient as protocols proceeding via first distilling shared secret keys and then using the shared keys to sign messages. There could also be other advantages with direct quantum protocols. If quantum channels of sufficiently high quality are available, then direct quantum signature protocols should need quantum channels only between the sender and each recipient, as opposed to QKD links between each party for protocols similar to P2. This means that the number of quantum channels scales only linearly with the number of recipients for direct quantum signature schemes, as opposed to quadratically for schemes similar to P2. Compared with work on QKD, very little work has been done on QDS schemes. This is surprising, given the wide usage and importance of signature schemes in modern communication. We are confident that demonstrating kilometer-range quantum signature schemes, using the same technical components as QKD, will stimulate wider interest in developing the next generation of quantum signature protocols for real-world optical networks.

All data created during this research are openly available from the Heriot-Watt University data archive [44].

ACKNOWLEDGMENTS

This work was supported by the UK Engineering and Physical Sciences Research Council (EPSRC) under Grants No. EP/G009821/1, No. EP/K022717/1, and No. EP/K015338/1. P.W. gratefully acknowledges support from the European Cooperation in Science and Technology (COST) Action MP1006. V.D. acknowledges support by EPSRC.

APPENDIX A: PROTOCOL

The protocol presented in this paper is similar to P1′ from Ref. [20], but with two important differences. First, we require Bob and Charlie to record whether each measurement outcome they hold came directly from Alice or whether it was forwarded to them by the other recipient. Second, the experiment uses weak coherent states instead of true single-photon states. This means that the security proofs presented for protocol P1′ do not apply, and instead we follow the methods applied in Ref. [13] for security against individual and collective forging attacks. The protocol is as follows.

1. Distribution stage

(1) For each future one-bit message $k = 0,1$, Alice generates two copies of sequences of coherent states, $\text{QuantSig}_k = \bigotimes_{l=1}^{L} \rho_l^k$ where $\rho_l^k = |b_l^k\alpha\rangle\langle b_l^k\alpha|$, α is a real positive amplitude, $b_l^k \in \{1,i,-1,-i\}$ are randomly chosen, and L is a suitably chosen integer (the signature length). The state QuantSig_k and the sequence of numbers $\text{PrivKey}_k = (b_1^k,\ldots,b_L^k)$ are called the *quantum signature* and the *private key*, respectively, for message k.

(2) Alice sends one copy of QuantSig_k to Bob and one to Charlie, for each possible message $k = 0$ and $k = 1$.

(3) Bob and Charlie measure each state received using quantum unambiguous state elimination (USE) for $\{|\alpha\rangle,|i\alpha\rangle,|-\alpha\rangle,|-i\alpha\rangle\}$. For every element of each quantum signature (for $k = 0,1$), they store which detectors detected photons; each detector rules out one possible phase state. They therefore store sets of six numbers (hexaplets) of the form $\{k,l',a_0^{k,l'},a_{\pi/2}^{k,l'},a_{\pi}^{k,l'},a_{3\pi/2}^{k,l'}\}$, where $1 \leqslant l' \leqslant L$ and $a_\phi^{k,l'} \in \{0,1\}$. Here, $a_\phi^{k,l'} = 0$ means that no photons were detected at the $\neg\phi$ detector (that is, the phase ϕ is not ruled out), while $a_\phi^{k,l'} = 1$ means that there was at least one photon detected at the $\neg\phi$ detector (that is, the phase ϕ is ruled out for this element). By $\neg\phi$ detector we symbolize the "not ϕ" detector. Note that, due to losses, many of the hexaplets will have $a_\phi^{k,l'} = 0$ for all ϕ.

(4) Once all states have been received and all hexaplets recorded, Bob and Charlie each independently choose half $(L/2)$ of their hexaplets and send them to the other participant. To do this, they use a secret classical channel so that Alice has no information regarding which participant holds which hexaplet. Bob and Charlie keep a record of whether a particular hexaplet came from Alice or whether it was forwarded by the other recipient.

2. Messaging stage

(1) To send a signed one-bit message m, Alice sends $(m,\text{PrivKey}_m)$ to the desired recipient (say, Bob).

(2) Bob checks whether $(m,\text{PrivKey}_m)$ matches both of his stored sequences—the one he received directly from Alice and the one he received from Charlie. In particular, he counts

the number of elements of $\mathrm{PrivKey}_m$ which disagree with his stored hexaplets. Therefore, for a given element l of the signature, if Alice's declaration was ϕ, Bob needs to check if a_ϕ is 0 or 1. If $a_\phi = 1$, he registers one mismatch. In other words, a mismatch is registered whenever Alice's declaration for a given element has been eliminated by Bob's USE measurement. Bob checks, for each of his stored sequences, whether the number of mismatches is below $s_a L/2$, where s_a is an authentication threshold. Bob accepts the message only if both of his sequences have fewer than $s_a L/2$ mismatches, i.e., both the sequence received directly from Alice and the sequence received from Charlie.

(3) To forward the message to Charlie, Bob forwards to Charlie the pair $(m,\mathrm{PrivKey}_m)$ he received from Alice. Charlie tests for mismatches similarly to Bob, but to protect against repudiation by Alice, he uses a different threshold. For each of his sequences—the one received directly from Alice and the one received from Bob—Charlie checks if the number of mismatches is below $s_v L/2$, where s_v is the verification threshold, with $s_a < s_v$. Charlie accepts the message only if both of his sequences have fewer than $s_v L/2$ mismatches.

APPENDIX B: SECURITY

The quantum signature protocol is designed to be secure against two types of dishonesty: forging and repudiation. Security against forging requires that any participant receiving a message will, with high probability, reject a message that did not originate with Alice. Security against repudiation requires that, with high probability, Alice cannot make Bob and Charlie disagree on the validity of her message, i.e., she cannot make one participant accept and the other reject her message. In this section we will show that the probabilities of forging and repudiation decay exponentially in the signature length, L. Further, we will show that the protocol is robust, i.e., if all participants are honest, the protocol works and does not abort, except with a probability exponentially small in L.

For forging one can distinguish different types of malicious attacks. In individual attacks, the cheating party employs a strategy separately and independently for each signature element. In collective attacks, there may be classical correlations between strategies for different signature elements. Coherent attacks are the most general type; here a cheating party can employ any type of correlations, including entanglement and measurements in an entangled basis. Note that the same distinctions apply in principle to repudiation attempts from Alice. However, when proving security against repudiation, we will assume that Alice can exactly control the number of mismatches her signature generates with Bob's and Charlie's measurement outcomes. This covers all types of attack from Alice and so the distinction between individual, collective, and coherent attacks is not made. Security is proven for all types of repudiation attacks, and all types of forging except coherent forging attacks. We will treat individual forging attacks in detail. Security against collective forging attacks then follows because the optimal collective forging strategy is actually an individual strategy, as argued in Ref. [13].

1. Model assumptions

Here, as in all previous QDS protocols, we assume that the quantum channels between participants do not allow tampering or eavesdropping from a third party. It is expected that this assumption could be removed by using a parameter estimation procedure analogous to that used in QKD [21]. By sacrificing part of the states sent during the distribution stage, participants should be able to estimate the level of tampering and eavesdropping.

All pairwise classical communication in the present protocol, just as for QKD, must be authenticated. Pairwise message authentication can be efficiently implemented with information-theoretic security using short preshared keys [11]. Without this authentication, it is not possible, even in principle, to prevent man-in-the-middle attacks in QKD or QDS schemes. Thus neither QKD nor QDS can be implemented without some prior interaction between parties. It is important to note that pairwise authentication between parties is far simpler to achieve than an authenticated broadcast channel and that pairwise authenticated channels do not imply an authenticated broadcast channel.

2. Security against repudiation

To repudiate, Alice aims to send a declaration (m,Sig_m), which Bob will accept and which Charlie will reject. To do this, Bob must accept both the elements that Alice sent directly to him and the elements that Charlie forwarded to him. In order for Charlie to reject he need only reject either the elements he received from Alice or the elements Bob forwarded to him. Intuitively, security against repudiation follows because of the symmetrization of measurement outcomes performed by Bob and Charlie using the secret classical channel. Bob and Charlie perform USE measurements on each of the states sent to them by Alice so that they hold the L hexaplets $(b_1,\ldots,b_L)$ and $(c_1,\ldots,c_L)$ respectively. We give Alice full powers and assume that later on, in the messaging stage, she is able to fully control the number of mismatches her signature declaration, $\mathrm{PrivKey}_m$, contains with the hexaplets $(b_1,\ldots,b_L)$ and $(c_1,\ldots,c_L)$. Call the mismatch rates e_B and e_C respectively. The symmetrization process means that Bob and Charlie will randomly (and unknown to Alice) receive $L/2$ of the others' hexaplets. We show that all choices of e_B and e_C lead to an exponentially decaying probability of repudiation.

Suppose Alice chooses $e_C > s_a$. In this case, Bob is selecting (without replacement) $L/2$ elements from the set $\{c_1,\ldots,c_L\}$, which contains exactly $e_C L$ mismatches with Alice's declaration. The number of mismatches Bob selects then follows a hypergeometric distribution $H(L,e_C L,L/2)$ with expected value $e_C L/2$. For the message to be accepted, Bob must select fewer than $s_a L/2$ errors. The tails of a hypergeometric distribution can be bounded, using Ref. [45], to give an inequality with the same form as a Hoeffding inequality. This enables us to bound the probability that Bob selects fewer than $s_a L/2$ mismatches as

$$\begin{aligned}&\Pr(\text{Bob receives fewer than } s_a L/2 \text{ mismatches from Charlie})\\&\quad\leqslant \exp[-(e_C - s_a)^2 L].\end{aligned}$$

To repudiate, Alice must make Bob accept the message, which means that Bob must accept both the part received from Alice and the part received from Charlie. Since $\mathbb{P}(A \cap B) \leqslant \min\{\mathbb{P}(A),\mathbb{P}(B)\}$, the probability of repudiation must be less than or equal to the above expression and so must also decrease exponentially.

Now suppose $e_C \leqslant s_a$. In this case, if $e_B > s_a$ the above argument shows that it is highly likely that Bob will reject the message, so we consider only the case where $e_B \leqslant s_a$. Consider first the set $\{b_1,\dots,b_L\}$. We can use the same arguments as above to bound the probability of selecting more than $s_v L/2$ mismatches as

$$\begin{aligned}&\Pr(\text{Charlie selects more than } s_v L/2 \text{ mismatches from Bob})\\ &\quad\leqslant \exp[-(s_v - e_B)^2 L].\end{aligned}$$

For Alice to successfully repudiate, Charlie must select more than $s_v L/2$ mismatches from either the set $\{b_1,\dots,b_L\}$ or the set $\{c_1,\dots,c_L\}$. Using $\Pr(A \cup B) \leqslant \Pr(A) + \mathbb{P}(B)$, we can see that, for the choice of $e_B, e_C \leqslant s_a$, we have

$$\begin{aligned}&\Pr(\text{Charlie selects more than } s_v L/2 \text{ mismatches})\\ &\quad\leqslant 2\exp[-(s_v - s_a)^2 L].\end{aligned}$$

So again, the probability of Alice successfully repudiating decreases exponentially in the size of the signature. Similar to that in Ref. [20], Alice's best strategy would be to pick $e_B = e_C = \frac{1}{2}(s_v + s_a)$, in which case

$$\Pr(\text{Repudiation}) \leqslant 2\exp\left[-\tfrac{1}{4}(s_v - s_a)^2 L\right]. \tag{B1}$$

3. Security against individual and collective forging

In order to forge, Bob must make a declaration with fewer than $s_v L/2$ errors with the $L/2$ elements Charlie received directly from Alice. To bound the probability of Bob being able to make such a declaration, we will follow the cost matrix analysis performed in Ref. [13]. For a given individual signature element, we define the cost matrix for Bob as a matrix where the rows correspond to which state Alice sent ($|\exp(i\theta)\alpha\rangle$), while the columns correspond to the detectors $D(\neg\theta)$. Each matrix element $C_{i,j}$ can be taken equal to the probability that if the ith state is sent, then Charlie's jth detector clicks. This is because Bob should avoid declaring a phase that Charlie has eliminated. His cost for making a particular declaration will therefore be proportional to the probability that Charlie has ruled out this state. When $|\alpha|^2 = 0.4$, and over a distance of 500 m, the experiment gives us the cost matrix

$$C = \begin{pmatrix} 8.41\times10^{-5} & 1.48\times10^{-3} & 2.00\times10^{-3} & 1.11\times10^{-3}\\ 1.15\times10^{-3} & 6.31\times10^{-5} & 1.22\times10^{-3} & 2.84\times10^{-3}\\ 2.41\times10^{-3} & 1.90\times10^{-3} & 1.53\times10^{-4} & 1.30\times10^{-3}\\ 1.15\times10^{-3} & 2.77\times10^{-3} & 1.15\times10^{-3} & 4.49\times10^{-5}\end{pmatrix}. \tag{B2}$$

From this matrix, we aim to find two important quantities. First, we want to find the honest cost, p_h, for Bob. This is the rate at which Charlie would find mismatches even if Bob acts honestly. This situation occurs when Charlie erroneously rules out the state that Alice actually sent. The experimentally found probability of this happening is given by the diagonal elements of C, and so the honest cost is simply the average of the diagonal elements, giving $p_h = 8.61 \times 10^{-5}$. This rate is important for two reasons: first, the parameter s_a must be set higher than p_h for the protocol to be robust (to avoid aborting due to noise in the honest run); second, to be secure against forging p_h must be smaller than the rate at which Charlie finds mismatches if Bob is dishonest; i.e., being dishonest must carry some positive cost for Bob.

We now consider the case of a dishonest Bob who tries to guess Alice's signature so that he can forge a message to Charlie. We consider only individual and collective forging attacks, where Bob acts on each quantum state individually, but the outcome of his measurement on one quantum state can affect his choice of measurement on the others. Security against coherent forging attempts remains an open question. We want to find $C_{\min}$, the minimum possible rate that Bob will declare single signature elements which have been eliminated by Charlie. To do this, we use the cost matrix C and note that $C_{\min}$ is the minimum cost associated with the matrix C. Finding minimum costs involves finding optimal measurements, which is in general a difficult problem. However, we are able to bound $C_{\min}$ following the method in Ref. [13]. To do this, we find the matrices C^h, C', and C^l, with

$$C^h = \begin{pmatrix} 8.41\times10^{-5} & 8.41\times10^{-5} & 8.41\times10^{-5} & 8.41\times10^{-5}\\ 6.31\times10^{-5} & 6.31\times10^{-5} & 6.31\times10^{-5} & 6.31\times10^{-5}\\ 1.53\times10^{-4} & 1.53\times10^{-4} & 1.53\times10^{-4} & 1.53\times10^{-4}\\ 4.49\times10^{-5} & 4.49\times10^{-5} & 4.49\times10^{-5} & 4.49\times10^{-5}\end{pmatrix}.$$

This is a constant-row matrix made up of the diagonal elements of the matrix C. The minimum cost achievable for this matrix is the honest cost, p_h. The matrix

$$C' = \begin{pmatrix} 0 & 1.40\times10^{-3} & 1.92\times10^{-3} & 1.02\times10^{-3}\\ 1.09\times10^{-3} & 0 & 1.15\times10^{-3} & 2.78\times10^{-3}\\ 2.26\times10^{-3} & 1.75\times10^{-3} & 0 & 1.15\times10^{-3}\\ 1.11\times10^{-3} & 2.72\times10^{-3} & 1.11\times10^{-3} & 0\end{pmatrix}$$

is the difference between C and C^h. It represents the difference between an honest strategy and a dishonest strategy. The minimum cost for this matrix is the minimum additional cost suffered from acting dishonestly. It is difficult to find the minimum cost for this matrix, so instead we can bound it below by reducing all nonzero elements to the the smallest nonzero element, to get the matrix

$$C^l = \begin{pmatrix} 0 & 1.02\times10^{-3} & 1.02\times10^{-3} & 1.02\times10^{-3} \\ 1.02\times10^{-3} & 0 & 1.02\times10^{-3} & 1.02\times10^{-3} \\ 1.02\times10^{-3} & 1.02\times10^{-3} & 0 & 1.02\times10^{-3} \\ 1.02\times10^{-3} & 1.02\times10^{-3} & 1.02\times10^{-3} & 0 \end{pmatrix}.$$

The matrix C^l corresponds to a lower bound on the additional probability Bob has of causing a mismatch if he is dishonest, when compared to the honest case. For this reason we define the constant, nonzero element, as *guad*, the guaranteed advantage an honest strategy has over a dishonest strategy. Since $C^h_{ij} + C^l_{ij} \leqslant C_{ij}$, the minimum cost of $C^h + C^l$ must be less than the minimum cost of C. The matrix C^l is of error type, so its minimum cost is proportional to $p_{\min}(\alpha)$, the minimum error probability, and can be achieved using a minimum-error measurement [19]. Since the optimal measurement is known, in this case, to be the square-root measurement (SRM), we can calculate $p_{\min}(\alpha)$ for all values of α from

$$p_{\min}(\alpha) = 1 - \frac{1}{16}\left|\sum_i \sqrt{\lambda_i}\right|^2,$$

where

$$\lambda_1 = 2e^{-|\alpha|^2}[\cos(|\alpha|^2) + \cosh(|\alpha|^2)],$$

$$\lambda_2 = 2e^{-|\alpha|^2}[\sin(|\alpha|^2) + \sinh(|\alpha|^2)],$$

$$\lambda_3 = 2e^{-|\alpha|^2}[\cosh(|\alpha|^2) - \cos(|\alpha|^2)],$$

$$\lambda_4 = 2e^{-|\alpha|^2}[\sinh(|\alpha|^2) - \sin(|\alpha|^2)].$$

Defining the gap, $g = p_{\min} \times guad$, we know $p_h + g \leqslant C_{\min}$. For the particular case of $|\alpha|^2 = 0.4$, $p_{\min} = 0.317$ and we obtain

$$p_h + g = 8.61\times10^{-5} + (0.317\times1.02\times10^{-3})$$
$$= 4.10\times10^{-4} \leqslant C_{\min}.$$

This is our lower bound on $C_{\min}$, and in what follows we conservatively assume $C_{\min} = p_h + g$. As long as we choose $s_v < C_{\min}$, we can use [46] to obtain

$$\Pr(\text{Forge}) \leqslant \exp[-(C_{\min} - s_v)^2 L]. \tag{B3}$$

Note that for simplicity we have only considered the case of Bob attempting to forge. We should also consider the possibility of Charlie trying to forge. In this case, we would replace the cost matrix (B2) with the corresponding experimentally generated cost matrix for Charlie. The analysis then follows exactly as above and we would arrive at another value of $C_{\min}$, valid for when Charlie is the forger. For the protocol to be secure against both Bob and Charlie attempting to forge, we would choose $C_{\min} = \min\{C^{\text{Bob}}_{\min}, C^{\text{Charlie}}_{\min}\}$. For our implementation, $C^{\text{Bob}}_{\min} < C^{\text{Charlie}}_{\min}$ and so $C_{\min}$ remains as above.

4. Robustness

Suppose all parties are honest. Bob aborts if either the $L/2$ states received from Alice result in mismatch rate greater than s_a or the measurement results for the $L/2$ states received from Charlie give mismatch rate greater than s_a. We suppose that the channel from Alice to Bob has an error rate of p^B_h and the channel from Alice to Charlie has an error rate of p^C_h. Then we have

$$\Pr(\text{Abort due to Alice}) \leqslant \exp\left[-\left(s_a - p^B_h\right)^2 L\right],$$

$$\Pr(\text{Abort due to Charlie}) \leqslant \exp\left[-\left(s_a - p^C_h\right)^2 L\right].$$

If we set $p_h = \max(p^B_h, p^C_h)$ then the probability of an honest abort is bounded by

$$\Pr(\text{honest abort}) \leqslant 2\exp[-(s_a - p_h)^2 L]. \tag{B4}$$

5. Signature length

Using the above analysis, we can calculate the length of the signature needed to securely sign a single-bit message. Following Ref. [13], we assume that there is no reason in general to favor one type of security over another, so we pick parameters s_a and s_v so as to make the probabilities of honest abort, forgery, and repudiation all equal. If all these probabilities are all below 0.01%, we say that the protocol is secure to a level of 0.01%. By setting

$$s_a = p_h + g/4, \quad s_v = p_h + 3g/4, \tag{B5}$$

the probabilities of repudiation, forging, and honest abort all become approximately equal. More explicitly, considering the terms in the exponent of equations (B1), (B3), and (B4), we see that they are equal when

$$\left(\frac{s_v - s_a}{2}\right)^2 - \frac{\ln(2)}{L} = (C_{\min} - s_v)^2$$
$$= (s_a - p_h)^2 - \frac{\ln(2)}{L}, \tag{B6}$$

where the prefactors of 2 have been taken inside the exponential. As L increases, the choice of s_a and s_v satisfying Eq. (B6) tends to those given in Eq. (B5).

Determining the value of the coherent state amplitude, α, that leads to the smallest possible signature length is, in general, a difficult problem, especially for a real experimental situation. Higher values of $|\alpha|^2$ lead to lower loss and a smaller bit error rate but come at the cost of making the states $\{|\alpha\rangle, |i\alpha\rangle, |-\alpha\rangle, |-i\alpha\rangle\}$ more distinguishable for a potential forger. Thus we need to strike a balance between correctly transmitting the states and giving power to a forger. In the previous QDS experiment [13], the magnitude of α was varied in increments of 1 between 1 and 10. In order to minimize the signature length, the magnitude of α is chosen so as to maximise the gap, g, defined above. It was found that $|\alpha|^2 = 1$ gave the largest gap for the range considered, and extrapolation of subsequent experimental data suggested that $|\alpha|^2 \approx 0.5$ would be optimal. In fact, we found in this experiment that the optimal value was around $|\alpha|^2 = 0.4$, for which the corresponding value of $p_{\min}$ is 0.317.

We now have everything in place to calculate the signature length, L, needed to securely sign a message for $|\alpha|^2 = 0.4$. Over a distance of 500 m, experimental data give the honest cost as $p_h = \max(p_h^B, p_h^C) = 1.26 \times 10^{-4}$. Note that this differs from the value used in the analysis above because in fact Charlie's cost matrix gave a higher honest cost than Bob's. We also find $C_{\min} = \min\{C_{\min}^{\text{Bob}}, C_{\min}^{\text{Charlie}}\} = 4.10 \times 10^{-4}$, as above. This gives the gap, $g = C_{\min} - p_h = 2.84 \times 10^{-4}$, from which we can find the parameters s_a, s_v using Eq. (B5). Putting it all together, we find that a signature length of $L = 1.96 \times 10^9$ is required to sign a message to a security level of 0.01%.

Although this is a significant improvement over the last QDS experiment [13], there are a number of ways to further improve the efficiency of the protocol. The simplest would be to increase the clock rate and therefore the transmission rate. This would not decrease the signature length but would decrease the time needed to transmit a given signature length. The pulse rate used in this QDS system was 100 MHz, and there is scope to increase this to >1 GHz as is typically found in modern QKD systems [25,47–49]. Despite the clock rate increasing by a factor of 10, the increased effects of inter- and intrasymbol interference mean that the corresponding decrease in the signature time will not be as great as a factor of 10. The exact improvement strongly depends on the characteristics of the employed coherent source, single-photon detectors, and timing electronics.

Another possible improvement would be to switch to an operational wavelength of 1550 nm as in Ref. [47], rather than the 850 nm used in this experiment. At 1550 nm, we would expect to see losses of about 0.22 dB per kilometer, a significant improvement over the 2.2 dB per kilometer in the current setup. This switch in wavelengths would enable a new QDS experiment to be carried out over tens of kilometers with similar performance to our QDS system at short distances. A wavelength of 850 nm was selected for these experiments as it provides a good compromise between the detection efficiency response of the mature, low-noise, low-timing-jitter, high-efficiency, thick-junction, silicon single-photon avalanche diodes at room temperature and the attenuation profile of fused silica optical fibers.

As the system used in these experiments is similar in layout to that used in a number of QKD experiments, we can make an approximate comparison of the performance of our QDS system with that of a state-of-the-art QKD system [47] by examining the quantum bit error rate (QBER). Reducing the QBER would decrease the size of the diagonal elements in the cost matrix (B2). This would lead to a larger gap, g, and therefore a smaller signature. There is perhaps less scope for improvement in this respect since the current setup achieved a QBER of around 4% over the range of distances investigated, which is comparable to the QKD system in Ref. [47] where the QBER at 50 km was 3.85%. The differing achievable transmission distances between the work presented here and Ref. [47] is largely due to the increased loss of the fused silica optical fibers for light with a wavelength of 850 nm.

[1] D. R. Stinson, *Cryptography: Theory and Practice*, 3rd ed. (Chapman and Hall, Boca Raton, Florida, 2006).

[2] R. L. Rivest, A. Shamir, and L. Adleman, Commun. ACM **21**, 120 (1978).

[3] T. Elgamal, IEEE Trans. Inf. Theory **31**, 469 (1985).

[4] D. Johnson, A. Menezes, and S. Vanstone, Int. J. Inf. Secur. **1**, 36 (2001).

[5] P. W. Shor, SIAM J. Comput. **26**, 1484 (1997).

[6] D. Gottesman and I. Chuang, arXiv:quant-ph/0105032.

[7] E. Andersson, M. Curty, and I. Jex, Phys. Rev. A **74**, 022304 (2006).

[8] C. Swanson and D. Stinson, in *Information Theoretic Security*, 1st ed., edited by S. Fehr (Springer, Berlin, 2011), Chap. 10, pp. 100–116.

[9] D. Chaum and S. Roijakkers, in *Proceedings of the 10th Annual International Cryptology Conference on Advances in Cryptology*, edited by A. Menezes and S. A. Vanstone (Springer-Verlag, London, UK, 1991), pp. 206–214.

[10] G. Hanaoka, J. Shikata, Y. Zheng, and H. Imai, in *Advances in Cryptology ASIACRYPT 2000*, edited by T. Okamoto (Springer, Kyoto, Japan, 2000), pp. 130–142.

[11] M. N. Wegman and J. L. Carter, J. Comput. Syst. Sci. **22**, 265 (1981).

[12] P. J. Clarke, R. J. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G. S. Buller, Nat. Commun. **3**, 1174 (2012).

[13] 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).

[14] F. Bussières, N. Sangouard, M. Afzelius, H. de Riedmatten, C. Simon, and W. Tittel, J. Mod. Opt. **60**, 1519 (2013).

[15] C. Simon, M. Afzelius, J. Appel, A. Boyer De La Giroday, S. J. Dewhurst, N. Gisin, C. Y. Hu, F. Jelezko, S. Kröll, J. H. Müller *et al.*, Eur. Phys. J. D **58**, 1 (2010).

[16] H. P. Specht, C. Nölleke, A. Reiserer, M. Uphoff, E. Figueroa, S. Ritter, and G. Rempe, Nature (London) **473**, 190 (2011).

[17] K. F. Reim, P. Michelberger, K. C. Lee, J. Nunn, N. K. Langford, and I. A. Walmsley, Phys. Rev. Lett. **107**, 053603 (2011).

[18] V. Dunjko, P. Wallden, and E. Andersson, Phys. Rev. Lett. **112**, 040502 (2014).

[19] P. Wallden, V. Dunjko, and E. Andersson, J. Phys. A **47**, 125303 (2013).

[20] P. Wallden, V. Dunjko, A. Kent, and E. Andersson, Phys. Rev. A **91**, 042304 (2015).

[21] R. Amiri, P. Wallden, A. Kent, and E. Andersson, arXiv:1507.02975.

[22] J. Carter and M. N. Wegman, J. Comput. Syst. Sci. **18**, 143 (1979).

[23] A. Abidin and J.-Å. Larsson, Quant. Info. Proc. **13**, 2155 (2014).

[24] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[25] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka *et al.*, Opt. Express **19**, 10387 (2011).

[26] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Photon. **7**, 378 (2013).

[27] H. Singh, D. Gupta, and A. Singh, IOSR J. Comput. Eng. **16**, 01 (2014).

[28] P. J. Clarke, R. J. Collins, P. A. Hiskett, P. D. Townsend, and G. S. Buller, Appl. Phys. Lett. **98**, 131103 (2011).

[29] P. J. Clarke, R. J. Collins, P. A. Hiskett, M.-J. García-Martínez, N. J. Krichel, A. McCarthy, M. G. Tanner, J. A. O'Connor, C. M. Natarajan, S. Miki *et al.*, New J. Phys. **13**, 075008 (2011).

[30] Nufern, Polarization Maintaining Short Wavelength Fibers, http://www.nufern.com/pam/optical_fibers/961/PM780-HP/.

[31] C. Marand and P. D. Townsend, Opt. Lett. **20**, 1695 (1995).

[32] Corning SMF-28e Optical Fiber Product Information, http://www.tlc.unipr.it/cucinotta/cfa/datasheet_SMF28e.pdf.

[33] Nufern, Nufern 780 nm Select Cut-off Single-Mode Fiber, http://www.nufern.com/pam/optical_fibers/883/780-HP/.

[34] K. J. Gordon, V. Fernandez, P. D. Townsend, and G. S. Buller, IEEE J. Quantum Electron. **40**, 900 (2004).

[35] Perkin-Elmer, SPCM-AQR Single Photon Counting Module, Perkin-Elmer Datasheet, www.optoelectronics.perkinelmer.com.

[36] G. S. Buller and R. J. Collins, Meas. Sci. Technol. **21**, 012002 (2010).

[37] R. J. Collins, R. H. Hadfield, and G. S. Buller, J. Nanophoton. **4**, 040301 (2010).

[38] G. S. Buller and R. J. Collins, in *Springer Series on Fluorescence: Methods and Applications: Advanced Photon Counting*, edited by P. Kapusta, M. Wahl, and R. Erdmann (Springer, Heidelberg, 2014), Chap. 3.

[39] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin *et al.*, Nat. Photon. **7**, 210 (2013).

[40] C. M. Natarajan, M. G. Tanner, and R. H. Hadfield, Supercond. Sci. Technol. **25**, 063001 (2012).

[41] M. Wahl, H.-J. Rahn, T. Röhlicke, G. Kell, D. Nettels, F. Hillger, B. Schuler, and R. Erdmann, Rev. Sci. Instrum. **79**, 123113 (2008).

[42] Mathworks, MATLAB 2014b (8.4.0.118713) (2014), http://mathworks.com/products/matlab/.

[43] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, Nat. Photon. **9**, 163 (2015).

[44] Heriot-Watt University data archive doi:10.17861/a10d9898-9a3c-4a9e-8d3f-2c0995c7310f.

[45] V. Chvátal, Discrete Math. **25**, 285 (1979).

[46] W. Hoeffding, J. Am. Stat. Assoc. **58**, 13 (1963).

[47] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe ,and A. J. Shields, Appl. Phys. Lett. **96**, 161102 (2010).

[48] S. Wang, W. Chen, J.-F. Guo, Z.-Q. Yin, H.-W. Li, Z. Zhou, G.-C. Guo, and Z.-F. Han, Opt. Lett. **37**, 1008 (2012).

[49] N. Namekata, H. Takesue, T. Honjo, Y. Tokura, and S. Inoue, Opt. Express **19**, 10632 (2011).