Article:
Roberts, G. L., Lucamarini, M., Dynes, J. F. et al. (2018) A direct GHz-clocked phase and intensity modulated transmitter applied to quantum key distribution. Quantum Science and Technology. 045010. ISSN: 2058-9565

https://doi.org/10.1088/2058-9565/aad9bd

PAPER • **OPEN ACCESS**

A direct GHz-clocked phase and intensity modulated transmitter applied to quantum key distribution

To cite this article: G L Roberts *et al* 2018 *Quantum Sci. Technol.* **3** 045010

Quantum Science and Technology

PAPER

A direct GHz-clocked phase and intensity modulated transmitter applied to quantum key distribution

G L Roberts[1,2], M Lucamarini[1], J F Dynes[1], S J Savory[2], Z L Yuan[1] and A J Shields[1]

[1] Toshiba Research Europe Ltd, 208 Cambridge Science Park, Milton Road, Cambridge CB4 0GZ, United Kingdom
[2] Cambridge University Engineering Department, 9 JJ Thomson Avenue, Cambridge CB3 0FA, United Kingdom

E-mail: zhiliang.yuan@crl.toshiba.co.uk

Keywords: quantum cryptography, quantum key distribution, quantum communications

OPEN ACCESS

RECEIVED
3 May 2018

REVISED
20 July 2018

ACCEPTED FOR PUBLICATION
13 August 2018

PUBLISHED
29 August 2018

Abstract

Quantum key distribution (QKD), a technology that enables perfectly secure communication, has evolved to the stage where many different protocols are being used in real-world implementations. Each protocol has its own advantages, meaning that users can choose the one best-suited to their application, however each often requires different hardware. This complicates multi-user networks, in which users may need multiple transmitters to communicate with one another. Here, we demonstrate a direct-modulation based transmitter that can be used to implement most weak coherent pulse-based QKD protocols with simple changes to the driving signals. This also has the potential to extend to classical communications, providing a low chirp transmitter with simple driving requirements that combines phase shift keying with amplitude shift keying. We perform QKD with concurrent time-bin and phase modulation, alongside phase randomisation. The acquired data is used to evaluate secure key rates for time-bin encoded BB84 with decoy states and a finite key-size analysis, giving megabit per second secure key rates, 1.60 times higher than if purely phase-encoded BB84 was used.

1. Introduction

Quantum key distribution (QKD) allows users to communicate with information theoretic security [1, 2]. This is possible by encoding the key on single photons so that a malign party trying to measure a key bit will alter its state in a manner observable to the legitimate parties. The security provided is of great value to anyone wishing to future-proof the secrecy of their information transfer. The technology is also practical and is currently implemented in a number of metropolitan networks [3, 4] and even in ground-satellite links [5–7].

Research developments tend to aim at improving the secure key rate and the achievable distance of QKD systems [8–11]. For example, the decoy-state BB84 protocol has security against coherent attacks, is able to reach distances of hundreds of kilometres and can achieve megabit per second secure key rates [12, 13]. However, this often makes systems more complex, requiring stabilisation routines and extra consideration to protect against side channels, where Eve attacks the practical implementation [14, 15].

QKD can be carried out using orthogonal states within two or more non-orthogonal bases. This means the result is non-deterministic if the state encoded in a certain basis is measured in a different basis. Time-bin qubits, prepared with the setup in figure 1(a), are the natural choice in optical fibres because the pulses travel along the fibre with their phase reference, meaning that perturbations apply to both pulses. Their state can be conveniently represented using the Bloch sphere, as depicted in figure 1(b). The equatorial bases, X and Y, correspond to two equal intensity pulses with a phase difference between them. States in X and Y can be realised by separating a single phase-randomised pulse into a signal and reference pulse using an asymmetric Mach–Zehnder interferometer (AMZI), then encoding a phase difference using a phase modulator (PM). This can be decoded using an identical AMZI. The polar basis, Z, corresponds to a pulse in just one of the two potential time bins. States in this basis can be decoded by measuring the arrival time of the time-bins in the receiver's detectors.

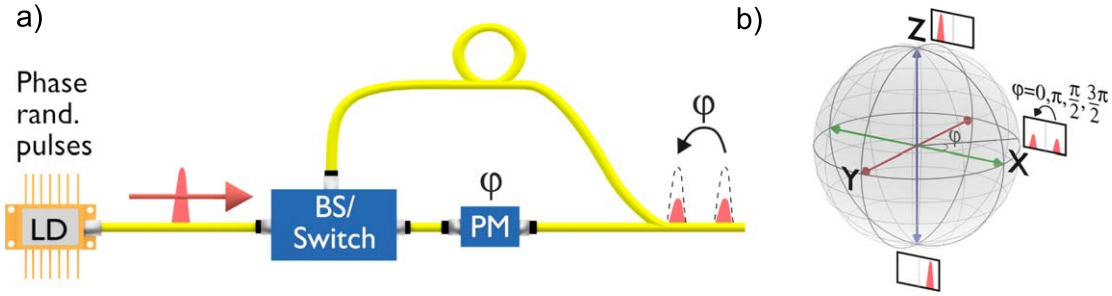

Figure 1. X, Y, Z QKD bases (a) a possible schematic to produce all the necessary QKD states using a phase-randomised pulse source and a device that can act as a beamsplitter (BS) and a high-speed switch, plus a phase modulator (PM) producing a phase shift ϕ. To produce the X and Y bases, the device acts as a beamsplitter (BS), phase modulating one half of the pulse using the PM and delaying the other half with an optical delay line. To produce the Z basis, the device acts as a switch, routing the pulse down one path to place it in the desired time-bin and (b) Bloch sphere representation of qubit states.

In this manuscript, we refer to the QKD protocol using the Z basis alongside either the X or Y bases as *polar BB84*, and the protocol using the X and Y bases as *phase-encoded BB84*. Polar BB84 could theoretically be implemented using the BS/switch component shown in figure 1(a). However this is not a commonly available component and it is challenging to build a device that can act reliably as a high-speed switch and beamsplitter at the rates required by QKD systems. One of the most practical setups to implement polar BB84 [16] uses a phase-randomised pulsed laser diode as the source, separated into a reference and signal pulse by an AMZI and then encoded using another intensity modulator (IM) and a PM. This setup is bulky and would require stabilisation routines to ensure the AMZI delay line is matched to that in Bob's receiver for a real-world implementation. Another drawback is that the transmitter is not versatile, requiring modifications if one wishes to implement another QKD protocol, for example differential phase shift [17, 18], coherent one way [19, 20] or differential quadrature phase shift [21, 22].

A promising QKD transmitter that mitigates these aforementioned drawbacks modulates the phase of one laser, which is then inherited by the pulses of another laser via optical injection locking (OIL) [23]. This enables the precise control of the output phase of pulses, as well as the ability to perform on-demand phase randomisation [24]. OIL also gives an enhanced modulation bandwidth, allowing time-bin encoding to be carried out on gain-switched pulses at 2 GHz, whilst maintaining a coherent phase [25]. However, it has not yet been possible to simultaneously directly modulate the phase and intensity of a light source with the high purity necessary for QKD.

Here, we use direct laser modulation to concurrently modulate the phase and intensity of the transmitter to provide six states that can be used to perform QKD without the need for an interferometer in the transmitter. The directly-modulated system produces signal and vacuum states, allowing a single IM to be used to prepare the decoy states and to equalise the mean photon number in the phase bases. We use the Z and X bases to implement the polar BB84 protocol and compare the results to phase-encoded BB84 implemented with the Y and X bases. The low quantum bit error rate (QBER) of the polar basis relative to the equatorial bases means that its use as the signal state allows for fewer bits to be lost to error correction, enhancing the secure key rate.

2. Experimental realization

The transmitter we use is based on OIL and is shown in figure 2. The protocols implemented are decoy-state polar BB84 and decoy-state phase-encoded BB84 [26–28].

The phase preparation laser encodes a relative phase between pulse pairs using a 750 ps signal to bring the laser above threshold and to coincide temporally with two pulse preparation laser pulses 500 ps apart. A 250 ps modulation is applied in the middle of this signal to control the relative phase between the two pulses. The laser is then driven below threshold for 250 ps to ensure the global phase of every pulse pair is completely random due to the random phase of spontaneous emission photons [23, 24]. The optical signal is injected into the pulse preparation laser via a circulator, where pulses adopt the phase of the phase preparation laser. This removes the need for a high-speed PM and an extra random number generator for phase-encoding and randomisation. A 1550 nm DFB laser diode with a 10 GHz bandwidth (Gooch & Housego AA0701) is used as the phase preparation laser and a custom-made laser without an optical isolator as the pulse preparation laser.

The electrical signal into the pulse preparation laser is patterned to produce intensity-modulated gain-switched pulses [25]. For polar BB84 with decoy states, empty pulses are required to prepare Z basis states and vacuum states. 250 ps electrical pulses are input to the pulse preparation laser at a frequency of 2 GHz and the

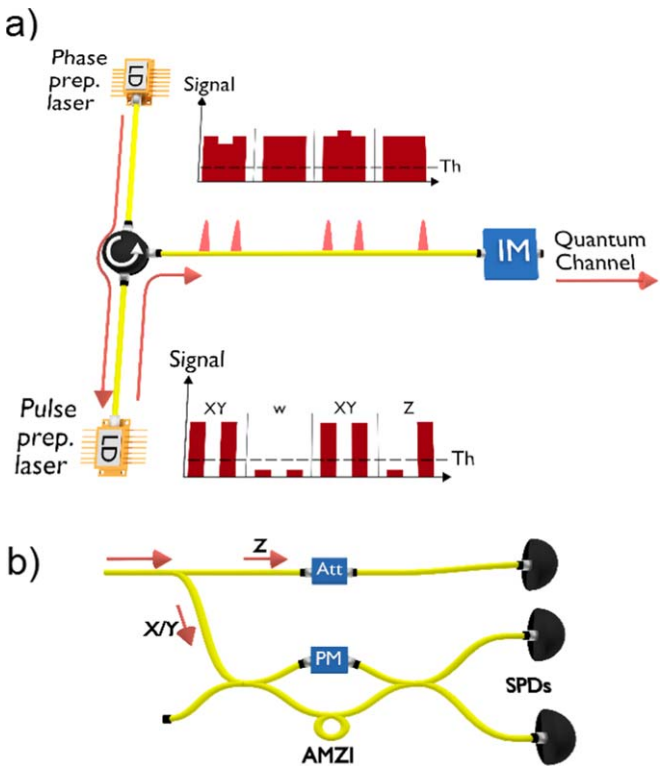

Figure 2. Experimental design. (a) Light from the phase preparation laser diode (LD) is injected into the pulse preparation laser diode via a circulator. The applied electrical signals are shown beside each laser and the pulse intensities are shown along the fibre. An intensity modulator (IM) can then be used to prepare decoy states and to equalise the polar and equatorial state intensities before attenuation and transmission through the quantum channel. (b) The Z basis is measured through direct detection whereas X/Y basis detection uses an asymmetric Mach–Zehnder interferometer (AMZI) with a phase modulator (PM) on one arm. An attenuator (Att) on the Z detection arm balances the losses of the X/Y detection arm.

DC is set to below the lasing threshold. When a signal or decoy pulse is required, the electrical signal is above the lasing threshold. To prepare a vacuum state the electrical signal is below the lasing threshold, as shown in figure 2. The X and Y bases can then be attenuated by 3 dB so that they contain the same mean photon number as the Z basis. Although only two bases are used for BB84, we take experimental data for the X, Y and Z bases, allowing us to demonstrate the versatility of the transmitter.

The transmission basis probabilities are set to $P_Z = 0.8$, $P_X = P_Y = 0.1$ and the probabilities of sending a signal (photon flux s), decoy (photon flux v) and vacuum (photon flux w) state are $P_s = 0.8$, $P_v = P_w = 0.1$ respectively. The photon fluxes are 0.5, 0.038 and 0.001 for s, v and w respectively. A proof of principle experiment is then carried out, where data is measured for 20 min per basis at each distance, giving 40 min of key time for both the polar BB84 protocol and phase-encoded BB84. This allows us to maximise the number of key bits, whilst providing a sufficient number of bits in the check basis to keep the fluctuations low.

The pulse preparation laser is clocked at 2 GHz, giving an effective system clock rate of 1 GHz. This is because two time bins are required to encode a single qubit. A 2^{10}-bit pseudorandom sequence is generated as Alice's pattern, allowing the corresponding electrical signals to be input to drive the laser diodes. A fixed 12 GHz spectral filter (Advanced Optics Solutions—ASE Filter) at 1 550.12 nm is placed at Alice's output to reduce any amplified spontaneous emission. The pulses are then attenuated to the required photon number before being sent through the quantum channel to Bob.

The X and Y data are collected using an AMZI with a 500 ps time delay on one arm to interfere consecutive pulses. A polariser is placed at the output of the AMZI to clean the signal, necessitating the use of a polarisation controller in Alice for alignment. The AMZI has a 1.7 dB loss and half of the photons (the reference pulses) contain no information so are discarded. A fixed attenuation of 4.7 dB must be placed on the Z measurement arm to balance the detection efficiencies for each measurement basis. This is because the security of BB84 relies on identical basis-independent detection probabilities [2, 29, 30].

The detected counts are tagged using a digitizer and binned into 2^{11}-bin histograms for extraction of the counts and error rates. A 10 ns subset of this histogram before creation of decoy states and equalisation of the X and Y bases intensities can be seen in figure 3. Random interference occurs in the X and Y bases when two pulses from separate blocks interfere, giving an average interference intensity of half the maximum intensity. An empty pulse followed by a full pulse has no interference, thus producing a quarter of the maximum intensity.

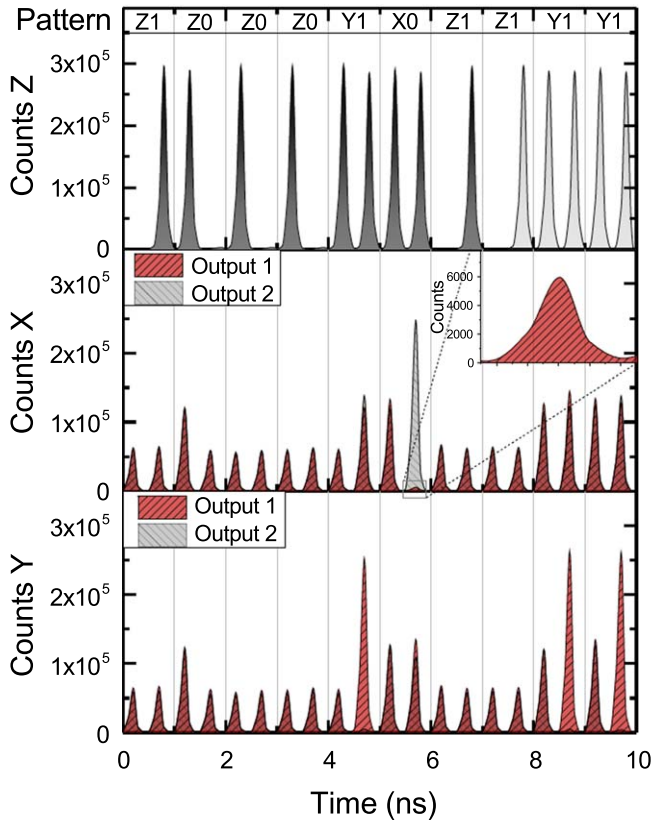

Figure 3. Directly-modulated traces. Measurement traces before decoy-state preparation and basis intensity equalisation. The *Z* basis (top) has only a single trace, whereas the *X* and *Y* bases (middle and bottom) have two AMZI outputs. The corresponding input pattern values are displayed at the top, labelled as *Bb*, where *B* is the basis and *b* is the logical bit value inside that basis. A red (grey) peak in the *X* and *Y* bases corresponds to a '0' ('1') logical bit, where the photon exits through the upper (lower) AMZI port. Peaks in output 1 (2) counts of the AMZI are complemented by small counts in output 2 (1) (middle inset), showing the high distinguishability between bits.

The detectors used are superconducting nanowire SPDs with a detection efficiency of 34%, a dark count rate of 30 Hz and a deadtime of <20 ns. The jitter increases and efficiency decreases with increasing count rate, so measurements are not taken at count rates over 10 MCounts s^{-1}.

A digitizer with 100 ps time bins and constant factor discrimination then processes the counts. The detectors have a polarisation dependence, so a polarisation controller is used for optimal detection efficiency. Although the receiver is adapted to each specific protocol, the transmitter remains entirely unchanged. This is a necessary feature for a multi-protocol QKD transmitter.

3. Results

The number of signal and decoy counts measured in each basis is shown in figure 4(a). These decrease exponentially because the measurement time remains constant at 20 min, regardless of the distance, whereas received counts scales exponentially with channel loss. Figure 4(b) highlights the 2.6 percentage point drop in QBER between the *XY* bases and *Z* basis. Simulations using the experimental parameters and the predicted count rate based on the system losses are also shown. The finite key-size analysis is detailed by Lim *et al* [12], which quantifies the security and correctness of the protocol through the parameters ε_{sec} and ε_{cor}. In this implementation, these values are set to 2×10^{-11} and 1×10^{-15} respectively. The key rate, R_L is calculated using

$$R_L = [s_{ZZ;0} + s_{ZZ;1}(1 - h(\phi_z)) - \lambda_{EC} - \Delta(\varepsilon_{\text{sec}}, \varepsilon_{\text{cor}})]/t, \quad (1)$$

where $s_{XX,ZZ;\,n}$ is the number of counts measured by Bob in the *X* or *Z* basis, given that Alice prepared an *n*-photon state in the *X* or *Z* basis respectively, ϕ_Z is the single photon phase error rate in *Z*, λ_{EC} is the error correction information, Δ is the finite key-size correction term and *t* is the time used to collect the experimental data block [12]. The key rates displayed in 4(c) show an experimental secure key rate of 1.26 megabits per second at an equivalent distance of 40 km (assuming optical fibre with a 0.2 dB km^{-1} loss) using an attenuator and 246

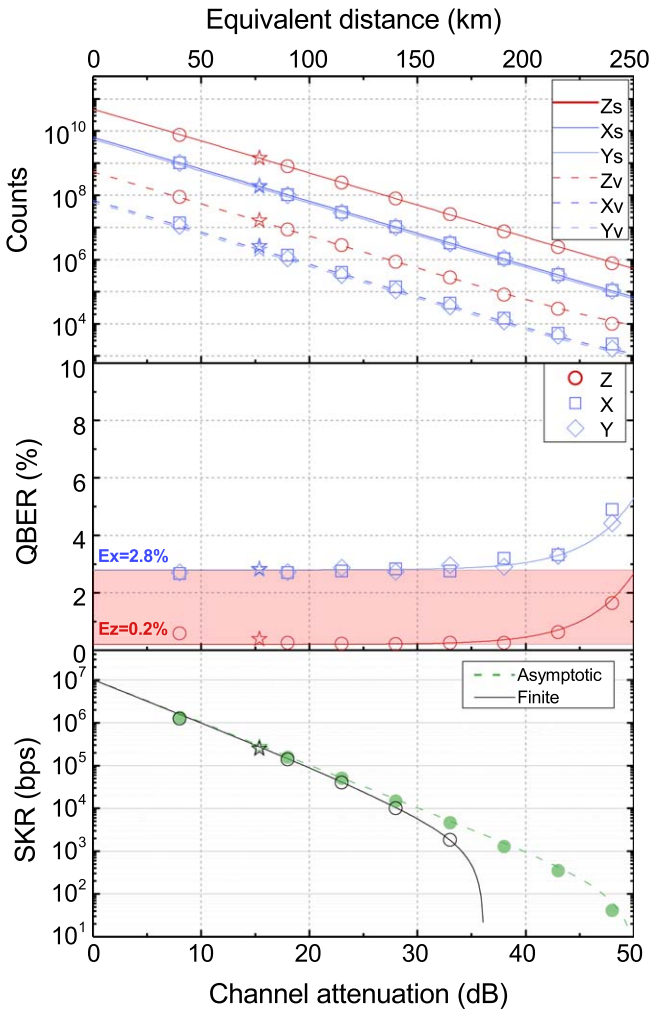

Figure 4. Polar BB84 results with decoy states, secure against coherent attacks. Lines are theoretical results and symbols are experimentally measured or calculated values. (a) Number of counts measured in each basis, (b) QBER for each basis, (c) secure key rate (SKR) in the asymptotic (filled symbols, dotted line) and finite key-size regimes (empty symbols, solid line). The star symbols are data measured with real fibre as the quantum channel.

kilobits per second in real fibre of length 75 km. A positive secure key rate could be achieved up to 250 km in the asymptotic limit and up to 180 km with the finite key-size analysis of equation (1) for just 40 min of key time.

To compare between polar BB84 and phase-encoded BB84, we looked at the secure key rate in the asymptotic limit using the experimental parameters obtained in the *ZX* and the *YX* bases respectively. The transmission basis probabilities are renormalised to allow for a fair comparison. The key rate is improved by 1.60 times when using the *ZX* bases compared to the *YX* bases. Also, phase-encoded BB84 is able to reach an attenuation of 48.5 dB with a positive secure key rate, whereas polar BB84 can reach slightly further, at 50.1 dB.

4. Discussion

Our implementation produced six states in order to show the versatility of the source, however only used four for the QKD implementations. Six-state QKD is possible and has a slightly higher tolerance to noise than its four-state counterpart, leading to the ability to share secure keys at slightly longer distances [2]. The main drawback is found in the receiver. Polar BB84 can be implemented with three SPDs (phase-encoded BB84 would require two SPDs in an active receiver and four SPDs in a passive receiver). Six-state QKD, on the other hand, requires an extra AMZI and two extra SPDs if it is to remain passive, or a high-speed PM in the AMZI to choose the basis in an active implementation. Both of these options add significant complexity when compared to their meager increase in secure key distance. Indeed, four-state QKD could be carried out for a longer time-period to reduce statistical fluctuations and increase the achievable distance. Reference frame independent-QKD [31] is another protocol that requires three bases, allowing two bases to drift in time while the other stays constant. This basis drift is a problem for polarisation-encoded systems in real fibre, however is not an issue for phase-encoded

systems like the one demonstrated here because the signal travels along the fibre with the phase reference. Multi-protocol transmitters have also been demonstrated in [32, 33], although these have the drawbacks of being complex and not offering phase randomisation, respectively.

As well as the aforementioned benefit of requiring one fewer SPD for polar BB84 compared to phase-encoded BB84, the key rates are also improved by a factor of 1.60 times. This is made possible by the reduced QBER of the signal basis from 2.8% to 0.2%, which reduces the bits lost to error correction, hence improving the secure key rate.

Direct preparation of decoy states can be realised by driving the pulse preparation laser at different levels above the lasing threshold to reach different intensities. This is ideal because no external hardware, for example an IM, is required. This would also be useful for classical communications, increasing the number of bits encoded per symbol [34]. We have achieved intensity modulation using this method. This creates a patterning effect for the decoy states, however, where the intensity of a pulse is correlated with the intensity of the preceding pulse, opening the door to side-channel attacks [16]. To avoid this security loophole, the QKD decoy states are instead produced using a two-level Sagnac-based IM [35].

The transmitter also shows promise to be useful in classical communications. The patterning effects that proved prohibitive for QKD when directly producing multiple intensity states are not a major concern here, it will just add a slight degradation to the distinguishability between states. The direct modulation means that the system is not reliant on multiple external modulators, making it cheaper, less complex and also easier to integrate with other components. The OIL ensures that all pulses have the same wavelength. This removes a side channel for QKD, but also means the system has low chirp, reducing the inter-symbol interference caused by dispersion effects. In this paper we have shown the accurate production of four phase states, however this can easily be increased by using more phase-preparation levels. Different intensities can be produced directly, and also a vacuum state can be produced, further increasing the amount of information encoded per symbol.

5. Conclusion

In this paper, we have demonstrated a transmitter capable of performing all weak coherent pulse-based QKD protocols, performing phase and intensity encoding simultaneously. With this system, we have demonstrated the decoy-state polar BB84 protocol and the decoy-state phase-encoded BB84 protocol in a single experiment, preparing the six states in three different bases required by the simultaneous execution of these two protocols from a single transmitter. In both bases we found a secure key rate in the order of 1 megabit per second at 8 dB attenuation, with the decoy-state polar BB84 protocol providing a 1.6 times larger secure key rate on average and a slightly higher tolerance to losses.

The ability to adapt to different protocols with simple software changes makes the transmitter more robust in network scenarios where all the users could potentially have different receivers. Alongside this, the system is more simple than many other transmitters that are dedicated to a single protocol, which is appealing for real-world implementations. Also the relatively few components ensure it has a good power efficiency and make it ideal for on-chip implementations. The versatility, low power consumption and stability of this transmitter make it the natural choice for use in metropolitan multi-user quantum networks.

Acknowledgments

G L R gratefully acknowledges financial support from the EPSRC CDT in Integrated Photonic and Electronics Systems, Toshiba Research Europe Limited and an industrial fellowship with The Royal Commission for the Exhibition of 1851. This work has been supported by funding through the EPSRC Quantum Communications Hub EP/M013472/1.

ORCID iDs

G L Roberts https://orcid.org/0000-0002-7318-0669

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[2] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301
[3] Peev M *et al* 2009 *New J. Phys.* **11** 075001
[4] Sasaki M *et al* 2011 *Opt. Express* **19** 10387
[5] Vallone G, Bacco D, Dequal D, Gaiarin S, Luceri V, Bianco G and Villoresi P 2015 *Phys. Rev. Lett.* **115** 040502

[6] Liao S-K et al 2017 Nat. Photon. 11 509
[7] Takenaka H, Carrasco-Casado A, Fujiwara M, Kitamura M, Sasaki M and Toyoshima M 2017 Nat. Photon. 11 502
[8] Ma X, Qi B, Zhao Y and Lo H-K 2005 Phys. Rev. A 72 012326
[9] Dixon A R, Yuan Z L, Dynes J F, Sharpe A W and Shields A J 2008 Opt. Express 16 18790
[10] Bacco D, Christensen J B, Castaneda M A U, Ding Y, Forchhammer S, Rottwitt K and Oxenløwe L K 2016 Sci. Rep. 6 36756
[11] Yin H-L et al 2016 Phys. Rev. Lett. 117 190501
[12] Lim C C W, Curty M, Walenta N, Xu F and Zbinden H 2014 Phys. Rev. A 89 022307
[13] Fröhlich B, Lucamarini M, Dynes J F, Comandar L C, Tam W W-S, Plews A, Sharpe A W, Yuan Z and Shields A J 2017 Optica 4 163
[14] Dixon A R et al 2017 Sci. Rep. 7 1978
[15] Lo H-K, Curty M and Qi B 2012 Phys. Rev. Lett. 108 130503
[16] Yoshino K-I, Fujiwara M, Nakata K, Sumiya T, Sasaki T, Takeoka M, Sasaki M, Tajima A, Koashi M and Tomita A 2018 NPJ Quantum Inf. 4 8
[17] Shibata H, Honjo T and Shimizu K 2014 Opt. Lett. 39 5078
[18] Inoue K 2015 IEEE J. Sel. Top. Quantum Electron. 21 109
[19] Korzh B, Lim C C W, Houlmann R, Gisin N, Li M J, Nolan D, Sanguinetti B, Thew R and Zbinden H 2015 Nat. Photon. 9 163
[20] Branciard C, Gisin N and Scarani V 2008 New J. Phys. 10 013031
[21] Inoue K and Iwai Y 2009 Phys. Rev. A 79 022319
[22] Kawakami S, Sasaki T and Koashi M 2016 Phys. Rev. A 94 022332
[23] Yuan Z L, Fröhlich B, Lucamarini M, Roberts G L, Dynes J F and Shields A J 2016 Phys. Rev. X 6 031044
[24] Roberts G L, Lucamarini M, Dynes J F, Savory S J, Yuan Z and Shields A J 2017 Appl. Phys. Lett. 111 261106
[25] Roberts G L, Lucamarini M, Dynes J F, Savory S J, Yuan Z L and Shields A J 2017 Laser Photonics Rev. 11 1700067
[26] Hwang W-Y 2003 Phys. Rev. Lett. 91 057901
[27] Wang X-B 2005 Phys. Rev. Lett. 94 230503
[28] Lo H-K, Ma X and Chen K 2005 Phys. Rev. Lett. 94 230504
[29] Koashi M 2006 arXiv:quant-ph/0609180
[30] Tomamichel M, Lim C C W, Gisin N and Renner R 2012 Nat. Commun. 3 634
[31] Laing A, Scarani V, Rarity J G and O'Brien J L 2010 Phys. Rev. A 82 012304
[32] Sibson P et al 2017 Nat. Commun. 8 13984
[33] Korzh B, Walenta N, Houlmann R and Zbinden H 2013 Opt. Express 21 19579
[34] Noguchi T, Daido Y and Nossek J A 1986 IEEE Commun. Mag. 24 21
[35] Roberts G L, Pittaluga M, Minder M, Lucamarini M, Dynes J F, Yuan Z L and Shields A J 2018 arXiv:1807.07414