Zhang, P., Aungskunsiri, K., Martín-López, E., Wabnig, J., Lobino, M., Nock, R. W., Munns, J., Bonneau, D., Jiang, P., Li, H. W., Laing, A., Rarity, J. G., Niskanen, A. O., Thompson, M. G., & O'Brien, J. L. (2014). Reference-frame-independent quantum-key-distribution server with a telecom tether for an on-chip client. *Physical Review Letters*, *112*(13), [130501]. https://doi.org/10.1103/PhysRevLett.112.130501

Reference-Frame-Independent Quantum-Key-Distribution Server with a Telecom Tether for an On-Chip Client

P. Zhang,[1,2] K. Aungskunsiri,[1] E. Martín-López,[1] J. Wabnig,[3] M. Lobino,[1,4] R. W. Nock,[5] J. Munns,[1,6] D. Bonneau,[1] P. Jiang,[1] H. W. Li,[3] A. Laing,[1,*] J. G. Rarity,[5] A. O. Niskanen,[3] M. G. Thompson,[1] and J. L. O'Brien[1]

[1]*Centre for Quantum Photonics, H. H. Wills Physics Laboratory and Department of Electrical and Electronic Engineering, University of Bristol, Bristol BS8 1UB, United Kingdom*

[2]*MOE Key Laboratory for Nonequilibrium Synthesis and Modulation of Condensed Matter and Department of Applied Physics, Xi'an Jiaotong University, Xi'an 710049, China*

[3]*Nokia Research Center, Broers Building, 21 J.J. Thomson Avenue, Cambridge CB3 0FA, United Kingdom*

[4]*Centre for Quantum Dynamics and Queensland Micro and Nanotechnology Centre, Griffith University, Brisbane, Queensland 4111, Australia*

[5]*Department of Electrical and Electronic Engineering, University of Bristol, Bristol BS8 1UB, United Kingdom*

[6]*Bristol Centre for Functional Nanomaterials, Centre for NSQI, University of Bristol, Bristol BS8 1FD, United Kingdom*

(Received 15 August 2013; published 2 April 2014)

We demonstrate a client-server quantum key distribution (QKD) scheme. Large resources such as laser and detectors are situated at the server side, which is accessible via telecom fiber to a client requiring only an on-chip polarization rotator, which may be integrated into a handheld device. The detrimental effects of unstable fiber birefringence are overcome by employing the reference-frame-independent QKD protocol for polarization qubits in polarization maintaining fiber, where standard QKD protocols fail, as we show for comparison. This opens the way for quantum enhanced secure communications between companies and members of the general public equipped with handheld mobile devices, via telecom-fiber tethering.

DOI: 10.1103/PhysRevLett.112.130501 PACS numbers: 03.67.Dd, 03.65.Vf, 42.50.Ar, 42.50.Ex

The principle of quantum mechanics that requires microscopic systems to be changed upon observation has perplexed physicists since its formulation, yet understanding that the effect could be harnessed as a resource gave birth to the field of quantum cryptography [1–13]. Quantum enhanced security in communication is available through quantum key distribution (QKD), which exploits the behaviour of single photons to allow two parties to exchange the binary string, or key, that is used in the encryption of sensitive information. Now implementable with current technologies [14–16], QKD has matured to the stage where it is moving from research laboratories towards commercial applications [17]. Here we demonstrate the feasibility of equipping mobile communication devices with quantum cryptographic capabilities by making a QKD server accessible over a telecom fiber, to which a client may tether.

The transmission of quantum information, suitable for QKD, normally requires that a state sent by Alice is faithfully received by Bob, unless an eavesdropper, Eve, observes the state and reveals her presence as an otherwise unexplainable disturbance. Yet even in the absence of Eve, an unstable fiber communication link or instability in the sending and receiving apparatus, is equivalent to an unknown or varying reference frame, and has the effect of unhelpfully transforming the states that Bob receives [18].

Attempts to overcome potential reference frame misalignment by encoding qubits within larger systems [19–21] require creation, manipulation, and detection of many-photon entangled states, which is technically challenging and very loss-sensitive. Encoding information into the modes available from the transverse spatial profile of light [22–25], may facilitate communication between misaligned parties, through air or vacuum, but encounters problems such as mode dispersion when transmitting through fiber. Protocols that exploit the arrival time of photons as a logical basis necessitate stable interferometers to perform encoding and decoding, requiring active stabilization in fiber [26], or precise temperature regulation in on-chip QKD with highly asymmetric interferometers [27].

An alternative time-multiplexing scheme is the plug-and-play system which sends each light pulse back and forth along the same fiber, with the aid of a Faraday mirror, to cancel the effects of birefringence [28–32]. Interferometric stability results from both halves of the time-split pulse retracing each other's path. A drawback to this double-pass arrangement is the potential for an increased error rate due to Rayleigh backscattering, which requires the addition of a storage line to hold a train of pulses which must complete a round trip before the next train is sent. A further stability constraint, related to the length of transmission, is that fluctuations in the fiber and interferometer should be slow on the time scale of the double pass.

The reference frame independent QKD protocol (rfiQKD) [33–36], deployed here, operates between unknown and changing reference frames, is independent of any particular choice of apparatus or information encoding, requires no entanglement, and is implementable with two-level systems encoded onto single photons that

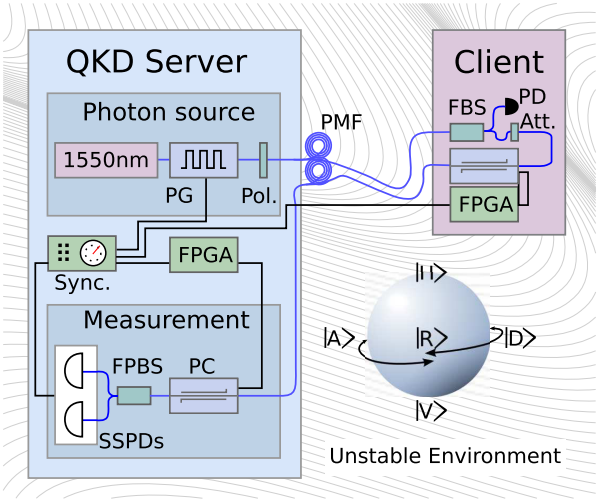

FIG. 1 (color online). Experimental setup for client-server rfiQKD. The server side holds a telecom wavelength (1550 nm) laser with a 1 MHz pulse generator (PG) and fixed polarizer, to send light pulses to the client through a polarization maintaining fiber (PMF). At the client side, an integrated polarization controller (PC) encodes qubits into the polarization of the attenuated (Att.) light. A fiber beam splitter (FBS) and photodetector (PD) continuously monitor power for malicious attacks. Qubits received back at the server side are measured with a similar PC, fiber polarizing beam splitter (FPBS), and superconducting single photon detectors (SSPDs), all controlled by an electronic board synchronization (Sync.), function programmable gate array (FPGA), and processor. The Bloch sphere illustrates the effects of an unstable environment on polarization.

may be approximated with weak coherent laser pulses, making it intrinsically practical. The protocol will generate a secret key as long as the rate of change between reference frames is slow on the rate of particle repetition.

With freedom to choose the physical two-state encoding and no requirement for phase stability, the rfiQKD protocol allowed us to exploit commercially available lithium niobate integrated polarization controllers [37] to implement QKD with photon-polarization qubits over an unstabilized fiber link. Larger resources, such as the photon source and superconducting detectors [38,39], are situated on Bob's side, which can be regarded as the server side, while Alice, as the client, requires only the capability to perform single qubit operations. The scenario is one in which the client tethers a hand held device, with an integrated photonic chip, to a telecom fiber to receive dim laser pulses from the QKD server, which the client attenuates to the single photon level, before encoding each pulse with a qubit of information for return transmission to the server, along a different fiber.

Here, we demonstrate a stable, constant, and continuously positive secret key rate over the unstabilized fiber link using the rfiQKD protocol, while the rate for the BB84 QKD protocol falls. We go on to show that our rfiQKD system automatically and passively recovers from the deliberate introduction of large amounts of noise in the form of rapid fluctuations.

Although formulated as an entanglement-driven protocol, rfiQKD can be implemented with weak coherent states that sufficiently approximate single photons, where Alice randomly prepares and sends the polarization states $\{D/A, R/L, H/V\}$ corresponding to the eigenvectors of the Pauli matrices, which we label as $\{X, Y, Z\}$ [40]. In our experiment, the requirement of one known and stable basis, used to encode the key, is fulfilled with the horizontal (H) and vertical (V) polarization states, which are preserved throughout transmission in polarization maintaining fiber (PMF). The other four states, superpositions of H and V used to guarantee security, are unhelpfully transformed by phase fluctuations in PMF due to environmental influences on the birefringence of the fiber; while this effect is troublesome for other protocols, rfiQKD operates in the presence of phase drifts that are slow on the repetition rate of sent photons. For fluctuations sufficiently rapid to force protocol failure, rfiQKD will automatically recover in calmer periods without the need for realignment, as we demonstrate.

The operation of the protocol, with its phase invariant security measure, works as follows. Expressing Alice and Bob's measurement bases as $Z_A = Z_B$, $X_B = \cos(\beta)X_A + \sin(\beta)Y_A$, and $Y_B = \cos(\beta)Y_A - \sin(\beta)X_A$, where β slowly changes with time in an unknown way, Alice randomly prepares quantum states which she sends to Bob, who measures in his randomly chosen basis; later they publicly reveal their choice of bases. The raw key is obtained when they both measure in the Z direction, providing a quantum bit-error rate,

$$Q = \frac{1 - \langle Z_A Z_B \rangle}{2}. \quad (1)$$

The other two slowly rotating bases are used to estimate the knowledge of a potential Eve. The quantity

$$C = \langle X_A X_B \rangle^2 + \langle X_A Y_B \rangle^2 + \langle Y_A X_B \rangle^2 + \langle Y_A Y_B \rangle^2, \quad (2)$$

is independent of the relative angle β. If there is no Eve and the communication channel is ideal with a fixed (although unknown) phase, then the correlation function $\langle Z_A Z_B \rangle$ is equal to 1 whereas $\langle X_A X_B \rangle$, $\langle X_A Y_B \rangle$, $\langle Y_A X_B \rangle$, and $\langle Y_A Y_B \rangle$ each take a constant value between -1 and 1 determined by β. Also, $\langle Z_A X_B \rangle$, $\langle Z_A Y_B \rangle$, $\langle X_A Z_B \rangle$, and $\langle Y_A Z_B \rangle$ should be zero as X, Y, and Z are mutually unbiased. With Z bases aligned, $Q = 0$ and $C = 2$ will be achieved, but in a realistic implementation, Q will be greater than zero and C will be less than 2.

The correlation functions involved in (1) and (2) are calculated from the rates of photon detections by assigning positive or negative signs to correlated or anticorrelated detections, respectively. For example, if Bob labels his pair of detectors as $b = \{0, 1\}$, while Alice labels the pair of

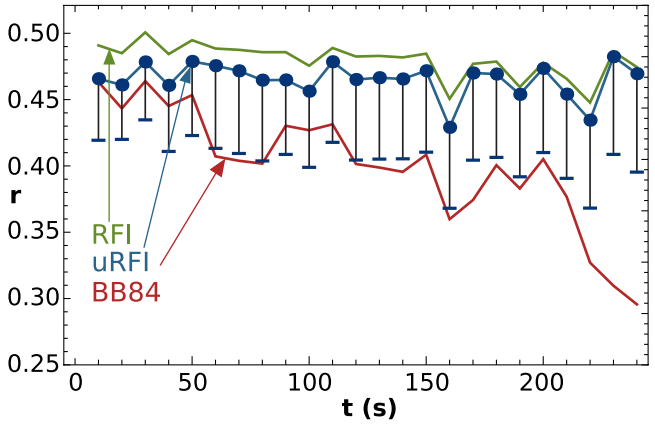

FIG. 2 (color online). Experimental data for secret key rate fraction r showing robustness to drift. Data are initially collected in the situation of well aligned client-server reference frames, but the unfixed PMF quantum channel is subject to ambient environmental influences, which effect a slowly varying reference frame. While the key rate for the rfiQKD protocols is constant, for BB84 it suffers a fall as the alignment drifts. Lower bounds on the secret key rate from the urfiQKD analysis are shown.

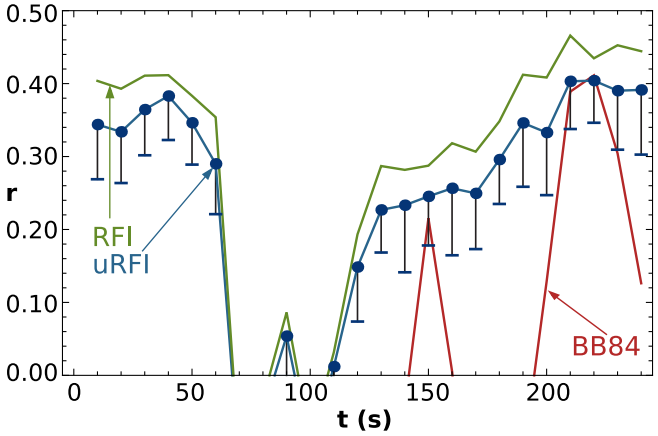

FIG. 3 (color online). Experimental data for secret key rate fraction r showing automatic recovery from rapid noise. During the initial 60 s, the unaligned and slowly varying reference frames result in BB84 failure while the rfiQKD protocols operate. Between $t = 60$ s and $t = 120$ s we deliberately introduced rapid PMF deformations to force an rfiQKD failure. However, an automatic and passive revival of r for the rfiQKD protocols is observed during the subsequent calm period.

states she sends (within a particular basis) as $a = \{0, 1\}$ then the $\langle AB \rangle$ expectation value is calculated from the number of detector clicks n_{ab} as $(n_{00} + n_{11} - n_{01} - n_{10})/(n_{00} + n_{11} + n_{01} + n_{10})$, which is essentially the normalized difference between correlated and anticorrelated detections.

The security proof of the rfiQKD protocol [33] shows that when $Q \lesssim 15.9\%$, Eve's information is given by

$$E(Q, C) = (1 - Q)h\left(\frac{1 + \tilde{u}}{2}\right) + Qh\left(\frac{1 + v(\tilde{u})}{2}\right), \quad (3)$$

where

$$\tilde{u} \equiv u_{\max} = \min\left[\frac{\sqrt{C/2}}{1 - Q}, 1\right],$$
$$v = \frac{1}{Q}\sqrt{C/2 - (1 - Q)^2 u_{\max}^2},$$

and the $h(x)$ is the binary entropy. The secret key rate is given by

$$r = 1 - h(Q) - E(Q, C). \quad (4)$$

The experimental setup is shown in Fig. 1. At the server side, light from a 1550 nm continuous-wave laser source is sent through a pulse generator (PG) to produce pulses of 100 ns width with a repetition rate of 1 MHz, which are filtered by a horizontal polarizer and transmitted to the client through PMF. At the client side, a fiber beam splitter and photodetector expose hypothetical attacks (for example, [41]). A ≈75 dB attenuator reduces the light intensity to the single photon level of ≈0.1 photons per pulse so that the probability of more than one photon per pulse ≈ 0.005. The client randomly prepares among the six polarization states $\{D, A, R, L, H, V\}$ using a $LiNbO_3$ [42,43] polarization controller (PC) commanded from a field programmable gate array (FPGA) and associated driver circuits. Photonic qubits are returned to the server, along another unstabilized 5 m length of PMF, where a similar PC and FPGA, together with a fiber polarization beam splitter and superconducting single photon detectors, perform projective measurements chosen randomly among the three relevant bases. With the efficiency of the SSPDs at 10%, the final average repetition rate is 10 kHz.

All system elements are synchronized to the SYNC-FPGA platform, which allows for precise timing of all stages within the transmission period. Each repetition begins with an optical pulse from the server side PG; when the pulse arrives at the client PC, it is set to prepare a particular polarization state; then, timed appropriately for the return of the pulse, the server PC is set to measure in a particular basis; finally, the state of the detectors is recorded by the FPGA.

In addition to demonstrating the feasibility of QKD between telecom-fiber-linked integrated photonic devices in the described client-server scheme, we aim to show two features of the rfiQKD protocol that are particularly relevant: robustness to phase drift which is inevitable in long-range fiber and automatic passive recovery from rapid noise.

We also present analysis for the uncalibrated variant urfiQKD protocol, which assumes not only unaligned reference frames but also removes the assumption for alignment within a reference frame, allowing for non-orthogonality within a basis and mutual bias between bases, and differing detector efficiencies that arise in a real-world

implementation [35]. This is achieved by using an explicit device model and minimizing the key rate over possible model parameters.

We demonstrated drift robustness of the rfiQKD and urfiQKD generated key rates in comparison with that of BB84, beginning key exchange with well aligned client-server reference frames, so that states prepared by the client PC had a high fidelity with projectors determined by the server PC. The PMF quantum channel was unfixed but undisturbed for the duration of the key exchange, subject only to ambient environmental influences. Figure 2 shows the secret key rate fraction, r, as a function of time for the BB84, rfiQKD, and urfiQKD protocols. The duration of key exchange is 240 s, so each of the 24 points corresponds to data integrated over 10 seconds, which is long enough to collect sufficient data to produce small error bars, corresponding to a precision of three standard deviations, but short enough to avoid significant depletion of the value of r, from integration over largely different values β. For clarity, these error bars are not displayed, instead we show the lower bound on r from the urfiQKD analysis. While the secret key fraction for BB84 falls as a function of time, the rfiQKD protocols maintain a secret key fraction of ≈ 0.44–0.49.

We demonstrated the automatic, passive recovery capability of our system after periods of rapid and substantial noise that force a protocol failure. Figure 3 shows r as a function of time for 24 points, each corresponding to 10 seconds of data, as before. During the initial 60 s of key exchange, the PMF quantum channel is unfixed and undisturbed but unaligned so that the BB84 protocol immediately fails. However the changes resulting from the ambient environment are slow enough for the rfiQKD protocols to operate successfully. Between $t = 60$ s and $t = 120$ s we deliberately introduced a large amount of noise by continually and significantly deforming the PMF to simulate a rapidly changing reference frame, forcing r to fall below zero. At $t = 120$ s, the noise ceases and as the PMF relaxes from the mechanical strains, a positive key rate automatically returns and achieves initial values for the rfiQKD protocols. In contrast, BB84 achieves a positive r only in brief transitionary periods of near-alignment. Again, the lower bound on r for the urfiQKD analysis is displayed.

In conclusion, we demonstrated a client-server QKD protocol where all large resources reside at server side, and the client requires only an integrated photonic device that could be further integrated into a hand held communication device. The key is exchanged though a PMF telecom-fiber tether using the rfiQKD protocol, that is shown to be passively robust to typical environmental drift effects and can automatically recover from large noise levels to re-establish QKD in calmer periods with no requirement for alignment. As is the case for other QKD schemes, photon loss becomes an issue as fiber length increases, leading to a potential photon number splitting (PNS) attack [44] for a photon source of weak coherent pulses. Considering the PMF loss rate of approx 0.5 dB/km in our proof of principle demonstration, even with high efficiency detectors [45,46], key exchange would be limited to a few km before a true single photon source [47] or decoy state strategies [48] are required to maintain security against PNS attacks. In addition, a comparative study of the effect of phase noise for security in different protocols as fiber length increases would be useful.

Here, rfiQKD is used to facilitate key exchange with polarization encoding in integrated photonic devices, yet the protocol itself is independent of any particular choice of encoding or apparatus. We were able to immediately exploit off-the-shelf components such as PMF and commercial polarization controllers to realize client QKD hardware, and we expect that the features demonstrated here will apply generally. In particular the adoption of the rfiQKD protocol in commercially available systems could simplify their operation.

Miniaturization of QKD devices is integral to the widespread adoption of QKD and our results pave the way for quantum enhanced security for the general public with handheld mobile devices. Future directions are to develop time multiplexing with rfiQKD to avoid the requirement for temperature-stabilized Mach Zehnder interferometers, allow for fiber fluctuations between Alice and Bob, and for drift between interferometers local to Alice and Bob. A time multiplexed rfiQKD system would be well suited to take advantage of existing (non-PMF) telecom-fiber networks.

This work was supported by EPSRC, ERC, QUANTIP, PHORBITECH, and NSQI. P. Z. acknowledges support from the Fundamental Research Funds for the Central Universities and the National Natural Science Foundation of China (Grants No. 11004158 and No. 11374008). J. M. acknowledges EPSRC Grant Code No. EP/G036780/1. J. L. OB. acknowledges a Royal Society Wolfson Merit Award and a Royal Academy of Engineering Chair in Emerging Technologies.

*anthony.laing@bristol.ac.uk

[1] C. H. Bennett and G. Brassard, *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), p. 175.
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
[4] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).
[5] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[6] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[7] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys., **74**, 145 (2002).

[8] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity, Nature (London) **419**, 450 (2002).
[9] T. Honjo, K. Inoue, and H. Takahashi, Opt. Lett. **29**, 2797 (2004).
[10] H. Takesue and K. Inoue, Phys. Rev. A **72**, 041804(R) (2005).
[11] E.-L. Miao, Z.-F. Han, T. Zhang, and G.-C. Guo, Phys. Lett. A **361**, 29 (2007).
[12] C. Bonato, A. Tomaello, V. D. Deppo, G. Naletto, and P. Villoresi, New J. Phys. **11**, 045017 (2009).
[13] M. Fujiwara, M. Toyoshima, M. Sasaki, K. Yoshino, Y. Nambu, and A. Tomita, Appl. Phys. Lett. **95**, 261103 (2009).
[14] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[15] M. Dušek, N. Lütkenhaus, and M. Hendrych, Prog. Opt. **49**, 381 (2006).
[16] H.-K. Lo and Y. Zhao, *Quantum Cryptography in Encyclopedia of Complexity and System Science* (Springer, New York, 2009), Vol. 8, p. 7265.
[17] N. Gisin and R. Thew, Nat. Photonics, **1**, 165 (2007).
[18] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, arXiv:1306.6134.
[19] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, Phys. Rev. Lett. **91**, 027901 (2003).
[20] J.-C. Boileau, D. Gottesman, R. Laflamme, D. Poulin, and R. W. Spekkens, Phys. Rev. Lett. **92**, 017901 (2004).
[21] T.-Y. Chen, J. Zhang, J.-C. Boileau, X.-M. Jin, B. Yang, Q. Zhang, T. Yang, R. Laflamme, and J.-W. Pan, Phys. Rev. Lett. **96**, 150504 (2006).
[22] F. M. Spedalieri, Opt. Commun. **260**, 340 (2006).
[23] L. Aolita and S. P. Walborn, Phys. Rev. Lett. **98**, 100501 (2007).
[24] C. E. R. Souza, C. V. S. Borges, A. Z. Khoury, J. A. O. Huguenin, L. Aolita, and S. P. Walborn, Phys. Rev. A **77**, 032345 (2008).
[25] V. D'Ambrosio, E. Nagali, S. P. Walborn, L. Aolita, S. Slussarenko, L. Marrucci, L. Lorenzo, and F. Sciarrino, Nat. Commun. **3**, 961 (2012).
[26] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré, and N. Gisin, Phys. Rev. Lett. **93** 180502 (2004).
[27] A. Tanaka, M. Fujiwara, S. Woo Nam, Y. Nambu, S. Takahashi, W. Maeda, K. Yoshino, S. Miki, B. Baek, Z. Wang, A. Tajima, M. Sasaki, and A. Tomita, Opt. Express **16**, 11354 (2008).
[28] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, Appl. Phys. Lett. **70**, 793 (1997).
[29] H. Zbinden, J. D. Gautier, N. Gisin, B. Huttner, A. Muller, and W. Tittel, Electron. Lett. **33**, 586 (1997).
[30] G. Ribordy, J. D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, Electron. Lett. **34**, 2116 (1998).
[31] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, New J. Phys. **4**, 41 (2002).
[32] P. Eraerds, N. Walenta, M. Legre, N. Gisin, and H. Zbinden, New J. Phys. **12**, 063027 (2010).
[33] A. Laing, V. Scarani, J. G. Rarity, and J. L. O'Brien, Phys. Rev. A **82**, 012304 (2010).
[34] L. Sheridan, T. P. Le, and V. Scarani, New J. Phys. **12**, 123019 (2010).
[35] J. Wabnig, D. Bitauld, H. W. Li, A. Laing, J. L. O'Brien, and A. O. Niskanen, New J. Phys. **15**, 073001 (2013).
[36] T. P. Le, L. Sheridan, and V. Scarani, Int. J. Quantum. Inform. **10**, 1250035 (2012).
[37] D. Bonneau, M. Lobino, P. Jiang, C. M. Natarajan, M. G. Tanner, R. H. Hadfield, S. N. Dorenbos, V. Zwiller, M. G. Thompson, and J. L. O'Brien, Phys. Rev. Lett. **108**, 053601 (2012).
[38] S. N. Dorenbos, E. M. Reiger, U. Perinetti, V. Zwiller, T. Zijlstra, and T. M. Klapwijk, Appl. Phys. Lett. **93**, 131101 (2008).
[39] M. G. Tanner, C. M. Natarajan, V. K. Pottapenjara, J. A. OConnor, R. J. Warburton, R. H. Hadfield, B. Baek, S. Nam, S. N. Dorenbos, E. Bermudez Urena, T. Zijlstra, T. M. Klapwijk, and V. Zwiller, Appl. Phys. Lett. **96**, 221109 (2010).
[40] As is typical, $\{D, A, R, L, H, V\} \equiv \{$diagonal, antidiagonal, right circular, left circular, horizontal, vertical$\}$.
[41] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).
[42] S. Thaniyavarn, Appl. Phys. Lett. **47**, 674 (1985).
[43] S. Thaniyavarn, Opt. Lett. **11**, 39 (1986).
[44] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[45] R. Hadfield, Nat. Photonics **3**, 696 (2009).
[46] W. H. P. Pernice, C. Schuck, O. Minaeva, M. Li, G. N. Goltsman, A. V. Sergienko, and H. X. Tang, Nat. Commun. **3**, 1325 (2012).
[47] J. W. Silverstone, D. Bonneau, K. Ohira, N. Suzuki, H. Yoshida, N. Iizuka, M. Ezaki, C. M. Natarajan, M. G. Tanner, R. H. Hadfield, V. Zwiller, G. D. Marshall, J. G. Rarity, J. L. O'Brien, and M. G. Thompson (to be published).
[48] H. K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).