Fibre polarisation state compensation in entanglement-based quantum key distribution

YICHENG SHI,[1] HOU SHUN POH,[1] ALEXANDER LING,[1,2] CHRISTIAN KURTSIEFER,[1,2,*]

[1]*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore, 117543*
[2]*Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore, 117542*
[*]*phyck@nus.edu.sg*

Abstract: Quantum Key Distribution (QKD) using polarisation encoding can be hard to implement over deployed telecom fibres because the routing geometry and the birefringence of the fibre link can alter the polarisation states of the propagating photons. These alterations cause a basis mismatch, leading to an increased Quantum Bit Error Rate (QBER). In this work we demonstrate a technique for dynamically compensating fibre-induced state alteration in a QKD system. This compensation scheme includes a feedback loop that minimizes the QBER using a stochastic optimization algorithm. The effectiveness of this technique is implemented and verified in a polarisation entanglement QKD system over a deployed telecom fibre.

1. Introduction

As first proposed in 1984, Quantum Key distribution enables two users to share an identical, random key that remains unknown to any third parties [1]. Information-theoretic secure communication can be established when QKD is used in conjunction with the one-time pad scheme [2, 3]. A number of QKD protocols with proven security [4–6] have been considered, which can be categorized as either "prepare-and-measure" schemes or entanglement based protocols. In practical implementations, qubits can be encoded into single photons (or approximations thereof) through their polarisation or arrival times, and are transmitted between two parties either over free space to establish long distance links [7–10], or through optical fibres for medium distance applications [11–14].

Encoding qubits into the polarisation of light has been widely adopted in many quantum information schemes, as different polarisation states can be easily prepared and measured for both weak optical pulses or single photons. Polarisation encoded qubits are typically very robust against decoherence when propagating though free space or optically isotropic media. However, polarisation encoding faces a particular drawback as an optical fibre is not a pure loss channel for transmitting the polarisation states of photons. When propagating through the fibre, the state of polarisation (SOP) of a photon is altered due to the birefringence as well as the routing geometry of the fibre [15]. In particular, fibre birefringence can be sensitive to changes in the ambient environment which makes this alteration somewhat random and time dependent [16]. This fibre-induced state alteration (or a rotation of a polarisation when characterized as a point on the Poincaré sphere) causes basis mismatch, and eventually leads to an increased quantum bit error rate (QBER) in a QKD system, eventually preventing keys from being generated. Moreover, chromatic dispersion and polarisation mode dispersion of an optical fibre also degrades the timing correlation and degree of polarisation of the transmitted photons and further introduce errors to the system [17, 18].

While the dispersion effects of optical fibres can be mitigated with dispersion-shifted fibres or simply narrowing the optical bandwidth of the photons [19], fibre-induced polarisation alteration needs to be actively monitored and compensated. This is usually achieved by placing a polarisation controller in the fibre link which is controlled with a feedback loop. The polarisation

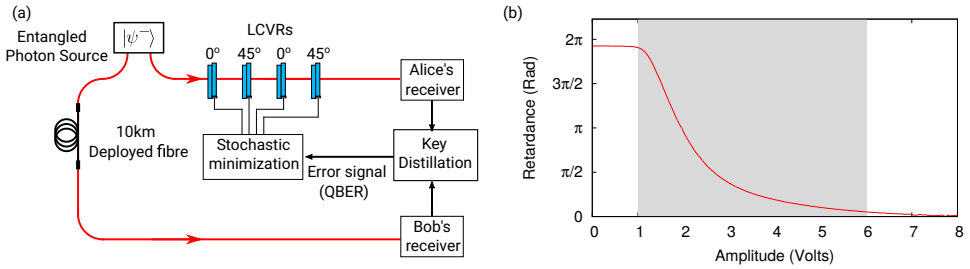

Fig. 1. (a) Experimental setup of a polarisation entanglement QKD system implemented over 10 km of deployed fibre link. The polarisation compensation setup consists of 4 liquid crystal variable retarders placed before Alice's receiver. (b) LCVR retardance versus applied voltage amplitude of 2 kHz square wave at 1310 nm.

controller is set to implement a unitary transformation that inverts the polarisation alteration of fibre. The resulting transformation of the entire channel is neutralized to the identity such that the polarisation state of photons transmitted through the fiber remains unchanged.

The optimal setting of the controller can be found by measuring the polarisation of two reference signals sent across the same fibre. This pair of reference signals needs to be prepared into two non-orthogonal polarisation states, and the polarisation controller then is adjusted to reach a configuration where it restores the states of both reference signals at the output of the fibre. The reference signals can co-exist with the QKD photons in the same fibre via either time-division or wavelength-division multiplexing [20–22]. This type of compensation can operate at a high bandwidth at the cost of increasing hardware complexity, and is suitable for QKD systems with rapidly oscillating environmental noise [22].

A different compensation scheme was proposed more recently that does not require any reference light signals [23, 24]. In this scheme, one utilizes the number of erroneous bits in the revealed portion of the sifted keys during error correction process, which has to be monitored in a QKD protocol anyways to assess potential information leakage to an eavesdropper. This error rate, which is an estimation of the system's QBER, is used to generate an error signal for the polarisation controller. This compensation simplifies the physical setup at the cost of a relatively low bandwidth of the feedback loop [24].

In this work, we present a similar polarisation compensation technique, but implement it in a polarisation-entanglement based QKD system [25]. Our technique uses a stack of liquid crystal variable retarders as polarisation controller and is optimized in a feedback loop using the estimated QBER as error signal. We also show that for polarisation-entanglement based QKD, this technique exploits the rotational invariance of the distributed entangled state and only requires one of the two fibre links to be compensated. The compensation setup is implemented in a QKD system over a deployed telecom fibre link and achieves optimal compensation in under 20 minutes. This technique requires minimal hardware overhead and is suitable for fiber-based QKD systems with slowly drifting environmental noise.

2. Experimental setup

A simplified diagram of our QKD setup with polarisation compensation is shown in Fig. 1 (a). An entangled photon pair source prepares photons pairs in a state $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|H_A V_B\rangle - |V_A H_B\rangle)$. The photons are generated via Spontaneous Parametric Down-Conversion (SPDC), which converts pump light at 658 nm to a signal and idler photon at around 1316 nm. The bandwidth of down-converted photons are limited to about 20 nm by a bandpass filter. The signal and idler photons are sent to two receivers, Alice and Bob, respectively. The signal photons are transmitted

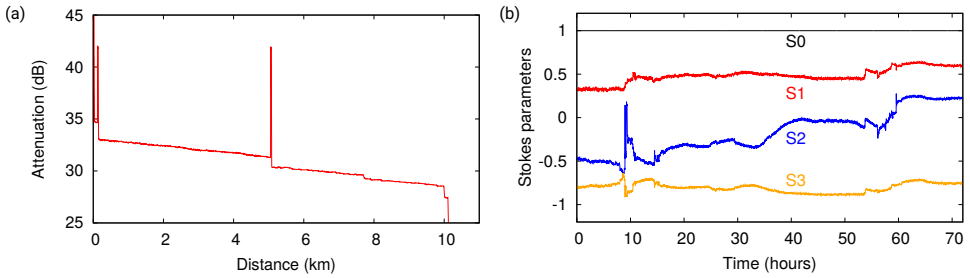

Fig. 2. (a) OTDR trace of the 10 km deployed fibre. (b) Stokes parameters of polarisation state at the fibre output logged over 3 days showing drifts on a time scale of days.

through a deployed telecom fiber to Bob, while Alice receive the idler photons locally via a short patchcord. The two receivers follow the BBM92 protocol [26] and randomly measure the polarisation of each photon in one of two bases: horizontal/vertical and diagonal/anti-diagonal. The basis is randomly chosen through a non-polarizing beam splitter [27], and exchanged between the two receivers via a classical channel during the key sifting procedure. Error correction is applied, which also allows to estimate an eavesdropper's potential knowledge of the key, and corresponding privacy amplification is applied to generate the final keys.

As shown in Fig. 2 (a), the telecom fibre is about 10 km long with approximately 7 dB of optical attenuation. To simplify experimental procedures, the fibre is deployed underground in a loop configuration with both ends connected to the lab. The stability of the deployed fibre is tested by sending in light with fixed polarisation and monitoring the output state with a polarimeter [28]. Figure 2 (b) shows a 72-hour measurement; the Stokes parameters of the output state show only a slow drift with occasional jumps. The change of the polarisation state due to environmental influence appears only to take place on a time scale of several minutes.

To compensate for this slow drift of polarisation state transmitted over fiber, a polarisation controller based on Liquid Crystal Variable Retarders (LCVRs) is adequate. The reaction time of the LCVRs was measured to be about 5 ms, which is sufficiently fast to compensate the polarsation drifts we encounter. Moreover, the LCVRs include no macroscopically moving parts and offer a high transparency at telecom wavelengths (>95%). A set of four LCVRs is placed before Alice's receiver to serve as the polarisation controller. Each LCVR can provide a voltage-controlled retardance from 0 to about $\frac{3}{2}\pi$ at 1310 nm (see Fig. 1 (b)). The LCVRs' optical axes are oriented at 0°, 45°, 0°, and 45° to allow for sufficiently independent polarisation transformations (see Fig. 1 (a)). While an arbitrary polarisation transfer is completely described by a rotation direction and angle in the Poincaré sphere, and thus 3 degrees of freedom should be sufficient to encode any transformation required by the compensator, we chose four polarisation retarders to ensure that there is a continuous evolution of the control parameters within their limited range, and that a gimbal lock situation is avoided. In this way, any continuously varying unitary transformation between any arbitrary pairs of input and output states can be implemented.

3. polarisation compensation for entangled states

While QKD implementations based on "prepare-and-measure" protocols only require a single fibre linking the sender and receiver, an implementation based on entangled photon pairs needs two fibers to distribute photons to both receivers. In this case, both fibers will alter the polarisation states of propagating photons. However, it is sufficient to only use a single polarisation compensator in one of the fibers, as the polarisation of both photons are correlated.

To see this, consider a source that generates photon pairs in a rotationally invariant Singlet polarisation state $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|H_A V_B\rangle - |V_A H_B\rangle)$. Photons A and B undergo different fibre-

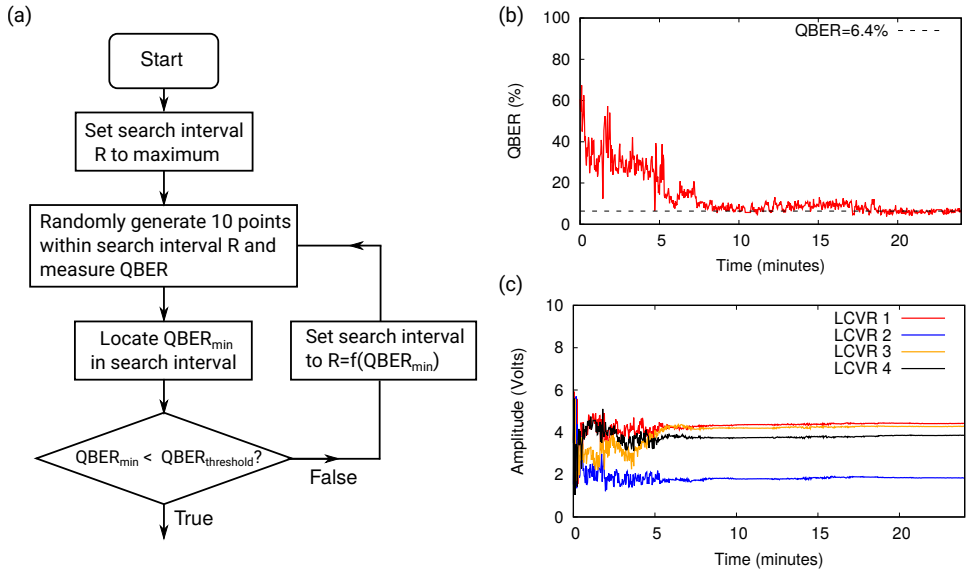

Fig. 3. (a) Flow chart of the stochastic search algorithm. (b) System QBER recorded during the stochastic search. (b) Applied voltage amplitudes for the LCVRs during stochastic search.

induced polarisation rotations $\hat{R}_A$ and $\hat{R}_B$. The resulting photon pair state is $(\hat{R}_A \otimes \hat{R}_B)|\psi^-\rangle$. A polarisation controller acting on photon A can be set to perform a transformation $\hat{T}_A$ such that $\hat{T}_A\hat{R}_A = \hat{R}_B$. The resulting state

$$(\hat{T}_A\hat{R}_A \otimes \hat{R}_B)|\psi^-\rangle = (\hat{R}_B \otimes \hat{R}_B)|\psi^-\rangle = |\psi^-\rangle$$

is again the singlet state $|\psi^-\rangle$ due to its rotational invariance. Thus, a single polarisation compensation operation on one side is sufficient to remove the state-changing actions of the fiber rotations $\hat{R}_A$ and $\hat{R}_B$ on both transmission channels.

4. QBER minimization with stochastic method

With the setup shown in the previous section, the control loop for the polarisation compensation can be considered as an optimization problem. The goal of this optimization is to find the minimum of the estimated QBER of the QKD system. This is now considered as a function of four variables, QBER $= f(V_1, V_2, V_3, V_4)$, namely the control voltages $V_{1...4}$ of the LCVRs. While this minimization problem can be solved using gradient-descend algorithms in principle, we adopted a different approach in this work due to practical considerations.

Firstly, it is impractical to obtain an accurate expression of the estimated QBER as a function of the control voltages as the response curve of a LCVR varies from unit to unit. Secondly, the estimated QBER cannot be measured with a very high accuracy due to the limitation of finite sample sizes. These limitations make it difficult to compute the gradients of $f(V_1, V_2, V_3, V_4)$ from measurements, and a gradient-descend algorithm cannot be efficiently implemented. Instead, we use a stochastic search algorithm depicted in Fig. 3 (a).

The algorithm conducts a random search within a finite 4-dimensional parameter space (V_1, V_2, V_3, V_4). Each control voltage takes a value between 1 V and 6 V which corresponds to retardation from 0 to about $\frac{3}{2}\pi$ at 1310 nm. The search algorithm randomly picks a set of sample points in the entire parameter space and measures the QBER for each point. The point with the smallest QBER in the set will be chosen as the center of a next search iteration, which will be

conducted with the same number of points within a parameter hypercube of smaller size R. The size R decreases with decreasing minimal QBER obtained in each iteration. As the algorithm proceeds, the center point of the search will gradually approach the minimum in the entire space.

During QKD operation, the two receivers registered a coincidence rate of about $670\,\mathrm{s}^{-1}$ and a sifted key rate of $340\,\mathrm{s}^{-1}$ after basis reconciliation. To reduce Poissonian noise, the system QBER is evaluated from sifted keys accumulated over every 2 seconds. A typical starting condition before polarisation compensation leads to a QBER of $58 \pm 2.6\%$, where the uncertainty is infered from the Poissonian counting statistics. With this initial QBER, the stochastic search begins its first iteration with a set of 10 points. The reduction of the search range R in the parameter space in the iteration is accomplished with an ad-hoc chosen function $R = A \times (\mathrm{QBER}_{\mathrm{min}} - \mathrm{QBER}_{\mathrm{threshold}})^B$, where $\mathrm{QBER}_{\mathrm{min}}$ is the minimal QBER in any given iteration. The coefficients A and B set the rate at which the search algorithm converges to the global minimum, while the offset $\mathrm{QBER}_{\mathrm{threshold}}$ sets a lower bound of the QBER given by other elements than the optical fiber in the QKD system. The last choice assures that the parameter space is still probed in a reasonable neighborhood of the global QBER minimum. Continuously operating this algorithm allows to follow a drift of this minimum location in the parameter space over time in a control-loop-like fashion. We found that in our system, a choice of $A = 6.5$ Volts, $B = 2$, and $\mathrm{QBER}_{\mathrm{threshold}} = 4\%$ worked well.

Fig. 3 (b) shows the performance of our polarisation compensation technique in an exemplary single run. The stochastic search algorithm reduces the system QBER from its initial value of $58 \pm 2.6\%$ to about $7 \pm 0.7\%$ after about 10 minutes (about 30 iterations of search). We then observed a small increase of QBER by about 3%, possibly due to a disturbance to the fiber, but the algorithm eventually lowers the QBER down to $6.4 \pm 0.7\%$. The corresponding control voltages of the LCVRs during the search process are shown in Fig. 3 (c). They converge to stable values as the QBER approaches its minimum given by other system constraints such as accidental coincidences and dispersion effects of the fibre. Once the minimum is reached, the LCVR voltages remain constant and the QKD operation runs continuous for another 5.7 hours without manual intervention [25].

5. Conclusion

We demonstrated polarisation compensation in an entanglement-based QKD system over a deployed telecom fibre. This technique, which utilizes the estimated QBER as the error signal for a feedback control loop, does not require any reference light sources or extra detectors in the setup. We show that by exploiting the rotational invariance property of the Bell $|\Psi^-\rangle$ state, one only needs to apply compensation of one of the fibre links in an entanglement QKD system. The control loop of the polarisation compensation runs a stochastic search algorithm that actively minimizes the estimated QBER and is able to achieve optimal compensation in under 20 minutes.

While this technique is slower compared to methods based on reference signals used to measure out the fiber transformation, it is very simple to implement and requires minimal hardware overhead. The only hardware required is a polarisation controller. This technique is suitable for deployed fibre-QKD systems with slowly drifting environmental polarisation noise. The compensation process does not leak any information through any channels, and therefore does not compromise the security of the QKD link.

Funding

This research was supported by the National Research Foundation, Prime Minister's Office, Singapore under its Corporate Laboratory@University Scheme, National University of Singapore, and Singapore Telecommunications Ltd.

Disclosures

The authors declare no conflicts of interest.

References

1. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Proc. IEEE Int. Conf. on Comput. Syst. Signal Process. pp. 175–179 (1984).
2. G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," Transactions Am. Inst. Electr. Eng. **XLV**, 295–301 (1926).
3. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Rev. Mod. Phys. **81**, 1301–1350 (2009).
4. D. Meyrs, "Quantum key distribution and string oblivious transfer in noisy channels," in *Advances in Cryptology - CRYPTO '96,* vol. 1109 N. Koblitz, ed. (Springer, Berlin, Heidelberg, 1996), p. 343.
5. H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," Science **283**, 2050–2056 (1999).
6. P. W. Shor and J. Preskill, "Simple proof of security of the bb84 quantum key distribution protocol," Phys. Rev. Lett. **85**, 441–444 (2000).
7. R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night," New J. Phys. **4**, 43–43 (2002).
8. C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity, "A step towards global key distribution," Nature **419**, 450 (2002).
9. T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," Phys. Rev. Lett. **98**, 010504 (2007).
10. S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, R. Ursin, T. Scheidl, C.-Z. Peng, J.-Y. Wang, A. Zeilinger, and J.-W. Pan, "Satellite-relayed intercontinental quantum network," Phys. Rev. Lett. **120**, 030501 (2018).
11. A. Poppe, B. Schrenk, F. Hipp, M. Peev, S. Aleksic, G. Franzl, A. Ciurana, and V. Martin, "Integration of quantum key distribution in metropolitan area networks," in *Research in Optical Sciences,* (Optical Society of America, 2014), p. QW4A.6.
12. D. Bunandar, A. Lentine, C. Lee, H. Cai, C. M. Long, N. Boynton, N. Martinez, C. DeRose, C. Chen, M. Grein, D. Trotter, A. Starbuck, A. Pomerene, S. Hamilton, F. N. C. Wong, R. Camacho, P. Davids, J. Urayama, and D. Englund, "Metropolitan quantum key distribution with silicon photonics," Phys. Rev. X **8**, 021009 (2018).
13. J. F. Dynes, A. Wonfor, W. W.-S. Tam, A. W. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. L. Yuan, A. R. Dixon, J. Cho, Y. Tanizawa, J.-P. Elbers, H. Greißer, I. H. White, R. V. Penty, and A. J. Shields, "Cambridge quantum network," npj Quantum Inf. **5**, 101 (2019).
14. S. K. Joshi, D. Aktas, S. Wengerowsky, M. Lončarić, S. P. Neumann, B. Liu, T. Scheidl, G. C. Lorenzo, Ž. Samec, L. Kling, A. Qiu, M. Razavi, M. Stipčević, J. G. Rarity, and R. Ursin, "A trusted node–free eight-user metropolitan quantum communication network," Sci. Adv. **6** (2020).
15. S. C. Rashleigh and R. Ulrich, "Polarization mode dispersion in single-mode fibers," Opt. Lett. **3**, 60–62 (1978).
16. G. B. Xavier, N. Walenta, G. V. de Faria, G. P. Temporão, N. Gisin, H. Zbinden, and J. P. von der Weid, "Experimental polarization encoded quantum key distribution over optical fibres with real-time continuous birefringence compensation," New J. Phys. **11**, 045015 (2009).
17. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145–195 (2002).
18. H. Hübel, M. R. Vanner, T. Lederer, B. Blauensteiner, T. Lorünser, A. Poppe, and A. Zeilinger, "High-fidelity transmission of polarization encoded qubits from an entangled source over 100 km of fiber," Opt. Express **15**, 7853–7862 (2007).
19. A. Treiber, A. Poppe, M. Hentschel, D. Ferrini, T. Lorünser, E. Querasser, T. Matyus, H. Hübel, and A. Zeilinger, "A fully automated entanglement-based quantum cryptography system for telecom fiber networks," New J. Phys. **11**, 045013 (2009).
20. G. B. Xavier, G. V. de Faria, G. P. Temporão, and J. P. von der Weid, "Full polarization control for fiber optical quantum communication systems using polarization encoding," Opt. Express **16**, 1867–1873 (2008).
21. J. Chen, G. Wu, L. Xu, X. Gu, E. Wu, and H. Zeng, "Stable quantum key distribution with active polarization control based on time-division multiplexing," New J. Phys. **11**, 065004 (2009).
22. D.-D. Li, S. Gao, G.-C. Li, L. Xue, L.-W. Wang, C.-B. Lu, Y. Xiang, Z.-Y. Zhao, L.-C. Yan, Z.-Y. Chen, G. Yu, and J.-H. Liu, "Field implementation of long-distance quantum key distribution over aerial fiber with fast polarization feedback," Opt. Express **26**, 22793–22800 (2018).
23. Y.-Y. Ding, W. Chen, H. Chen, C. Wang, Y.-P. Li, S. Wang, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, "Polarization-basis tracking scheme for quantum key distribution using revealed sifted key bits," Opt. Lett. **42**, 1023–1026 (2017).
24. C. Agnesi, M. Avesani, L. Calderaro, A. Stanco, G. Foletto, M. Zahidy, A. Scriminich, F. Vedovato, G. Vallone, and P. Villoresi, "Simple quantum key distribution with qubit-based synchronization and a self-compensating polarization

encoder," Optica **7**, 284–290 (2020).
25. Y. Shi, S. M. Thar, H. S. Poh, J. A. Grieve, C. Kurtsiefer, and A. Ling, "Stable polarization entanglement based quantum key distribution over metropolitan fibre network," Appl. Phys. Lett. **117**, 124002 (2020).
26. C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without bell's theorem," Phys. Rev. Lett. **68**, 557–559 (1992).
27. J. Rarity, P. Owens, and P. Tapster, "Quantum random-number generation and key sharing," J. Mod. Opt. **41**, 2435–2444 (1994).
28. A. Ling, K. P. Soh, A. Lamas-Linares, and C. Kurtsiefer, "An optimal photon counting polarimeter," J. Mod. Opt. **53**, 1523–1528 (2006).