Stable Polarization Entanglement based Quantum Key Distribution over Metropolitan Fibre Network

Yicheng Shi,[1, a)] Soe Moe Thar,[1] Hou Shun Poh,[1] James A. Grieve,[1] Christian Kurtsiefer,[1, 2, b)] and Alexander Ling[1, 2]

[1)]*Centre for Quantum Technologies, 3 Science Drive 2, National University of Singapore,*
117543 Singapore
[2)]*Department of Physics, National University of Singapore, Blk S12, 2 Science Drive 3,*
117551 Singapore

(Dated: 15 July 2020)

We demonstrate a quantum key distribution implementation over deployed dark telecom fibers with polarisation-entangled photons generated at the O-band. One of the photons in the pairs are propagated through 10 km of deployed fiber while the others are detected locally. Polarisation drifts experienced by the photons propagating through the fibers are compensated with liquid crystal variable retarders. This ensures continuous and stable QKD operation with an average QBER of 6.4% and a final key rate of 109 bits/s.

Quantum Key Distribution (QKD) enables two users to share a common encryption key that is secret to any third parties. Early QKD protocols such as BB84[1] were "prepare-and-measure" schemes, with practical derivatives such as SARG04[2] and decoy states[3]. This was complemented by the invention of entanglement-based protocols such as E91[4] and BBM92[5], with quantitative extensions through device-independent QKD[6]. Both types of QKD protocols have been proven theoretically secure and have been studied extensively over the decades[7–10].

For prepare-and-measure protocols, a trusted random number generator is required to provide randomness in the state preparation process. This is not required for entanglement-based QKD protocols, where randomness of the key originates from the measurement process itself. Entanglement-based QKD also does not rely on a true single photon source or a decoy state mechanism to mitigate a photon number splitting attack, and has fewer possible side channels than typical prepare-send scenarios. As such, entanglement based QKD is less vulnerable to attacks in practical implementations[11].

Both freespace and optical fibre links have been used as the transmission channel for distributing entangled photon pairs[12]. Due to low optical attenuation in the atmosphere, the channel loss over freespace links can be as low as 0.07 dB/km at high altitudes[13]. For protocols using polarisation entanglement, the state of the photons is well preserved during freespace transmission. Early implementations of freespace QKD used optical telescopes to send and receive photons over a range[14–16], reaching over hundred of kilometers[13]. Furthermore, this range can be extended to thousands of kilometers by utilizing satellites as intermediate nodes[17].

Optical fiber links, on the other hand, are suitable when a line-of-sight is not available. Fiber-based QKD generally operates over shorter range (<100 km) due to optical attenuation of light in the fiber. This is, however, enough to cover metropolitan areas where a fiber network is available[18–21].

[a)]Electronic mail: cqtsy@nus.edu.sg
[b)]Electronic mail: phyck@nus.edu.sg

The available telecom single mode fiber conforms to the ITU G.652 standard[22]. To maximize range, fiber-based QKD systems can use entangled photons generated at telecom C-band (1530-1565 nm) where fiber absorption is at its minimum (0.2 dB/km)[21,23–25]. The O-band in (1260-1360 nm) is another choice of wavelength, with an abosrption loss of about 0.32 dB/km. The total loss over fiber transmission in a realistic link is always higher due to the presence of splicing and patching points.

The presence of dispersion effects is another possible limiting factor to the performance of entanglement-based QKD over fiber. Entangled photon pairs are usually generated via a Spontaneous Parametric Down Conversion (SPDC) process, which leads to photons of relatively large bandwidth when performed in nonlinear optical crystals, compared to photons generated with lasers. Such wideband photons experience then significant chromatic dispersion in the fiber ($\sim$ 18 ps/nm/km at 1550 nm)[26]. This increases the uncertainty in timing correlation between the entangled photons, leading to a lower signal to noise ratio, eventually reducing the final key rate. The effect of chromatic dispersion can be migitated by using dispersion-shifted fiber[23], or by using entangled photons at telecom O-band operating on either side of the zero-dispersion wavelength of the fiber[27].

For QKD protocols using polarisation encoding, an optical fibre cannot be simply regarded as a pure loss channel. When propagating through the fibre, an arbitrary rotation is applied to the polarization state of photons and causes basis mismatch. In addition, fiber Polarisation Mode Dispersion (PMD) can cause degradation of polarisation entanglement for broadband photons[28,29]. Both effects increase the Quantum Bit Error Rate (QBER), reducing the rate of key generation. While the polarisation rotation can be compensated[30], the presence of polarisation mode dispersion has led to a preference of time-bin encoding over polarisation encoding in fiber-based QKD implementations[28,31,32]. However in recent years, manufacturers are able to make single mode telecom fibers with much lower PMD value ($\leq 0.04 \, \mathrm{ps}/\sqrt{\mathrm{km}}$)[26], which makes polarisation encoding possible even for relatively broadband entangled photons.

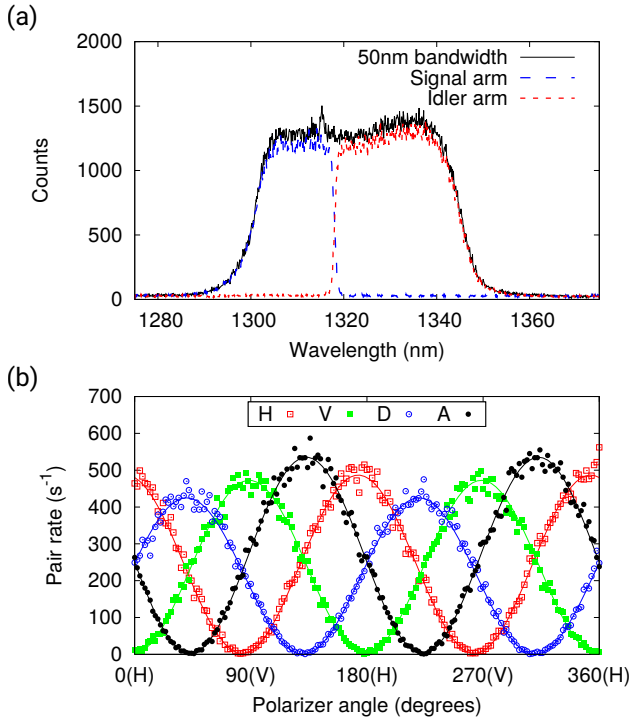In this work we report an entanglement-based QKD system

FIG. 1. (a) Spectrum of the Typr-0 SPDC photons. The black trace shows the 50 nm bandwidth defined by the bandpass filter applied. Signal (blue) and idler (red) photons are separated using a wavelength division demultiplexer. (b) Polarization correlation in both H/V and D/A bases measured at the entanglement source.

implemented over a 10 km deployed fibre in a metropolitan area. The setup uses the BBM92 protocol[5], with polarization entangled photon pairs generated at telecom O-band to minimize the effect of chromatic dispersion. The polarisation rotation due to the fiber is compensated using liquid crystal variable retarders (LCVRs) after which the polarisation state is stable during several hours of continuous QKD operation.

The entangled photon pairs are generated via type-0 SPDC inside a periodically-poled potassium titanyl phosphate (PP-KTP) crystal, shown in Fig. 2 (a). The crystal is pumped by a grating stabilized laser diode at 658 nm, emitting photon pairs that are degenerate at 1316 nm. The bandwidth of the down-converted photons is limited to about 50 nm by a bandpass filter. As shown in Fig. 1 (a), a wavelength division demultiplexer with an edge at approximately 1316 nm is used to separate the signal and idler photons. The entanglement state is prepared by placing the PPKTP crystal inside a linear beam-displacement interferometer[33]. The photon pairs are prepared in a state:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|H_A H_B\rangle + |V_A V_B\rangle)$$

with polarisation visibility over 98% in both horizontal/vertial (H/V) and diagonal/anti-diagonal (D/A) bases (Fig. 1 (b)). With the pump power of 2.4 mW, we observed a local pair rate of $4300\,\text{s}^{-1}$.

The setup of the QKD system is shown in Fig. 2 (b). The entangled photon pairs are distributed to two nodes, Alice and
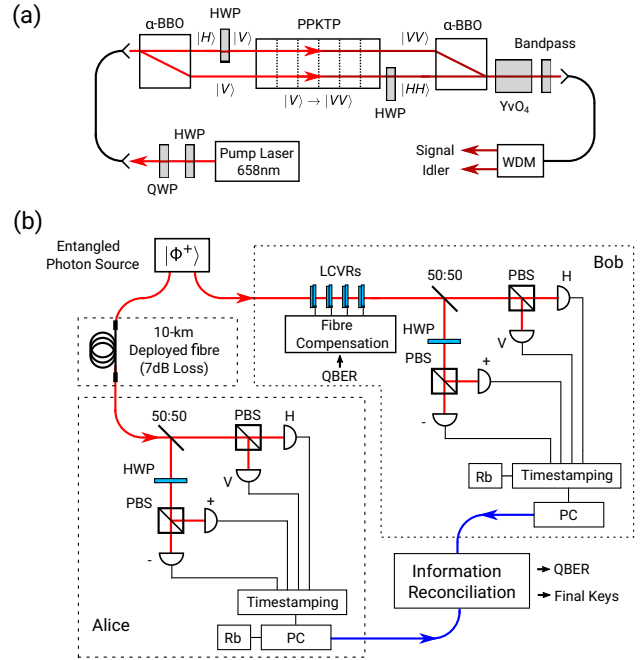

FIG. 2. (a) Experimental schematic of the entanglement source. The pump photons are split to two paths and undergo type-0 SPDC inside the PPKTP crystal. The polarization state in the lower path is rotated 90 degrees by a half-wave plate. The two paths are then recombined to create a $|\Phi^+\rangle$ state. (b) QKD setup over 10 km deployed fiber link. The fiber loops back to the lab to simplify the experimental procedure. The Alice and Bob nodes are run on independent clocks. Alice's analyzer is connected to the entanglement source via the 10 km deployed fiber while Bob's setup is locally connected using a short patch cord. The two hosting PCs are connected to the same local area network in order to exchange timestamp data for coincidence identification.

Bob, with a polarisation analyzer placed on each side. A 10 km telecom fiber connects the source to Alice's analyzer while Bob's setup is connected locally via a short patchcord.

The 10 km telecom fiber is deployed underground by Singapore Telecommunications Limited in a loop configuration with both ends located at Center for Quantum Technologies, National University of Singapore. Measurement using an optical time-domain reflectometer (OTDR) shows a total fiber length of 10.4 km with about -7 dB channel loss (Fig. 3). The optical absorption of the fiber contributes only about -4 dB to the total channel loss, with another -3 dB loss due to reflections at patching points and losses at splicing points. The total PMD of the fiber link is about 0.1 ps, which is smaller than the coherence time of the signal and idler photons (∼0.23 ps for 25 nm bandwidth at 1310 nm).

Polarization change due to fiber is compensated by placing a set of 4 LCVRs before Bob's analyzer setup. This compensation only needs to be applied to one of the photons from each pair to restore the initial $|\Phi^+\rangle$ state after fiber propagation. In some implementations with optical fibers on the surface[30], polarisation compensation needs to be constantly performed due to the rapid change of the polarization change, which severely limits the operation continuouity of QKD.
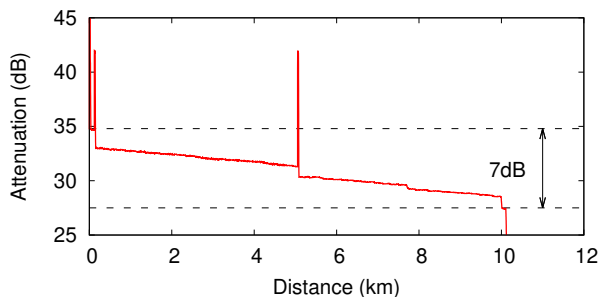
FIG. 3. Optical time-domain reflectometer trace of the deployed fibre, identifying a high reflection loss point about 5 km away from both end points. Two more points with high reflection/absorption loss are also identified about 100 meters from the end points, which is due to a 100 meter patching cable between the deployed fiber and the laboratory setup.

The polarization stability of 10 km deployed fibre in our setup was characterized by sending in light with well-defined polarization state across the fiber and monitoring the change in polarization with a polarimeter[34]. We find that the output polarization drift was slow, with a typical 24 h period associated with day-night temperature change. Once the polarization rotation is compensated, the fiber allows several hours of stable QKD operation even without running any active compensation scheme.

Upon receiving the photons, Alice and Bob follow the BBM92 protocol by measuring polarizations in one of the two bases: H/V and D/A[5]. The random detection basis choice is made by a non-polarizing beam splitter in each setup which transmits and reflects photons with equal probability[35]. Four commercial Indium Gallium Arsenide Avalanche Photodiodes (InGaAs APDs) are used in each analyzer setup for single photon detection. The APDs diodes are cooled down to below -40 °C and are operated in freerunning mode with a nominal detection efficiency around 10% and an average dark count rate of about $12000\,\mathrm{s}^{-1}$. On each side, detected photons are timetagged to a resolution of 125 ps with a 4-channel timestamping device locked to a rubidium frequency standard[36].

Recorded timestamp traces are continuously exchanged through a network connection between two hosting lab computers. To enable coincidence identification, the clocks on both sides are synchronized in advance by exploiting the intrinsic timing correlations of the SPDC photons[37]. The uncertainty in the coincidence time difference is about 1.9 ns (FWHM) due to fiber chromatic dispersion, detector timing jitter and other noise in the system[27]. For coincidence identification, a coincidence window of 0.5 ns was chosen to optimize the coincidence/accidental ratio without losing too many coincidence events.

Raw key data are generated after coincidence identification and key sifting following a typical BBM92 protocol. Error correction are then performed on each block of raw key data accumulated over 25 seconds[36] using a modified CASCADE/BICONF algorithm[38], following largely[39]. An estimated QBER is also obtained during error correction and is used to determine the amount of secure key bits to be extracted from the raw key bits. Privacy amplification is then performed on both sides for obtaining the final secure keys[40].

We estimate a total system loss of -33 dB in our entire QKD system, with -7 dB contributed by the total channel loss of the deployed fiber, -6 dB from the optical coupling loss in the polarisation compensation and analyzer setup, and another -20 dB solely due to the detection efficiency of the InGaAs APDs on both sides. Therefore, detector efficiency is the dominant contribution to the overall system loss in our setup.

With the 10 km deployed fiber connected, the rate of detected single photons is $40\,699\,\mathrm{s}^{-1}$ on Alice's analyzer, and $242\,125\,\mathrm{s}^{-1}$ at Bob's side, respectively. We observe a coincidence rate of $670\,\mathrm{s}^{-1}$ and an accidental coincidence rate of $19\,\mathrm{s}^{-1}$. After an initial fiber compensation, the QKD setup operated continuously over 5.7 hours until one of the detectors ceased operation due to a temperature overrun. The average sifted key rate after basis reconciliation is $340\,\mathrm{s}^{-1}$ with an average estimated QBER of 6.3%. The final key rate after error correction and privacy amplification is about 109 bits/second (Fig. 4).

Our final key rate is comparable to other reported entanglement-based implementations at telecom C-band[21], or at wavelengths detectable by Silicon APDs[41]. Secure transfer of messages with this key rate is practical using one-time pad encryption for low bandwidth communications such as command & control of industrial systems. Alternatively, the key can be utilized in fast encryption schemes using e.g. AES-256, with a much more frequent re-keying compared to conventional methods[20]. The key rate in our demonstration is mainly limited by the low detection efficiency ($\sim$10%) and high dark count rate ($\sim 10^4\,\mathrm{s}^{-1}$) of the InGaAs APDs in the setup. Significant increase in key rate is expected when replacing them with superconducting nanowire detectors ($\sim$80% detection efficiency)[42]. As practical advantage of photons at O-band, QKD can operate along the normal internet traffic with all channels in C-band concurrently over the same fiber link.
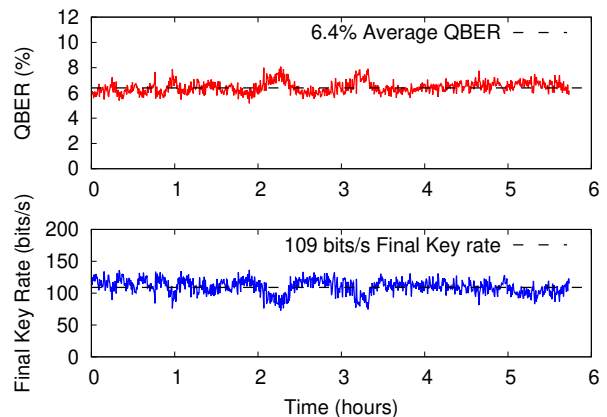

FIG. 4. QBER (top) and finaly key rate (bottom) logged over 5.7 hours of continuous operation. Error correction and privacy amplification are performed over blocks of raw key bits integrated over 25 seconds. Data collection stopped after 5.7 hours due to a detector failure.

To conclude, we have demonstrated a stable entanglement-based quantum key distribution system operating over a deployed telecom fiber of 10 km distance following the BBM92 protocol. Polarization-entangled photon pairs in the telecom O-band minimize the effect of chromatic dispersion. The polarisation change in the fiber due to fiber geometry and birefrincence is compensated with liquid crystal variable retarders, enabling stable transmission of photon polarisation states. We operated the systems continuously for 5.7 hours with an average QBER of 6.4% and a final key rate of 109 bits/s. The key rate performance is mainly limited by the detection efficiencies and high dark count rate of the InGaAs photodetectors.

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Proceedings of IEEE International Conference on Computers, Systems and Signal Processing , 175–179 (1984).

[2] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," Phys. Rev. Lett. **92**, 057901 (2004).

[3] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett. **94**, 230504 (2005).

[4] A. K. Ekert, "Quantum cryptography based on bell's theorem," Phys. Rev. Lett. **67**, 661–663 (1991).

[5] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without bell's theorem," Phys. Rev. Lett. **68**, 557–559 (1992).

[6] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks," Phys. Rev. Lett. **98**, 230501 (2007).

[7] D. Meyrs, "Quantum key distribution and string oblivious transfer in noisy channels," in *Advances in Cryptology — CRYPTO '96*, Vol. 1109, edited by N. Koblitz (Springer, Berlin, Heidelberg, 1996) p. 343.

[8] H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," Science **283**, 2050–2056 (1999), https://science.sciencemag.org/content/283/5410/2050.full.pdf.

[9] P. W. Shor and J. Preskill, "Simple proof of security of the bb84 quantum key distribution protocol," Phys. Rev. Lett. **85**, 441–444 (2000).

[10] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, "The universal composable security of quantum key distribution," in *Theory of Cryptography*, edited by J. Kilian (Springer Berlin Heidelberg, Berlin, Heidelberg, 2005) pp. 386–406.

[11] N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," Phys. Rev. A **61**, 052304 (2000).

[12] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, "Quantum cryptography with entangled photons," Phys. Rev. Lett. **84**, 4729–4732 (2000).

[13] 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).

[14] J. G. Rarity, P. M. Gorman, and P. R. Tapster, "Secure key exchange over 1.9 km free-space range using quantum cryptography," Electronics Letters **37**, 512 (2001).

[15] 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 Journal of Physics **4**, 43–43 (2002).

[16] 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).

[17] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L. Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-to-ground quantum key distribution," Nature **549**, 43–47 (2017).

[18] 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).

[19] 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.

[20] 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 Information **5**, 101 (2019).

[21] S. K. Joshi, D. Aktas, S. Wengerowsky, M. Lončarić, S. P. Neumann, B. Liu, T. Scheidl, Željko Samec, L. Kling, A. Qiu, M. Stipčević, J. G. Rarity, and R. Ursin, "A trusted-node-free eight-user metropolitan quantum communication network," (2019), arXiv:1907.08229 [quant-ph].

[22] "Characteristics of a single-mode optical fibre and cable," Telecommunication Standardization Sector of ITU (2016).

[23] 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 Journal of Physics **11**, 045013 (2009).

[24] S. Wengerowsky, S. K. Joshi, F. Steinlechner, J. R. Zichi, S. M. Dobrovolskiy, R. van der Molen, J. W. N. Los, V. Zwiller, M. A. M. Versteegh, A. Mura, D. Calonico, M. Inguscio, H. Hübel, L. Bo, T. Scheidl, A. Zeilinger, A. Xuereb, and R. Ursin, "Entanglement distribution over a 96-km-long submarine optical fiber," Proceedings of the National Academy of Sciences **116**, 6684–6688 (2019), https://www.pnas.org/content/116/14/6684.full.pdf.

[25] S. Wengerowsky, S. K. Joshi, F. Steinlechner, H. Hübel, and R. Ursin, "An entanglement-based wavelength-multiplexed quantum communication network," Nature **564**, 225–228 (2018).

[26] C. Inc., "Corning smf-28e optical fiber produt information," (2005).

[27] J. A. Grieve, Y. Shi, H. S. Poh, C. Kurtsiefer, and A. Ling, "Characterizing nonlocal dispersion compensation in deployed telecommunications fiber," Applied Physics Letters **114**, 131106 (2019), https://doi.org/10.1063/1.5088830.

[28] G. Ribordy, J. Brendel, J.-D. Gautier, N. Gisin, and H. Zbinden, "Long-distance entanglement-based quantum key distribution," Phys. Rev. A **63**, 012309 (2000).

[29] M. Brodsky, E. C. George, C. Antonelli, and M. Shtaif, "Loss of polarization entanglement in a fiber-optic system with polarization mode dispersion in one optical path," Opt. Lett. **36**, 43–45 (2011).

[30] 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 Journal of Physics **11**, 045015 (2009).

[31] S. Fasel, N. Gisin, G. Ribordy, and H. Zbinden, "Quantum key distribution over 30 km of standard fiber using energy-time entangled photon pairs: A comparison of two chromatic dispersion reduction methods," Eur. Phys. J. D **30**, 143–148 (2004).

[32] X. Liu, X. Yao, H. Wang, H. Li, Z. Wang, L. You, Y. Huang, and W. Zhang, "Energy-time entanglement-based dispersive optics quantum key distribution over optical fibers of 20 km," Applied Physics Letters **114**, 141104 (2019), https://doi.org/10.1063/1.5089784.

[33] A. Lohrmann, C. Perumangatt, A. Villar, and A. Ling, "Broadband pumped polarization entangled photon-pair source in a linear beam displacement interferometer," Applied Physics Letters **116**, 021101 (2020), https://doi.org/10.1063/1.5124416.

[34] A. Ling, K. P. Soh, A. Lamas-Linares, and C. Kurtsiefer, "An optimal pho-

ton counting polarimeter," Journal of Modern Optics **53**, 1523–1528 (2006), https://doi.org/10.1080/09500340600674242.

[35] J. Rarity, P. Owens, and P. Tapster, "Quantum random-number generation and key sharing," Journal of Modern Optics **41**, 2435–2444 (1994), https://doi.org/10.1080/09500349414552281.

[36] I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer, "Free-space quantum key distribution with entangled photons," Applied Physics Letters **89**, 101122 (2006), https://doi.org/10.1063/1.2348775.

[37] C. Ho, A. Lamas-Linares, and C. Kurtsiefer, "Clock synchronization by remote detection of correlated photon pairs," New Journal of Physics **11**, 045011 (2009).

[38] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Advances in Cryptology—EUROCRYPT '93*, Vol. 765, edited by T. Helleseth (Springer Verlag, New York, 1994) p. 410.

[39] T. Sugimoto and K. Yamazaki, "A study on secret key reconciliation protocol "cascade"," IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences **E83-A**, 1987 (2000).

[40] C. H. Bennett, G. Brassard, and J.-M. Robert, "Privacy amplification by public discussion," SIAM Journal on Computing **17**, 210–229 (1988), https://doi.org/10.1137/0217014.

[41] A. Poppe, A. Fedrizzi, R. Ursin, H. R. Böhm, T. Lorünser, O. Maurhardt, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein, and A. Zeilinger, "Practical quantum key distribution with polarization entangled photons," Opt. Express **12**, 3865–3871 (2004).

[42] V. B. Verma, B. Korzh, F. Bussières, R. D. Horansky, A. E. Lita, F. Marsili, M. D. Shaw, H. Zbinden, R. P. Mirin, and S. W. Nam, "High-efficiency wsi superconducting nanowire single-photon detectors operating at 2.5 k," Applied Physics Letters **105**, 122601 (2014), https://doi.org/10.1063/1.4896045.