Bacco et al. *EPJ Quantum Technology* (2019) 6:5
https://doi.org/10.1140/epjqt/s40507-019-0075-x

EPJ Quantum Technology
a SpringerOpen Journal

RESEARCH Open Access

Field trial of a three-state quantum key distribution scheme in the Florence metropolitan area

Davide Bacco[1*], Ilaria Vagniluca[2,3], Beatrice Da Lio[1], Nicola Biagi[3], Adriano Della Frera[4], Davide Calonico[5], Costanza Toninelli[3,6], Francesco S. Cataliotti[3,6], Marco Bellini[3,6], Leif K. Oxenløwe[1] and Alessandro Zavatta[3,6]

*Correspondence:
dabac@fotonik.dtu.dk
[1]CoE SPOC, DTU Fotonik, Department of Photonics Engineering, Technical University of Denmark, Kgs. Lyngby, Denmark
Full list of author information is available at the end of the article

Abstract

In-field demonstrations in real-world scenarios boost the development of a rising technology towards its integration in existing infrastructures. Although quantum key distribution (QKD) devices are already adopted outside the laboratories, current field implementations still suffer from high costs and low performances, preventing this emerging technology from a large-scale deployment in telecommunication networks. Here we present a simple, practical and efficient QKD scheme with finite-key analysis, performed over a 21 dB-losses fiber link installed in the metropolitan area of Florence (Italy). Coexistence of quantum and weak classical communication is also demonstrated by transmitting an optical synchronization signal through the same fiber link.

1 Introduction

In a society based on the continuous exchange of sensitive data and information, the importance of secure and trustful communications is essential. Quantum key distribution (QKD) allows to share data in an information-theoretical secure way, no longer based on computational assumptions but exploiting the basic principles of quantum mechanics [1–3]. During the last 30 years, many QKD protocols have been developed and tested over optical fiber spools in laboratory demonstrations, achieving long transmission distances and key generation rates up to tens of Mbit/s in complete system implementations [4–9]. However, this technology is still far from a large-scale deployment in existing fiber networks and telecom infrastructures, due to multiple factors: limited distance between users, lack of applications, high costs and high requirements in terms of low-noise fiber links. In order to reveal practical controversies in real-world deployments, several QKD field trials have been implemented by exploiting installed fiber links on a metropolitan scale, with tens of kilometers of typical distance between nodes [10–21].

Deployed commercial channels inherently suffer from higher losses and noise (due to splices, connections, bends and interfiber cross-talk), moreover their long-term stability is affected by changes in the environmental conditions and physical stress. Although many field trials were performed on a dark fiber (thus requiring a dedicated link for quan-

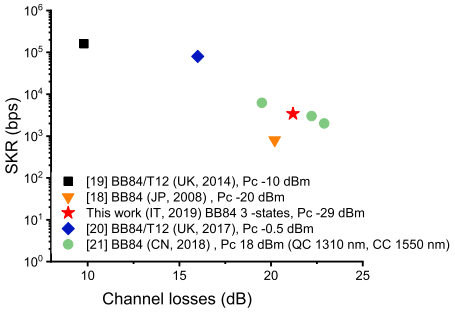

Figure 1 State of the art of QKD field trials. Recent QKD demonstrations with classical and quantum signal propagated through the same installed fiber. Total classical launch power Pc is reported in dBm. Ref. [18] used SNSPDs detectors, all the other used InGaAs detectors. Ref. [21] used wide-range wavelength multiplexing for classical and quantum channels (QC and CC)

tum key transmission), other experiments tested the coexistence between weak quantum signals and classical intense pulses propagated through the same installed fiber [18–21]. Classical light includes ancillary signals for QKD [18] or high-speed data traffic [19–21] and is mixed with quantum signals by means of dense wavelength division multiplexing (DWDM) schemes, often combined with polarization multiplexing [20] and wide-range wavelength multiplexing in C- and O-band [21]. Recent demonstrations are presented in Fig. 1, where the average secret key rate (SKR) achieved is reported with the corresponding transmission losses and total classical launch power.

In this work we present a field demonstration of a low-cost QKD scheme, performed over an installed fiber link situated in Florence and exhibiting 21 dB of transmission losses. A secret key rate of 3.4 kbit/s is evaluated with a finite-key analysis, in the case of simultaneous transmission of synchronization signal (with −29 dBm launch power) and quantum signal through the same fiber at a different wavelength in the C-band. Time stability of the apparatus is demonstrated as well, by employing a servo-locked fiber-based interferometer for security checking.

The fiber link adopted for quantum states exchange is a portion of a dark-fiber network connecting the entire Italian peninsula, from Turin National Institute of Metrological Research (INRiM) to Matera Space Center. This installed fiber of about 1700 km in length, currently employed for time standard dissemination, constitutes the proper environment for a future setup of a large-scale quantum communication network, referred as the Italian Quantum Backbone [22].

1.1 Protocol

We performed the three-state BB84 protocol with time-bin encoding, which has the advantage of being a simple and efficient solution for practical QKD [23]. Quantum states belonging to $\mathcal{Z}$ basis (adopted for key bits encoding) and $\mathcal{X}$ basis (implemented for security checking) are portrayed in Fig. 2. In each state of $\mathcal{Z}$ basis, only one of the two time bins (early and late) is occupied by a photon, while the third state ($\mathcal{X}$ basis) is the linear superposition of $\mathcal{Z}$ basis with null relative phase. This relative phase is altered as a result of any attack that is addressed to quantum states, during their trip along the fiber channel. The receiver checks the relative phase of $\mathcal{X}$ state by monitoring the outputs of a delay-line interferometer with two single-photon detectors, while the projection on $\mathcal{Z}$ basis is made by another single-photon detector which measures the photon arrival time. The security of this protocol against general attacks has been proven to be maintained, with finite-key analysis, when only one detector is employed for $\mathcal{X}$ basis measurements, thus simplifying considerably the experimental resources. In addition, whenever weak coherent pulses

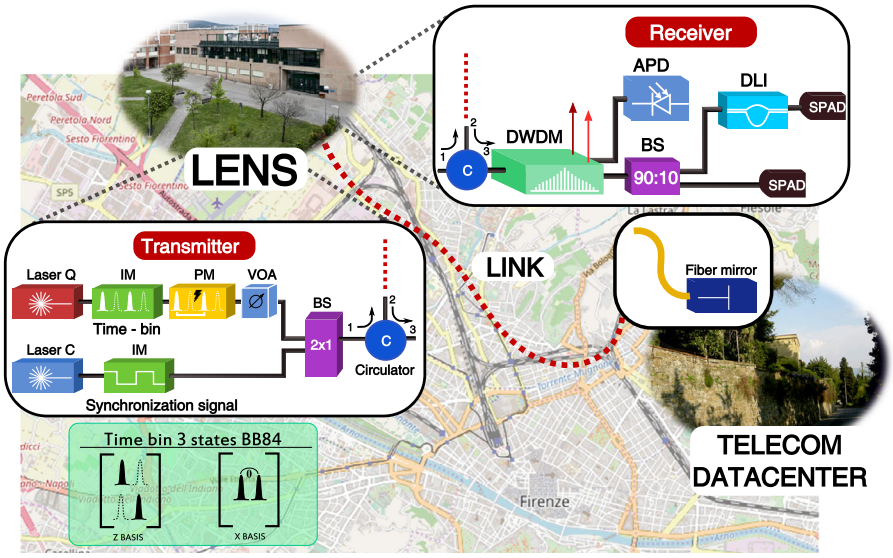

Figure 2 Experimental setup. The transmission channel is a dark fiber link connecting LENS laboratory, where Alice and Bob are located, to a telecom datacenter, where a standard optical mirror is installed at the end of the fiber. Laser Q: continuous wave laser at 1560.61 nm; Laser C: continuous wave laser at 1536.61 nm; IM: intensity modulator; PM: phase modulator; BS: beam splitter; VOA: variable optical attenuator; DWDM: dense wavelength division multiplexing filter; DLI: delay-line interferemoter; SPAD: single-photon avalanche detector; APD: avalanche photodiode. In the green square we reported the three quantum states prepared by Alice and propagated through the channel

(WCPs) are prepared instead of single photons, a very efficient one-decoy state scheme can be implemented in order to detect photon number splitting attacks [24–26]. The SKR length (ℓ) per privacy amplification block is given by the following formula:

$$\ell \leq D_0^{\mathcal{Z}} + D_1^{\mathcal{Z}}\left[1 - h\left(\phi_1^{\mathcal{Z}}\right)\right] - \lambda_{\mathrm{EC}} - 6\log_2(19/\epsilon_{\mathrm{sec}}) - \log_2(2/\epsilon_{\mathrm{corr}}), \tag{1}$$

where $D_0^{\mathcal{Z}}$ and $D_1^{\mathcal{Z}}$ are the lower bounds of vacuum events and single-photon events in the $\mathcal{Z}$ basis, $h(\cdot)$ is the binary entropy function, $\phi_1^{\mathcal{Z}}$ is the upper bound on the phase error rate and λ_{EC} is the number of bits that are publicly announced during error correction [24]. Finally, ϵ_{sec} and ϵ_{corr} are the secrecy and correctness parameters. In our computations we used a block size of 10^9 bits and $\epsilon_{\mathrm{sec}} = \epsilon_{\mathrm{corr}} = 10^{-9}$.

2 Experimental setup

As illustrated in Fig. 2, the experimental setup consists of a transmitter (Alice) and a receiver (Bob) connected by a metropolitan dark-fiber link in a loop-back configuration. A standard optical mirror is installed at the other end of the fiber (situated at the telecom datacenter in Florence) in order to drive light back to the European Laboratory for Non-linear Spectroscopy (LENS) where Alice and Bob are located. Reflected light coming back from telecom datacenter is collected with an optical circulator, as shown in Fig. 2. The total length of the loop-back fiber is about 40 km, with an overall transmission loss of 21 dB. Channel stability in terms of attenuation was monitored for several hours, as reported in Fig. 3a. Figure 3b shows the dark fiber performances in terms of noise at the

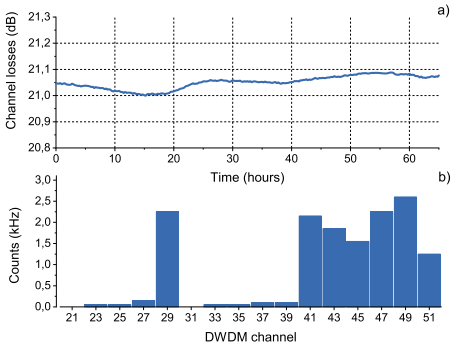

Figure 3 Characterization of the transmission channel. (**a**) channel losses during a three-days acquisition; (**b**) noise counts evaluated for different wavelengths with a single-photon detector after applying a 200 GHz DWDM filter

single-photon level. No light was injected in the fiber during this test: the count rate reported is acquired with a single-photon detector monitoring the end of the fiber, after applying a 200 GHz dense wavelength division multiplexing (DWDM) filter, with output wavelengths corresponding to ITU-T odd channels from 21 to 51. Detector dark counts, i.e. 2.7 kHz, are subtracted during these measurements. Since the fiber is completely dark, we expect this noise to be mainly due to interfiber cross-talk, coming from other fibers in the same bundle.

To prepare a train of modulated WCPs, Alice carves with an intensity modulator (IMs) the time-encoded pulses from a tunable continuous wave (CW) laser, emitting ITU-T channel 21 (1560.61 nm). Repetition rate of quantum states is 595 MHz. A second IM is used to implement the one-decoy state technique with $\mu_1 = 0.41$ and $\mu_2 = 0.15$ photons per pulse (only one intensity is reported in Fig. 2 for simplicity). Then, light is sent through a phase modulator (PM) for phase randomization of each state. An alternative solution would be employing a pulsed laser working in gain switching mode: in this way the phase of the weak coherent states is intrinsically random and the setup can be further simplified. Finally, a variable optical attenuator is used to reach the single-photon regime. In order to test the QKD scheme in a more practical scenario, the synchronization signal between users is carried by classical light copropagated through the same fiber together with quantum pulses, by using a 2x1 beam splitter as shown in Fig. 2. To prepare the optical synchronization signal, we used a second laser working at 1536.61 nm (ITU-T channel 51) and modulated by an extra IM with a custom pattern format at 0.145 Mbit/s. Classical light at −29 dBm launch power is then combined together with quantum pulses and sent through the dark fiber link. At Alice's side, four electrical outputs generated by a field programmable gate array (FPGA) are used to drive the IMs for quantum and synchronization signals. Electrical pulse width is approximately 100 ps, whereas the obtained optical pulse width is around 150 ps. The PM is driven by a digital-to-analog converter (DAC) which uses 8 bit to obtain $2^8 - 1$ different phase values. Furthermore, a pseudo random binary sequence of $l = 2^{12} - 1$ bit is used as a key generator, although a quantum random number generator should be used in a real implementation [27–29]. (This device can be included in future realization directly on Alice's FPGA board.) At Bob's side, a DWDM filter is used to separate classical and quantum light (channel 21 and 51 respectively). Classical pulses at 0.145 Mbit/s serve as reference signals for a time tagging unit, which collects also the electrical outputs from the two InGaAs single-photon avalanche detectors (SPADs) that are employed for quantum state measurements [30]. Bob's choice of measurement basis is made passively by a 10 dB beam splitter. In the $\mathcal{Z}$ basis, one SPAD is used for collecting

photons and detecting their arrival time, while pulses measured in the $\mathcal{X}$ basis are sent to a fiber-based delay-line interferometer (DLI). A second SPAD monitors one of the two outputs of the DLI, in order to check for potential eavesdropping disturbances. Additionally, to phase-stabilize Bob's DLI, a feedback scheme involving a counter-propagating CW laser (emitting ITU-T channel 35, 1549.32 nm) is employed. The optical power monitored at the other DLI input allows a piezoelectric system to lock the phase, thus auto-stabilizing $\mathcal{X}$ basis measurements.

3 Results and discussion

In Fig. 4 we present the in-field performances of our QKD scheme in terms of quantum bit error rate (QBER) achieved in both measurement bases and final secret key rate (SKR) evaluated with a finite-key analysis [24]. We started testing states exchange with the fiber completely dark, i.e. with only quantum pulses propagated and electric synchronization between the two stations (Fig. 4a). Electric synchronization is provided by Alice's FPGA, which is connected directly to Bob's time tagger during this acquisition. Our setup (including both states preparation and measurement as well as fiber channel) exhibits good stability for more than 10 hours, that is the reason why we fixed a block size of 10^9 for all our SKR evaluations. Then we performed a 4 hours continuous acquisition with simultaneous transmission of optical clock signals and quantum pulses (Fig. 4b). Our scheme is less stable in this case, because of the bias instability of the IM used for carving classical clock pulses. In addition, the average SKR evaluated with optical synchronization (3.40 kbit/s) is slightly lower than the one obtained with electric synchronization (4.53 kbit/s), because of background noise generated by classical pulses that results in higher QBER in both measurement bases. Another wavelength filter was added at the receiver in order to limit QBERs deterioration, but this also increased Bob's overall losses, thus resulting in a lower raw key rate (as shown in Fig. 4b). A different and more efficient filter can be employed in order to maximize the secret key parameter. As already mentioned, both of these long-term acquisitions are achieved without manual stabilization of the experimental setup, thanks to our servo-locking fiber-based interferometer.

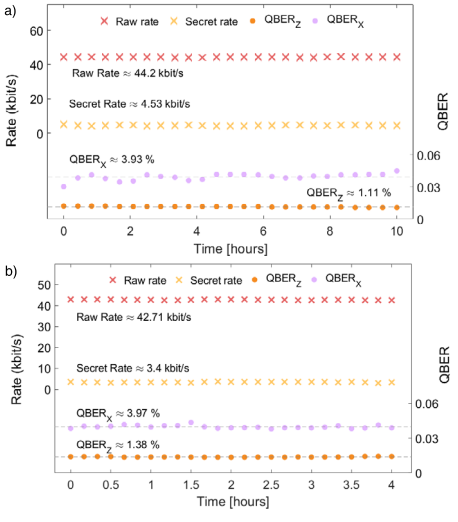

Figure 4 Stability of QKD scheme over time. Error rates, raw and secret key rates acquired for multiple hours with two different channel conditions: (**a**) only quantum signal in the channel; (**b**) both quantum and classical are copropagated through the fiber

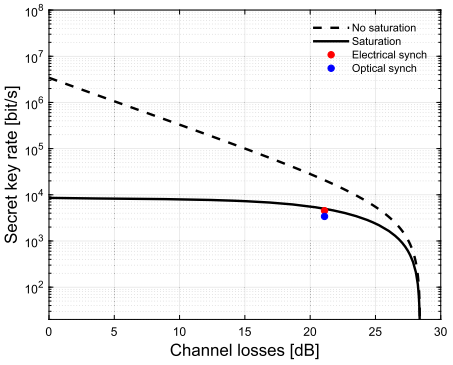

Figure 5 Secret key rate generation. Expected SKR as a function of channel losses, together with the experimental rates evaluated in our continuous states exchange for the two cases (see Fig. 4). The red dot represents the case with only quantum light, whereas the blue dot represents the case with both classical and quantum light propagated simultaneously through the same fiber. The experimental data are averaged over 10 hours and 4 hours of continuous acquisition respectively

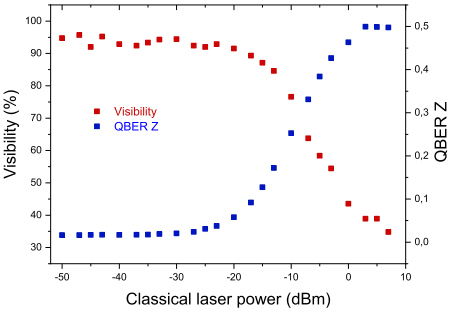

Figure 6 Errors robustness against classical power. $\mathcal{Z}$ basis quantum bit error rate and $\mathcal{X}$ basis visibility with increasing launch power of classical light copropagating through the same fiber. Secret key rate generation is feasible up to −27 dBm of classical launch power

As it is shown in Fig. 5, our SKR values are compatible with the expected rate achievable by this protocol when single-photon detectors operate in saturation regime, due to their dead time (20 µs) which limits the maximum detection rate achievable at the receiver. Furthermore, the simulations show the performances of our scheme in case of shorter (longer) fiber link with the same intrinsic optical attenuation. Our setup can generate a positive key rate up to 28 dB channel losses, which corresponds to 175 km of ultra-low loss single mode fiber.

Figure 6 shows the performances of our QKD scheme (evaluated with electric synchronization only) with increasing launch power of a CW laser emitting at ITU-T channel 51 and sent into the fiber channel together with quantum signals (ITU-T channel 21), by means of a DWDM scheme. As expected, the increasing classical power degrades both $\mathcal{Z}$ basis QBER and visibility of the interferometer (related to $\mathcal{X}$ basis QBER), in a way that at −27 dBm launch power the overall error exceeds the threshold value that prevents a secret key to be shared. At this power level, more advanced multiplexing schemes (including wide-range wavelength multiplexing and polarization multiplexing) are required for secret key exchange with this protocol and detectors. We set a launch power of −29 dBm for our long-term acquisition (Fig. 4b) in order to keep the QBERs low and, at the same time, to preserve a good signal to noise ratio for clock detection at the receiver. Indeed, a lower power level would increase the occurrence of zero detection for synchronization pulses, resulting in a decreasing raw key rate.

4 Conclusions

In conclusion, we demonstrated a simple and low-cost quantum key distribution scheme over a metropolitan fiber link. Quantum and weak classical light have been co-propagated

along the installed fiber, proving the stability of the entire setup for more than 4 hours. This work acts as a milestone for the future Italian quantum network, proving how the already installed fibers can be pursued for quantum communication over the whole country.

Acknowledgements
D. Bacco acknowledges financial support from the COST action MP 1403.

Funding
This work is supported by the Center of Excellence, SPOC-Silicon Photonics for Optical Communications (ref DNRF123), by the People Programme (Marie Curie Actions) of the European Union's Seventh Framework Programme (FP7/2007-2013) under REA grant agreement n° 609405 (COFUNDPostdocDTU). This research was sponsored by the NATO Science for Peace and Security program under grant G5485.

Abbreviations
QKD, Quantum Key Distribution; DWDM, Dense Wavelenght Division Multiplexing; InGaAs, Indium Gallium Arsenide; SNSPD, Superconducting Nanowire Single Photon Detector; bps, bit per second or bit/s; WCPs, weak coherent pulses; BB84, Bennett and Brassard 1984 QKD protocol; IM, Intensity Modulator; CW, continuous wave; PM, Phase Modulator; BS, beam splitter; VOA, variable optical attenuator; ITU-T, International Telecommunication Union-Telecommunication Standardization Bureau; C-band, 1530–1565 nm; O-band, 1260–1360 nm; FPGA, Field Programmable Gate Array; DAC, Digital-to-Analog converter; SPAD, Single Photon Avalanche Detectors; DLI, delay-line interferometer; QBER, Quantum Bit Error Rate; SKR, Secret Key Rate; APD, avalanche photodiode; LENS, European Laboratory for Non-linear Spectroscopy; INRiM, National Institute of Metrological Research.

Availability of data and materials
Not applicable. For all requests relating to the paper, please contact the first author.

Competing interests
The authors declare that they have no competing interests.

Authors' contributions
DB and AZ conceived the experiment. DB, IV, NB carried out the experimental work. DB and BDL carried out the theoretical analysis on the protocol. All authors discussed the results and contributed to the writing of the manuscript. All authors read and approved the final manuscript.

Author details
[1]CoE SPOC, DTU Fotonik, Department of Photonics Engineering, Technical University of Denmark, Kgs. Lyngby, Denmark. [2]Università degli Studi di Napoli Federico II, Napoli, Italy. [3]CNR-INO, Istituto Nazionale di Ottica, Firenze, Italy. [4]Micro Photon Devices S.r.l., Bolzano, Italy. [5]I.N.Ri.M., Istituto Nazionale di Ricerca Metrologica, Torino, Italy. [6]LENS, Università di Firenze, Firenze, Italy.

Publisher's Note

Received: 4 April 2019 Accepted: 21 October 2019 Published online: 28 October 2019

References

1. Bennett CH, Brassard G. Quantum cryptography: public-key distribution and coin tossing. In: Proceedings of IEEE international conference on computers systems and signal processing. 1984. p. 175–9.
2. Scarani V, Bechmann-Pasquinucci H, Cerf NJ, Dušek M, Lütkenhaus N, Peev M. The security of practical quantum key distribution. Rev Mod Phys. 2009;81(3):1301–50.
3. Diamanti E, Lo H-K, Qi B, Yuan Z. Practical challenges in quantum key distribution. npj Quantum Inf. 2016;2:16025.
4. Boaron A, Boso G, Rusca D, Vulliez C, Autebert C, Caloz M, Perrenoud M, Gras G, Bussières F, Li M-J, et al. Secure quantum key distribution over 421 km of optical fiber. Phys Rev Lett. 2018;121(19):190502.
5. Hwang W-Y. Quantum key distribution with high loss: toward global secure communication. Phys Rev Lett. 2003;91(5):057901.
6. Minder M, Pittaluga M, Roberts GL, Lucamarini M, Dynes JF, Yuan ZL, Shields AJ. Experimental quantum key distribution beyond the repeaterless secret key capacity. Nat Photonics. 2019;13:334–8.
7. Yin H-L, Chen T-Y, Yu Z-W, Liu H, You L-X, Zhou Y-H, Chen S-J, Mao Y, Huang M-Q, Zhang W-J, et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. Phys Rev Lett. 2016;117(19):190501.
8. Da Lio B, Bacco D, Cozzolino D, Da Ros F, Guo X, Ding Y, Sasaki Y, Aikawa K, Miki S, Terai H, et al. Record-high secret key rate for joint classical and quantum transmission over a 37-core fiber. In: 2018 IEEE photonics conference (IPC); 2018. p. 1–2.
9. Dynes JF, Tam WW, Plews A, Fröhlich B, Sharpe AW, Lucamarini M, Yuan Z, Radig C, Straw A, Edwards T, et al. Ultra-high bandwidth quantum secured data transmission. Sci Rep. 2016;6:35149.
10. Qiu J. Quantum communications leap out of the lab. Nat News. 2014;508(7497):441–2.
11. Peev M, Pacher C, Alléaume R, Barreiro C, Bouda J, Boxleitner W, Debuisschert T, Diamanti E, Dianati M, Dynes JF, et al. The SECOQC quantum key distribution network in Vienna. New J Phys. 2009;11(7):075001.

12. Yuan ZL, Shields AJ. Continuous operation of a one-way quantum key distribution system over installed telecom fibre. Opt Express. 2005;13(2):660–5.
13. Shimizu K, Honjo T, Fujiwara M, Ito T, Tamaki K, Miki S, Yamashita T, Terai H, Wang Z, Sasaki M. Performance of long-distance quantum key distribution over 90-km optical links installed in a field environment of Tokyo metropolitan area. J Lightwave Technol. 2014;32(1):141–51.
14. Tang Y-L, Yin H-L, Zhao Q, Liu H, Sun X-X, Huang M-Q, Zhang W-J, Chen S-J, Zhang L, You L-X, et al. Measurement-device-independent quantum key distribution over untrustful metropolitan network. Phys Rev X. 2016;6(1):011024.
15. Bunandar D, Lentine A, Lee C, Cai H, Long CM, Boynton N, Martinez N, DeRose C, Chen C, Grein M, et al. Metropolitan quantum key distribution with silicon photonics. Phys Rev X. 2018;8(2):021009.
16. Collins RJ, Amiri R, Fujiwara M, Honjo T, Shimizu K, Tamaki K, Takeoka M, Andersson E, Buller GS, Sasaki M. Experimental transmission of quantum digital signatures over 90 km of installed optical fiber using a differential phase shift quantum key distribution system. Opt Lett. 2016;41(21):4883–6.
17. Zhang Y-C, Li Z, Chen Z, Weedbrook C, Zhao Y, Wang X, Xu C, Zhang X, Wang Z, Li M, et al. Continuous-variable QKD over 50km commercial fiber. arXiv:1709.04618 (2017).
18. Tanaka A, Fujiwara M, Nam SW, Nambu Y, Takahashi S, Maeda W, Yoshino K, Miki S, Baek B, Wang Z, et al. Ultra fast quantum key distribution over a 97 km installed telecom fiber with wavelength division multiplexing clock synchronization. Opt Express. 2008;16(15):11354–60.
19. Choi I, Zhou YR, Dynes JF, Yuan Z, Klar A, Sharpe A, Plews A, Lucamarini M, Radig C, Neubert J, et al. Field trial of a quantum secured 10 Gb/s DWDM transmission system over a single installed fiber. Opt Express. 2014;22(19):23121–8.
20. Wonfor A, Dynes JF, Kumar R, Qin H, Tam WWS, Plews A, Sharpe AW, Lucamarini M, Yuan ZL, Penty RV, et al. High performance field trials of QKD over a metropolitan network. In: Quantum cryptography (QCrypt); 2017.
21. Mao Y, Wang B-X, Zhao C, Wang G, Wang R, Wang H, Zhou F, Nie J, Chen Q, Zhao Y, et al. Integrating quantum key distribution with classical communications in backbone fiber network. Opt Express. 2018;26(5):6010–20.
22. Calonico D. A fibre backbone in Italy for precise time and quantum key distribution. In: 4th ETSI/IQC workshop on quantum-safe cryptography; 2016.
23. Boaron A, Korzh B, Houlmann R, Boso G, Rusca D, Gray S, Li M-J, Nolan D, Martin A, Zbinden H. Simple 2.5 GHz time-bin quantum key distribution. Appl Phys Lett. 2018;112(17):171108.
24. Rusca D, Boaron A, Curty M, Martin A, Zbinden H. Security proof for a simplified Bennett–Brassard 1984 quantum-key-distribution protocol. Phys Rev A. 2018;98(5):052336.
25. Rusca D, Boaron A, Grünenfelder F, Martin A, Zbinden H. Finite-key analysis for the 1-decoy state QKD protocol. Appl Phys Lett. 2018;112(17):171104.
26. Lo H-K, Ma X, Chen K. Decoy state quantum key distribution. Phys Rev Lett. 2005;94(23):230504.
27. Avesani M, Marangon DG, Vallone G, Villoresi P. Source-device-independent heterodyne-based quantum random number generator at 17 Gbps. Nat Commun. 2018;9(1):5365.
28. Stefanov A, Gisin N, Guinnard O, Guinnard L, Zbinden H. Optical quantum random number generator. J Mod Opt. 2000;47(4):595–8.
29. Jennewein T, Achleitner U, Weihs G, Weinfurter H, Zeilinger A. A fast and compact quantum random number generator. Rev Sci Instrum. 2000;71(4):1675–80.
30. Tosi A, Della Frera A, Bahgat Shehata A, Scarcella C. Fully programmable single-photon detection module for InGaAs/InP single-photon avalanche diodes with clean and sub-nanosecond gating transitions. Rev Sci Instrum. 2012;83(1):013104.