Multiprotocol Quantum Key Distribution Receiver for Free Space

Proceedings Volume 12335, Quantum Technology: Driving Commercialisation of an Enabling Science III; 123350B (2023) https://doi.org/10.1117/12.2646456

PROCEEDINGS OF SPIE

SPIEDigitalLibrary.org/conference-proceedings-of-spie

Multiprotocol quantum key distribution receiver for free space

Alfonso Tello Castillo, Ugo Zanforlin, Gerald Buller, Ross Donaldson

Alfonso Tello Castillo, Ugo Zanforlin, Gerald Buller, Ross Donaldson, "Multiprotocol quantum key distribution receiver for free space," Proc. SPIE 12335, Quantum Technology: Driving Commercialisation of an Enabling Science III, 123350B (11 January 2023); doi: 10.1117/12.2646456

SPIE.

Event: SPIE Photonex, 2022, Birmingham, United Kingdom

Multiprotocol Quantum Key Distribution Receiver for Free Space

Alfonso Tello Castillo, Ugo Zanforlin, Gerald Buller, Ross Donaldson

Scottish Universities Physics Alliance, Institute of Photonics & Quantum Sciences, School of Engineering and Physical Sciences, Heriot-Watt University, David Brewster Building, Edinburgh EH14 4AS, Scotland, UK

ABSTRACT

Quantum Key Distribution (QKD), a technology for growing mathematically secure key encryption keys, is now on the verge of becoming widely commercially available. Due to lack of standardization, multiprotocol QKD receivers are particularly beneficial for satellite QKD, so that an optical ground station is not limited to a sub-set of satellites. Moreover, if both transmitter and receiver can operate with different protocols, they will be able to actively adapt to specific conditions by choosing the most suitable protocol. In this work, we present the design and performance of a multiprotocol reconfigurable free-space QKD receiver. The reconfigurability relies on polarization-based optical routing, which can also be used to optimize the performance of time-bin QKD protocols.

Keywords: quantum communication, free-space quantum key distribution, time-bin QKD, quantum technology, single-photon detection, time-bin encoding, phase encoding.

1. INTRODUCTION

Quantum Key Distribution (QKD) is believed to be the next quantum technology available in the market (after quantum random number generators). In fact, commercial examples can already be found[1,2]. However, these devices do not have the required capabilities for today's technology. QKD provides a mechanism to grow secure secret encryption keys between two parties to later use them with the one-time pad protocol[3], being this the only known way of securely encrypting messages without assumptions. The one-time pad codification scheme means that keys can only be used once and they must be as long as the message, which implies that QKD needs to create secret keys at similar rates to today's communications. The encryption key can also be used as a secure seed for post-quantum cryptography encryption algorithms, but there is the risk that future hacking methods could make those post-quantum cryptography algorithms insecure[4].

Because of the gap between today's communication data rate and QKD secret key rates (SKR), the research community is trying different technologies and protocols to boost the SKR. Many experiments in fiber[5,6] are being run with the Twin-Field protocol[7] and its variants[8–12]. These kinds of protocols can overcome the PLOB limit[13], a theoretical limit for point-to-point QKD systems, due to using a repeater architecture like measurement-device-independent[14] (MDI) QKD. Other groups are experimenting with the widely known polarization decoy BB84 protocol[15,16] (even though maintaining polarization in fiber is challenging and degradation can occur over long distances), and there are also efforts in protocols based on time-bin and phase encoding like Coherent-One Way[17] (COW) or Round Robin Differential Phase Shift[18] (RR DPS). In free space, experiments are dominated by the polarization decoy BB84 protocol because of the minimal atmosphere birefringence. Other encoding schemes such as time-bin or phase are considered challenges due to the difficulty of performing interferometry after a turbulent channel. However, recent works have proposed new designs to overcome the problem of multimodal interferometry[19,20] and a recent paper has demonstrated the potential of the COW protocol for free-space[21].

This variety in technology means that every deployed system relies on different architectures. Because of this, it is interesting to develop systems capable of handling multiple protocols. Such capability offers the possibility to operate the different protocols depending on the channel's conditions, always looking to optimize the SKR. This feature is especially interesting for free-space systems since a free space channel is expected to change with time.

Quantum Technology: Driving Commercialisation of an Enabling Science III, edited by Miles J. Padgett, Kai Bongs, Alessandro Fedrizzi, Alberto Politi, Proc. of SPIE Vol. 12335, 123350B
 · 0277-786X · doi: 10.1117/12.2646456

Multiprotocol QKD systems are not only interesting for point-to-point schemes. In the future, QKD aims for multi-user networks[22–24]. For instance, in a free-space scenario, this is expected to be achieved using a satellite network. Due to the lack of standardization in QKD, it is likely that each country or company will develop their own unique systems, at least till the technology is more mature. In this context, interoperability is a key feature, since this could allow communication between different friendly entities, and therefore, reduce the costs and complexity of needing to launch more satellites to offer greater coverage times.

This work presents the design for a multiprotocol free-space receiver QKD. In particular, the design can work with the time-bin version of the decoy BB84, COW, and DPS[25]. This work closes the gap with previous designs demonstrated for transmitters that could operate the same three protocols[26–28]. The multiprotocol feature is achieved using polarization routing, taking advantage of the fact that these protocols do not require a specific polarization state.

2. MULTIPROTOCOL QKD FREE SPACE RECEIVER

The free space receiver was designed following the work presented in[19], to make the interferometer robust against multi-modal beam profiles, a key future for systems working after a turbulent channel such as the atmosphere. The system depicted in Figure 1 is an evolution from previous work[21], where a new polarization beam-splitter (PBS) and a previous half-wave plate (HWP) were mounted to achieve a variable beam-splitter (VBS). This VBS will be used to route light in different ratios towards the different receiver areas, depending on the protocol in used. For decoy BB84 and DPS a 100%-0% transmittivity vs reflectivity ratio must be set, for COW the ratio is not define but a 20%-80% would optimize the secret key rate for the system noise.

Area I is the polarization controlling area. Here the input state is modified to achieve the desire ratio at the PBS. Area II is the COW key detection stage. Area III is the interferometer stage; this is an unbalanced Michelson design to interfere two consecutive pulses with a time separation of 1 ns. The relay lenses are used to passively compensate for the different path evolutions, which allow interference when the incident light has an angle different from zero. Other designs using glasses with different refractive indexes could be used[29]. The two quarter wave plates (QWP) are used to rotate the light 90 degrees so the recombine light directed to the PBS is reflected to the detector in area IV instead to area II. Finally, area IV is the interferometer detection area, detector D3 has an extra QWP to direct back reflections to D1 instead to back to the interferometer. If this is not handled, the visibility would decrease. The detection stages used in the setup are composed of a focusing lens and a free-space coupled silicon-based SPAD with a detection efficiency of 45% for 852 nm [Excelitas, SPCM-AQRH]. The dark counts for the SPAD closest to the output (D2) was 50 cps, while the other detector (D1 or D3) suffered 400 cps.

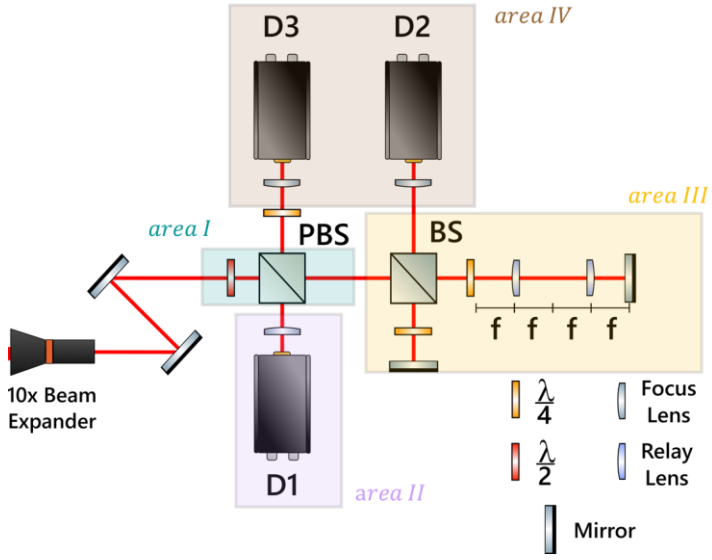

Figure 1. Free-space receiver design for a multiprotocol system. The receiver can work with the protocols COW, DPS and the time-bin version of decoy BB84. In area I the polarization state is manipulated to achieve the desired ratio at the PBS.

Area II is used for the key detection in the COW protocol. Area III is an unbalanced interferometer to interfere two consecutives pulses separated 1 ns in time. Area IV is the interferometer detection stage. The two QWP in area III are used to rotate the polarization 90 degrees so the light going back to the PBS is directed to D3. The extra QWP in D3 is used to direct back reflections to D1 instead of the interferometer, which would decrease the visibility.

The mirror at the interferometer short arm has been mounted on a z-translation stage with a piezo controller to tune the interferometer phase for stabilization purposes. The visibility can be constantly monitored at D2 or D3, sending a couple of reference pulses with a phase difference of 180 degrees. If the visibility drops from a target value, a voltage can be applied to the piezo to correct it.

To the best of our knowledge, this is the first free-space receiver design presented for a multiprotocol system. Depending on the requirements the protocols COW, DPS or decoy BB84 could be performed. The receiver work with a polarization routing technique taking advantage of not using polarization-based protocols. It also incorporates a stabilization module to allow for long-term measurements.

3. VISIBILITY STABILITY

In this section, the interferometer stability is presented. To increase the speed of data recording, and to achieve a system closer to real implementation capable of working in real time, the stabilization of the system was done automatically. As commented above, the mirror at the short arm is mounted on a piezo-controlled z-translation stage. In each protocol, every 30 pulses two reference pulses with a 180 degrees shift are sent to the interferometer. These pulses do not carry any information, although they are sent at single photon-level as the same transmitter was used. The visibility of these pulses is monitored after creating a histogram with the information provided by a time-tagger. Then, a voltage driver changes the applied voltage in the piezo controller depending on the results.

The logic was controlled with a PID controller. A PID controller is designed for linear systems, i.e. its response is linear. The output of the interferometer cannot be modeled as linear most of the time. However, if the temperature of the room was cooled down below room temperature, and the system was left alone for some hours the response was close to sinusoidal, which can be approximated as linear if the feedback loop corrects fast enough. The stability of the interferometer can be seen in Figure 2.

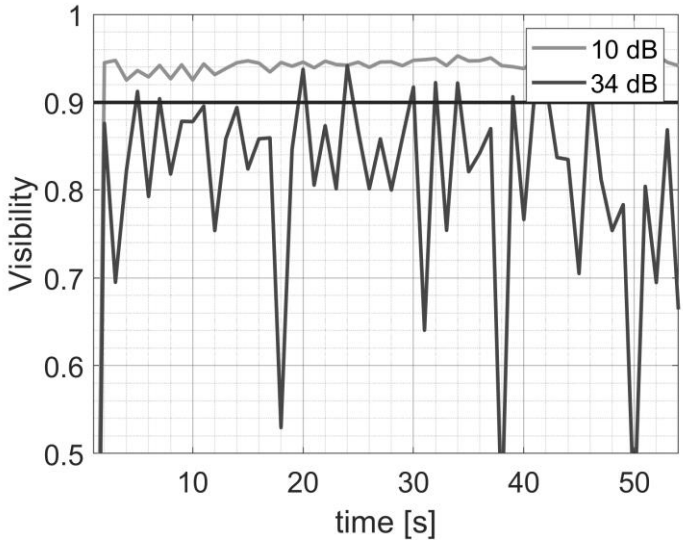

Figure 2. Visibility stability with time for different channel attenuations. When the signal to noise ratio (SNR) is high, the uncertainty in the visibility measurement is low and the PID controller can correct the deviation easily. On the other hand, with a low SNR the minimums are noisy, and the visibility uncertainty is bigger. This causes the PID controller to overestimate the error more frequently, therefore longer acquisition times were needed. This issue could be solved sending the reference pulses through another system that does not attenuate the pulses at single-photon level.

The visibility can be maintained in time if the signal to noise ratio (SNR) is high because the uncertainty in the measurement is low and the PID can accurately correct for deviations. However, when the SNR is decreased (higher channel attenuations) the visibility error is overestimated, hence, the controller tries to correct a bigger error. This is what explains the higher fluctuations in the measurements. This could be solved in the reference pulses are not attenuated to single-photon level. Nevertheless, the interferometer shows promising visibility results up to 98% which would allow for QKD measurements with the different protocols.

4. CONCLUSIONS

In this work, a design for a free-space multiprotocol QKD receiver has been presented. The design relies on polarization routing techniques to allow for different protocol operations. This is something possible due to using time-bin/phase encoding base protocols since the particular polarization state is not important. The system also includes a visibility feedback loop to stabilize the interferometer phase.

Results show how the visibility can achieve values up to 98% and can be maintained constant for long periods. These will result in high SKR for the three different protocols in use.

REFERENCES

[1] "Quantum Key Distribution Resource Centre.", <https://www.idquantique.com/resource-library/quantum-key-distribution/> (27 October 2022).

[2] "Products | Quantum Key Distribution | TOSHIBA DIGITAL SOLUTIONS CORPORATION.", <https://www.global.toshiba/ww/products-solutions/security-ict/qkd/products.html> (27 October 2022).

[3] Shannon, C. E., "Communication Theory of Secrecy Systems," Bell System Technical Journal **28**(4), 656–715 (1949).

[4] Grote, O., Ahrens, A. and Benavente-Peces, C., "A Review of Post-quantum Cryptography and Crypto-agility Strategies," 2019 International Interdisciplinary PhD Workshop, IIPhDW 2019, 115–120, Institute of Electrical and Electronics Engineers Inc. (2019).

[5] Chen, J.-P., Zhang, C., Liu, Y., Jiang, C., Zhang, W.-J., Han, Z.-Y., Ma, S.-Z., Hu, X.-L., Li, Y.-H., Liu, H., Zhou, F., Jiang, H.-F., Chen, T.-Y., Li, H., You, L.-X., Wang, Z., Wang, X.-B., Zhang, Q. and Pan, J.-W., "Twin-Field Quantum Key Distribution over 511 km Optical Fiber Linking two Distant Metropolitans," Nat Photonics **15**, 570–575 (2021).

[6] Wang, S., Yin, Z. Q., He, D. Y., Chen, W., Wang, R. Q., Ye, P., Zhou, Y., Fan-Yuan, G. J., Wang, F. X., Chen, W., Zhu, Y. G., Morozov, P. v., Divochiy, A. v., Zhou, Z., Guo, G. C. and Han, Z. F., "Twin-field quantum key distribution over 830-km fibre," Nature Photonics 2022 16:2 **16**(2), 154–161 (2022).

[7] Lucamarini, M., Yuan, Z. L., Dynes, J. F. and Shields, A. J., "Overcoming the rate-distance limit of quantum key distribution without quantum repeaters," Nature **557**(7705), 400–403 (2018).

[8] Cui, C., Yin, Z. Q., Wang, R., Chen, W., Wang, S., Guo, G. C. and Han, Z. F., "Twin-Field Quantum Key Distribution without Phase Postselection," Phys Rev Appl **11**(3), 034053 (2019).

[9] Xu, H., Yu, Z.-W., Jiang, C., Hu, X.-L. and Wang, X.-B., "Improved results for sending-or-not-sending twin-field quantun key distribution: breaking the absolute limit of repeaterless key rate," Phys Rev A (Coll Park) **101**(4) (2019).

[10] Yu, Z. W., Hu, X. L., Jiang, C., Xu, H. and Wang, X. bin., "Sending-or-not-sending twin-field quantum key distribution in practice," Scientific Reports 2019 9:1 **9**(1), 1–8 (2019).

[11] Wang, X. bin, Yu, Z. W. and Hu, X. L., "Twin-field quantum key distribution with large misalignment error," Phys Rev A (Coll Park) **98**(6), 062323 (2018).

[12] Ma, X., Zeng, P. and Zhou, H., "Phase-Matching Quantum Key Distribution," Phys Rev X **8**(3), 031043 (2018).

[13] Pirandola, S., Laurenza, R., Ottaviani, C. and Banchi, L., "Fundamental limits of repeaterless quantum communications," Nature Communications 2017 8:1 **8**(1), 1–15 (2017).

[14] Lo, H. K., Curty, M. and Qi, B., "Measurement-device-independent quantum key distribution," Phys Rev Lett **108**(13), 130503 (2012).

[15] Lo, H. K., Ma, X. and Chen, K., "Decoy state quantum key distribution," Phys Rev Lett **94**(23), 230504 (2005).
[16] Hwang, W. Y., "Quantum Key Distribution with High Loss: Toward Global Secure Communication," Phys Rev Lett **91**(5), 057901 (2003).
[17] Gisin, N., Ribordy, G., Zbinden, H., Stucki, D., Brunner, N. and Scarani, V., "Towards practical and fast Quantum Cryptography" (2004).
[18] Sasaki, T., Yamamoto, Y. and Koashi, M., "Practical quantum key distribution protocol without monitoring signal disturbance," Nature **509**(7501), 475–478 (2014).
[19] Jin, J., Agne, S., Bourgoin, J. P., Zhang, Y., Lütkenhaus, N. and Jennewein, T., "Demonstration of analyzers for multimode photonic time-bin qubits," Phys Rev A (Coll Park) **97**(4), 1–10 (2018).
[20] Cahall, C., Islam, N. T., Gauthier, D. J. and Kim, J., "Multimode Time-Delay Interferometer for Free-Space Quantum Communication," Phys Rev Appl **13**(2), 024047 (2020).
[21] Tello Castillo, A., Eso, E. and Donaldson, R., "In-lab demonstration of coherent one-way protocol over free space with turbulence simulation," Opt Express **30**(7), 11671 (2022).
[22] Fernandez, V., Collins, R. J., Gordon, K. J., Townsend, P. D. and Buller, G. S., "Passive optical network approach to gigahertz-clocked multiuser quantum key distribution," IEEE J Quantum Electron **43**(2), 130–138 (2007).
[23] Xue, P., Wang, K. and Wang, X., "Efficient multiuser quantum cryptography network based on entanglement," Sci Rep **7**(1), 1–7 (2017).
[24] Zhong, X., Wang, W., Mandil, R., Lo, H. K. and Qian, L., "Simple Multiuser Twin-Field Quantum Key Distribution Network," Phys Rev Appl **17**(1), 014025 (2022).
[25] Inoue, K., Waks, E. and Yamamoto, Y., "Differential phase shift quantum key distribution," Phys Rev Lett **89**(3), 379021–379023 (2002).
[26] Sibson, P., Erven, C., Godfrey, M., Miki, S., Yamashita, T., Fujiwara, M., Sasaki, M., Terai, H., Tanner, M. G., Natarajan, C. M., Hadfield, R. H., O'Brien, J. L. and Thompson, M. G., "Chip-based quantum key distribution," Nat Commun **8**(1), 1–6 (2017).
[27] de Marco, I., Woodward, R. I., Roberts, G. L., Paraïso, T. K., Roger, T., Sanzaro, M., Lucamarini, M., Yuan, Z. and Shields, A. J., "Real-time operation of a multi-rate, multi-protocol quantum key distribution transmitter," Optica **8**(6), 911 (2021).
[28] Korzh, B., Walenta, N., Houlmann, R. and Zbinden, H., "A high-speed multi-protocol quantum key distribution transmitter based on a dual-drive modulator," Opt Express **21**(17), 19579 (2013).
[29] Tello, A., Novo, C. and Donaldson, R., "Prospects of time-bin quantum key distribution in turbulent free-space channels," Emerging Imaging and Sensing Technologies for Security and Defence V; and Advanced Manufacturing Technologies for Micro- and Nanosystems in Security and Defence III **11540**, M. Farsari, J. G. Rarity, F. Kajzar, A. Szep, R. C. Hollins, G. S. Buller, R. A. Lamb, M. Laurenzis, A. Camposeo, L. Persano, L. E. Busse, M. Dušek, P. M. Alsing, M. L. Fanto, and R. Zamboni, Eds., 2, SPIE (2020).