Prospects of Chip-Based Multi-Protocol Quantum Key Distribution Transceivers

Citation for published version (APA):
Grebenchukov, A., Lui, H., Nazarikov, G., Cimoli, B., Rommel, S., & Monroy, I. T. (2023). Prospects of Chip-Based Multi-Protocol Quantum Key Distribution Transceivers. In M. Jaworski, & M. Marciniak (Eds.), *2023 23rd International Conference on Transparent Optical Networks, ICTON 2023* Article 10207518 Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/ICTON59386.2023.10207518

DOI:
10.1109/ICTON59386.2023.10207518

Document status and date:
Published: 08/08/2023

Document Version:
Accepted manuscript including changes made at the peer-review stage

Prospects of Chip-Based Multi-Protocol Quantum Key Distribution Transceivers

Alexander Grebenchukov[1], **Hui Lui**[1], **Gleb Nazarikov**[1], **Bruno Cimoli**[1], **Simon Rommel**[1], **and Idelfonso Tafur Monroy**[1]

[1]*Department of Electrical Engineering, Eindhoven University of Technology, 5623PD Eindhoven, The Netherlands*

e-mail: a.grebenchukov@tue.nl

ABSTRACT

Quantum communications enable the transmission of information in a secure way that is ensured by the laws of quantum physics. Current quantum-safe communication systems are based on quantum key distribution (QKD) technology at their core. In the most recent years, a remarkable effort has been put into practical implementations of QKD with a focus on their integration into classical optical networks, some of which are becoming commercially available. However, even with the ongoing development of QKD systems, there are efforts toward their miniaturization, power efficiency improvement, and enhancement of their flexibility and functionality.

In this paper, we outline major QKD protocols and review recent advances in QKD systems based on photonic integrated circuits. Finally, we will discuss the potential feasibility of multi-protocol QKD chips leveraging the advantages of different protocols in one solution.

Keywords: quantum key distribution, photonic integrated circuits, multi-protocol QKD.

1. Introduction

In conventional communications, two (or more) distant parties share encrypted information using symmetric encryption schemes such as Advanced Encryption Standard (AES). Symmetric encryption requires to share of secret keys that are shared with public-key encryption schemes such as Rivest–Shamir–Adleman (RSA) [1]. The confidentiality of the secret keys is commonly known as the key distribution problem [2]. The security of public-key encryption relies on the lack of the intruder's computational power for breaking the encryption algorithm. Unfortunately, quantum computers have been theoretically demonstrated to be capable of breaking classic public-key encryption standards with Shor's algorithm [3]. To prevent a situation where security in a network can be broken, a new generation of post-quantum cryptography (PQC) algorithms have been proposed [4]. However, PQC algorithms will rely on the assumption of the computational power of the adversaries. Another promising approach is to rely on quantum key distribution (QKD) solutions, which are based on the fundamental law of quantum mechanics, for sharing secret keys. QKD allows for the secure exchange of keys with real-time detection of unauthorized access to a quantum link. QKD security is independent of future improvements in computer performance or decryption algorithm advances [5].

Throughout the past few decades, numerous achievements in QKD development have been demonstrated, driven by its promising prospects, from the first prototypes [6] to commercially available products. Despite the gradual maturing of QKD systems, there are still multiple challenges to large-scale deployment and compatibility with existing communication systems. A crucial point for making this technology accessible is to replace bulk optical components with photonic integrated circuits (PIC), which enhance advantages in miniaturization, and compatibility with microelectronics, and are amenable to mass production.

In recent years, several photonic integration platforms for QKD have been proposed and investigated. Among them, there are QKD photonic chip devices on the basis of silicon (Si) [7], indium phosphide (InP) [8], and silicon nitride ($\mathrm{Si}_x\mathrm{N}_y$) [9] integrated platforms. The silicon-based photonic platform is based on well-established fabrication techniques. However, the Si platform requires external laser sources. The $\mathrm{Si}_x\mathrm{N}_y$-based platform possesses extremely low propagation loss and high tolerance to thermal fluctuations enabling low-temperature single photon detectors integration. InP-based photonic chips enable laser integration and high-speed modulation [10], but at the same time, this platform has several limitations, such as a requirement for higher driving signals and possessing higher losses. The most promising approach is hybrid integration when different platforms are exploited for specific parts of QKD systems.

Another significant challenge is the lack of standardization in the physical layer and therefore lack of compatibility between different QKD modules that rely on different technologies and specific protocols according to the vendor. When moving beyond point-to-point links, this lack of interoperability will lead to challenges in QKD deployment. This leads to another challenge which is the lack of interoperability between different QKD systems [11]. Most of the QKD chips are exclusively fabricated and operate using a specific protocol. Hence, the multi-protocol feature for QKD system is highly desirable for the accomplishment of QKD networks beyond point-to-point. Moreover, the possibility of using multiple protocols also allows for the optimization of the secret key rate (SKR) and achievable transmission distance depending on certain conditions.

In this work, we review the last achievements in the development of different QKD protocols in section 2. Next, in section 3 possible multi-protocol chip-based system which combines both the discrete and continuous variable QKD is considered.

2. QKD Protocols

Significant progress in the development of QKD protocols has been made since the introduction of the first Bennett-Brassard-1984 (BB84) protocol [12]. There are several classification criteria for QKD protocols. Depending on the approach to transmitting information, prepare-and-measure, and entanglement-based schemes are distinguished [13]. In the first one, Alice prepares a quantum state and sends it to Bob to be measured and restore the encoded data. The latter lies in the preparation of entangled quantum states by an external source which then sends them to Bob and Alice for measurements. According to the most common classification, all existing QKD protocols can be divided into two types: discrete-variable QKD (DV-QKD) and continuous-variables QKD (CV-QKD) depending on the type of quantum states utilized to encode information [14].

2.1 Discrete-Variable QKD

The key information in DV-QKD is encoded into the polarization, phase, or time bin of individual photons. A series of DV-QKD protocols have been developed, including the ones based on Heisenberg's uncertainty principle. Among them, there are BB84, differential phase shift (DPS) [15], coherent one-way (COW) [16], twin-field [17], and different types of measurement device independent (MDI) schemes [18], such as phase-matching (PM) [19] and mode-pairing (MP) [20] QKDs. Ekert-91 (E91) [21], and Bennett-Brassard-Mermin-1992 (BBM92) [22] protocols can be attributed to the DV-QKD schemes based on the quantum entanglement principle.

DV-QKD is a more mature technology allowing high key generation rates and the transmission of secret keys for a long distance of up to 833.8 km [23]. One of the key challenges for the implementation of chip-based DV-QKD systems is the technical complexity of fully integrated single-photon detectors.

2.2 Continuous-Variable QKD

In a CV-QKD system, the key information is encoded in the quadrature variables of the optical field and decoded by coherent detection methods [24]. CV-QKD protocols can be classified according to several criteria as well. Depending on the type of prepared state CV-QKD could be with either coherent or squeezed states. Another criterion is the detection method used, which can be classified by homodyne or heterodyne detection approach [2]. Additionally, CV-QKD systems can be divided into Gaussian-modulated (GM) [25] and discrete-modulated (DM) [26] protocols, based on the modulation type utilized.

The main advantages of CV-QKD is high secret key rate transmission on short distances and compatibility with standard communication technologies and infrastructure. This type of QKD is also characterized by high detection efficiency at room temperature.

3. Multi-Protocol QKD

Realization of the QKD network is an important task, as it enables secure communications between multiple users. Having a QKD device with versatile protocol options provides an advantage in adapting to different users with varying protocols, without the requirement for hardware changes. This feature is especially important for applications such as satellite QKD, where access to the hardware is difficult, making it impractical to make equipment changes for each specific protocol demand. Moreover, a QKD device that supports different protocols allows for combining the benefits of different protocols within one device depending on a specific task.

To implement this multi-protocol hybrid QKD system, we propose using a modulator-free transmitter that operates on both optical injection locking (OIL) and direct phase modulation techniques [11]. By applying different driving signals to the laser system of the transmitter, we can achieve hybrid modulation, including quadrature amplitude modulation (QAM) for encoding CV QKD protocols, or time-phase modulation (TPM) for encoding DV QKD protocols. For QAM the transmitter contains two slave lasers for modulation of the signal's in-phase and quadrature components which are injection locked to the same master laser [27]. This scheme can also be applied to the TPM. On the receiver side, two subsystems designed for both CV and DV QKD signal detection on a single chip are arranged. A micro-electromechanical system (MEMS) switcher is used to route between subsystems. Figure1 shows a schematic diagram of the proposed multi-protocol QKD system.

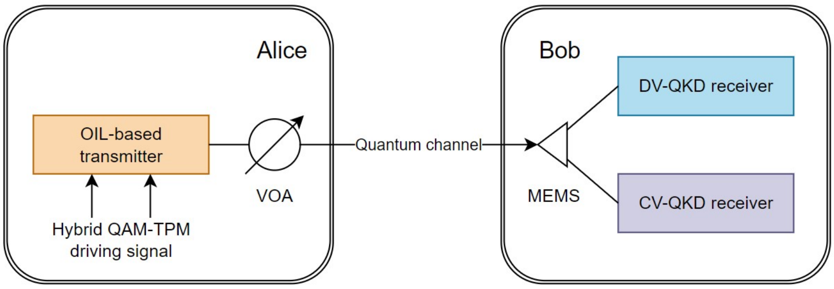

Figure 1: *Schematic diagram of multiprotocol QKD system. VOA: variable optical attenuator.*

4. Conclusions

Chip-based multi-protocol QKD system has great potential for resolving interoperability issues between existing QKD systems. In the proposed scheme, the transmitter and receiver chips allow operation using both the DV and CV QKD protocols. We believe, that the proposed versatile QKD system will have a positive impact on the large-scale development of quantum communication networks. Furthermore, the combination of several protocols within one device provides flexibility to adapt to specific conditions, enabling high-rate QKD over long distances.

Acknowledgments

This work was supported by the Horizon Europe project ALLEGRO (grant no. 101092766), ECSEL-JU project BRAINE (GA 876967), the NWO HTSM project FREEPOWER under project number 17094, and the Dutch Ministry of Economic Affairs and Climate Policy (EZK) as part of the Quantum Delta NL program.

REFERENCES

[1] R.L. Rivest, A. Shamir, and L. Adleman: A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, vol. 21(2), pp. 120-126, 1978.

[2] F. Xu, X. Ma, Q. Zhang, H.K. Lo, and J.W. Pan: Secure quantum key distribution with realistic devices, *Reviews of Modern Physics*, vol. 92(2), p. 025002, 2020.

[3] P.W. Shor: Algorithms for quantum computation: discrete logarithms and factoring, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pp. 124-134, 1994.

[4] D.J. Bernstein, and T. Lange: Post-quantum cryptography, *Nature*, vol. 549(7671), pp. 188-194, 2017.

[5] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden: Quantum cryptography, *Reviews of modern physics*, vol. 74(1), p. 145, 2002.

[6] H. Takesue, S.W. Nam, Q. Zhang, R.H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto: Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors, *Nature photonics*, vol. 1(6), pp.343-348, 2007.

[7] C. Ma, W.D. Sacher, Z. Tang, J.C. Mikkelsen, Y. Yang, F. Xu, T. Thiessen, H.K. Lo, and J.K. Poon: Silicon photonic transmitter for polarization-encoded quantum key distribution, *Optica*, vol. 3(11), pp. 1274-1278, 2016.

[8] P. Sibson, C. Erven, M. Godfrey, S. Miki, T.Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M.G. Tanner, C.M. Natarajan, and R.H. Hadfield: Chip-based quantum key distribution, *Nature communications*, vol. 8(1), p. 13984, 2017.

[9] F. Beutel, H. Gehring, M.A. Wolff, C. Schuck, and W. Pernice: Detector-integrated on-chip QKD receiver for GHz clock rates, *npj Quantum Information*, vol. 7(1), p. 40, 2021.

[10] L. Eldada: Advances in telecom and datacom optical components, *Optical Engineering*, vol. 40(7), pp. 1165-1178, 2001.

[11] I. De Marco, R.I. Woodward, G.L. Roberts, T.K. Paraïso, T. Roger, M. Sanzaro, M. Lucamarini, Z. Yuan, and A.J. Shields: Real-time operation of a multi-rate, multi-protocol quantum key distribution transmitter, *Optica*, vol. 8(6), pp. 911-915, 2021.

[12] C. Bennett, and G. Brassard: Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of International Conference on Computers, Systems & Signal Processing*, pp. 175–179, 1984.

[13] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S.X. Ng, and L. Hanzo: The evolution of quantum key distribution networks: On the road to the internet, *IEEE Communications Surveys & Tutorials*, vol. 24(2), pp. 839-894, 2022.

[14] Q. Liu, Y. Huang, Y. Du, Z. Zhao, M. Geng, Z. Zhang, and K. Wei: Advances in chip-based quantum key distribution, *Entropy*, vol. 24(10), p. 1334, 2022.

[15] K. Inoue, E. Waks, and Y. Yamamoto: Differential phase shift quantum key distribution, *Physical review letters*, vol. 89(3), p. 037902, 2002.

[16] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H.Zbinden: Fast and simple one-way quantum key distribution, *Applied Physics Letters*, vol. 87(19), p. 194108, 2005.

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

[18] H.K. Lo, M. Curty, and B. Qi: Measurement-device-independent quantum key distribution, *Physical review letters*, vol. 108(13), p. 130503, 2012.

[19] X. Ma, P. Zeng, and H. Zhou: Phase-matching quantum key distribution, *Physical Review X*, vol. 8(3), p. 031043, 2018.

[20] P. Zeng, H. Zhou, W. Wu, and X. Ma: Mode-pairing quantum key distribution, *Nature Communications*, vol. 13(1), p. 3903, 2022.

[21] A.K. Ekert: Quantum cryptography based on Bell's theorem, *Physical review letters*, vol. 67(6), p. 661, 1991.

[22] C.H. Bennett, G. Brassard, and N.D. Mermin: Quantum cryptography without Bell's theorem, *Physical review letters*, vol. 68(5), p. 557, 1992.

[23] S. Wang, Z.Q. Yin, D.Y. He, W. Chen, R.Q. Wang, P. Ye, Y. Zhou, G.J. Fan-Yuan, F.X. Wang, W. Chen, and Y.G. Zhu: Twin-field quantum key distribution over 830-km fibre, *Nature Photonics*, vol. 16(2), pp. 154-161, 2022.

[24] T.C. Ralph: Continuous variable quantum cryptography, *Physical Review A*, vol. 61(1), p. 010303, 1999.

[25] P. Jouguet, S. Kunz-Jacques, and A. Leverrier: Long-distance continuous-variable quantum key distribution with a Gaussian modulation, *Physical Review A*, vol. 84(6), p. 062317, 2011.

[26] T. Hirano, T. Ichikawa, T. Matsubara, M. Ono, Y. Oguri, R. Namiki, K. Kasai, R. Matsumoto, and T. Tsurumaru: Implementation of continuous-variable quantum key distribution with discrete modulation, *Quantum Science and Technology*, vol. 2(2), p. 024010, 2017.

[27] Z. Liu, and R. Slavík: Optical injection locking: From principle to applications, *Journal of Lightwave Technology*, vol. 38(1), pp. 43-59, 2020.