Experimental Validation of DV-QKD-based Qline Architecture for Metropolitan Network on Berlin OpenQKD Testbed

Matheus Sena[(1)], Georg Harder[(2)], Ronny Döring[(1)], Ralf-Peter Braun[(3)], Michaela Ritter[(1)], Marc Kaplan[(2)], Marc Geitz[(1)]

[(1)] Deutsche Telekom AG, Winterfeldstraße 21, 10781 Berlin, Germany, matheus.ribeiro-sena@telekom.de
[(2)] VeriQloud, 13 Rue Victor Hugo, 92120 Montrouge, France.
[(3)] ORBIT Ges. für Applikations- und Informationssysteme mbH, Mildred-Scheel-Str.1, 53175 Bonn, Germany.

Abstract *We demonstrate a trusted-node-free design for integration of a DV-QKD system into the Berlin OpenQKD optical testbed. By utilizing conventional telecom modulators and a standard WDM-AWG, our scheme offers flexible multi-partner communication, and full connectivity between non-adjacent nodes over multiple C-band frequencies and metropolitan distances. ©2023 The Author(s)*

Introduction

Quantum key distribution (QKD) has emerged as a solution for quantum-secure encryption key exchange. Yet, despite the rather mature status of QKD technologies for point-to-point (p2p) links, scaling such schemes to more flexible network-like scenarios in a cost-effective way is still a major challenge [1]. In that regard, it has been shown that the implementation of trusted-node-free topologies can partially relax the budget-prohibitive implications of this scalability problem [2], while providing full connectivity between multiple partners. In addition to that, the compatibility of QKD technology with passive wavelength division multiplexing (WDM) elements (e.g., arrayed waveguide gratings (AWG)) facilitates the aggregation of quantum services into the network operator's optical fibre infrastructure [3]. These two favourable aspects, namely, (1) the cost attractiveness of using trusted-node-free solutions, and (2) compatibility with passive WDM devices, create the ideal environment to support the extension of QKD from p2p links to more flexible network-like designs.

Therefore, in this work we propose and experimentally demonstrate a discrete-variable (DV)-QKD system design tailored for metropolitan QKD networks, named Qline [4], that complies with the aspects (1) and (2). Concerning (1), we employ intermediate nodes (Charlies) that possess neither a laser nor a detector, turning the realization of such a proposal very cost attractive. With respect to (2), we utilize a standard WDM-AWG to devise a frequency-multiplexing scheme in which a single Bob can arbitrarily exchange secret keys with other two Alices and multiple intermediate nodes, thus enabling multi-user connectivity. To validate our solution, we carry out lab-based assessments as well as a field trial investigation on Deutsche Telekom AG (DTAG) Berlin OpenQKD Testbed [5]. Our results show stable key exchange between Qline (non)-adjacent nodes over day-long intervals as well as a good response to different C-band frequencies and transmission distances (up to 39.8 km) in field-deployed optical fibre links.

Qline working principle

As can be observed in Fig. 1a, all four nodes depicted in the Qline's schematic are connected using a single quantum communication channel (e.g., optical fibre) and a classical channel. The end terminals of this Qline are named Alice and Bob, whereas the intermediate nodes are called Charlies. Each name implies a specific role in the scheme. Alice generates Qubits, Charlie

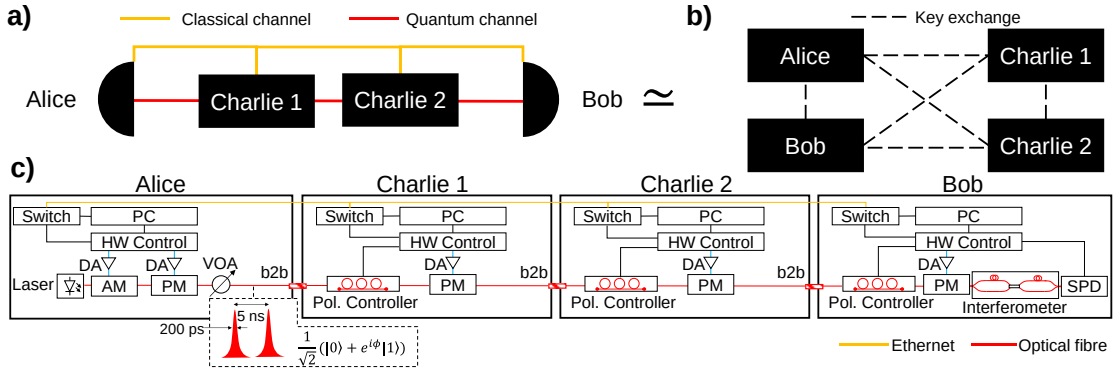

Fig. 1: a) Schematic of the Qline. **b)** Concerning key exchange, the Qline is equivalent to a fully connected QKD network. **c)** Hardware-level diagram of the Qline. PC: personal computer.

modulates them and Bob performs the measurement. In this system [4], we implement a BB84-type protocol with phase encoding such that the Qubit after projection onto a single photon can be written as:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{j\phi}|1\rangle\right), \quad (1)$$

where $\phi \in \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$ [6]. Then, each p-th player in the Qline has a phase modulator (PM) that adds a phase ϕ_p onto the incoming Qubit. This means that the final state (before Bob's measurement) is rotated by an angle Φ that is equivalent to the sum over all phases applied by each individual player in the Qline. That is:

$$\Phi = \sum_{p \in \mathbb{Q}} \phi_p, \quad (2)$$

where $\mathbb{Q}$ is the set of players in the Qline. To illustrate, in the case shown in Fig. 1a, $\mathbb{Q}$ = {Alice, Charlie 1, Charlie 2, Bob}. Moreover, the phase ϕ_p can be written as $\phi_p = \pi(b_p/2 + s_p)$, where one can think of $b_p, s_p \in \{0,1\}$ being two random bits corresponding to the basis and state bit, respectively. If the bases match, i.e.:

$$\sum_{p \in \mathbb{Q}} b_p \oplus 2 = 0, \quad (3)$$

the players share a secret $\sum_{p \in \mathbb{Q}} s_p \oplus 2 = m$, where $m \in \{0,1\}$ is the measurement result at Bob and $\oplus \equiv$ modulo-2. From this secret, one can generate key pairs between any two players. Let us take the successful key exchange between Charlie 1 and Charlie 2. In this case, Alice and Bob publish their secret bits (s_{Alice}, s_{Bob}) and the measurement result (m). Then, we have $s_{Charlie1} \oplus s_{Charlie2} \oplus d_{pub} = 0$, where d_{pub} is publicly known from the published bases, the measurement result and the state bits of Alice and Bob [4]. The postprocessing steps, namely, error correction and privacy amplification, are analogous to standard QKD.

The advantage of this scheme is that the Charlies do neither require a laser nor a quantum detector. Furthermore, this is not a key relaying scheme: no third node is trusted. When Alice and Bob exchange a key, Charlie 1 and Charlie 2 cannot learn it, thus, lowering the trust assumptions and enhancing the security of the network in comparison to conventional QKD schemes. In addition to that, the Qline concept enables full connectivity even between non-adjacent nodes as all players can exchange keys with one another. This is possible because each Qline node is embedded with a PM, what is further detailed in the next section. That means that concerning key exchange possibilities, the linear Qline diagram shown in Fig. 1a corresponds, in essence, to the meshed topology illustrated in Fig. 1b.

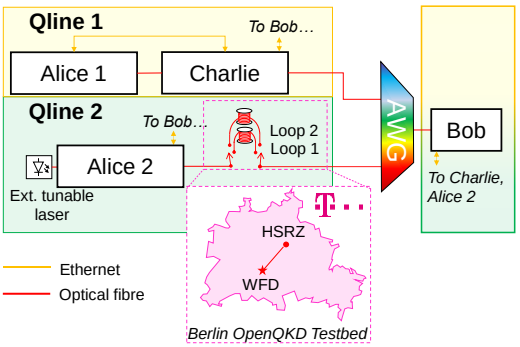

Fig. 2: Schematic of the second experimental setup, where two Qlines were integrated into Berlin OpenQKD Testbed.

Experimental setup

This study investigated two experimental setups: (1) a lab-based testbed used to demonstrate the working principle of Qline (Fig. 1c), and (2) the deployment of two Qlines on Berlin OpenQKD testbed (Fig. 2).

In Fig. 1c, at Alice, a bit sequence is generated by a HW-Control unit that contains a true random number generator. Then, the HW-control produces an analog signal onto two driver amplifiers (DA) that drive an amplitude modulator (AM) and a standard 10-GHz telecom PM. We use time-bin encoding (depicted in the Fig. 1c) to generate the initial state $|\psi\rangle$. Then, $|\psi\rangle$ is attenuated by a variable optical attenuator (VOA) before forwarded back-to-back (b2b) to the next partner, i.e., Charlie 1. At Charlie 1, the incoming photons are fed to a polarization controller (Pol. Controller in Fig. 1c) for eventual correction of

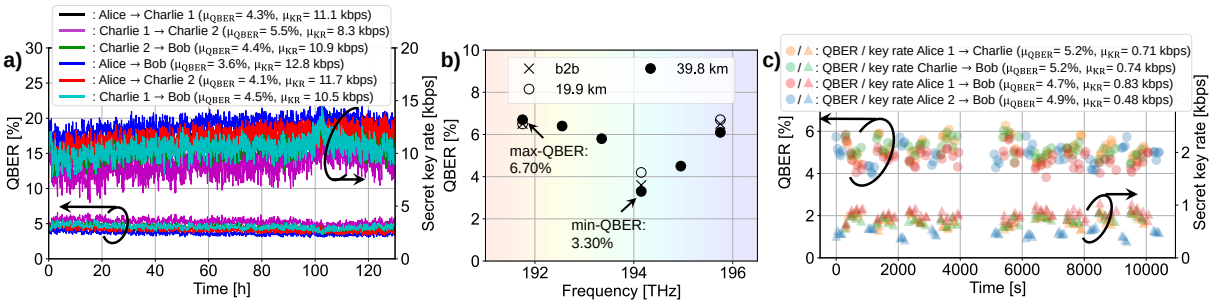

Fig. 3: a) Secret key rate and QBER performance for the setup shown in Fig. 1c. **b)** QBER response of Qline 2 (Fig. 2) to different frequencies and transmission distances. **c)** QBER and secret key rate between pairs of players in Qline 1 and 2. μ_{QBER}: mean QBER. μ_{KR}: mean key rate.

polarization rotations that may arise in the fibre connecting Alice and Charlie 1. After that, Charlie 1 performs the unitary transform (phase modulation) already mentioned in the previous section by adding a phase $\phi_{Charlie1}$ to the incoming state and forwards it to Charlie 2, who also proceeds similarly by adding $\phi_{Charlie2}$ before finally delivering it to Bob. Note that Bob also applies a phase ϕ_{Bob} before projecting the final Qubit on the bases $\{|+\rangle, |-\rangle\}$, or $\{|i\rangle, |-i\rangle\}$, where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ and $|\pm i\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$, using an unbalanced Mach-Zehnder interferometer and a single-photon detector (SPD). Upon measurement of the Qubits, Charlie 1 and 2 broadcast their selected computational basis in a basis reconciliation session (classical channel via Ethernet switches in Fig. 1c). This session is then followed by Quantum Bit Error Rate (QBER) estimation, error correction (via CASCADE code [7]), and privacy amplification (via Toeplitz hashing [8]).

The second experimental setup (shown in Fig. 2) comprises two Qlines, namely, Qline 1 (yellow-shaded area) and Qline 2 (green-shaded area), which are coupled to a WDM 12x12 AWG (400-GHz/band). Qline 1 consists of Alice 1, Charlie and Bob. Both Alice 1 and Charlie are installed at the Winterfeldstraße 21 (WFD), central node of the Berlin OpenQKD testbed. As for Qline2, it is composed of Alice 2 (located at WFD), two field-installed single mode fibre (SMF) loops (Loop 1: 19.9 km, Loop 2: 39.8 km) between WFD and the DTAG's office at the Hauptstadtrepräsentanz (HSRZ), and Bob. Note that one single Bob is shared by both Qlines. The AWG and Bob were also positioned at WFD. In this setup, we attached an external C-band tunable laser (external cavity laser, 25-kHz linewidth, 13 dBm output power) to freely adapt the frequency of Alice 2 (191.75 - 195.75 THz), while Alice 1 is operated with a fixed-frequency laser (external cavity laser, 50-kHz linewidth, 16 dBm output power) at 193.4 THz.

Results and Discussion

Fig. 3a shows the temporal performance of the QBER and the secret key rate for the setup depicted in Fig. 1c. As it can be noticed, the curves indicate not only a relatively low QBER ($\mu_{\mathrm{QBER}} < 5.5\%$) but also a rather stable key rate between nodes in the Qline architecture over approximately 130 hours ($\approx$ 5.4 days). It is also important to emphasize that the key exchange is successful for adjacent (Alice to Charlie 1, Charlie 1 to Charlie 2, Charlie 2 to Bob) as well as for non-adjacent partners (Alice to Bob, Alice to Charlie 2, Charlie 1 to Bob), validating the argument that the Qline, although linear, enables connectivity as if in a meshed topology (Fig. 1b).

In Fig. 3b, the performance of the Qline 2 in second experimental setup (Fig. 2) is tested for different frequencies. This procedure is performed for three link configurations: (1) b2b (bypassing Berlin OpenQKD Testbed), (2) with Loop 1 (19.9 km) and with Loop 2 (39.8 km). The results of this investigation are shown in Fig. 3b, where it is possible to observe a strong frequency dependency of the QBER (global minimum around 194.15 THz). Despite this dependency, the Qline shows a good response across the C-band yielding a maximum QBER of approximately 6.70% (at 191.75 THz), at the same time as a rather negligible influence of the propagation distance can be also noticed.

Finally, Alice 2's external laser is configured to 194.15 THz and the Loop 2 is connected to Qline 2. The QKD session is started and the QBER along with the secret key rate between all players within Qlines 1 and 2 are recorded for approximately 10,000 seconds. In Fig. 3c, it is possible to visualize a relatively stable response of the QBER and key rate between each pair of players. In Fig. 3c, one can also notice that while the mean QBERs for pairs of players do not substantially deviate from one another, the same does not hold for the mean secret key rate. To exemplify, Qline 2 (Alice 2 to Bob) presents a mean key rate significantly lower (0.48 kbps) than the pairs in Qline 1 (Alice 1 to Charlie: 0.71 kbps, Charlie to Bob: 0.74 bps, Alice to Bob: 0.83 kbps). This can be explained by the higher losses originated from the SMF Loop, which impair the key exchange performance. This shows that while the Qline guarantees low-QBER operation, it comes at the expense of sub-optimal key rates.

Conclusions

In this work, we have experimentally presented the concept of Qline, an inexpensive trusted-node-free scheme that offers a flexible yet robust solution for QKD networks. In our results, we have observed stable QBER ($<$ 5.5%) as well as key rate ($\approx$ 10 kbps) performance over 5.4 days. By employing a WDM-AWG, we have also demonstrated how frequency multiplexing enables multi-partner connectivity over different wavelengths and transmission distances (up to 39.8 km). The Qline has shown to be a suitable solution to scale QKD links to more metropolitan-like topologies.

Acknowledgements

This study was supported by the H2020 project OPENQKD under grant agreement No. 857156. The authors would also like to thank the Fraunhofer Heinrich Hertz Institute for lending some additional equipment to carry out this work.

References

[1] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S.-X. Ng, L. Hanzo, “The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet,” in IEEE Communications Surveys & Tutorials, vol. 24, no. 2, pp. 839-894, 2022, DOI: 10.1109/COMST.2022.3144219.

[2] O. Alia, R. S. Tessinari, E. Hugues-Salas, G. T. Kanellos, R. Nejabati, D. Simeonidou., “Dynamic DV-QKD Networking in Trusted-Node-Free Software-Defined Optical Networks,” in *IEEE/OPTICA Journal of Lightwave Technology*, vol. 40, no. 17, pp. 5816-5824, 2022, DOI: 10.1109/JLT.2022.3183962.

[3] X. Duan, J. Pearse, A. Wonfor, C. White, A. Bahrami, A. Straw, T. Edwards, R. Penty, A. Lord, R. Kumar, T. Spiller, “Performance Analysis on Co-existence of COW-QKD and Classical DWDM Channels Transmission in UK National Quantum Networks," in *IEEE/OPTICA Journal of Lightwave Technology*, Early Access, 2023, DOI: 10.1109/JLT.2023.3246175.

[4] M. Doosti, L. Hanouz, A. Marin, E. Kashefi, M. Kaplan, “Establishing shared secret keys on quantum line networks: protocol and security," *arXiv preprint, 2023,* arXiv:2304.01881.

[5] R. -P. Braun and M. Geitz, “The OpenQKD Testbed in Berlin”, in *Asia Communications and Photonics Conference* (ACP), Shanghai, China, pp. 1-3, 2021, Link.

[6] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, vol. 175, pp. 8, 1984, Link.

[7] G. Brassard, L. Salvail, “Secret-Key Reconciliation by Public Discussion,” in *Advances in Cryptology — EUROCRYPT ’93. EUROCRYPT 1993. Lecture Notes in Computer Science*, vol. 765. Springer, Berlin, DOI: https://doi.org/10.1007/3-540-48285-7_35.

[8] C.-H. Fung, X. Ma, H. F. Chau., “Practical issues in quantum-key-distribution postprocessing,” in *Physical Review A*, vol. 81, no. 1, 2010, DOI: https://doi.org/10.1103/PhysRevA.81.012318.