Multi-node quantum key distribution network using existing underground optical fibre infrastructure

Mariella Minder,[1,*] Andreas Siakolas,[1] Stephanos Yerolatsitis,[1] Konstantinos Katzis,[1] and Kyriacos Kalli[1]

[1] *Department of Electrical Engineering, Computer Engineering and Informatics, Cyprus University of Technology, Limassol 3036, Cyprus*

(Dated: May 29, 2025)

Quantum key distribution (QKD) offers unconditional information security by allowing two distant users to establish a common encryption key resilient to hacking. Resultingly, QKD networks interconnecting critical infrastructure and enabling the secure exchange of classified information, can provide a solution to the increasing number of successful cyberattacks. To efficiently deploy quantum networks, the technology must be integrated over existing communication infrastructure, such as optical fibre links. Yet, QKD poses stringent requirements on the conditions of the network over which it is deployed. This work demonstrates the first quantum communication network in Cyprus via the deployment of a multi-node quantum network, exploiting existing commercial underground optical fibre. The network employs bidirectional occupation of fibres and wavelength multiplexing in a ring architecture to achieve, with minimal use of dark fibres, high-rate QKD. Results obtained reveal consistent key generation rates across all nodes, confirming reliable operation in a real-world environment. This deployment highlights the feasibility of leveraging existing telecom infrastructure for quantum-secured communication, marking a significant step toward scalable and cost-effective quantum networks suited for critical applications.

Keywords: quantum network, quantum key distribution, quantum communications

I. INTRODUCTION

With the radical growth of digital communication needs, the threat of cyberattacks on sensitive information has risen. Conventional encryption systems base their security on computational complexity and are therefore fundamentally vulnerable to attackers with computational power beyond the assumed limit, particularly quantum computers. Instead, quantum key distribution (QKD) leverages the principles of quantum mechanics to guarantee that eavesdropping attempts will be detected as noise in the measured quantum states [1]. This achieves information-theoretic security, a level of protection unattainable by classical cryptographic techniques.

Similar to classical communications, to enable secure communication at scale, QKD must be deployed over networked architectures, facilitating key exchange between multiple distant users. However, integrating QKD into existing infrastructure presents significant challenges. The quantum states required to perform QKD are generated by encoding information on properties of single photons, as opposed to conventional communications where bright light is used. Consequently, quantum channels connecting end-users must be low-loss and low noise and, in deployments, dark fibre is often used to meet these stringent requirements. This threatens the practical integration of the technology into current infrastructure and its scalability potential due to the limited availability of dark fibre within existing networks.

At the same time, a multi-user QKD network deployed over real-life infrastructure must adapt to the fibre architecture available. Existing fibre networks, designed for classical data transmission, are complex and layered. End-users are interconnected via distribution nodes with multiple communication links sharing common optical paths. These environments are a hurdle for the integration of QKD and may require trade-offs in functionality, performance and latency, or the use of tools with limited commercial readiness such as optical switching and wavelength multiplexing. Overcoming these barriers without compromising the security of QKD is crucial for the timely adoption of quantum communications. Significant progress has been made in the development of quantum communication networks, with various demonstrations over the past decade. Early experiments focused on point-to-point QKD links over dedicated optical fibres, proving the feasibility of secure key exchange over tens to hundreds of kilometres [2] in dark or live fibre [3]. More recent efforts have expanded toward multi-node networks [4], as well as long-distance deployments using trusted relays [5] and novel protocols [6]. Additionally, researchers have explored the feasibility of quantum networking over fibre channels under special conditions such as undersea fibre [7, 8], aerial fibre [9, 10] and even hollow-core fibre [11]. Despite these achievements, most demonstrations rely on simple fibre infrastructure limiting the research into real-life integration, scalability and resource-effectiveness.

Our work builds upon prior research by exploring the integration of QKD into existing dark fibre infrastructure, aiming to demonstrate a practical and resilient approach for real-world quantum-secured networks. Specifically, we present the deployment and performance analysis of a four-node QKD ring network implemented over

* Corresponding author: mariella.minder@cut.ac.cy

existing but restricted fibres in a metropolitan area. We utilise bidirectionality and wavelength multiplexing techniques to reduce fibre infrastructure requirements without affecting the resulting performance. The network encompasses all layers required for real-life quantum communication, including a key management service and an application layer. The network's feasibility and key generation performance are evaluated, demonstrating the potential for integrating QKD within real-world telecommunications networks.

II. NETWORK DETAILS

In this work, we present the first quantum communication network in Cyprus and the broader Southeast European region, marking a cybersecurity milestone. The network interconnects four governmental authorities in Nicosia over existing underground commercial fibre infrastructure. Originally designed for classical communication, the fibre network connects nodes via optical distribution frames (ODFs), which act as intermediate points between links, Fig. 1a. Two fibres were available per segment—fibre 1 for quantum signals and fibre 2 for classical traffic. By physically separating quantum and classical signals, noise is reduced, enhancing QKD performance.

A ring topology was implemented at the QKD layer, with each node serving as a trusted node enabling efficient any-to-any key distribution, Fig. 1b. Each fibre segment supports two QKD links in opposite directions, enabling bidirectional use without wavelength multiplexing. A four-port circulator at ODF 3 enforces anti-clockwise signal flow, while ODFs 1 and 2 remain passive. At the user end, Fig. 2a, each node includes a QKD transmitter (Alice), receiver (Bob), and a three-port circulator. The second fibre carries synchronisation, key management (KMS), and application-layer traffic. The application layer uses 10 G layer 1 encryptors in a two-way ring, the sync signal mirrors the quantum ring, and the KMS uses a full-mesh configuration. ODF 3 integrates DWDMs, an optoelectrical switch for mesh relaying, and a circulator for synchronisation handling, Fig. 2b. In total, seven ITU-T grid wavelengths are used, one per classical signal.

III. RESULTS

The QKD devices deployed in the network, QTI QuellX [12], implement the time-bin encoded, three-state BB84 QKD protocol [13] with weak coherent pulses at a source repetition rate of 600 MHz and a central wavelength of 1545.32 nm. We test the resulting performance of the links in terms of secret key rate (SKR) and quantum bit error rate (QBER) over a period of 5 days. The results are shown in Fig. 3. The Alice-Bob pairs achieve an average SKR over all links of 2.4 ± 0.2 kbps. While the SKR variation is significant, this agrees with the values observed in the pre-deployment in our lab, indicating this is an intrinsic characteristic of the devices and not an effect of the environment over which they are deployed. To assess the performance, we plot the average SKR and QBER vs channel loss per link alongside the corresponding theoretical lines by adapting the three-state analysis in [13, 14] to the systems' architecture. For the simulation, we assume 4% total detection efficiency, a 40 μ s average detector deadtime and a dark count probability, p_{dc}, of 8.5×10^{-7}, consistent with the experimental parameters of the systems. The deployment results align closely with theoretical predictions, confirming that the devices operate near their optimal performance given their intrinsic parameters. Even though the deployed fibres were part of cables carrying live traffic on adjacent fibres, no measurable leakage impacting the QBER was observed, confirming the suitability of integrating quantum communication systems into Cyprus's commercial fibre network.

IV. CONCLUSION

This work presents the first deployment of a QKD network in Cyprus and the broader Southeast European region, leveraging existing underground fibre infrastructure. The network interconnects four governmental authorities in a metropolitan setting using a ring architecture with trusted nodes, bidirectional transmission, and wavelength multiplexing to achieve high-performance QKD with minimal infrastructure requirements. By separating quantum and classical signals and carefully adapting to the constraints of a commercial fibre environment, the deployment demonstrates a scalable, resource-efficient, and operationally resilient solution for real-world quantum-secured communication.

Performance evaluation over several days confirms stable secret key generation across all links, with results matching theoretical expectations. The integration of a full quantum layer, key management service, and application-layer encryption illustrates the system's completeness and readiness for practical use. This demonstration underscores the viability of QKD in realistic telecom environments and marks a step toward broader adoption of quantum networks for securing sensitive information in critical infrastructure. Future work will focus on expanding network scale, exploring dynamic reconfiguration, and integrating quantum-safe technologies alongside QKD to support evolving cybersecurity demands.

ACKNOWLEDGMENTS

This work is co-funded by the European Commission and the Cyprus Deputy Ministry of Research, Innovation and Digital Policy under the Grant Agreement No.

101091655.

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science* **560**, pp. 7–11, 2014.

[2] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Secure quantum key distribution over 421 km of optical fiber," *Physical Review Letters* **121**, p. 190502, 11 2018.

[3] J. F. Dynes, W. W. Tam, A. Plews, B. Fröhlich, A. W. Sharpe, M. Lucamarini, Z. Yuan, C. Radig, A. Straw, T. Edwards, and A. J. Shields, "Ultra-high bandwidth quantum secured data transmission," *Scientific Reports 2016 6:1* **6**, pp. 1–6, 10 2016.

[4] T. Y. Chen, X. Jiang, S. B. Tang, L. Zhou, X. Yuan, H. Zhou, J. Wang, Y. Liu, L. K. Chen, W. Y. Liu, H. F. Zhang, K. Cui, H. Liang, X. G. Li, Y. Mao, L. J. Wang, S. B. Feng, Q. Chen, Q. Zhang, L. Li, N. L. Liu, C. Z. Peng, X. Ma, Y. Zhao, and J. W. Pan, "Implementation of a 46-node quantum metropolitan area network," *npj Quantum Information 2021 7:1* **7**, pp. 1–6, 9 2021.

[5] Y. A. Chen, Q. Zhang, T. Y. Chen, W. Q. Cai, S. K. Liao, J. Zhang, K. Chen, J. Yin, J. G. Ren, Z. Chen, S. L. Han, Q. Yu, K. Liang, F. Zhou, X. Yuan, M. S. Zhao, T. Y. Wang, X. Jiang, L. Zhang, W. Y. Liu, Y. Li, Q. Shen, Y. Cao, C. Y. Lu, R. Shu, J. Y. Wang, L. Li, N. L. Liu, F. Xu, X. B. Wang, C. Z. Peng, and J. W. Pan, "An integrated space-to-ground quantum communication network over 4,600 kilometres," *Nature 2020 589:7841* **589**, pp. 214–219, 1 2021.

[6] M. Pittaluga, Y. S. Lo, A. Brzosko, R. I. Woodward, D. Scalcon, M. S. Winnel, T. Roger, J. F. Dynes, K. A. Owen, S. Juárez, P. Rydlichowski, D. Vicinanza, G. Roberts, and A. J. Shields, "Long-distance coherent quantum communications in deployed telecom networks," *Nature* **640**, pp. 911–917, 2025.

[7] B. Amies-King, K. P. Schatz, H. Duan, A. Biswas, J. Bailey, A. Felvinti, J. Winward, M. Dixon, M. Minder, R. Kumar, S. Albosh, and M. Lucamarini, "Quantum communications feasibility tests over a uk-ireland 224 km undersea link," *Entropy 2023, Vol. 25, Page 1572* **25**, p. 1572, 11 2023.

[8] D. Ribezzo, F. S. Cataliotti, M. Zahidy, A. Petitjean, E. Conca, A. Zavatta, A. Xuereb, D. Bacco, G. Lemmi, C. D. Lazzari, T. Occhipinti, L. K. Oxenløwe, A. Tosi, and I. Vagniluca, "Qkd protocol over 100 km long submarine optical fiber assisted by a system-in-package fast-gated ingaas single photon detector," *Optical Fiber Communication Conference (OFC) 2023 (2023), paper M2I.4* , p. M2I.4, 3 2023.

[9] A. R. Dixon, J. F. Dynes, M. Lucamarini, B. Fröhlich, A. W. Sharpe, A. Plews, S. Tam, Z. L. Yuan, Y. Tanizawa, H. Sato, S. Kawamura, M. Fujiwara, M. Sa-saki, A. J. Shields, L. Yuan, Q. Zhang, H. Takesue, T. Honjo, K. Wen, T. Hirohata, M. Suyama, Y. Takiguchi, H. Kamada, Y. Tokura, O. Tadanaga, Y. Nishida, M. Asobe, Y. Yamamoto, S. Wang, W. Chen, J. f Guo, Z. q Yin, H. w Li, Z. Zhou, G. c Guo, Z. f Han, K. Patel, J. Dynes, I. Choi, A. Sharpe, Z. Yuan, R. Penty, A. Shields, J. Mora, W. Amaya, A. Ruiz-Alba, A. Martinez, D. Calvo, V. G. Muñoz, and J. Capmany, "High speed prototype quantum key distribution system and long term field trial," *Optics Express, Vol. 23, Issue 6, pp. 7583-7592* **23**, pp. 7583–7592, 3 2015.

[10] Y.-L. Tang, Y.-L. Tang, Y.-L. Tang, Z.-L. Xie, Z.-L. Xie, Z.-L. Xie, C. Zhou, D. Zhang, M.-L. Xu, J. Sun, D. Sun, Y.-X. Xu, L.-W. Wang, Y. Ma, Y.-K. Zhao, M.-S. Jiang, Y. Wang, J. Li, K. Xue, K. Xue, N. Yu, M.-S. Zhao, M.-S. Zhao, M.-S. Zhao, D.-D. Li, D.-D. Li, D.-D. Li, D.-D. Li, W.-S. Bao, W.-S. Bao, S.-B. Tang, S.-B. Tang, S.-B. Tang, and S.-B. Tang, "Field test of quantum key distribution over aerial fiber based on simple and stable modulation," *Optics Express, Vol. 31, Issue 16, pp. 26301-26313* **31**, pp. 26301–26313, 7 2023.

[11] M. Minder, S. Albosh, O. Alia, R. Slavík, R. Kumar, F. Poletti, G. T. Kanellos, and M. Lucamarini, "Phase noise characterisation of a 2-km hollow-core nested antiresonant nodeless fibre for twin-field quantum key distribution," *Quantum Technology: Driving Commercialisation of an Enabling Science III* , p. 29, 1 2023.

[12] S. Francesconi, C. D. Lazzari, D. Ribezzo, I. Vagniluca, N. Biagi, T. Occhipinti, A. Zavatta, and D. Bacco, "Scalable implementation of temporal and phase encoding qkd with phase-randomized states," *Advanced Quantum Technologies* **7**, p. 2300224, 2 2024.

[13] D. Rusca, A. Boaron, M. Curty, A. Martin, and H. Zbinden, "Security proof for a simplified bennett-brassard 1984 quantum-key-distribution protocol," *Physical Review A* **98**, p. 52336, 11 2018.

[14] D. Rusca, A. Boaron, F. Grünenfelder, A. Martin, and H. Zbinden, "Finite-key analysis for the 1-decoy state qkd protocol," *Applied Physics Letters* **112**, p. 171104, 4 2018.

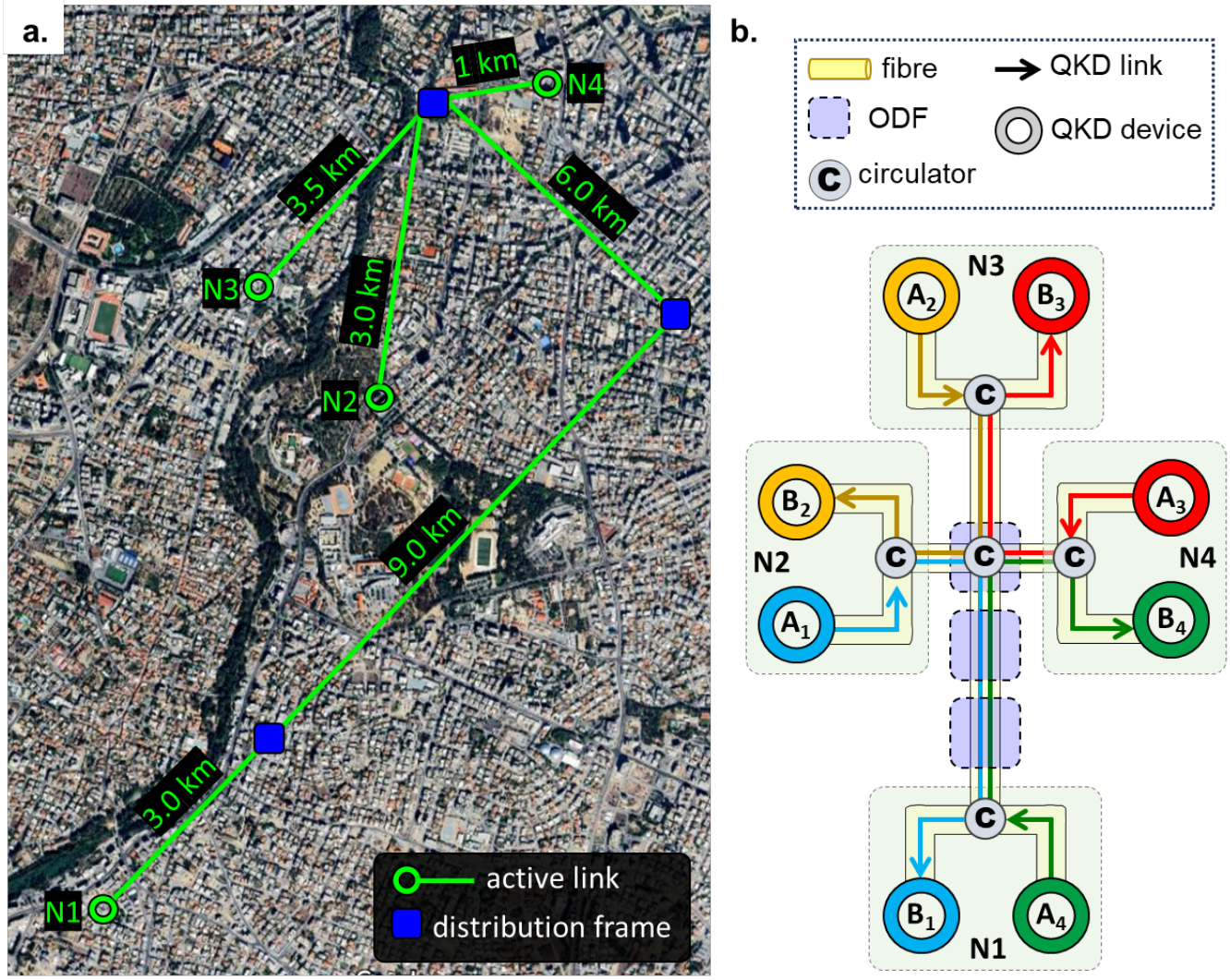

FIG. 1. **a.** Map of the four-node (N1-N4) quantum network in Nicosia. The available fibre infrastructure interconnects the nodes via optical distribution frames (ODFs). Each link segment (green line) consists of two dark fibres which vary in length. **b.** Architecture of the quantum channels. A single fibre per segment carries all quantum signals. Circulators at the nodes direct the light from the transmitters, A_N, to the channel and then to the receivers, B_N. A circulator at an ODF directs the signals from N4-N1.

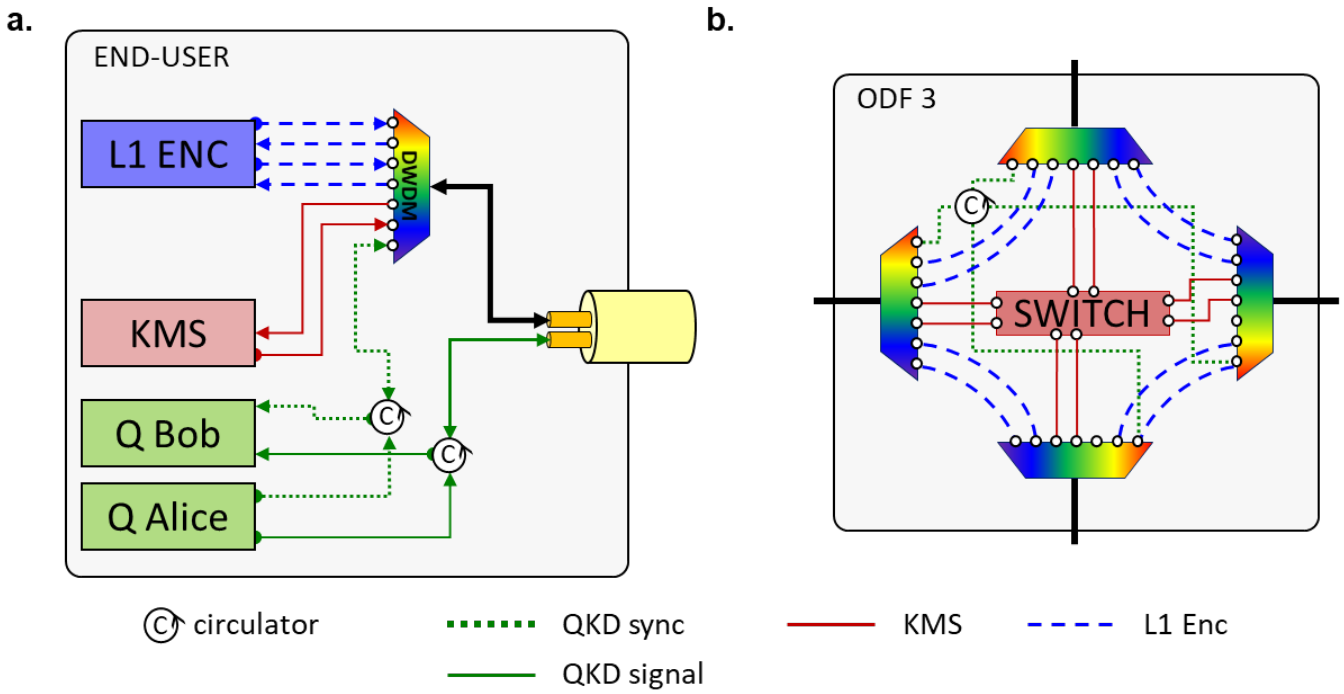

FIG. 2. **a.** End-user setup: Each node includes two QKD devices, a KMS unit, and a layer 1 encryptor (L1 ENC). Classical signals are multiplexed via DWDM and sent over one fibre; quantum signals use a separate fibre. **b.** ODF 3 design: Encryption and clock signals follow a ring topology using DWDMs and a circulator, while the KMS layer maintains mesh connectivity.

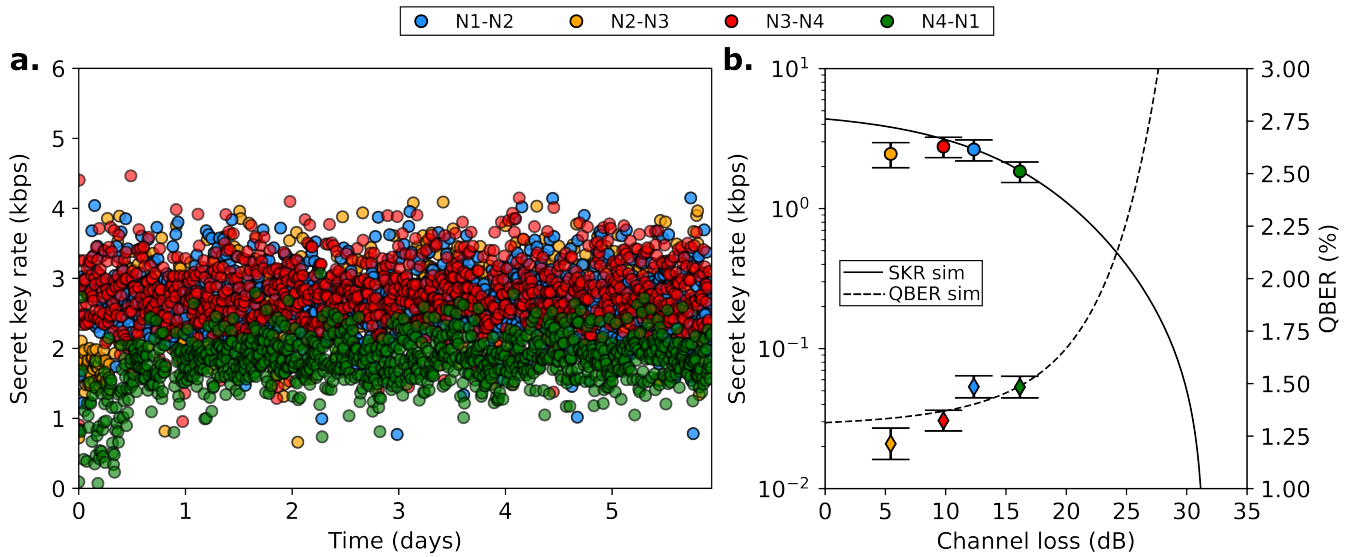

FIG. 3. **a.** Secret key rates acquired over all links for the duration of 5 days. **b.** Average secret key rate (circles) and QBER (diamonds) per link compared with the theoretically expected lines (SKR sim, QBER sim).