

Field Demonstration of a Fully Managed, L1 Encrypted 3-Node Network with Hybrid Relayed-QKD and Centralized Symmetric Classical Key Management

Nikolas Makris⁽¹⁾, Konstantinos Tsimvraakis⁽¹⁾, Alkinoos Papageorgopoulos⁽¹⁾, Persefoni Konteli⁽¹⁾, Yannick Gautier⁽²⁾, Marco Terenziani⁽²⁾, Eric Daudin⁽²⁾, Dimosthenis Ntoulas⁽²⁾, Thanasis Fragkioudakis⁽²⁾, Ian Meletios⁽²⁾, Michele Mosca⁽³⁾, Dale Hobbs⁽³⁾, Tony Rosati⁽³⁾, Ilias Papastamatiou⁽⁴⁾, Ognjen Prnjat⁽⁴⁾, Kostas Koumantaros⁽⁴⁾, Dimitris Mitropoulos^(1, 4), Jean-Robert Morax⁽⁵⁾, Bruno Huttner⁽⁵⁾, Kostas Christodouloupoulos⁽¹⁾, George T. Kanellos⁽¹⁾, Dimitris Syvridis⁽¹⁾

⁽¹⁾ National and Kapodistrian University of Athens, Athens, Greece, gtkanellos@di.uoa.gr

⁽²⁾ Nokia, Espoo, Finland

⁽³⁾ EvolutionQ Inc., Waterloo, Canada

⁽⁴⁾ GRNET S.A. – National Infrastructures for Research and Technology, Athens, Greece

⁽⁵⁾ ID QUANTIQUE S.A., Geneva, Switzerland

Abstract We successfully demonstrated a fully-managed, field-deployed, three-node QKD ring network with L1-OTNsec encryption. The network employs a hybrid scheme of QKD and classical yet quantum-safe centrally-generated symmetric keys to support point-to-point and relay consumers.

©2024 The Authors

Introduction

Quantum networks leverage quantum key distribution (QKD) to ensure communication security. To efficiently integrate QKD networks into existing infrastructure and be operational, the European and International QKD standards [1]-[4] have proposed a layered framework, comprising of the quantum layer, the key management (KMS) layer and the application layer. This architecture is essential to enable encrypted communication across various applications and users. The first major quantum network was implemented by DARPA that followed a three-layer architecture adopting a hybrid switched/relayed implementation [5]. Later developments including the SECOQC [6] network that focused on relayed-QKD (trusted repeater prototype) setups, the Tokyo project [7] and the Cambridge quantum network [8]. Recently, China presented a 46-node quantum metropolitan area network [9] connecting 40 user nodes including three trusted relays and three optical switches. However, without

centralized orchestration, the management of the network remains suboptimal and inefficient. Software – Defined QKD (SDQKD) offers a potential solution to address this issue and improve the efficiency and flexibility of a network. The Madrid SDQKD was the first successful full-scale integration of QKD technology in an SDN environment serving encrypted communication between 3 relayed nodes [10]. The Subcarrier Wave [11] was utilized to enable communication in a 3 node SDN enabled network configuration. Finally, a recent development involved a new framework for Software Defined Network for QKD as a service (SDQaaS) [12].

In this work we present, to the best of our knowledge, the first fully managed, operational three-node quantum cryptography network serving OTN circuits with (Layer 1 - OTNsec) encryption. Fig. 1a illustrates the architecture of our network. Each node implements a fully integrated vertical stack featuring a managed quantum layer, a KMS layer and, an application layer that

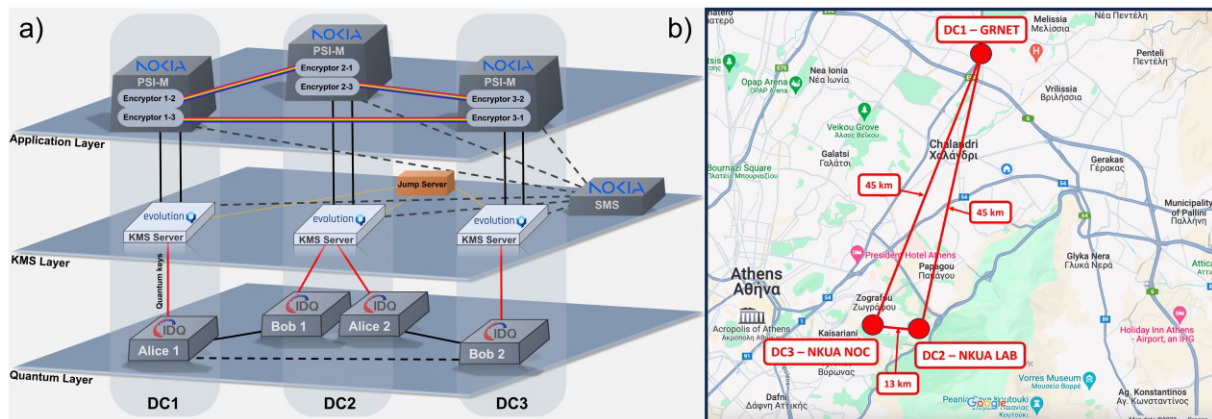


Fig. 1: a) Illustration of the layered architecture depicting the quantum layer, the KMS layer, the application layer and their interconnections. b) DC1, DC2 and DC3 marked by their approximated physical location on the Athens city map.

are all jointly orchestrated. In particular, the quantum layer features two IDQuantique Cerberis XGR QKD pairs used to establish 2 point-to-point QKD links that are then enhanced by the KMS layer (using a relay) to support all-to-all communication and in particular serve 3 bidirectional OTN circuits. In this way our system minimizes the QKD resources as the QKD pair for the third link is omitted. The quantum layer complies to the ETSI GS QKD 014 for secure quantum key extraction and delivery to the KMS layer [1]. On the KMS layer, we deployed an EvolutionQ BasejumpQDN key management software and the Network Controller for the QKDN that acts as per ETSI GS QKD 015 [2], and pulls the generated quantum keys, stores them in dedicated buffers and synchronizes and schedules the key delivery to the Secure Application Entities (SAEs). Note that the network encrypts OTN circuits between all the 3 nodes pairs while employing only 2 QKD pairs, allowing the key consumption in the intermediate relay node while enabling the application of priorities or QoS attributes to the key consumption. Such an addition is most valuable, but the key management process requires additional scheduling, buffering and key monitoring. The KMS layer is controlled and managed by the Nokia 1830 Security Management Server (SMS) fitted to control the EvolutionQ key management software. The SMS functions as a security network orchestrator, similar to the ETSI GS QKD 18 [3]. Specifically, it orchestrates the keys across the nodes of the network but also coordinates the key requirements with the classical OTN layer. Additionally, in a novel feature not demonstrated before in quantum encrypted networks, the SMS offers seamless transition to a classical (yet quantum-safe) encryption in the event of a DoS (Denial of Service) attack on the QKD layer or a QKD failure in key generation/distribution. To do so, it implements a scheme of centralized symmetric classical keys generation and distribution using encryption based on AES256. On the application layer, each node hosts a Nokia layer 1/OTN Photonic Service Interconnection - Modular (PSI-M) encryptor (300Gbps) for encrypting data with the requested quantum keys at key rotation rates as small as 1key/min.

Experimental Setup

The experimental testbed, shown in Fig. 1b, comprises 3 trusted nodes: DC1 (GRNET DC node), DC2 (NKUA Optical Communications and Photonic Technologies Lab) and DC3 (NKUA Networks Operation Centre-NOC). DC1 hosted the QKD Alice1 (A1), DC2 was the relay node and hosted QKD Bob1 (B1) and Alice2 (A2), and DC3 hosted QKD Bob2 (B2). The fiber link between DC1 and DC2 was ~45km, while DC2 and DC3 were in separate sites in the NKUA campus and connected through a fiber spool of ~13km to emulate a longer distance. The physical optical connectivity for the QKD pairs and the PSI-M encryptors are demonstrated in Fig. 2. DC2 and DC3 (NKUA nodes) were connected to DC1 (GRNET) through two unidirectional dark fibers. The 1550nm quantum channel occupied solely one of the two dark fibers to avoid in-band noise that would degrade the QKD performance, deemed essential as the A1-B1 link encountered losses of 18dB, approaching the operational limit for the IDQuantique Cerberis XGR QKD pair. The PSI-M OTN data channels (C36, C34) and the QKD service channel (C30) were multiplexed together, and circulators were employed to operate the second fiber in both directions. The additional losses were 2.8dB in total. The OTN data channel between the PSI-M 2 and PSI-M 3 (C38 channel) were established via an intra-campus link also used for the communication between Alice 2 and Bob 2. Every PSI-M line had a configuration that supported a data rate of 300Gbps via 67GBaud and 16SQAM with SDFEC-G2 for flex OTU in OTSiG. Regarding the management network, each node had a local and private ethernet connection between the QKD and KMS server to deliver the secure generated quantum keys from the quantum layer to the KMS layer. Moreover, a VLAN in the GRNET-NKUA domain was established to facilitate management, orchestration, and communication among the components within the deployed multi-layer architecture.

Results and Discussion

The system was tested under different key rotation intervals (1, 5, 15, 30, 60 min) for extended periods. Tab. 1 includes the percentages for the various key rotation options. We observed 98%

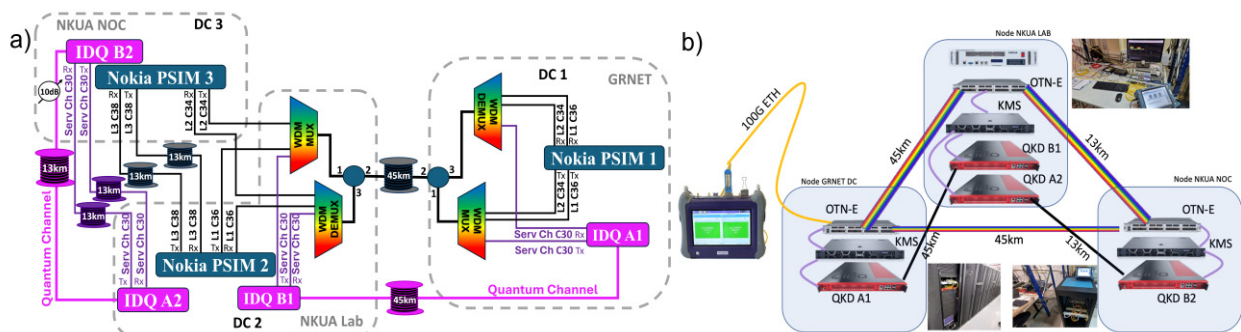


Fig. 2: a) Optical connections of the three-node relayed quantum network. b) Schematic demonstration of the layered setup.

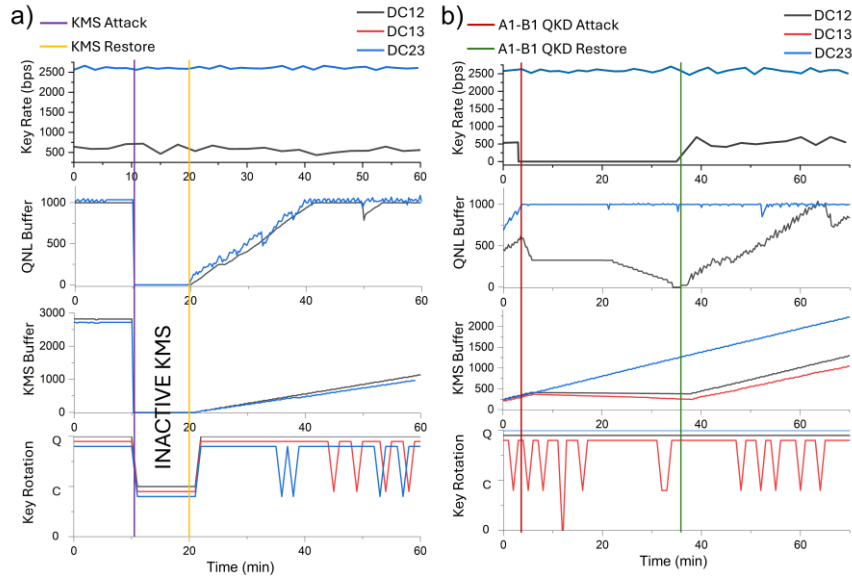


Fig. 3: Joint diagrams for the SKR, QNL buffers, KMS buffers and SMS key rotation for all links at the emulated KMS (a) and QKD (b) attacks. The key rotation is characterized as 'Q' for quantum key rotation, 'C' for the SMS' classical key rotation and, '0' for no key rotation.

successful key rotation using QKD or classical key distribution in the stress condition of 1key/min. For the remaining 2%, the encryption was continued using the previous key and a new rotation request was issued after 30sec. Thus, the data were always encrypted, and the reported failures indicate only issues in the key rotation at specific key rotation junctures. Furthermore, a 100Gb/s Exfo Network Analyzer was constantly monitoring the overall network performance, recording average jitter and latency values of <0.015ms and 2.06ms respectively. Network robustness was tested by emulating two separate attacks: i) a KMS attack causing a temporary disruption in the communication between the application and KMS layers and ii) a QKD attack that would nullify SKR. The KMS attack is emulated by shutting down the KMS server in all nodes, whereas the QKD attack is emulated by plugging off the quantum channel fiber. For both tests the key rotation interval was set to 1 minute, the QNL

launching an attack in each KMS server, the KMS layer cannot provide the encryptors with quantum keys. In that case, the SMS generates and supplies the PSI-Ms with classical quantum-safe keys. Once the key management servers become available again, the QNL (KMS input) buffers start to fill up again. After a brief interval, they begin supplying the KMS (output) buffers with keys which are then used for quantum key rotation. Then, in Fig. 3b, a QKD attack is demonstrated in link DC12. During the attack, the network uses the buffered keys, resulting in a linear reduction in the key count, along with some overhead. Then, depending on the attack duration, the system may run out of keys or avoid exhaustion. In our experiment, the attack duration was brief enough to maintain uninterrupted quantum key transmission. Following the restoration of the QKD link, the QNL buffers began to replenish, extending the buffering process within the KMS.

Conclusions

We report on the successful demonstration of a fully managed field deployed three-node QKD relayed network in a ring configuration, where each node comprises a fully integrated vertical stack. We demonstrated the network's stable operation providing Layer 1 (OTNsec) data encryption with quantum keys. In case of an attack or unavailability of quantum keys, we demonstrated the network's capability to seamlessly transition to classical encryption with symmetric quantum-safe keys provided by the central security manager / SMS, exhibiting, thus, a reliable hybrid network operation and ensuring the continuous supply of keys. Notably, the keys were consumed in all three nodes, including the intermediate relayed node, and we demonstrated that the operations, including relaying, recover against various attacks.

Tab. 1: Network's key rotation percentages for different key rotation intervals.

Rotation Interval (min)	Classical Key Rotation (%)	Quantum Key Rotation (%)	SNMP error (%)
1	8.8	89.2	2.0
5	10	90	0.0
15	14.8	83.6	1.6
30	33	66.4	0.6
60	7.8	90.7	1.5

buffer (EvolutionQ KMS input buffer where keys are stored after retrieved from the quantum layer) capacity was 1000 keys, and the key expiration time was set to 4 hours. As presented in Fig. 3a, by emulating a KMS attack on the network, we demonstrate the network's hybrid operation. By

Acknowledgements

This work was funded by the EU quantum flagship project QSNP (GA 101114043) and the HeliasQCI project (GA 101091504).

References

- [1] ETSI GS QKD 014 - Quantum Key Distribution (QKD); Protocol and Data Format of REST-based Key Delivery API (2019). https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_qkd014_v010101p.pdf
- [2] ETSI GS QKD 015 - Quantum Key Distribution (QKD); Control Interface for Software Defined Network, (2022). https://www.etsi.org/deliver/etsi_gs/QKD/001_099/015/02.01.01_60/gs_QKD015v020101p.pdf
- [3] ETSI GS QKD 018 - Quantum Key Distribution (QKD); Orchestration Interface for Software Defined Networks, (2022). https://www.etsi.org/deliver/etsi_gs/QKD/001_099/018/01.01.01_60/gs_qkd018_v010101p.pdf
- [4] Recommendation ITU-T Y.3803, Quantum key distribution – Key management (2020). <https://www.itu.int/rec/T-REC-Y.3803-202012-l/en>
- [5] C. Elliott, A. Colvin, D. L. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the DARPA quantum network (Invited Paper)," *Proceeding of SPIE, San Diego, California, USA*, DOI: <https://doi.org/10.1117/12.606489>.
- [6] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Broui, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden and A. Zeilinger, "The secoqc quantum key distribution network in vienna," *New Journal of Physics*, vol. 11, no. 7, p. 075001, 2009.
- [7] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger "Field test of quantum key distribution in the Tokyo QKD network," *Optics express*, vol. 19, no. 11, pp. 10 387–10 409, 2011.
- [8] J. F. Dynes, A. Wonfor, W. W. -S. Tam, A. W. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. L. Yuan, A. R. Dixon, J. Cho, Y. Tanizawa, J. -P. Elbers, H. Greißer, I. H. White, R. V. Penty, A. J. Shields "Cambridge quantum network". *Npj Quantum Information*, vol. 5, Issue 1, DOI: 10.1038/s41534-019-0221-4
- [9] T. -Y. Chen, X. Jiang, S. -B. Tang, L. Zhou, X. Yuan, H. Zhou, J. Wang, Y. Liu, L.-Kan 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, J. -W. Pan "Implementation of a 46-node quantum metropolitan area network". *Npj Quantum Information*, vol. 7 Issue 1, DOI: <https://doi.org/10.1038/s41534-021-00474-3>
- [10] Diego Lopez "Demonstration of Software Defined Network Services Utilizing Quantum Key Distribution Fully Integrated with Standard Telecommunication Network" *Quantum Reports*, vol. 2, DOI: 10.3390/quantum2030032.
- [11] V.I. Egorov, V.V. Chistyakov, O.L. Sadov, A.B. Vasiliev, P.V. Fedchenkov, V.A. Grudin, O.I. Lazo, A.E. Shevel, N.V. Buldakov, S.M. Kynev, A.V. Gleim, S.E. Khoruzhnikov, S.A. Kozlov "Software-defined subcarrier wave quantum networking operated by OpenFlow protocol", presented at QCrypt, Cambridge, UK, 2017 DOI: <https://doi.org/10.48550/arXiv.1709.09081>
- [12] Y. Cao, Y. Zhao, J. Wang, X. Yu, Z. Ma, and J. Zhang, "SDQaaS: software defined networking for quantum key distribution as a service", *Optics Express*, vol. 27, pp. 6892-6909 DOI: 10.1364/OE.27.006892