# The National Quantum-Safe Network in Singapore

Hao Qin<sup>\*(1)</sup>, Jing Yan Haw<sup>\*(1)</sup>, Xiao Duan<sup>(3)</sup>, Yu Cai<sup>(5)</sup>, Ramana Murthy<sup>(1)</sup>, Nelly Ng<sup>(5)</sup>, Biplab Sikdar<sup>(4)</sup>, Christian Kurtsiefer<sup>(1,2)</sup>, Michael Kasper<sup>(3)</sup>, Alexander Ling<sup>(1,2)</sup>

<sup>(1)</sup> Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, 117543, Singapore <u>hao.qin@nus.edu.sq</u>, <u>iy.haw@nus.edu.sq</u>

<sup>(2)</sup> Department of Physics, National University of Singapore, 2 Science Drive 3, 117551, Singapore
<sup>(3)</sup> Fraunhofer Singapore Research Centre@NTU, Nanyang Technological University, 50 Nanyang Avenue, 639798, Singapore

<sup>(4)</sup> Department of Electrical and Computer Engineering, National University of Singapore, 119077, Singapore

<sup>(5)</sup> School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, 637371, Singapore

\* These authors contributed equally

**Abstract** We introduce the National Quantum-Safe Network, which is a nationwide collaborative fielddeployed testbed aimed at demonstrating quantum-safe cryptography solutions. With several key aspects including testbed, security evaluation, standardisation, and ecosystem building, the network aims to achieve a vendor-neutral, multi-protocol platform that complies with international standards. ©2023 The Author(s)

# Introduction

As the quantum technology landscape evolves, it is difficult to predict when powerful quantum capable of breaking computers current cryptography will be available. Thus, applications and communication infrastructure handling highvalue assets or requiring long-term protection needs to be equipped with quantum-safe security enhancements as soon as possible. Quantum Key Distribution (QKD), a tamper-evident secure communication technique based on quantum physics, whose security is independent of computation power, could potentially fulfil such requirement. In recent years, various QKD networks have been deployed worldwide [1-3]. The National Quantum-Safe Network (NQSN) in Singapore is a nationwide collaborative platform and a field-deployed testbed aimed at quantum-safe cryptography demonstrating solutions. The NQSN testbed, which links up academic, public and private members, targets trials for QKD network, augmented with the Post-Quantum Cryptography (PQC) technologies. PQC refers to mathematics-based cryptographic algorithms (software) which are believed to be secure against known attacks from quantum computers.

As shown in Figure 1, NQSN is a star type QKD network with the central node connected to the remote nodes across the island from east to west, and consists of four logical layers [4]: quantum layer, key management (KM) layer, network management layer and application layer (Figure 2). Beyond the terrestrial metropolitan area network setting, a satellite-based QKD is



Fig. 1: NQSN star-type QKD network.

planned to be launched to serve as a moving node in the future phase. NQSN can be further linked up with other global QKD networks via the satellite node.

# Quantum Layer

In the quantum layer, commercial ready and production grade QKD devices will be deployed to connect the central node with each remote nodes, via the existing production grade fibre protocols infrastructure. Different QKD implementations from various QKD vendors will be considered with regard to the distances and losses featured by each point-to-point fibre link. The candidate protocols include BB84, coherent one way (COW), continuous-variable (CV) and entanglement-based (EB) QKD protocols. Under such operation, each pair of the QKD devices continuously outputs QKD keys to the KM layer, which are established over the quantum channel (fibre) and the classical channel (fibre or



Fig. 2: Different layers of NQSN. From Bottom to Top: Quantum Layer, Key Management Layer, Network Management Layer, Application Layer

Ethernet). In this layer, it aims to achieve one of the main goals of the NQSN testbed - to serve as a vendor-neutral platform that demonstrates multi-QKD protocols, supporting different quantum channel conditions.

# **Key Management Layer**

In the KM layer, a high performance, customized, centralized key manager system will be installed in the central node and enable interoperability, connectivity, scalability of the QKD network. Remote key managers will also be paired with QKD devices in the remote nodes, connecting with the central node via KM links. With the star type configuration, the centralized key manager features a multi-input and multi-output interfaces. The input interface is to receive QKD keys provided by different QKD devices in the quantum layer [5]. The output interface is to supply keys to applications upon request by the application layer and network management layer (e.g. ETSI GS QKD 014 [6]). These key managers also process and store the received QKD keys into the formats that are required by specific applications. The key relaying and routing functions in the central key manager further enables symmetric key establishments between any of the two nodes in the network via KM links. Integration of PQC solutions such as hybrid key combination of QKD key and PQC exchanged key is among the considered architecture in the KM layer.

# **Network Management Layer**

The network management layer is responsible for controlling and managing network resources across different nodes of the NQSN testbed network. A centralized network management server is in charge of the controlling and managing functions, which will be installed in the central node and hold a global view of the entire QKD network operation. The server gives controlling instructions to the quantum layer and KM layer to create the key delivery path across network nodes and to configure components such as switches, servers and QKD devices. The managing functions consist of monitoring and collecting performance parameters, detecting and reporting any fault events, collecting event logs for networking analysis from the quantum layer and the KM layer.

# Application Layer

The application layer in the NQSN QKD network acts as an open platform that allows for the integration & deployment of different applications at various layers of the Open Systems Interconnection (OSI) model. Some examples include physical encryption in the physical layer, link encryptor in the data link layer and IPSec in the network layer. These applications consume keys provided by the KM layer, via supported interfaces such as ETSI GS QKD 014 [6]. Different reference use cases & trials are explored for field trials, interoperability, and performance quantum-safe evaluation of technologies.

# **Quantum Security Lab**

Along with the NQSN testbed, a testing lab dedicated to testing, evaluation and certification of QKD devices and their supporting units is established. The main objective of the lab is to verify the functionality and the security of the QKD network, and formalize certification framework towards industry applications of QKD technologies. Main activities include (i) research on quantum hacking and countermeasures, (ii) development of functional, performance and security evaluation methodologies, (iii) testing tools developments and building up certification capabilities with industry & academic labs. Lab facilities are also co-located within some of the nodes, which open possibilities for novel remote



Fig. 3: (Left) A quantum secured data transfer utilizing pairs of symmetric keys generated from QKD devices. (Right) The secret key rate over the trial period.

testing and evaluation methods on the quantum layer and other layers under a network configuration.

# Standardisation

A quantum communication networks task force under local regulatory authority is also formed, with members from governmental agencies and industry partners. The main objective of the task force is to develop local standards to facilitate the deployment, operation, and adoption of the QKD technologies in different domains. The standardisation developments will also support certifications of QKD devices and other entities in the QKD network.

# **Reference Use Cases**

One example reference use case is а demonstration of direct data centre interconnect (DCI) secured by QKD-keys, as shown in Fig. 3. In this demonstration, which was performed over two physically separated commercial data centres of ST Telemedia Global Data Centres (STT-GDC), we confirmed the feasibility of operating QKD systems (ID Quantique Cerberis XGR) over a production-grade fibre network (Netlink Trust). During the field test of the QKD devices, the secret key rate and the quantum bit error rate (QBER) are relatively stable and continuous over a fibre link of around 20 km. As shown in Figure 3, an average secret key rate of 2.39 kbps and QBER of 1.90% is achieved. A total of more than 2 Gbits of AES-256 keys are accumulated, with the rates of around 690 keys per minutes. A subset of the keys is used by a software-based Quantum Virtual Private Network (Q-VPN), which consumed the QKD symmetric keys to establish a VPN tunnel using QKD keys for quantum-secured file transfer.

# Conclusions

The Singapore's NQSN focuses on developing a network that addresses several scopes, including multiple vendors, standards compliance and

requirements, various infrastructure and implementations of QKD protocols. In particular, NQSN seeks to significantly improve the quantum-safe technologies by enhancing testing and assessment capabilities, promoting the broader availability of quantum-safe technology, and increasing awareness about it. End-users and stakeholders can take advantage of integrating quantum-safe security applications and solutions, catalysing future innovations and quantum-related products and services on a regional and global level.

### Acknowledgements

We acknowledge funding support from the National Quantum-Safe Network project (NRF2021-QEP2-04-P01) and start-up grant for Nanyang Assistant Professorship of Nanyang Singapore. Technological University, We acknowledge NQSN partners (www.nqsn.sg) for their support. For the reference use cases, we acknowledge ST Telemedia Global Data Centre for providing secured physical locations to host the QKD trial, Netlink Trust for the provisioning of the fibre network and ID Quantique SA for the loan of the QKD system. We thank KaiWei Qiu for his contribution to the reference use case, and Isaac Ng for his contribution to the testbed characterisation.

#### References

- [1] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, H. Yeh, "Current status of the DARPA quantum network," in Quantum Information and computation III, vol. 5815, *International Society for Optics and Photonics*, 2005, pp. 138–149. DOI:10.1117/12.606489.
- [2] 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-Brouri, 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. DOI 10.1088/1367-2630/11/7/075001

- [3] 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, et al., "Field test of quantum key distribution in the Tokyo QKD network," *Optics Express*, vol. 19, no. 11, pp. 10 387–10 409, 2011. DOI <u>10.1364/OE.19.010387</u>.
- [4] ITU-T Recommendation Y.3800 (2019), plus Corrigendum 1 (2020), Overview on networks supporting quantum key distribution, 2020.
- [5] ITU-T Recommendation Y.3803, Quantum key distribution networks Key management.

[6] ETSI GS QKD 014, Quantum key distribution; Protocol and data format of key delivery API to Applications, 2019.

# **Additional Information**

# I) <u>Submission Specification for Conference Papers</u>

This 'Submission Specification for Conference Papers' document provides instructions for the submission of Conference Papers for publication on the IET Digital Platform.

This document is to be used in conjunction with the 'Manuscript-template.docx'. The Conference Paper is to be prepared in MS Word format and then printed to PDF.

# 1. Submission requirements

Conference papers must satisfy the following requirements:

# 1.1 Manuscript Submission

**1.1.1 Originality**: Is the work scientifically rigorous, accurate and novel? Does the work contain significant additional material to that already published? Has its value been demonstrated?

**1.1.2 Plagiarism**: All conference papers submitted to the IET for publication must record original work which has not been published previously. Any alleged cases of plagiarism will be dealt with according to the '<u>IET Policy in Relation to Plagiarism</u>, <u>Infringement of Copyright and Infringement of Moral Rights and Submission to Multiple Publications</u>'.

**1.1.3 Multiple submissions:** The IET does not permit manuscripts included in its conference proceedings to be simultaneously under review for another conference or publication. Once a case of multiple submissions has been established, the paper/s in question will be immediately declined for publication by the IET.

1.1.4 Relevance: Is the material appropriate to the scope of the conference to which it is submitted?

**1.1.5 Clarity:** Is the English clear and well written? Poorly written English may obscure the scientific merit of your paper. Are the ideas expressed clearly and concisely? Are the concepts understandable?

# 2. Post-print Policy

2.1.1 The author may post post-prints of their conference papers published by the IET on repositories, servers and websites of any sort, provided that these servers are operated by the author's institution or the funding body contributing to the research. To comply with funding requirements, authors may also deposit their conference papers in repositories (or mirror sites) designated by the funding body.

The conditions attached to this are as follows:

2.1.2 Access to such servers is not for commercial use and does not depend on payment of access, subscription, or membership fees.

2.1.3 The following wording clearly appears on the front page of the post-print:

"This paper is a post-print of a paper submitted to and accepted for publication in Conference Proceedings of *conference title* and is subject to Institution of Engineering and Technology Copyright. The copy of record is available at IET Digital Library"

2.1.4 The post-print must be the author's version and not the IET version/PDF.

2.1.5 The post-print must not be posted prior to publication of the paper by the IET and when posted any preprint version should be removed.

# 3.1 Copyright

3.1.1It is expected that copyright in the content will be assigned to the IET.

3.1.2 The author submitting the paper should ensure that: i) they own all rights in respect of the content (including content produced from contributing authors) to enable the assignment of copyright to the IET; ii) they have authority to enter into the assignment agreement; iii) the content does not infringe third party copyright; and iv) the content does not contain anything which is (or may be considered) defamatory.

3.1.2. Please contact us (by emailing ecoc@theiet.org) if:

i) the author has prepared the content in the course of their employment, as the assignment agreement will need to executed by the author's employer. (A different form of agreement will be required for this purpose).

ii) the content is subject to "United Kingdom Crown copyright" or is "a work of the US Government and in the Public Domain", as alternative arrangements will need to be made.

iii) there is another reason why you cannot agree to the terms of the assignment agreement (for example, you don't own those rights in the content prepared by co-authors)

# 4.1 Permissions to Reproduce

4.1.1 All authors must secure permission from the copyright holder for reproducing previously published text, figures and tables. The source of the reproduced material must be given in full and the words 'Reproduced by permission of .....' included with the illustration.

# II) PDF format requirement

All PDFs shall be set as follows:

Version: Adobe PDF Version 1.5-1.8 (Acrobat 5-8)

Fonts: All fonts must be 'embedded subset'.

# **Document Properties:**

**Title:** Full title of the paper.

Authors: All contributing author names to be included.

Subject: Full conference name and abbreviation.

**Keywords:** Keywords as set in the paper at Item 2, Keywords.

# III) IET Digital Library and Inspec Indexing requirements

Papers that will be submitted for publication on the IET Digital Library, and subsequent indexing in Inspec, IEEE Xplore and EI Compendex, must be submitted in the following format:

All PDFs must be in the format as specified as stated in Paragraph 2 above (PDF format requirement).