

Original Article

Open Access



Quantum-Secured Data Centre Interconnect in a field environment

Kaiwei Qiu¹, Jing Yan Haw², Hao Qin², Nelly H. Y. Ng¹, Michael Kasper^{2,3}, Alexander Ling^{2,4}

¹School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, Singapore 637371, Singapore.

²Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543, Singapore.

³Department of Electrical and Computer Engineering, National University of Singapore, Singapore 117583, Singapore.

⁴Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore 117551, Singapore.

Correspondence to: Dr. Jing Yan Haw, Dr. Hao Qin, Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543, Singapore. E-mail: jy.haw@nus.edu.sg; hao.qin@nus.edu.sg

How to cite this article: Qiu K, Haw JY, Qin H, Ng NHY, Kasper M, Ling A. Quantum-Secured Data Centre Interconnect in a field environment. *J Surveill Secur Saf* 2024;5:184-97. <http://dx.doi.org/10.20517/jsss.2024.02>

Received: 20 Jan 2024 **First Decision:** 15 Apr 2024 **Revised:** 8 Aug 2024 **Accepted:** 3 Sep 2024 **Published:** 29 Sep 2024

Academic Editor: Josef Pieprzyk **Copy Editor:** Dong-Li Li **Production Editor:** Dong-Li Li

Abstract

In the evolving landscape of quantum technology, the increasing prominence of quantum computing poses a significant threat to the security of conventional public key infrastructure. Quantum key distribution (QKD), an established quantum technology at a high readiness level, emerges as a viable solution with commercial adoption potential. QKD facilitates the establishment of secure symmetric random bit strings between two geographically separated, trustworthy entities, safeguarding communications from potential eavesdropping. In particular, data centre interconnects can leverage the potential of QKD devices to ensure the secure transmission of critical and sensitive information in preserving the confidentiality, security, and integrity of their stored data. In this article, we present the successful implementation of a QKD field trial within a commercial data centre environment that utilises the existing fibre network infrastructure. The achieved average secret key rate of 2.392 kbps and an average quantum bit error rate of less than 2% demonstrate the commercial feasibility of QKD in real-world scenarios. As a use case study, we demonstrate the secure transfer of files between two data centres through the Quantum-Secured Virtual Private Network, utilising secret keys generated by the QKD devices.

Keywords: Quantum cryptography, quantum key distribution, quantum-safe application, quantum networks



© The Author(s) 2024. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License (<https://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, sharing, adaptation, distribution and reproduction in any medium or format, for any purpose, even commercially, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.



1. INTRODUCTION

As the quantum technology landscape evolves, there is recognition of a threat on the horizon: quantum computing poses a threat to the security of existing asymmetric encryption techniques^[1,2]. In order to circumvent possible breaches of long-term information security, it would be prudent to begin evaluating possible quantum-safe technologies as candidate solutions. An existing quantum technology that is of relevant high readiness level and ready for commercial adoption is quantum key distribution (QKD). QKD enables two distant, honest parties to work together to create shared symmetric random bit strings that remain secure from a potential eavesdropper. Current-day key establishment protocols, such as the Rivest Shamir Adleman (RSA), rely on the assumption that an adversary has limited computational power relative to the hardness of a mathematical problem. In contrast, the security of QKD protocol can be proven even against an eavesdropper with unbounded computational power (including quantum computers). This security is called information-theoretic security (ITS)^[3]. Furthermore, QKD is among the first technologies based on quantum information that is commercially available and has been deployed in fibre networks and free space setups worldwide.

The overall performance of QKD hardware in a commercial environment is indicated by two key parameters: the secret key rate (SKR) and quantum bit error rate (QBER)^[4]. The SKR indicates the achieved rate of secret keys produced by the QKD devices, whereas QBER provides an error percentage for quantum signal transmissions between the QKD end nodes over a quantum channel. (For a continuous variable type QKD system, the quantum channel is characterised by the channel transmission and the excess noise^[5].) To get a glimpse of the performance of production-grade QKD deployments in a commercial environment, as early as 2008, one of the QKD networks in the SECOQC project recorded an average SKR of 3.1 kbps and QBER of 2.6% over a 33 km fibre distance with a fibre loss of 7.5 dB in Vienna^[5]. In Switzerland, an average SKR of 2.5 bps and QBER of 5% were achieved with the QKD system that uses the coherent one-way (COW) protocol^[6,7] over a fibre link of 150 km with loss of 43 dB from Neuchatel to Geneva^[8]. In 2012, a long-term field demonstration of a QKD network that links two metropolitan cities with a trusted node was established in China, where the longest link spans a distance of 85.1 km, with a fibre loss of 18.4 dB, recorded an average SKR of 0.77 kbps and QBER of 5.26% for decoy-state BB84 protocol^[9]. More recently, the quantum network established in Cambridge, United Kingdom, which uses BB84 protocol^[10], recorded an average SKR of 2,580 kbps and an average QBER below 2.5% over a fibre distance of 10.6 km with a loss of 3.9 dB^[11]. Beyond the general performance of the QKD system, the potential for seamless integration between QKD technology and encryption-based applications offers a captivating prospect for its potential commercial use cases. For instance, the generated QKD keys can be used to establish point-to-point quantum-secure communication links to transfer data^[4,12] and perform video conferencing^[13]. Furthermore, the possibility of a secure financial transaction over a quantum-secure optical channel with a QKD system using BB84 protocol has been demonstrated by a financial bank in a lab environment recently^[14].

Securing the transmission of private and sensitive data is an important application for the integration of QKD devices, especially for critical information infrastructure. Data centres, in particular, can leverage the QKD devices for this very purpose^[15-17]. They are infrastructures for companies or organisations to house their IT equipment, allowing them to perform tasks such as data storage, remote applications, and accessing cloud computation services. The data traffic experienced by these data centres is growing rapidly and a forecast done by Cisco in 2018 shows that this traffic will reach 19.5 zettabytes by the year 2021 globally^[18]. This is expected to increase even more in recent years given the increasing demand for cloud storage and advancement of cloud services, and more data centres will be needed to handle these large amounts of data traffic. In addition, communication between these data centres is required to fetch and retrieve data seamlessly. This communication link is called the Data Centre Interconnect and it is responsible for establishing a network connecting all data centres together^[19]. Most often, these interconnects are established using a virtual private network (VPN), and it is crucial for them to be secure to prevent compromising the confidentiality, security and integrity of the data within the data centres^[17]. Therefore, various stakeholders have begun to employ quantum-safe cryp-

tography solutions by deploying QKD devices to provide secure keys for encrypting these interconnects for secure data transfer^[15,20] and cloud computing^[21]. In addition, an essential consideration when integrating QKD devices into the data centre is that this process should not require any major modification to their current network configuration, or building a new fibre infrastructure specifically for the QKD devices; in fact, these QKD devices should be seen as an upgrade to their existing interconnect network for quantum-safe readiness. Field trials done under this consideration will provide a good indication of the commercial viability of QKD devices.

In this article, we report the demonstration of a successful QKD field trial in a commercial data centre environment over existing fibre network infrastructure. This deployment was conducted by the National Quantum-Safe Network of Singapore (NQSN), a nationwide testbed for quantum-safe technology, in collaboration with Singapore Technologies Telemedia Global Data Centres (STT-GDC). The goal was to examine the technical feasibility and reliability of production-grade QKD equipment in the context of Singapore's commercial operating environment. We covered the entire deployment life cycle: starting from the installation of QKD devices in the data centres and network equipment setup, to the subsequent monitoring of the physical layer of the quantum network. At the same time, as a case study, we explore the possibility of utilising the keys generated via the QKD devices to create a quantum-secured virtual private network to demonstrate secure data transmission between two interconnected data centres.

2. METHODS

2.1 QKD background and QKD protocol

The basic functionalities of a general QKD commercial system are illustrated in [Figure 1](#). The QKD system is made up of two parts: a QKD transmitter and a QKD receiver, commonly known as Alice and Bob, respectively. Alice and Bob will generate identical random bit strings as QKD-keys based on the underlying protocol consisting of two stages: raw data exchanges over the quantum channel and post-processing over the classical channel to produce symmetric secret keys^[22]. Finally, the key management organises these symmetric secret keys for use in different encryption applications via the designated interfaces. The key management channel is required when expanding the QKD network with multiple users, as it can securely distribute and relay these secret keys within this network.

For this field trial, the QKD equipment vendor collaborating for this demonstration is ID Quantique (IDQ), and the QKD system used is the Cerberis XGR Series^[23]. This system has a repetition rate of 1.25 GHz^[24] and uses the coherent one way (COW) protocol^[6,7], which is patented by IDQ. The implemented COW protocol is secure against restricted types of collective attacks^[25-27]. The schematic description of the COW protocol is illustrated in [Figure 2](#). In this demonstration, the latest version of the COW protocol with an additional vacuum state, specifically referred to as the COW-4 protocol here, is employed to foil the zero-error attacks against COW protocol^[28,29]. We note that the QKD system deployed is an implementation of a QKD protocol, where there is necessarily a gap with the ideal theoretical QKD protocol (which is ITS) and its realistic implementation.

In the setup, the laser in the transmitter in Alice emits a continuous wave (CW) beam, which is subsequently modulated at the intensity modulator, to provide coherent optical pulses with bit patterns corresponding to the bit value of zeros, ones, decoy and vacuum states. These pulses are attenuated at the optical attenuator to reach single photon levels and travel from Alice to Bob via the quantum channel. In the receiver at Bob, some pulses reach the bit-generation detector, denoted by D_{bit} , through the beam splitter and they are used for generating the QKD keys in the key distillation process. The other pulses, reflected by the beam splitter, enter the path containing the monitoring interferometer to measure the coherence between adjacent pulses at the monitoring detector, denoted by D_{mon} , to monitor for the presence of eavesdroppers^[23]. For this above

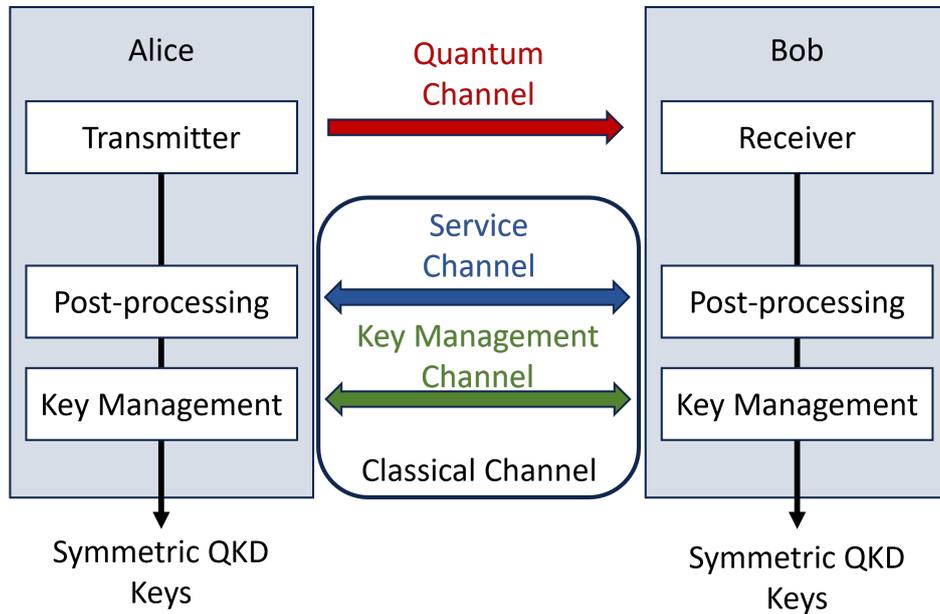


Figure 1. The basic components for a QKD system. The quantum channel (red arrow) exchanges the raw keys between Alice and Bob. Afterwards, post-processing takes place over the classical service channel (blue arrow), while the key management channel (green arrow) organises these secret keys and supplies them upon demand to different encryption applications. QKD: Quantum key distribution.

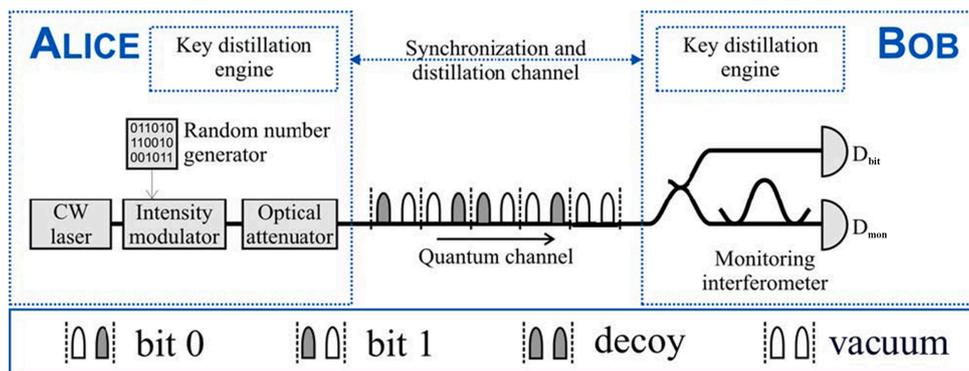


Figure 2. The schematic description of COW-4 protocol. Single-photon-level pulses with bit values of zeros, ones, decoy and vacuum states are sent from Alice to Bob via the quantum channel. At Bob, the bit-generation detector D_{bit} generates the QKD keys, while the monitoring interferometer measures the coherence between adjacent pulses at detector D_{mon} . The key distillation process commences thereafter and the sifting, error correction, privacy amplification and key management process happen over the classical channel (indicated by the blue dashed arrow) to generate the secret keys. COW: Coherent one-way; QKD: quantum key distribution.

process to work, Alice and Bob need to be synchronised through the classical channel. After the pulses are exchanged between Alice and Bob, the key distillation process commences on the classical channel, where the QKD keys are generated through processes such as sifting, error correction with Low Density Parity Code (LDPC) algorithm, and privacy amplification using the Wegman-Carter Strongly Universal Hashing to obtain secret keys that are uniformly random, identical and secure against an eavesdropper^[23]. These keys are then forwarded to the key management, where a portion is employed for authenticating the classical channel, while the remainder becomes the secret keys shared among Alice and Bob^[30,31].

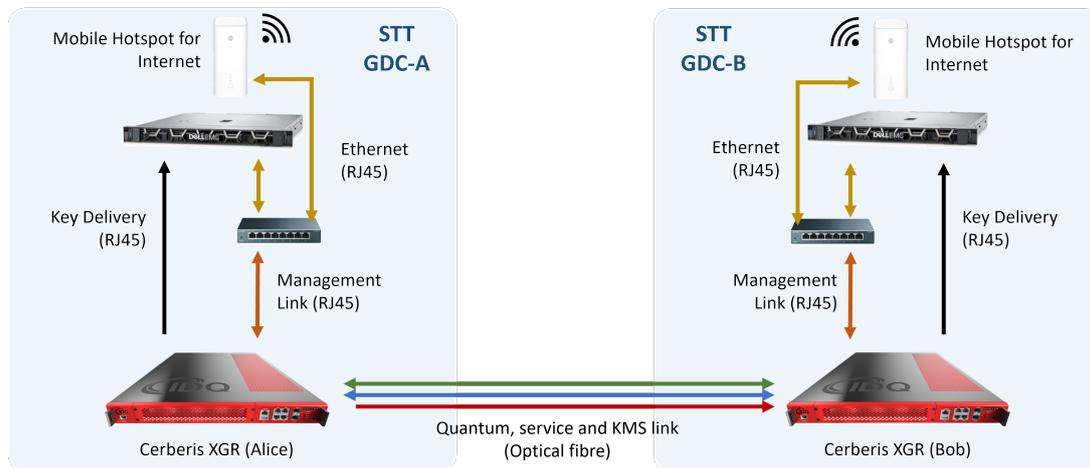


Figure 3. The quantum (red arrow), service (blue arrow) and KMS (green arrow) channels of the QKD systems are connected via optical fibres. The connections established between each QKD system and the IT equipment are made by RJ45 (brown arrow). Within the server, various software containers are deployed, including the QMS, as well as the Web API container, which is managed by the management link (orange arrows). The QKD keys are pushed out of the QKD devices into the server using the ETSI GS QKD 014 REST API via the key delivery link (black arrow). KMS: Key management system; QKD: quantum key distribution; IT: information technology; QMS: Quantum Management System; API: application programming interface; STT GDC: Singapore Technologies Telemedia Global Data Centres.

2.2 QKD deployment

The architecture for the physical setup of the field trial demonstration is depicted in Figure 3. The quantum, service and key management system (KMS) channels of the two QKD devices are made via optical fibres for transmitting signals with different wavelengths at C-band. The connections for the quantum channel are Subscriber Connector (SC)/Ultra Physical Contact (UPC), whereas each of the service and KMS channel connections are established with Lucent Connector (LC)/UPC (duplex) connecting to a transceiver. All three channels are transmitted through their own dedicated fibres. At each site, the QKD device is set up as follows:

1. Two RJ45 Ethernet connections are available from the IDQ Cerberis XGR device, one for the key delivery link and the other for the management of the appliances. The connection for the appliance management is extended into an Ethernet network switch.
2. A typical server with dual Ethernet connections is subsequently connected to the switch to control the management of the appliances, while the other is used to control the key delivery link.
3. Within the server, various software containers are deployed. Important containers include the quantum management system (QMS), as well as the Web API container^[23], which can set up, control, and monitor the QKD devices, and the ETSI GS QKD 014^[32] Representation State Transfer (REST) API container that pushes the secret keys out of the QKD devices via the key delivery link.
4. A mobile hotspot router is used for internet purposes. The router utilises publicly available consumer mobile networks with either 4G or 5G connectivity. The router is connected to the switch for the management network. We note that the cellular networks are from different operators, and there is no direct communication link setup between both locations; hence, both locations reside in two separate IP networks.

In our demonstration, the QKD deployment employs the trusted node configuration. In particular, the server and the QKD, which is connected via the ETSI GS QKD 014 REST API interface, are co-located within a trusted environment. We note that in this trusted node setting, we have assumed that the eavesdroppers do not have access to the ETSI GS QKD 014 API interface. The performance of the deployed QKD over time is evaluated and the most critical parameters to monitor are the following:

- **QBER.** This is defined as the ratio of non-identical bits between the QKD transmitter (Alice) and QKD receiver (Bob), which is an error rate due to the quantum signal transmitting via the open quantum channel. In the security proof, all errors are attributed to the eavesdropping action on the open channel. In other

Table 1. Results for fibre network infrastructure for the optical fibres between the two data centres

Location 1	Location 2	Measured fibre length (OTDR)	Measured fibre loss at 1,550 nm (OTDR)
STT GDC-A	STT GDC-B	19.87 km	12.47 dB

OTDR: Optical time-domain reflectometer; STT GDC: Singapore Technologies Telemedia Global Data Centres.

words, QBER directly impacts the final SKR, and thus the QKD channel security and performance. A high QBER will result in the aborting of QKD protocol^[33], and for a given QKD protocol, a certain threshold of QBER forbids the QKD protocol to generate any secret key. For instance, in a BB84 QKD protocol, QBER \approx 11% is the theoretical limit to have a positive key rate^[34,35]. In practice, the noise presence in the quantum channel and imperfection of realistic QKD transmitter and receiver will also contribute to QBER.

- **SKR.** This indicates the amount of secret keys that can be generated per time period, with the unit of bits per second (bps). Here, the SKR for the COW protocol is derived as a function of QBER, other security parameters and accounting for various eavesdropping attack models, such as sequential^[36], collective^[25] or zero-error attack^[37] that could potentially be executed on the QKD system^[22,33]. In practical implementations, the actual SKR will involve a real-time QKD operation time period, which includes the time for the key distillation and post-processing^[30,31]. Generally, a QKD system with a higher SKR will have a greater advantage in supporting applications that consume keys rapidly.

2.3 Fibre network infrastructure

The production-grade fibre network infrastructure is provided by NetLink Trust (NLT). As mentioned in the INTRODUCTION Section, minimal alterations need to be made to this existing fibre network in this deployment. In particular, apart from the establishment of the last-mile connectivity, the QKD devices can be connected to the existing fibre networks without laying new fibre cables in between. Based on theoretical fibre study conducted by NLT to estimate the fibre length distance and fibre loss via the network planning tool, two data centres from STT-GDC are chosen for this trial demonstration, where QKD Alice and Bob are located at STT GDC-A and STT GDC-B, respectively. The location of the two sites is depicted in Figure 4. The fibre connection consists of a total of seven hops from STT GDC-A to STT GDC-B that are in compliance with G.657A standards^[38] and the G.652D standards^[39]. Upon completion of the fibre connection, an end-to-end optical time-domain reflectometer (OTDR) measurement on the final fibre cable link is conducted. The equipment used in the measurement is a VIAVI SmartOTDR measurement tool. The measured fibre cable link results between these two data centres are shown in Table 1. These results are crucial to ensure the QKD equipment continues to operate within its acceptable capability and operation range.

2.4 QKD application

To emulate a secure file transfer using the QKD system, we demonstrate the application of using symmetric QKD-generated keys to encrypt and decrypt the data that is sent across the two data centres. To this end, a quantum-secured VPN (Q-VPN) application is deployed over the connecting sites. This Q-VPN consumes the QKD keys from the key buffer storage in the QKD system and performs Advanced Encryption Standard-256 (AES-256) encryption thereafter to establish a quantum-safe VPN tunnel for secure data transfer. AES-256 is a symmetric algorithm that is quantum-safe and remains secure even against quantum attacks such as Grover's algorithm. When used in conjunction with a QKD protocol, the overall security of the Q-VPN remains quantum-safe at the protocol level. For the purpose of this demonstration of functionality, cloud resources are utilised to establish the VPN tunnel due to their robustness and ease of implementation in a simplified network setting (In practice, the edge cloud resources can also be located at the trusted nodes, as demonstrated by the NQSN in another trial^[21]).

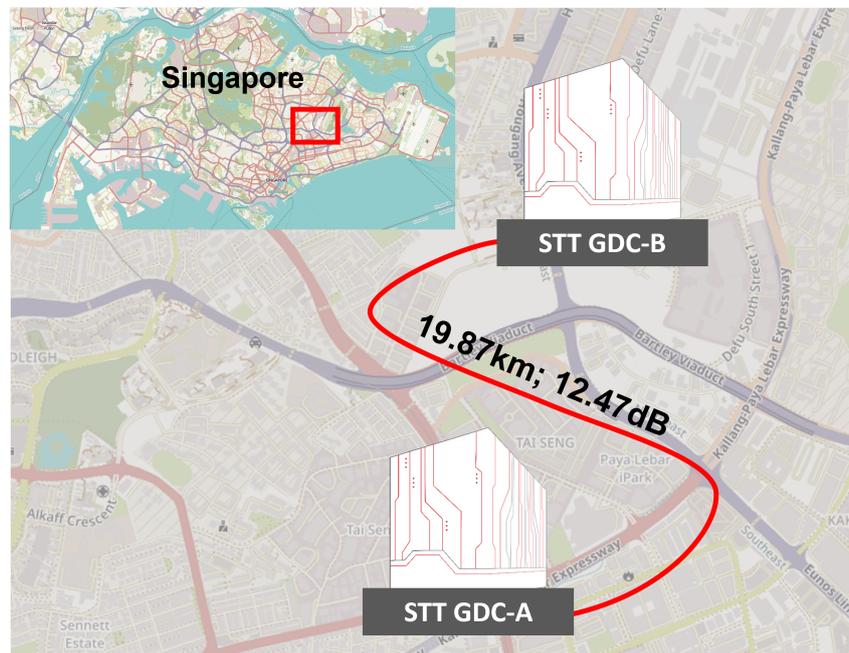


Figure 4. Location of QKD devices at STT GDC-A and STT GDC-B shown on the map. The red line indicates the fibre connection between the two sites with a measured length of 19.87 km and a measured loss of 12.47 dB. QKD: Quantum key distribution; STT GDC: Singapore Technologies Telemedia Global Data Centres.

The architecture of the QKD application is illustrated in [Figure 5](#). The symmetric secret keys generated by both Alice and Bob are channelled via the ETSI GS QKD 014 REST API to the server, then onto the cloud computers. After the Transport Layer Security (TLS) handshake is established between Alice and Bob, these secret keys are stored in the internal SQLite3 database of the Q-VPN application. We note that the connection between the server and the cloud is not assumed to be quantum-safe and only for demonstration purposes. These stored keys are synced between the two points and can be accessed to encrypt the network between them using AES-256 encryption, with the keys renewed every ten seconds. The used keys will be discarded and the Q-VPN will request more secret keys from the QKD devices to replenish keys in its database. A file transfer client/server application can be achieved. The data is transferred from the sender to the receiver using the Secure Copy Protocol (SCP) command between the cloud computers via this encrypted Q-VPN tunnel.

3. RESULTS

3.1 Performance and reliability analysis of the QKD equipment

The stability of SKR and QBER is monitored continuously, and the results are shown in [Figure 6](#). The SKR and QBER from the QKD equipment are relatively consistent throughout the time window of ten days. The standard deviation of SKR is less than 4.3% of its average, indicating a relatively stable performance over the operating period. Meanwhile, the average QBER is relatively low at 1.9%. More than 97% of the data points recorded are below 2.9% of QBER, and maximum recorded QBER is less than 6%. The total key generated amounts to more than 2 Gigabits, or equivalently more than 8 million AES-256 keys.

There are two other parameters that are crucial to the performance and reliability specifically to the COW protocol: the dark-count corrected (Dcc) Visibility and the Total Detection Count. The Dcc Visibility is the interference visibility detected at the D_{mon} after correcting for the dark counts (detection without incident light). Preferably, the Dcc Visibility should be near, but strictly below, 100% and the recorded result is sufficiently high, averaging 99.12% with a small standard deviation of 0.16%. The Total Detection Count accounts for

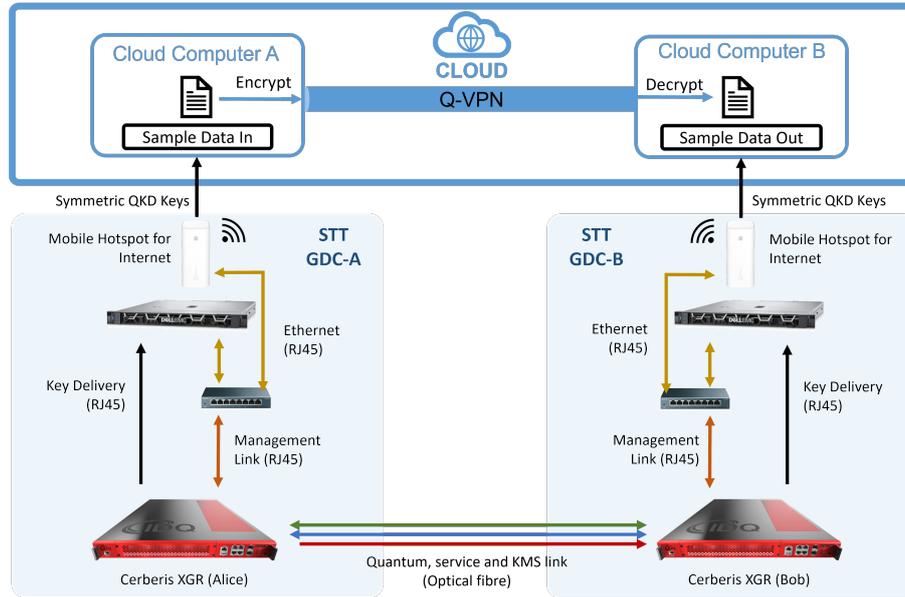


Figure 5. QKD application architecture. The secret keys generated by Alice and Bob are sent to their respective cloud computer via the ETSI GS QKD 014 REST API with the help of the key delivery link (black arrow) and the Ethernet link (brown arrow). These secret keys are stored in the internal SQLite3 database of the Q-VPN application. These stored keys are synced between the two points to encrypt the link between them. Once the Q-VPN link is established, a file transfer client/server application can be achieved. QKD: Quantum key distribution; Q-VPN: quantum-secured virtual private network.

Table 2. Average and standard deviation of the key parameters for the stability test

Key parameters	Average	Standard deviation
Secret key rate	2,392 bps	126 bps
QBER	1.90%	0.50%
Dcc visibility	99.12%	0.16%
Total detection count	18,199	65

QBER: Quantum bit error rate; Dcc: dark-count corrected.

the total number of detection, including incoming photons and dark counts at D_{bit} . The respective plots for the Dcc Visibility and Total Detection Count are also presented in [Figure 6](#). The average and the standard deviation of these parameters are presented in [Table 2](#).

3.2 Attenuation test on key parameters

An attenuation test is done to ascertain the relationship between the attenuator added and the two key parameters. This analysis could provide an estimation of the potential QKD performance on the fibre for scenarios of different distances. The attenuation is added using fixed attenuators to the optical fibre for the quantum channel. [Figure 7](#) illustrates the combined results obtained for the key parameters and [Table 3](#) shows the values of the key parameters with the respective attenuation added. The SKR decreases with the increase in attenuation. During the test, we have further added an attenuation of 12 dB, which has resulted in a zero key rate. This indicates that the loss value has exceeded the QKD system tolerable limit.

3.3 QKD application integration

The QKD application showcases a secure file transfer via the Q-VPN tunnel from Alice to Bob (without additional attenuation). The sample files are successfully encrypted and transferred through the Q-VPN every minute, and the content is successfully decrypted at the receiving end. Since the Q-VPN uses AES-256 encryption, the average SKR generated by the QKD devices can provide an AES-256 key refresh rate of 11 keys per second. Given that the Q-VPN renews its key every ten seconds, the QKD devices operating in the commercial

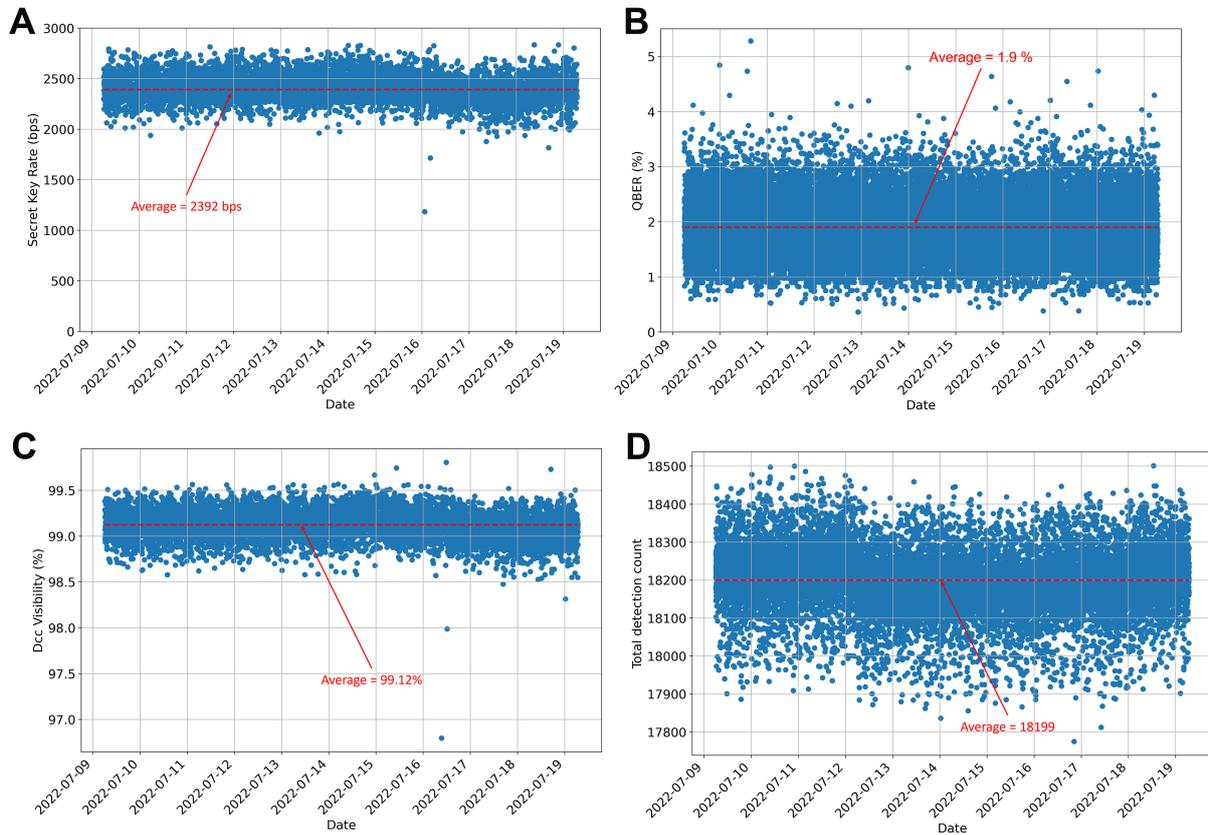


Figure 6. The SKR, QBER, Visibility and Total Detection Count measurement over a period of 10 days. (A) The recorded SKR over time, with an average SKR of 2,392 bps (indicated by the red dotted line); (B) the recorded QBER over time, with an average QBER of 1.9% (indicated by a red dotted line) and all the recorded QBER is less than 6%; (C) the Dcc Visibility recorded over time, with an average of 99.12% (indicated by a red dotted line); (D) the Total Detection Count recorded over time, with an average of 18,199 (indicated by a red dotted line). SKR: Secret key rate; QBER: quantum bit error rate; Dcc: dark-count corrected.

Table 3. Attenuation test for key parameters

Attenuator added (dB)	Secret key rate (bps)	QBER (%)
3 ± 0.2	2,303 ± 135	1.62 ± 0.84
5 ± 0.2	1,730 ± 126	1.13 ± 0.48
7 ± 0.2	1,473 ± 141	1.30 ± 0.47
8 ± 0.4	1,016 ± 164	1.13 ± 0.59
10 ± 0.4	746 ± 110	1.19 ± 0.66

environment have the capability to generate sufficient keys to support the operation of the Q-VPN tunnel.

4. DISCUSSION AND OUTLOOK

The successful demonstration of the QKD keys distributed among the two secured sites, together with a simple application of establishing a Q-VPN, paves the way for quantum-safe connectivity in real-world use cases and further advanced applications. In the case of the QKD systems, this field trial demonstrates the commercial viability of QKD integration with the existing production-grade fibre network in Singapore within a data centre environment. This is an important milestone, without taking for granted that the data centre environment is ideal for QKD devices. For instance, these QKD devices can be co-located with other telecommunication equipment, including encryptors, servers, plus computational intensive devices, impacting the surrounding temperature stability. In comparison to other works demonstrating a similar QKD protocol in controlled lab

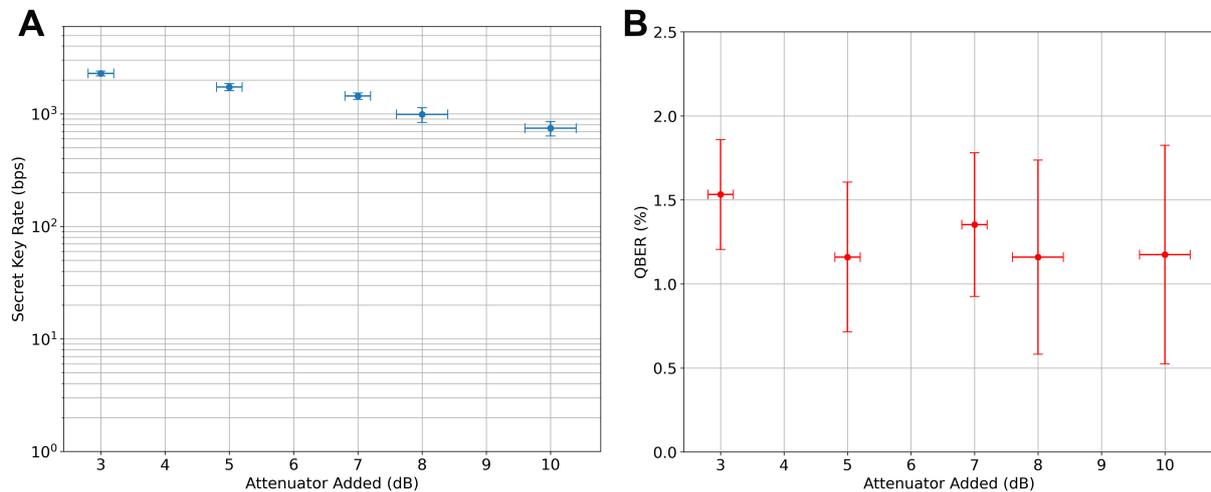


Figure 7. The graphs of attenuation added and its impact on the respective key parameters. (A) SKR against Attenuator(s) Added. The SKR axis scales in a logarithmic manner to illustrate the relationship between the SKR and added attenuation. The standard deviation for the SKR is included in the figure as error bars. The error bars are relatively small, indicating a relatively constant SKR; (B) QBER against Attenuator Added. The standard deviation for the QBER is included in the figure as error bars. In both plots, the error bars for the attenuation account for the insertion loss uncertainties, with the larger uncertainty indicating a combination of two attenuators. SKR: Secret key rate; QBER: quantum bit error rate.

settings^[26,40], by showcasing stable secret keys exchanged, our work bears a better resemblance to an operational environment and provides insight into understanding the practical challenges for the QKD system.

Another important aspect studied in our demonstration covers the organisation of fibre connectivity for the QKD deployment. For this demonstration, there are seven patches across Alice and Bob, giving a measured fibre distance of 19.87 km and 12.47 dB of fibre loss. Apart from ensuring that the total fibre loss is within the capability and operation range of the QKD devices, no further optimisation is required. In principle, the insertion loss from the fibre patches can be further minimised via fibre splicing to reduce the number of patches. In our demonstration, while dedicated dark fibres are used for the quantum and the classical channels, in principle one can utilise wavelength-division multiplexing (WDM) technique to conserve the fibre resources. For instance, by having the quantum signal operating at a different optical band (e.g., O-band) with respect to the classical data signals, channel multiplexing over a single fibre core can be performed^[23].

In this demonstration, a point-to-point QKD architecture linking two data centres was employed. It is crucial to recognise that these data centres are part of an interconnected network made up of multiple data centres, which ultimately need to be scaled beyond mere point-to-point connections to guarantee quantum safety across the network. With the multi-layer approach of QKD network architecture^[41,42], it allows scalability and interoperability from point-to-point QKD to multi-point QKD network topology. Under the trusted relay node-based QKD network, this is enabled by the key management (KM) layer to interconnect the QKD pairs with key supply interfaces as well as key relaying and storage functions inside KM layers. Beyond trusted nodes, there are other quantum technologies under active development to extend and enhance the QKD network, such as measurement-device-assisted QKD (measurement-device-independent QKD^[43], twin-field QKD^[44]) and quantum repeater^[45]. Examples of multi-point QKD topology include a mesh^[5,9,13], a ring^[11], a star^[46-48] or a mixed type architecture^[49]. Moreover, the performance study of different QKD protocols and vendors in the market can also be done to analyse their performance and commercial viability within the data centre or other mission critical infrastructure environment. Some examples of the QKD protocols are the BB84 system, entanglement-based system, and continuous variable system. The utilisation of emerging technologies could further enhance the performance of QKD devices and their realisation could also be examined in future

Table 4. Comparison between PQC and QKD

	PQC	QKD
Implementation	Software and hardware	Hardware
Protocol security	Computational complexity	ITS
Implementation loopholes	Exist	Exist
Application and usage	Public-key encryption and key establishment, Digital signature	Key establishment
Migration	Software and hardware upgrade	Infrastructure and hardware upgrade
Standardisation and certification	Required	Required

PQC: Post quantum cryptography; QKD: quantum key distribution; ITS: information-theoretic security.

demonstrations. These advancements include fast single photon detectors^[50], integrated transmitter and receiver^[51], qubit-based time synchronisation technique^[52] and digital signal processing^[53,54]. Apart from the Q-VPN applications, different use cases at different Open Systems Interconnection (OSI) layers could also be explored in the future.

On the other hand, it is instructive to mention another quantum-safe cryptography alternative, which is the post-quantum cryptography (PQC)^[55]. PQC is a cryptographic algorithm that is believed to be secured and resilient under known quantum algorithm attacks. It finds applications in cryptography such as digital signatures, public-key encryption and key establishment. PQC, being primarily software based, suggests that quantum-safe migration and implementation could be cost-effective and scalable. However, to maintain a certain degree of performance, hardware upgrade might be required as well. For QKD and PQC, though both offer quantum-safe solution in the post-quantum era, they still require standardisation and certification. This is to ensure that the respective encryption protocols are implemented properly, preventing potential vulnerability and loopholes in their implementation security before its widespread adoption. Here, we provide a high-level comparison between PQC and QKD in Table 4. A hybrid framework that captures the strengths of the QKD devices and PQC could be implemented to improve the overall resiliency^[56,57].

5. CONCLUSIONS

We confirmed the feasibility of operating QKD devices over an existing production-grade fibre network within a commercial data centre environment. In terms of the QKD device's performance, the secret key rate and QBER are stable and consistent over the trial period. In particular, we achieved an average SKR of 2.392 kbps, which is largely achievable due to a low average QBER of less than 2%. A total of more than 2 Gigabits of AES-256 keys are accumulated, with the rates of around 690 sets of keys per minute. The attenuation test verifies the functionality of the QKD equipment over different quantum channel losses between Alice and Bob. For the application, files are successfully transferred between two data centres via the Q-VPN which makes use of the secret key generated by the QKD devices. Our efforts mark the inaugural stride towards the widespread deployment of QKD throughout Singapore, thereby bolstering the infrastructure for practical, quantum-safe communication.

DECLARATIONS

Acknowledgements

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 and providing the image in Figure 2. We also thank Yu Cai for helpful discussion. Additionally, we are grateful to the Department of Electrical and Computer Engineering, National University of Singapore, for supporting the logistics of the field trial.

Authors' contributions

Made substantial contributions to conception and design of the study: Qiu K, Haw JY, Qin H, Kasper M

Provisioning and setting up of the field trial environment: Qiu K, Haw JY, Qin H, Kasper M, Ling A

Performed data acquisition, data analysis and interpretation: Qiu K, Haw JY, Qin H

Drafting the manuscript: Qiu K, Haw JY, Qin H, Ng NHY, Ling A

Discussion of the main idea and scientific contribution: Qiu K, Haw JY, Qin H, Ng NHY, Kasper M, Ling A

Availability of data and materials

Not applicable.

Financial support and sponsorship

We acknowledge funding support from the National Research Foundation, Singapore and A*STAR under its Quantum Engineering Programme (National Quantum-Safe Network, NRF2021-QEP2-04-P01) and start-up grant for Nanyang Assistant Professorship awarded to Ng NHY of Nanyang Technological University, Singapore.

Conflicts of interest

All authors declared that there are no conflicts of interest.

Ethical approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

Copyright

© The Author(s) 2024.

REFERENCES

1. Mavroeidis V, Vishi K, Zych MD, Jøssang A. The impact of quantum computing on present cryptography. arXiv. [Preprint.] Mar 31, 2018 [accessed 2024 Sep 9]. Available from: <https://arxiv.org/abs/1804.00200>.
2. Chen L, Jordan S, Liu YK, et al. Report on post-quantum cryptography. 2016. Available from: <https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf>. [Last accessed on 9 Sep 2024]
3. Renner R, Gisin N, Kraus B. Information-theoretic security proof for quantum-key-distribution protocols. *Phys Rev A* 2005;72:012332. DOI
4. Stucki D, Legré M, Buntschu F, et al. Long-term performance of the SwissQuantum quantum key distribution network in a field environment. *New J Phys* 2011;13:123001. DOI
5. Peev M, Pacher C, Alléaume R, et al. The SECOQC quantum key distribution network in Vienna. *New J Phys* 2009;11:075001. DOI
6. Gisin N, Ribordy G, Zbinden H, Stucki D, Brunner N, Scarani V. Towards practical and fast quantum cryptography. arXiv. [Preprint.] Nov 3, 2004 [accessed 2024 Sep 9]. Available from: <https://arxiv.org/abs/quant-ph/0411022>.
7. Stucki D, Brunner N, Gisin N, Scarani V, Zbinden H. Fast and simple one-way quantum key distribution. *Appl Phys Lett* 2005;87:194108. DOI
8. Stucki D, Barreiro C, Fasel S, et al. Continuous high speed coherent one-way quantum key distribution. *Opt Express* 2009;17:13326-34. DOI
9. Wang S, Chen W, Yin ZQ, et al. Field and long-term demonstration of a wide area quantum key distribution network. *Opt Express* 2014;22:21739-56. DOI
10. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. *Theor Comput Sci* 2014;560:7-11. DOI
11. Dynes JF, Wonfor A, Tam WWS, et al. Cambridge quantum network. *npj Quantum Inf* 2019;5:101. DOI
12. Braun RP, Geitz M. The OpenQKD testbed in Berlin. In: Chang-Hasnain C, Willner A, Shieh W, Shum P, Su Y, Li G, Eggleton B, Essiambre R, Dai D, Ma D, editors. Technical digest series. Optica Publishing Group; 2021. p. M4C.2. DOI
13. Sasaki M, Fujiwara M, Ishizuka H, et al. Field test of quantum key distribution in the Tokyo QKD Network. *Opt Express* 2011;19:10387-409. DOI
14. Pistoia M, Amer O, Behera MR, et al. Paving the way toward 800 Gbps quantum-secured optical channel deployment in mission-critical environments. *Quantum Sci Technol* 2023;8:035015. DOI

15. Cao Y, Zhao Y, Wang Q, Zhang J, Ng SX, Hanzo L. The evolution of quantum key distribution networks: on the road to the Qinternet. *IEEE Commun Surv Tutor* 2022;24:839-94. DOI
16. Liu R, Rozenman GG, Kundu NK, Chandra D, De D. Towards the industrialisation of quantum key distribution in communication networks: a short survey. *IET Quantum Commun* 2022;3:151-63. DOI
17. Jain N, Hoff U, Gambetta M, Rodenberg J, Gehring T. Quantum key distribution for data center security - a feasibility study. arXiv. [Preprint.] Jul 24, 2023 [accessed 2024 Sep 9]. Available from: <https://arxiv.org/abs/2307.13098>.
18. Global cloud index projects cloud traffic to represent 95 percent of total data center traffic by 2021. 2018. Available from: <https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2018/m02/global-cloud-index-projects-cloud-traffic-to-represent-95-percent-of-total-data-center-traffic-by-2021.html>. [Last accessed on 9 Sep 2024]
19. Cheng Q, Bahadori M, Glick M, Rumley S, Bergman K. Recent advances in optical technologies for data centers: a review. *Optica* 2018;5:1354-70. DOI
20. Zatoukal B, Kutschera F, Poppe A, et al. OpenQKD use-case for securing sensitive medical data at rest and in transit. In: 2021 Conference on Lasers and Electro-Optics Europe & European Quantum Electronics Conference (CLEO/Europe-EQEC); 2021 Jun 21-25; Munich, Germany. IEEE; 2021. p. 1. DOI
21. Moreno J, Proctor C. Implementing a quantum-secured network in a metropolitan area. 2023. Available from: <https://aws.amazon.com/blogs/quantum-computing/implementing-a-quantum-secured-network-in-a-metropolitan-area/>. [Last accessed on 9 Sep 2024]
22. Scarani V, Bechmann-Pasquinucci H, Cerf NJ, Dušek M, Lütkenhaus N, Peev M. The security of practical quantum key distribution. *Rev Mod Phys* 2009;81:1301-50. DOI
23. Redefining security: XGR series – QKD platform: quantum key distribution designed for academia & research institutes. 2023. Available from: https://marketing.idquantique.com/acton/attachment/11868/f-5f50c28e-bac2-40a7-bc5a-30971c980753/1/-/-/-/XGR%20Series_Brochure.pdf. [Last accessed on 9 Sep 2024]
24. Redefining security: Cerberis XG QKD system. 2024. Available from: https://marketing.idquantique.com/acton/attachment/11868/f-2e621d25-e414-4772-a482-b1b272c24c11/1/-/-/-/Cerberis%20XG%20QKD%20System_Brochure.pdf. [Last accessed on 9 Sep 2024]
25. Branciard C, Gisin N, Scarani V. Upper bounds for the security of two distributed-phase reference protocols of quantum cryptography. *New J Phys* 2008;10:013031. DOI
26. Korzh B, Lim CCW, Houlmann R, et al. Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nat Photonics* 2015;9:163-68. DOI
27. Walenta N, Burg A, Caselunghe D, et al. A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing. *New J Phys* 2014;16:013047. DOI
28. Curty M. Foiling zero-error attacks against coherent-one-way quantum key distribution. *Phys Rev A* 2021;104:062417. DOI
29. Gao RQ, Xie YM, Gu J, et al. Simple security proof of coherent-one-way quantum key distribution. *Opt Express* 2022;30:23783-95. DOI
30. Constantin J, Houlmann R, Preyss N, et al. An FPGA-based 4 Mbps secret key distillation engine for quantum key distribution systems. *J Signal Process Syst* 2017;86:1-15. DOI
31. Yuan Z, Plews A, Takahashi R, et al. 10-Mb/s quantum key distribution. *J Lightwave Technol* 2018;36:3427-33. DOI
32. ETSI GS QKD 014. Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API. 2019. Available from: https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_qkd014v010101p.pdf. [Last accessed on 9 Sep 2024]
33. Djordjevic IB. Physical-layer security and quantum key distribution. Springer; 2019. DOI
34. Christandl M, Renner R, Ekert A. A generic security proof for quantum key distribution. arXiv. [Preprint.] Feb 18, 2004 [accessed 2024 Sep 9]. Available from: <https://arxiv.org/abs/quant-ph/0402131>.
35. Shor PW, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys Rev Lett* 2000;85:441-4. DOI
36. González-Payo J, Trényi R, Wang W, Curty M. Upper security bounds for coherent-one-way quantum key distribution. *Phys Rev Lett* 2020;125:260510. DOI
37. Trényi R, Curty M. Zero-error attack against coherent-one-way quantum key distribution. *New J Phys* 2021;23:093005. DOI
38. ITU-T recommendations. ITU-T G.657: Characteristics of a bending-loss insensitive single-mode optical fibre and cable. 2016. Available from: <https://handle.itu.int/11.1002/1000/13078>. [Last accessed on 9 Sep 2024]
39. ITU-T recommendations. ITU-T G652: Characteristics of a single-mode optical fibre and cable. 2016. Available from: <https://www.itu.int/rec/T-REC-G.652-201611-I/en>. [Last accessed on 9 Sep 2024]
40. Da Lio B, Bacco D, Cozzolino D, Ding Y, Dalgaard K, Rottwitz K, Oxenløwe LK. Experimental demonstration of the DPTS QKD protocol over a 170 km fiber link. *Appl Phys Lett* 2019;114:011101. DOI
41. Telecommunications Standards Advisory Committee (TSAC). Reference specification. Quantum key distribution networks. IMDA RS QKDN. 2023. Available from: <https://www.imda.gov.sg/-/media/Imda/Files/Regulation-Licensing-and-Consultations/ICT-Standards/Telecommunication-Standards/Reference-Spec/IMDA-RS-QKDN-final.pdf>. [Last accessed on 3 Sep 2024]
42. ITU-T recommendations:ITU-T Y.3800 (2019) Corrigendum 1 (04/20): overview on networks supporting quantum key distribution. 2020. Available from: <https://www.itu.int/rec/T-REC-Y.3800/en>. [Last accessed on 3 Sep 2024]
43. Lo HK, Curty M, Qi B. Measurement-device-independent quantum key distribution. *Phys Rev Lett* 2012;108:130503. DOI
44. Lucamarini M, Yuan ZL, Dynes JF, Shields AJ. Overcoming the rate - distance limit of quantum key distribution without quantum repeaters. *Nature* 2018;557:400-3. DOI
45. Azuma K, Economou SE, Elkouss D, et al. Quantum repeaters: from quantum networks to the quantum internet. *Rev Mod Phys* 2023;95:045006. DOI
46. Chen TY, Jiang X, Tang SB, et al. Implementation of a 46-node quantum metropolitan area network. *npj Quantum Inf* 2021;7:134. DOI

47. Fröhlich B, Dynes JF, Lucamarini M, et al. A quantum access network. *Nature* 2013;501:69-72. DOI
48. Fan-Yuan GJ, Lu FY, Wang S, et al. Robust and adaptable quantum key distribution network without trusted nodes. *Optica* 2022;9:812-23. DOI
49. Chen YA, Zhang Q, Chen TY, et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature* 2021;589:214-19. DOI
50. Grünenfelder F, Boaron A, Resta GV, et al. Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems. *Nat Photonics* 2023;17:422-26. DOI
51. Sax R, Boaron A, Boso G, et al. High-speed integrated QKD system. *Photon Res* 2023;11:1007-14. DOI
52. Huang C, Chen Y, Luo T, et al. A cost-efficient quantum access network with qubit-based synchronization. *Sci Chi Phys Mechan Astron* 2024;67:240312. DOI
53. Matsuura T, Maeda K, Sasaki T, Koashi M. Finite-size security of continuous-variable quantum key distribution with digital signal processing. *Nat Commun* 2021;12:252. DOI
54. Chen Z, Wang X, Yu S, Li Z, Guo H. Continuous-mode quantum key distribution with digital signal processing. *npj Quantum Inf* 2023;9:28. DOI
55. Bernstein DJ, Lange T. Post-quantum cryptography. *Nature* 2017;549:188-94. DOI
56. Renner R, Wolf R. The debate over QKD: a rebuttal to the NSA's objections. arXiv. [Preprint.] Jul 27, 2023 [accessed 2024 Sep 9]. Available from: <https://arxiv.org/abs/2307.15116>.
57. Brauer M, Vicente RJ, Buruaga JS, et al. Linking QKD testbeds across Europe. *Entropy* 2024;26:123. DOI