Received: 3 July 2023 | Revised: 11 August 2023 | Accepted: 27 August 2023

IET Quantum Communication

DOI: 10.1049/qtc2.12073

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH

Towards quantum-secure software defined networks

Mohammad Reza Nosouhi[1] | Keshav Sood[1] | Vinay Chamola[2] | Jongkil Jay Jeong[1] | Anuroop Gaddam[3]

[1]Centre for Cyber Resilience and Trust (CREST), School of Information Technology, Deakin University, Burwood, Australia

[2]EEE Department, BITS Pilani, Rajasthan, India

[3]School of Information Technology, Deakin University, Burwood, Australia

Correspondence

Vinay Chamola and Mohammad Reza Nosouhi. Email: vinay.chamola@pilani.bits-pilani.ac.in and m.nosouhi@deakin.edu.au

Funding information

SEBE Faculty, Deakin University, PRESS 2021 Internal Grant Scheme

Abstract

The evolution of quantum computers is considered a serious threat to public-key cryptosystems (e.g. RSA, ECDSA, ECDH, etc.). This is indeed a big concern for security of the Internet and other data communication and storage systems. The reason is that public-key schemes are the basis in the generation of shared symmetric keys that are used to perform data encryption/decryption in communication and data transfer protocols. One possible approach to address this issue is to use Quantum Key Distribution (QKD) (instead of public-key schemes) for the ultra-secure generation of symmetric keys. QKD is a physical layer technology that allows two parties (equipped with optical communication interfaces) to generate secure random keys over a quantum channel that is immune to eavesdropping threats. The keys are then used by symmetric encryption schemes (e.g. AES) to encrypt data over classical channels. This allows us to have data encryption/decryption without needing a public-key scheme. However, due to its inherent characteristics, the implementation of QKD has mostly been considered in particular contexts only (e.g. backhaul networks, point-to-point connections, optical networks, etc.). This indeed limits the utility of QKD technology to only some particular applications while it has the potential to be used in a wide range of used cases. Motivated by this (increasing the usability of QKD technology), in this study, the authors propose a model that enables SDN-based networks to utilise QKD technology and provide QKD security service (i.e., random key generation service) to network applications and security protocols in a practical and efficient way. In the proposed approach, secret keys are generated based on the distribution of quantum entanglement between QKD nodes deployed in the network. The significant characteristic of our proposed model is that it does not rely on quantum repeaters to operate. This also improves the efficiency of the employed QKD mechanisms in terms of the key generation rate.

KEYWORDS

public key cryptography, quantum communication, quantum computing, quantum cryptography, quantum entanglement, quantum information, quantum noise, quantum optics

1 | INTRODUCTION

Public-key cryptosystems are an essential component of the currently used security protocols (e.g. SSL, TLS, SSH, digital sig-natures, etc). They are mostly used for the secure exchange of symmetric keys between two communicating parties, thus, playing a critical role in network security. However, it has been proven that the commonly used public-key cryptosystems are insecure in the post-quantum era [1–4]. The reason is that the security of these public key schemes relies on the difficulty of mathematical problems (i.e. integer factorisation or discrete logarithm problems) which are considered computationally hard in classical computation models [5]. However, it is shown that a quantum computer with enough resources will be able to solve these problems efficiently (in polynomial time) by running the relevant quantum algorithms [2] It should be

noted that such quantum algorithms have already been developed (i.e., Shor's algorithm [6] and Grover's algorithm [7]). However, the required quantum computation hardware that runs such algorithms does not exist yet. This is indeed a serious threat to the security of the Internet and other data communication and storage systems.

In this regard, the research community has been working on two separate approaches to address this issue. In the first approach, a lot of effort has been made to develop quantum-safe public-key and key exchange/encapsulation mechanisms [8–13]. These schemes will replace the currently used public-key cryptosystems in the future [5]. For instance, the National Institute of Standards and Technology is currently undertaking a standardisation project on post-quantum cryptography to standardise cryp-tosystems and key exchange mechanisms that are secure against quantum-enabled attacks [14, 15].

The second approach, on the other hand, attempts to utilise the laws of quantum physics to establish symmetric keys between two communicating parties in an ultra-secure way. This approach is based on quantum key distribution (QKD) which is in fact one application of quantum communication in the field of quantum cryptography [16, 17]. Quantum Key Distribution provides an information-theoretically safe solution to the key exchange problem [18]. It discusses the generation of shared secret keys between two parties via quantum signal transmission [19]. In fact, in QKD, the quantum physics properties of light are utilised by two communicating parties to generate a random secret encryption key that can be securely exchanged (shared) by them even in the presence of an eavesdropper (see Figure 1). The significant characteristic of QKD technology is that the two commu-nicating parties automatically detect it if the key generation process is being monitored by an eavesdropper [18]. The generated key is then used by both parties to encrypt/decrypt data. In simple words, QKD is deployed to support classical communications in terms of security, that is, the symmetric encryption key is regularly updated over ultra-secure quantum channels (e.g. once in a few seconds). The updated key is used to encrypt the data using a symmetric encryption scheme (e.g., AES). The encrypted data is then transmitted over a classical channel (see Figure 1). Note that with some increase in the key length, symmetric encryption schemes are quantum-safe. Thus, the whole package will be secure against quantum-enabled attacks.

The unique advantage of QKD is that if an adversary attempts to eavesdrop the quantum information in transit, their fragile quantum state collapses. This can be effectively detected by the receiver terminal, meaning that QKD is inherently secure against eavesdropping [20–22]. This is indeed a precious advantage that makes QKD a promising alternative of the currently used public-key cryptosystems.

However, there are two main restrictions that limit the adoption of QKD technology to particular scenarios only. Firstly, in QKD-based symmetric key generation, the two communicating parties need to be equipped with an optical interface to transmit and receive quantum information. This is because in quantum communications, the standard carriers are

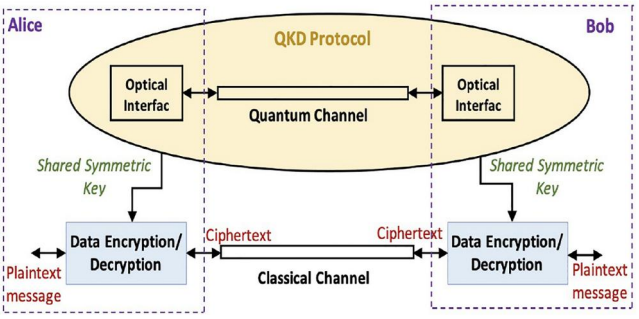

FIGURE 1 Simple illustration of quantum key distribution (QKD).

light photons that are transferred through either optical fibres or free space line-of-sight optical links (using laser interfaces).

Secondly, the two parties must communicate over a *point-to-point* quantum channel in order to generate the secret key. Although the deployment of quantum repeaters (QRs) can mitigate the second restriction to some extent, employing QRs can impose new technical challenges (regardless of additional costs) as they have their own limitations and technical issues [23, 24]. It is evident that the mentioned restrictions make the QKD technology adoptable in specific application scenarios only, for example, point-to-point connections, adhoc network structures, backhaul optical links etc., thus, prevent networks from taking advantage of the QKD technology at different layers of their structure in a post-quantum era [25].

To increase the usability of QKD technology, in this study, an abstraction model is proposed for SDN-enabled networks which provides QKD-based secret key generation service in such networks. In the proposed model, the QKD technology is integrated into a network architecture as a security service which enables the network management unit to provide quantum-safe secret key generation service to a wide range of network applications, virtual network functions (VNFs), and security protocols that rely on data encryption. In particular, using the proposed approach, two communicating parties can establish a shared secret key over a network where each party trusts its own local section of the network while the infrastructure between the two local sections may not be trusted.

In the proposed approach, we develop a QR-free model in which SDN-enabled QKD nodes are deployed at the physical layer of the network as hardware resources. On top of these resources, the network virtualisation layer coordinates the access to the QKD resources for VNFs and security protocols through the SDN virtualised infrastructure manager.

Moreover, in the proposed model, any pair of QKD nodes are able to collaboratively generate symmetric keys without needing any QRs. This is achieved through the adoption of an entanglement-based QKD solution in which a pair of entangled photons are shared between the two QKD nodes. After measuring the received photons, the two QKD nodes will obtain the same quantum state with a high probability that is used as the basis for the generation of a symmetric key. Using this approach, the number of required quantum channels between QKD nodes is significantly reduced. This makes the

proposed approach efficient in terms of both implementation costs and key generation rate. This is because deploying QRs in a QKD architecture reduces the ultimate rate of symmetric key generation [23]. Our contributions are as follows.

- We propose an abstraction model that enables the integration of QKD-based secret key generation service in SDN-enabeld networks. The proposed model provides quantum-safe key exchange as a security service that is the basis of quantum-secure networks.
- We further improve the proposed model by developing a QKD architecture that is QR-free. This modification not only results in cost efficiency but also increases the rate of symmetric key generation.

The rest of the paper is organised as follows. We introduce the proposed abstraction model in Section 2 and provide the results of our experiments along with some discussions in Section 3. Finally, Section 4 summarises the paper and provides the potential future work directions.

2 | THE PROPOSED ARCHITECTURE

In this section, we present our proposed abstraction model and describe the QR-free quantum key generation architecture. In our system model, we assume a pair of communicating parties that exchange data over a network. For the sake of security, the parties encrypt their data using a symmetric encryption scheme, thus, they need to share a symmetric key and update it regularly. In addition, the parties trust their local section of the network. However, they may not trust the infrastructure that connects the two local sections.

2.1 | Abstraction model

Generally, QKD protocols and systems have a complex structure, that is, they include different hardware modules and software subroutines. For a well-designed QKD-enabled network architecture, this complex structure must be hidden from upper layers. This allows the integration of different types of QKD systems into the network architecture.

Considering the standard SDN–NFV network architecture [26], the proposed abstraction model is shown in Figure 2. To better describe the model, we explain the network integration of hardware and software units of a QKD system separately. Firstly, the hardware components of the QKD system are integrated into the hardware resources of the SDN network. This integration must be taken place according to the relevant security considerations/recommendations provided by vendors/standard organisations (e.g. ETSI QKD Module Security Specification available in Ref. [27]). On top of the hardware resources, the virtualisation layer coordinates the access of virtualised network functions (VNFs) to the QKD hardware resources. The virtualised infrastructure manager (VIM) unit handles the virtualised hardware resources (i.e. virtualised infrastructure) in terms of management and orchestration (MANO) operations, for example, driver updates, change of configuration, firmware update etc. [28].

Secondly, the software subroutines of the QKD system are integrated into the model as VNFs to provide the QKD service for a separate unit that acts as an interface between the QKD system functions and other network functions (that rely on data encryption) or network security apps. We name this unit as Quantum Key Manager (QKM) that handles secure access to the QKD system. It can be implemented and integrated into the model either as a hardware entity or in the form of a security VNF. In both cases, the implementation must be performed based on a standard security specification (e.g. ETSI Implementation Security of Quantum Cryptography [29] or NIST's QKD recommendations [30]).

Based on this structure, the network integration of a QKD system from a different perspective is shown in Figure 3. As

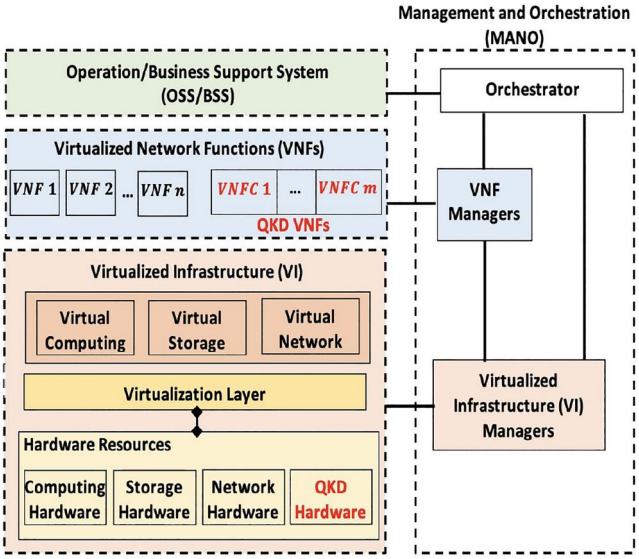

FIGURE 2 Integration of Quantum Key Distribution (QKD) service into the SDN–NFV standard architecture. The access of QKD-related Virtualised Network Functions (VNFs) to QKD hardware is securely managed using the VNF and VI mangers. This enables the network manager to securely share the QKD hardware between a range of QKD-specific VNFs that are involved in the provision of QKD service to different applications and security services in the network.

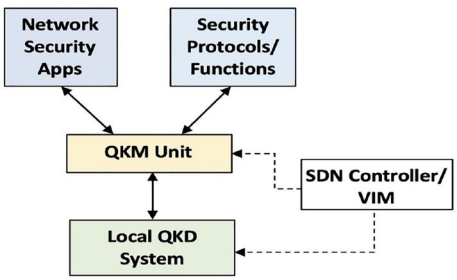

FIGURE 3 The Quantum Key Manager (QKM) unit handles different network security applications/protocols/functions that need the QKD service.

this figure shows, any network security application or any security protocol/function that needs the QKD service for data encryption is served by the QKM unit which takes the symmetric keys (generated over the quantum channel) from the QKD system and distribute/store/manage them to the relevant apps/protocols/functions. Note that each local QKD node is securely handled by its own QKM unit.

Depending on the type of the deployed QKD system, several individual VNFs might be created (based on different QKD subroutines) that are finally combined as individual VNF components (VNFCs) to create a super VNF that offers QKD service in the NFV environment. Similar to hardware integration, the design and integration of QKD-related VNFs must be accomplished in accordance with the security recommendations provided by vendors/organisations (e.g. Ref. [27]).

Regarding the positioning of SDN controllers, several configurations are possible. In this regard, we follow the first configuration recommended by ETSI [26] and consider SDN controllers as it is merged with the (VIM) unit. Note that adopting other configurations would (e.g. SDN controller is virtualised as a VNF). In fact, selecting the optimum position of SDN controllers is normally done based on the characteristics of each application scenario.

2.2 | The proposed QR-free architecture

As discussed before, we utilise the entanglement-based QKD approach to generate shared symmetric keys between two QKD nodes. Using this approach, we further adopt the star topology for QKD nodes to make the implementation of entanglement-based solution more efficient since it allows any pair of QKD nodes to collaboratively generate symmetric keys over their quantum channel.

In the proposed architecture, the central node of the star topology is defined as the Entangled Photon Distributor (EPD) node. It generates pairs of entangled photons that are then separated and sent to the two distant QKD nodes that want to generate a symmetric key (Figure 4). Each QKD node then receives one half of the pair of entangled photons over its quantum channel and measures its quantum state by choosing a random basis. Note that in quantum state measurement, the result of measurement depends on the basis selected by the measuring party (refer to Ref. [31] for more information about the measurement of quantum states). If both QKD nodes selected the same basis, they will obtain the same quantum state from their measurement which results in a shared random key (quantum states are decoded to bit values) as long as they have been really entangled. According to the laws of quantum physics, if an adversary who is eavesdropping on one of the quantum channels measures the quantum state of the relevant photon, the quantum state of that photon will change to a different state than the other half of the entangled pair of photons. Thus, the two QKD nodes will obtain different quantum states which makes them to disregard the bits decoded from this particular pair of photon.

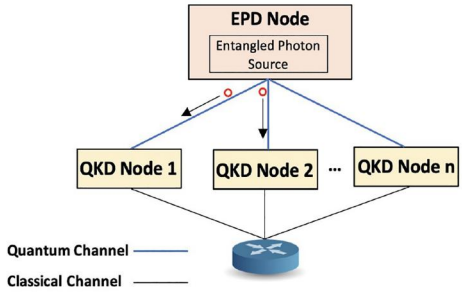

FIGURE 4 In the proposed QR-free architecture, the Entangled Photon Distributor (EPD) node generates entangled photons for every pair of Quantum Key Distribution (QKD) nodes that want to generate a shared key. The selected basis for quantum state measurement is exchanged between QKD nodes over the classical channel that does not need to be secure.

Note that the two QKD nodes need to communicate over a classical channel to inform each other about their selected basis. In fact, if they find that the same basis has been used by both of them, the bit value decoded from the measured quantum state is considered as one bit of the shared key. Note that they do not exchange the decoded bits. Instead, they just share the selected basis. This information brings no useful knowledge to an adversary, thus, it can be exchanged as a plaintext message over a classical channel.

3 | EVALUATIONS

In this section, we present the results of our experiments. We considered different scenarios in the experiments and compared Quantum Bit Error Rate (QBER) and Secret Key Rate (SKR) of each scenario. These are two critical metrics for the evaluation of a QKD system. We utilised the system model presented in Ref. [32] to model the QKD systems in MATLAB. In this model, QBER and SKR are obtained in the presence of destructive phenomena such as chromatic dispersion (CD) and inter symbol interference.

In our experiments, we changed the distance of quantum channels from 0.3 to 5 Km to measure QBER and SKR in two different scenarios. In the first scenario, the quantum channel (operating at wavelength 1551.7 nm with a loss of 0.2 dB/Km and dispersion 17 ps/nm/Km) coexisted with one classical channel operating at 1550.2 nm with a distance of 1.5 nm from the quantum channel. In the second scenario, we considered four classical channels operating at 1548.7, 1549.2, 1549.7 and 1550.2 nm with a distance of 1.5 nm from the quantum channel. Figure 5 shows the result.

As you see in the figures, increasing the length of quantum channel results in higher error rates in the process of key generation which reduces the overall rate of key generation. Note that the distance shown on the figures is the distance between EPD node and each individual QKD node. Thus, they should be doubled to obtain the actual distance between two QKD nodes since we considered the case when the QKD nodes are located at an equal distance to the EPD node.

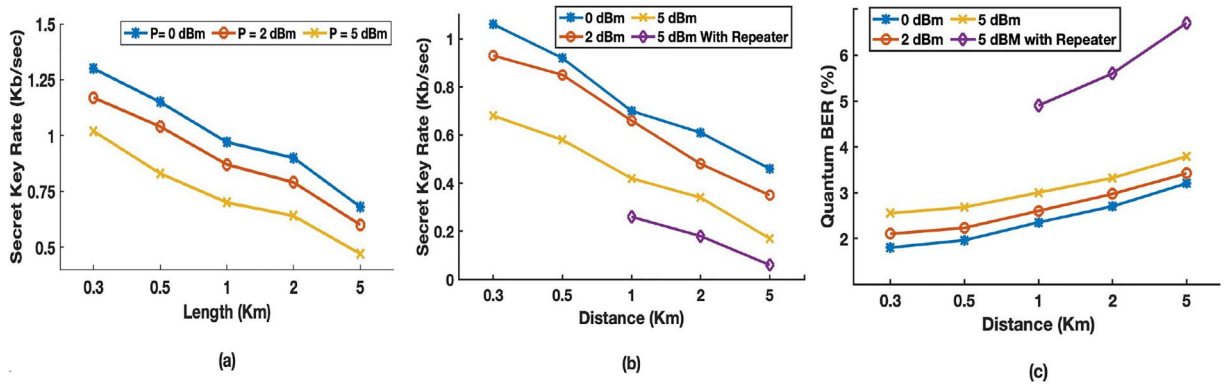

FIGURE 5 Secret Key Rate (SKR) of the Quantum Key Distribution (QKD) key generation when the quantum channel and (a) one classical channel (scenario 1) (b) four classical channels (scenario 2) operate at the same fibre link. (c) Quantum Bit Error Rate (QBER) of key generation with the quantum channel and one classical channel. As expected, employing a quantum repeater (QR) negatively affects the SKR and QBER.

Moreover, increasing the power has a negative impact on the key generation rate. This is mainly due to the effect of the deployed classical channels on the quantum channel. It is evident that increasing the number of classical channels (that operate over the same fibre) negatively impacts QBER and SKR. This is due to the noise leakage caused from the Raman scattering into the receiver circuits of QKD nodes.

Note that if the QKD system generates the secret keys at an average rate of R and assuming there are N network communications that need a symmetric key at the same time, the effective key generation rate allocated to each communication is R/N.

In addition, suppose the symmetric key generated for every communication is of length L and needs to be updated at the rate of U key/min. In this case, the QKD service can support network communications by updating their symmetric keys at the rate of $U = 60$ R/NL. This will be 0.47 key/min for a key size of 128 bit, if $R = 1$ Kb/sec and $N = 1000$.

4 | SUMMARY AND FUTURE WORK

In this study, an abstraction model and a QR-free architecture are proposed to enable the QKD security service in SDN networks. It is specifically proposed for scenarios in which two communicating parties need to share a secret key over a network where the parties trust their local section of the network, but the infrastructure between the two local sections may not be trusted. This approach allows quantum-safe symmetric encryption schemes to work using the ultra-secure symmetric keys generated by the QKD service. In the proposed approach, secret keys are generated based on the distribution of quantum entanglement between QKD nodes deployed in the network. The proposed architecture has a simple architecture and does not rely on QRs to operate. In the future, we intend to investigate the utilisation of space-based QKD systems in SDN-enabled IoT networks in which fibre-based QKD solutions may not be efficient in terms of the key generation rate. This would enable the QKD service in wide-area IoT networks that extend over large geographic areas.

AUTHOR CONTRIBUTIONS

Mohammad Reza Nosouhi: Conceptualisation; Writing – original draft. **Keshav Sood**: Conceptualisation; Writing – original draft. **Vinay Chamola**: Conceptualisation; Writing – review & editing. **Jongkil Jay Jeong**: Writing – review & editing. **Anuroop Gaddam**: Writing – review & editing.

ACKNOWLEDGEMENTS

This project is partially funded by SEBE Faculty, Deakin University, PRESS 2021 Internal Grant Scheme issued to Dr. Keshav Sood.

CONFLICT OF INTEREST STATEMENT

The authors have no conflicts of interest to declare. All co-authors have seen and agree with the contents of the manuscript, and there is no financial interest to report. We also certify that the submission is original work and is not under review at any other publication.

DATA AVAILABILITY STATEMENT

There is no data availability statement.

ORCID

Mohammad Reza Nosouhi https://orcid.org/0000-0001-6959-0975
Keshav Sood https://orcid.org/0000-0002-2127-1438
Vinay Chamola https://orcid.org/0000-0002-6730-3060
Jongkil Jay Jeong https://orcid.org/0000-0003-3491-687X

REFERENCES

1. Joseph, D., et al.: Transitioning organizations to post-quantum cryptography. Nature 605(7909), 237–243 (2022). https://doi.org/10.1038/s41586-022-04623-2
2. Mosca, M.: Cybersecurity in an era with quantum computers: will we be ready? IEEE Security & Privacy 16(5), 38–41 (2018). https://doi.org/10.1109/msp.2018.3761723
3. Bernstein, D.J., Lange, T.: Post-quantum cryptography. Nature 549(7671), 188–194 (2017). https://doi.org/10.1038/nature23461
4. Chamola, V., et al.: Information secu-rity in the post quantum era for 5g and beyond networks: threats to existing cryptography, and post-quantum cryptography. Comput. Commun. 176, 99–118 (2021). https://doi.org/10.1016/j.comcom.2021.05.019

5. Nosouhi, M.R., et al.: Bit flipping key encapsulation for the post-quantum era. IEEE Access 11, 56181–56195 (2023). https://doi.org/10.1109/access.2023.3282928
6. Shor, P.W.: Algorithms for quantum computation: discrete logarithms and fac-toring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science, pp. 124–134 (1994)
7. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Pro-Ceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, pp. 212–219 (1996)
8. Kumar, A., et al.: Securing the future internet of things with post-quantum cryptography. Security and Privacy 5(2), e200 (2022). https://doi.org/10.1002/spy2.200
9. Bavdekar, R., et al.: Post quantum cryptography: a review of techniques, challenges and standardizations. In: 2023 International Conference on Information Networking (ICOIN), pp. 146–151 (2023)
10. Baldi, M., Santini, P., Cancellieri, G.: Post-quantum cryptography based on codes: state of the art and open challenges. In: 2017 AEIT International Annual Conference, pp. 1–6 (2017)
11. Seyhan, K., et al.: Lattice-based Cryptosys-Tems for the Security of Resource-Constrained Iot Devices in Post-quantum World: A Survey, pp. 1–20. Cluster Computing (2021)
12. Misoczki, R., et al.: Mdpc-mceliece: new mceliece variants from moderate density parity-check codes. In: 2013 IEEE International Symposium on Information Theory. (IEEE), pp. 2069–2073 (2013)
13. Alkim, E., et al.: Post-quantum key exchange—a new hope. In: 25Th USENIX Security Symposium (USENIX)
14. NIST post-quantum cryptography project. Available from: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography. Accessed 10 March 2023
15. Alagic, G., et al.: Status Report on the Second Round of the Nist Post-quantum Cryptography Standardization Process. US Department of Commerce (2020). NIST
16. Sharma, P., et al.: Quantum key distribution secured optical networks: a survey. IEEE Open J. Commun. Soc. 2, 2049–2083 (2021). https://doi.org/10.1109/ojcoms.2021.3106659
17. Hassija, V., et al.: Forthcom-ing applications of quantum computing: peeking into the future. IET Quan. Commun. 1(2), 35–41 (2020). https://doi.org/10.1049/iet-qtc.2020.0026
18. Kasliwal, K., et al.: Enhancing Satellite-To-Ground Commu-Nication Using Quantum Key Distribution. IET Quantum Communication (2023)
19. Yuen, H.P.: Security of quantum key distribution. IEEE Access 4, 724–749 (2016). https://doi.org/10.1109/access.2016.2528227
20. Cao, Y., et al.: The evolution of quantum key distribution networks: on the road to the qinternet. IEEE Commun. Surv. & Tutorials 24(2), 839–894 (2022). https://doi.org/10.1109/comst.2022.3144219
21. Zhang, Q., et al.: Large scale quantum key distribution: challenges and solutions. Opt Express 26(18), 24260–24273 (2018). https://doi.org/10.1364/oe.26.024260
22. Hassija, V., et al.: Present landscape of quantum computing. IET Quan. Commun. 1(2), 42–48 (2020). https://doi.org/10.1049/iet-qtc.2020.0027
23. Lucamarini, M., et al.: Overcoming the rate– distance limit of quantum key distribution without quantum repeaters. Nature 557(7705), 400–403 (2018). https://doi.org/10.1038/s41586-018-0066-6
24. Liorni, C., Kampermann, H., Bruß, D.: Quantum repeaters in space. New J. Phys. 23(5), 053021 (2021). https://doi.org/10.1088/1367-2630/abfa63
25. Aguado, A., et al.: The engineering of software-defined quantum key distribution networks. IEEE Commun. Mag. 57(7), 20–26 (2019). https://doi.org/10.1109/mcom.2019.1800763
26. 'Sdn in nfv architectural framework'. Accessed 15 March 2023. Available from: https://sdn.ieee.org/newsletter/may-2016/sdn-in-nfv-architectural-framework
27. Etsi qkd module security specification. Accessed 15 March 2023. Available from: https://www.etsi.org/deliver/etsi_gs/qkd/001_099/008/01.01.01_60/gs_qkd008v010101p.pdf
28. Sood, K., et al.: Alleviating heterogeneity in sdn-iot networks to maintain qos and enhance security. IEEE Internet Things J. 7(7), 5964–5975 (2020). https://doi.org/10.1109/jiot.2019.2959025
29. 'Etsi implementation security of quantum cryptography'. Accessed 15 March 2023. Available from: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp27_qkd_imp_sec_FINAL.pdf
30. Mink, A., Frankel, S., Perlner, R.: Quantum key distribution (qkd) and commodity security protocols: introduction and integration', arXiv preprint arXiv:10040605, 2010
31. Rieffel, E.G., Polak, W.H.: Quantum Computing: A Gentle Introduction. MIT Press (2011)
32. Mlejnek, M., Kaliteevskiy, N.A., Nolan, D.A.: Modeling high quantum bit rate qkd systems over optical fiber. Quan. Tech. 2018 10674, 1067416 (2018). International Society for Optics and Photonics

How to cite this article: Nosouhi, M.R., et al.: Towards quantum-secure software defined networks. IET Quant. Comm. 5(1), 66–71 (2024). https://doi.org/10.1049/qtc2.12073