We are IntechOpen,
the world's leading publisher of
Open Access books
Built by scientists, for scientists

4,800
Open access books available

122,000
International authors and editors

135M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities

CLARIVATE ANALYTICS
BOOK CITATION INDEX
INDEXED

WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com

Quantum Key Distribution (QKD) over Software-Defined Optical Networks

Yongli Zhao, Yuan Cao, Xiaosong Yu and Jie Zhang

Abstract

Optical network security is attracting increasing research interest. Currently, software-defined optical network (SDON) has been proposed to increase network intelligence (e.g., flexibility and programmability) which is gradually moving toward industrialization. However, a variety of new threats are emerging in SDONs. Data encryption is an effective way to secure communications in SDONs. However, classical key distribution methods based on the mathematical complexity will suffer from increasing computational power and attack algorithms in the near future. Noticeably, quantum key distribution (QKD) is now being considered as a secure mechanism to provision information-theoretically secure secret keys for data encryption, which is a potential technique to protect communications from security attacks in SDONs. This chapter introduces the basic principles and enabling technologies of QKD. Based on the QKD enabling technologies, an architecture of QKD over SDONs is presented. Resource allocation problem is elaborated in detail and is classified into wavelength allocation, time-slot allocation, and secret key allocation problems in QKD over SDONs. Some open issues and challenges such as survivability, cost optimization, and key on demand (KoD) for QKD over SDONs are discussed.

Keywords: optical network, SDON, security, QKD, architecture, resource allocation

1. Introduction

As more than two billion kilometers of optical fibers deployed worldwide [1], optical networks have currently served as one of the most important underlying infrastructures. Large confidential data transferred daily over the Internet relies on the secrecy and reliability of data channels (DChs) in optical networks against several types of cyberattacks, e.g., physically tapping or listening to the residual crosstalk from an adjacent channel [2, 3]. With the evolution of network intelligence, software-defined networking (SDN) [4] is emerging and developing toward practical application, which is a promising technique to add flexibility and programmability in the optical layer. Hence, software-defined optical networking (SDON) is potential to become the next generation optical network architecture [5]. However, the control and configuration signaling messages transferred via the control channels (CChs) are also facing a variety of security attacks, e.g., anomaly attacks and intrusion attacks [6]. Therefore, two essential channels (i.e., DChs transferring sensitive data/services and CChs interchanging control/configuration messages) are vulnerable to cyberattacks in SDONs.

Data encryption is an effective way to enhance the security of SDONs. However, classical key distribution methods are based on the mathematical and computational complexities, which will suffer from increased computational power and developed quantum computing in the near future [7]. Quantum key distribution (QKD) is a promising technique to secure key exchange and protect communications from security attacks in SDONs [8]. It can achieve information-theoretic security based on the fundamentals of quantum physics, such as the Heisenberg uncertainty principle and quantum no-cloning theorem [9, 10]. Moreover, these fundamentals guarantee that the senders or receivers can detect the presence of any third party who is trying to obtain the secret keys. Optical fibers can be used in QKD systems to achieve good transmission performance of quantum signals. Nevertheless, the dark fibers utilized for QKD systems are inconvenient and expensive, while a potential solution is to use wavelength division multiplexing (WDM) technique for QKD integration in existing optical networks [11]. A lot of experiments and field trials have demonstrated the feasibility and practicability of integrating QKD into optical networks [12–18]. Therefore, based on above works, the objective of this chapter is to find how to deploy and employ QKD to enhance the security of SDONs.

2. Basic principles and enabling technologies of QKD

2.1 Principle of point-to-point QKD

The basic principle of point-to-point QKD is introduced based on the first invented QKD protocol, i.e., BB84 protocol proposed by Bennett and Brassard in 1984 [19], as illustrated in **Figure 1**. Nowadays, BB84 protocol is widely used in practical QKD systems [20, 21]. The BB84 protocol based QKD process is summarized in the following three stages.
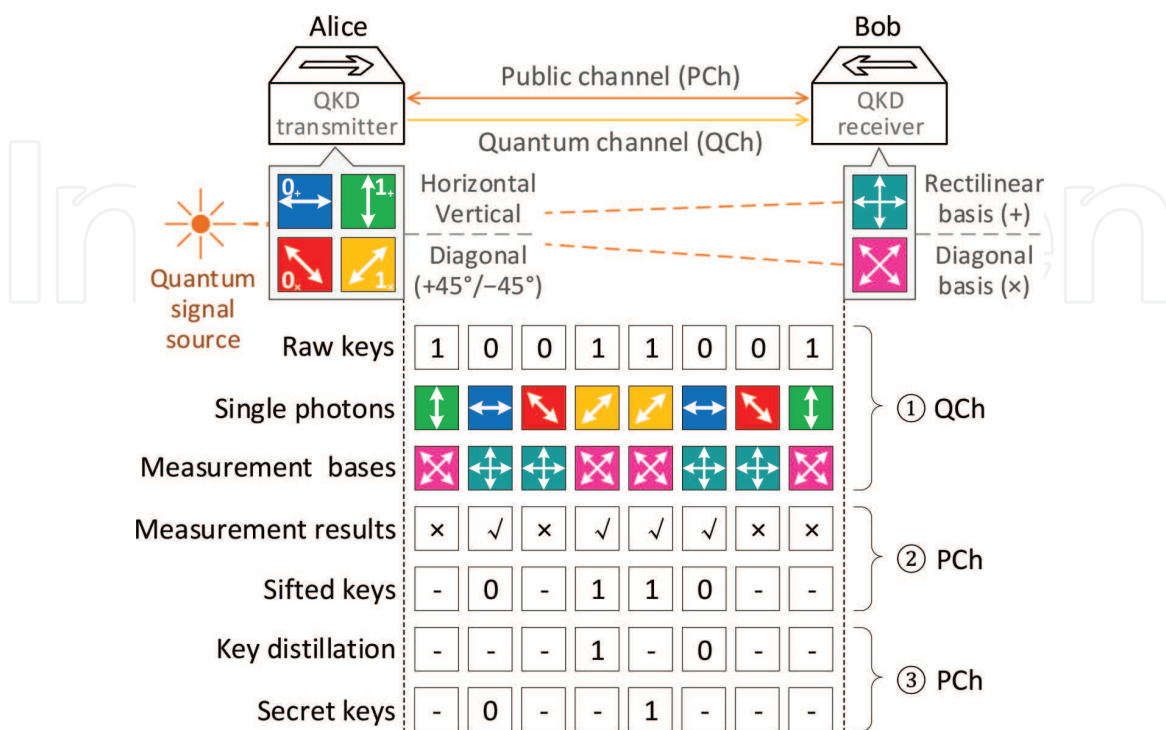

Figure 1.
Principle of point-to-point QKD based on BB84 protocol.

1. Qubit exchange: QKD transmitter (called Alice) generates qubits and sends them to the QKD receiver (called Bob) via a quantum channel (QCh). The qubits are generated by encoding a string of classical bits into single-polarization photons with different states. For instance, the horizontal, vertical, and diagonal ±45° polarization states randomly selected from two conjugate bases (i.e., rectilinear$_+$ and diagonal$_\times$) are encoded with 0_+, 1_+, $1_\times$, and $0_\times$, respectively. In order to achieve accurate qubit synchronization, a clock channel is also required here. Bob receives the incoming qubits and measures each single-polarization photon with one of the two conjugate bases (i.e., rectilinear$_+$ and diagonal$_\times$), and it will record the measurement results and the selected bases.

2. Key sifting: Alice and Bob exchange their selected bases via a pubic channel (PCh), and then discard the qubits sent and measured with different conjugate bases. The remaining qubits will be decoded into a string of classical bits as sifted keys.

3. Key distillation: For error estimation and correction, a random substring of classical bits in sifted keys is exchanged and compared between Alice and Bob via the PCh. Finally, privacy amplification and authentication are implemented to decide the remaining secure bits as secret keys.

Additionally, to improve the secret key rate in QKD systems in practice, decoy-state can be integrated with BB84 protocol to basically reach the single-photon sources performance and estimate the number of single-polarization photons detected by Bob more precisely [8].

2.2 Trusted repeaters for distance extension

The secret key rate and distance of QKD are limited due to the attenuation of weak quantum signals in QChs. This limitation can be overcome by using quantum repeaters, but they are beyond any practical technologies today [22]. A compromise and a practical solution to this challenge are using trusted repeaters, and this technique has been applied in the deployment of most QKD networks up to date [23–25]. In a QKD network based on trusted repeaters, the secret keys generated on the first QKD link can be relayed to the destination node by encrypting them with the secret keys generated in the intermediate nodes. One-time pad algorithm is applied for encryption to ensure the information-theoretic security of secret keys verified by Shannon [26], while the size of secret keys generated and encrypted here should be the same. Hence, secret keys are known by all intermediate nodes, making the secret key secure only as long as all the repeaters are trusted.

An example of QKD distance extension based on a trusted repeater between the source and destination nodes is illustrated in **Figure 2**. The QKD transmitter in the source node establishes a QKD link with the forthcoming QKD receiver in the intermediate node, whereas the QKD receiver in the destination node establishes a QKD link with the previous QKD transmitter in the intermediate node. Both QKD links produce, independently, secret keys Sk_1 and Sk_2 with the same key size. Then, the secret key Sk_1 is encrypted with the secret key Sk_2 and relayed to the destination node. Specifically, secret key Sk_1 can be used later to secure communications between the source and destination nodes. This relay process can continue with any amount of intermediate nodes, but each intermediate node with the trusted repeater will know the secret key information.
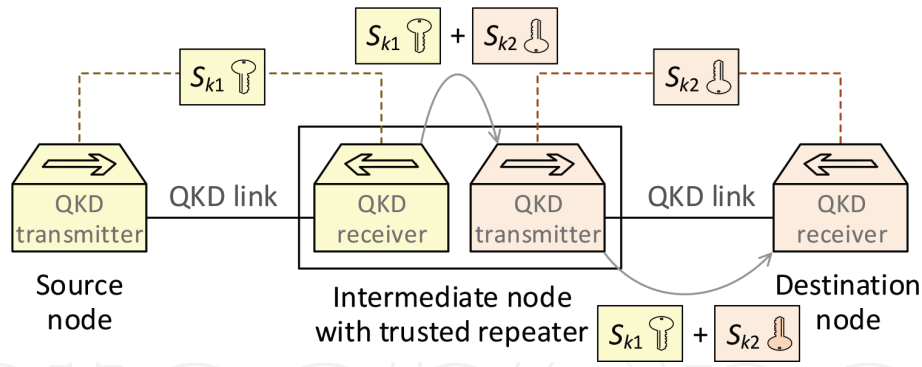
Figure 2.
An example of QKD distance extension based on a trusted repeater between the source and destination nodes.
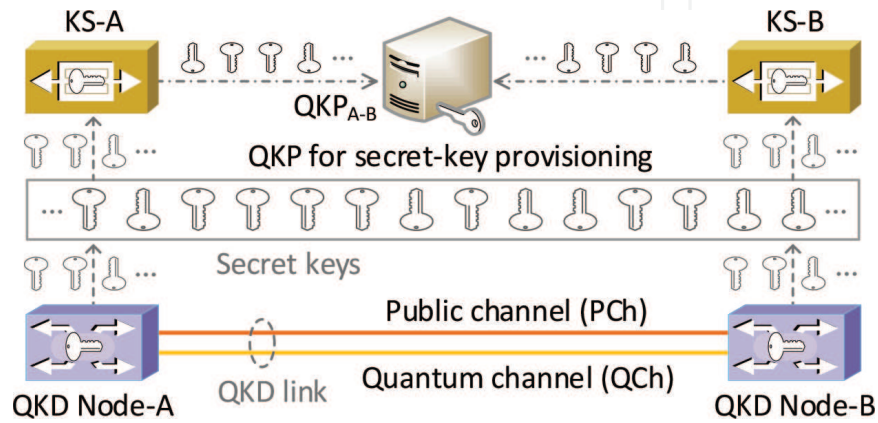

Figure 3.
An example of QKP for secret key provisioning between Node-A and Node-B.

2.3 Quantum key pool (QKP) for secret key provisioning

Currently, the secret key rate in most QKD systems can only reach 1–2 Mbit/s over a 50 km fiber link [27]. Therefore, the efficient management of precious secret key resources is important. Recently, quantum key pool (QKP) technique is proposed in QKD networks to timely provision secret keys for satisfying the security demands of communications crossing the networks [6], which is beneficial to enhance secret key management when the QKD develops from point-to-point links to networks. The secret keys generated between the two end nodes can be stored in the key store (KS) which is embedded in each of the two end-nodes and can be managed by a QKP. QKP will know the real-time remaining number of secret keys in the KS, which can decide when to connect the QKD link for secret key provisioning. Hence, efficient QKP construction is beneficial for efficiently employing QKD.

An example of QKP between Node-A and Node-B is illustrated in **Figure 3**. The QKD node is composed of several components based on the existing QKD technologies, e.g., QKD transceiver, trusted repeater, and switch [23]. The generated secret keys between QKD Node-A and QKD Node-B can be stored in KS-A and KS-B, which are embedded in Node-A and Node-B, respectively. Specifically, the generated secret keys are managed by QKP_{A-B} to monitor the real-time remaining number of secret keys and provision secret keys between Node-A and Node-B.

3. QKD over SDON Architecture

An architecture of QKD over SDONs is illustrated in **Figure 4(a)**, which consists of four layers from top to bottom: application (App) layer, control layer, QKD layer,
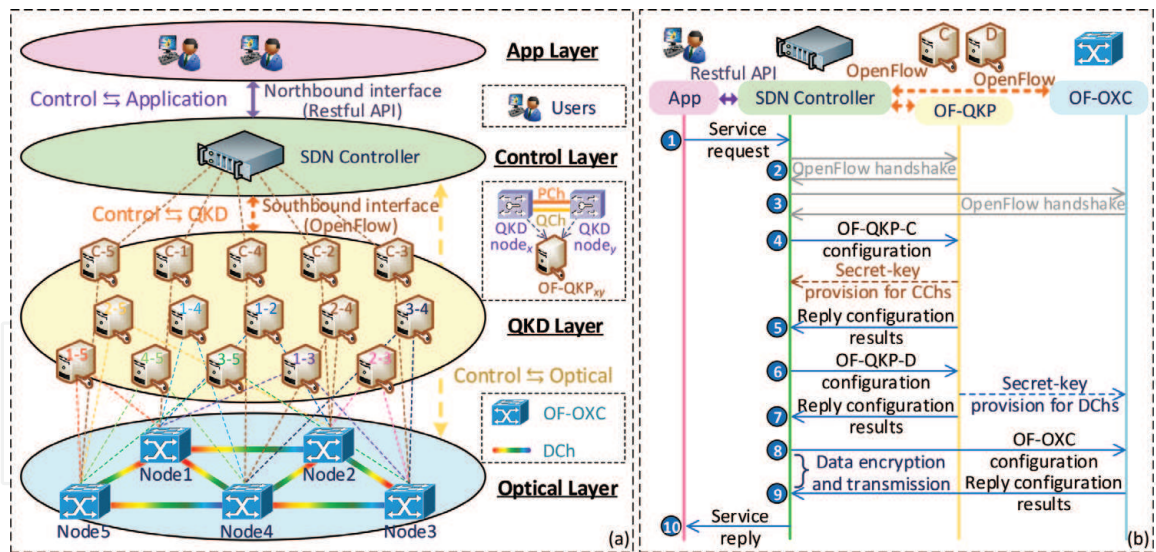
Figure 4.
(a) QKD over SDON architecture; and (b) the configuration signaling procedure.

and optical layer. This architecture is different from the previous QKD-integrated
optical networks [11] and decouples QKD layer from the optical layer via construct-
ing several QKPs in the QKD layer. Two types of QKPs are constructed to enhance
the security of control signaling messages over the CChs, and confidential data
services over the DChs, respectively. The QKP between the SDN controller and
each node is called QKP-C (i.e., QKP-CCh), whereas the QKP between two nodes
is called QKP-D (i.e., QKP-DCh). The SDN controller in the control layer controls
and manages the QKD layer and optical layer via the southbound interface protocol
(e.g., OpenFlow and NETCONF). Here we use OpenFlow protocol as an example.
The SDN controller is capable of realizing flexible and programmable global opti-
cal network management, which can be utilized as the effective implementation
technique for control layer. Moreover, it has been demonstrated in the recent study
on time-shared QKD resources in SDN-controlled optical networks [28].

Optical layer and QKD layer can share the fiber bandwidth resources from exist-
ing WDM networks, in which at least two wavelengths need to be utilized as QCh
and PCh to construct OpenFlow-enabled QKPs (OF-QKPs), and then the remaining
wavelength resources can be utilized to transport confidential data services. The
constructed OF-QKPs can provision secret keys to guarantee the security of CChs
and DChs. In addition, OpenFlow-enabled optical cross connects (OF-OXCs) are
placed in the optical layer. The SDN controller is capable of managing the entire
network efficiently, whereas the OF-QKPs and OF-OXCs are capable of operating
based on the instructions from SDN controller.

The App layer generates service requests with different security demands and
interacts with control layer via the Restful API, in which Restful API is applied as
northbound interface protocol. Based on the different security demands, CChs and
DChs may require different number of secret keys. In particular, this QKD over
SDON architecture can manage and control the network-wide secret key resources,
which is beneficial to adapt diverse security demands and dynamic scenarios.

Figure 4(b) illustrates the configuration signaling procedure among the four
layers in QKD over SDON architecture. This procedure can be described in the
following five stages: (1) upon receiving a service request (e.g., the service request
from Node 1 to Node 2) from the App, SDN controller first computes/selects
path and then implements OpenFlow handshake with related OF-OXCs as well as
OF-QKPs on the selected path; (2) after the establishment of first stage, OF-QKP-C_1
and OF-QKP-C_2 are configured by the SDN controller to provision secret keys for

control/configuration messages over the CChs; (3) OF-QKP-D$_{1-2}$ is configured by the SDN controller to provision secret keys for the service request from OF-OXC$_1$ to OF-OXC$_2$ over the DCh; (4) the SDN controller configures OF-OXC$_1$ and OF-OXC$_2$ to encrypt data and transport the service; and (5) at last, SDN controller replies to the App.

4. Resource allocation in QKD over SDONs

4.1 Wavelength allocation

Since three types of channels (i.e., QChs, PChs, and DChs) are coexisting in a single fiber with WDM technique, wavelength allocation for these three types of channels becomes an essential issue. The total number of wavelengths for QChs, PChs, and DChs should conform to existing WDM networks, e.g., 40 wavelengths (with 100 GHz channel spacing) or 80 wavelengths (with 50 GHz channel spacing). Given the DCh is usually located at C-band (1530–1565 nm) in existing WDM networks, some previous studies have demonstrated QKD at O-band (1260–1360 nm) [29, 30] to achieve strong isolation from data transmission. Nevertheless, the faint quantum signals may suffer from more losses at O-band compared with C-band, which will limit the transmission distance and rate. Therefore, the three types of channels can be placed at C-band to achieve better quantum-signal transmission performance, as illustrated in **Figure 5**.

In particular, the physical layer impairments (e.g., Raman scattering and four-wave-mixing effects) induced by PCh and DCh may have negative impacts on the QCh transmission performance. Raman scattering effects can be effectively reduced by placing the QCh at high frequency [31], thereby the wavelength reserved as QCh starts from 1530 nm. Besides, four-wave-mixing effects can be reduced by allocating 200 GHz guard band between QCh and other classical channels (i.e., PChs and DChs) [17]. Moreover, appropriate channel isolation and stable QKD operation can be achieved by using multistage band-stop filtering technique [32]. The PCh that transmits classical signals for key sifting and distillation as introduced in the principle of point-to-point QKD can share the same wavelengths with DCh or utilize the dedicated wavelengths at fiber C-band. The latter can be selected to ensure one-to-one relationship between the PCh and QCh, although the wavelength resources for data transmission may be degraded. This is because allocating dedicated wavelengths for QCh and PCh is essential in a stable scenario. The intermediate nodes with trusted repeaters and erbium-doped fiber amplifiers (EDFAs) can be deployed for QCh and PCh/DCh, respectively, to extend quantum and classical signal transmission distance, in which EDFA bypass scheme [30, 33] can be utilized
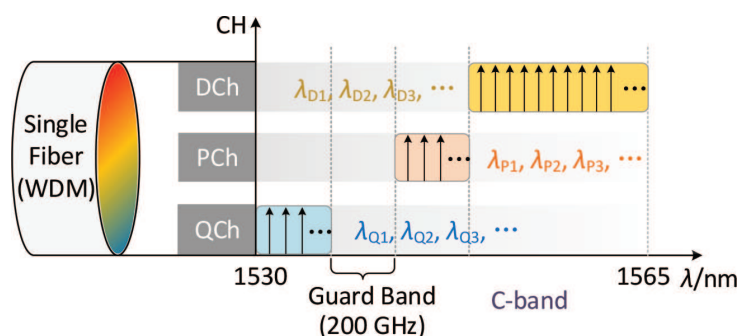

Figure 5.
Wavelength allocation for the three types of channels (i.e., QChs, PChs, and DChs) over the C-band in a single fiber.

for quantum and classical signal coexistence in a single fiber to suppress the noise from the EDFA's amplified spontaneous emission (ASE).

4.2 Time-slot allocation

Given the finite wavelength resources in a single fiber and the high cost of establishing QChs and PChs, each wavelength for QCh/PCh is segmented into multiple time slots according to optical time division multiplexing (OTDM) technique [34]. Hence, each time slot can be utilized to establish a QCh/PCh for improving resource utilization. We assume that the secret keys provisioned for a service request with specific security demand are exchanged between the source and destination nodes within a fixed time t, thereby each QCh/PCh occupies a time slot. On the basis of the principle of point-to-point QKD described above, t consists of channel estimation and calibration time, qubit exchange time, key sifting time, and key distillation time. In particular, the scattering and loss may impact the secret key rate between two nodes, which will lead to different number of secret keys shared between different node pairs within t in QKD over SDONs. In the network model, to fix t with a realistic and simplified manner, the size of t can be set as the secret key exchange time for a fixed key size (e.g., 128, 192, and 256 bit while using AES encryption algorithm [35]) under the worst scenario in QKD over SDONs.

Additionally, to prevent attacks for enhancing the data encryption security, the secret keys provisioned for each service request with specific security demand can be updated in a period T. The parameter, T, is the period after which the secret key must be changed between two nodes. The security level increases while decreasing the value of T. This is because the secret keys provisioned for a service request with specific security demand are updated more frequently, thereby increasing the difficulty of cracking the encryption key by a third party [36]. Accordingly, considering the key-updating period, time-slot allocation for QCh/PCh becomes a new topic to be studied. Also, routing, wavelength, and time-slot allocation (RWTA) strategy for establishing the three types of channels (i.e., QChs, PChs, and DChs) needs to be considered.

For instance, **Figure 6** illustrates two security level configuration solutions, in which the parameter, t, is the secret key exchange time between the source and destination nodes for each service request with specific security demand, and the parameter, T, is the key-updating period ($t < T$, which guarantees that the secret keys can be exchanged within a period). In solution 1, we fix T for all the QCh/PCh wavelengths and each service request with specific security demand has the same security level value of T. Note that the QCh/PCh wavelengths are the wavelengths in WDM optical networks that are reserved as QCh/PCh. The solution 1 can only provide one security level, which may limit the flexibility of security demands of service requests. However, service requests triggered from numerous security-hungry applications may have different security demands with different security levels. Hence, each QCh wavelength has a flexible T values in solution 2, thereby different security levels can be provisioned. For different service requests with security demands, this solution can provision more security level types.

4.3 Secret key allocation

Data encryption algorithms need to be considered for CChs and DChs while performing secret key allocation. One-time pad (OTP) encryption algorithm was invented to achieve information-theoretic security, in which the secret key size should be as long as the data size [26]. Hence, OTP encryption algorithm requires much execution time/storage to perform data encryption, which is difficult to be
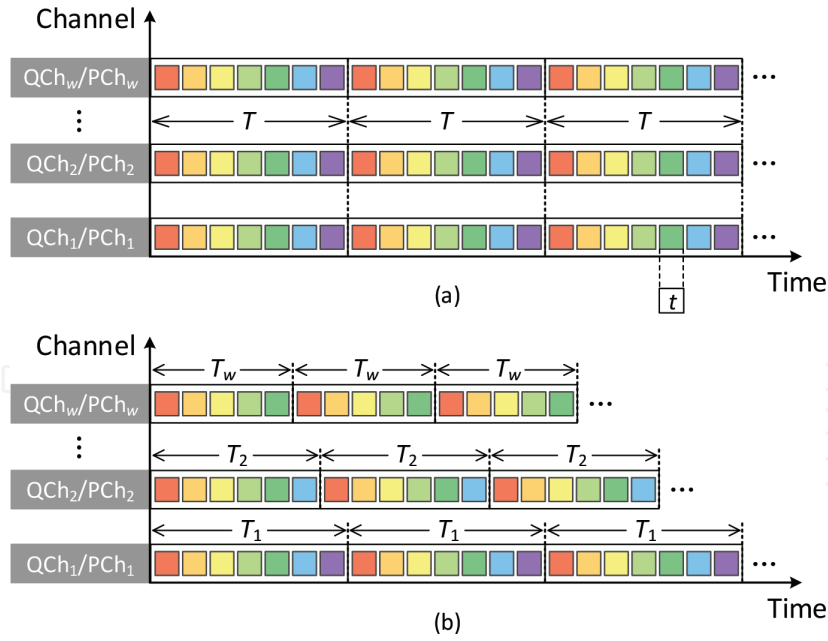
Figure 6.
Two security-level provisioning solutions: (a) solution 1: fixed T for all the QCh/PCh wavelengths; and (b) solution 2: flexible T for each QCh/PCh wavelength.

utilized for high-bit-rate data encryption in SDONs and has negative impacts on the efficiency of SDONs. Nevertheless, symmetric encryption algorithms [37] can be used to perform large amount of data encryption with small secret key size and fast execution time. A commonly used symmetric encryption algorithm is advanced encryption standard (AES) algorithm, which can be integrated with QKD to implement high-bit-rate data encryption [38, 39]. Using secret key lengths of 128, 192, and 256 bit, the AES algorithm can encrypt/decrypt large amount of data in blocks of 128 bit [35]. Hence, the secret key receiving module and data encryption module can be added in optical transport nodes to perform secret key communication and processing.

Nevertheless, the third party can eavesdrop a sequence of encrypted data to crack the secret keys while using AES algorithm. Then, two important factors, i.e., data size and data transmission time, need to be considered during a crack [40, 41]. In order to degrade the probability of encrypted data being cracked, the secret key can be frequently changed between two nodes based on the key-updating period. Key updating is essential to enhance the security of data encryption while using AES algorithm to secure CChs and DChs. Accordingly, the time complexity and data complexity of attacks can be considered for key updating in which time complexity is the maximum available time for a secret key and data complexity is the maximum encrypted data size by a secret key. The security level increases with the increase of secret key length or the decrease of secret key-updating period. Therefore, we can qualitatively evaluate the security level based on secret key length and updating period.

Given the secret key resources are limited and precious in QKPs, the secret key allocation issue for CChs and DChs needs to be solved. The control/configuration messages crptsmitted over the CChs in SDONs are usually at megabit-per-second transmission rate, which are low compared with the data complexity of attacks [40]. Accordingly, secret key allocation and updating are accomplished for each CCh in the SDON to enhance its security. Through the path of a data service, each node along the path will be configured by the SDN controller via the corresponding CCh. According to the specific security demand of each CCh, QKP-C allocates the required secret keys between SDN controller and each node to enhance the security
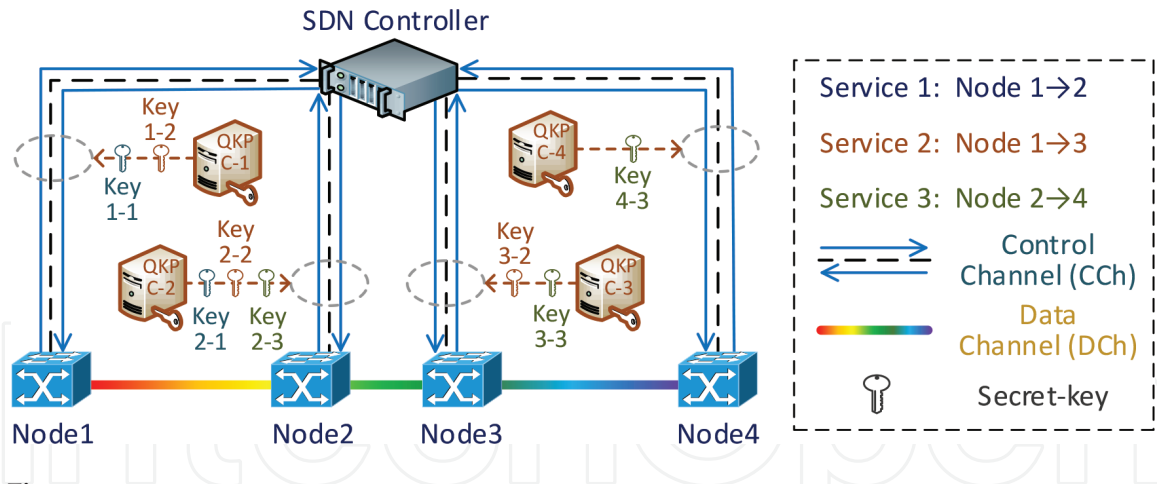
Figure 7.
Secret key allocation and updating for CChs.

of each CCh. Hence, we can allocate different number of secret keys to CChs between SDN controller and each node for encrypting/decrypting the control/configuration messages. As illustrated with an example in **Figure 7**, Keyx_y denotes the required number of secret keys in which x and y represent the node serial number and service serial number, respectively. Key$_{1-1}$/Key$_{2-1}$ is allocated to CChs between the SDN controller and Node 1/Node 2 for Service 1, whereas Key$_{1-2}$/Key$_{2-2}$/Key$_{3-2}$ is allocated to CChs between the SDN controller and Node 1/Node 2/Node 3 for Service 2.

The required number of secret keys for each data service over the DChs is associated with the secret key length and updating period. The QKP-D can allocate the required number of secret keys to enhance the security of data services over the DChs in SDONs. As illustrated with an example in **Figure 8**, three data services (i.e., r_1, r_2, and r_3) have different security demands. In **Figure 8(a)** and **(b)**, we consider the time complexity of attacks (i.e., T_y) and data complexity (i.e., D_y) of attacks for secret key updating, respectively, in which the parameter, y, represents the data service serial number. Based on AES algorithm, the required secret key lengths of r_1, r_2, and r_3 are 128, 192, and 256 bit, respectively. Additionally, as shown in **Figure 8(a)**, the required secret key-updating periods of r_1, r_2, and r_3 are T_1, T_2, and T_3 ($T_1 < T_2 < T_3$), respectively; whereas in **Figure 8(b)**, the required secret key-updating periods of r_1, r_2, and r_3 are D_1, D_2, and D_3 ($D_1 < D_2 < D_3$), respectively. Specifically, the data service with longer secret key length and shorter secret key-updating period demands shows higher security level and will require more secret keys to be allocated for data encryption. Thus, routing, wavelength, and secret key allocation (RWKA) strategy for CChs and DChs in a timely manner on demand is necessary to be considered.
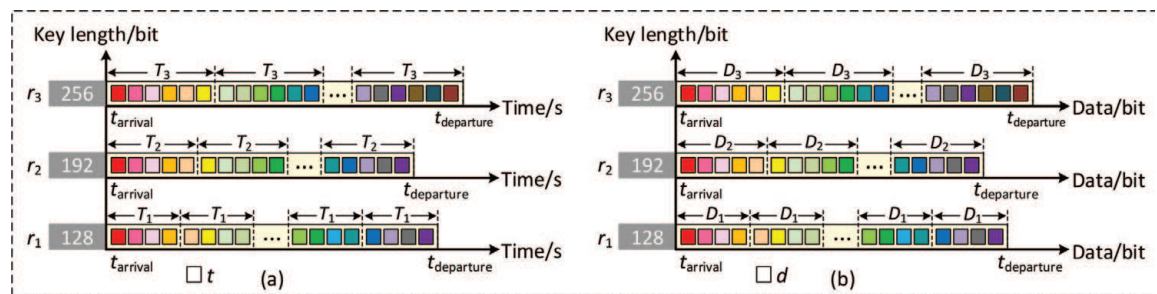

Figure 8.
Secret key allocation and updating for services with different security requirements based on (a) case 1: time complexity of attacks and (b) case 2: data complexity of attacks.

5. Open issues and challenges

5.1 Survivability for QKD over SDONs

QKD can provide secret keys for end-to-end paths and improve the security of SDONs. However, how to guarantee survivability in a QKD over SDON is an important topic. QCh and PCh should be protected simultaneously in a QKD over SDON. Especially due to the utilization of key-updating period (security level) with different time slots, protection action will occur at a subwavelength level. Synchronization might also be a difficult problem for QCh, PCh, and DCh.

5.2 Cost optimization for QKD over SDONs

In a QKD network, two types of nodes should be deployed, i.e., QKD node and intermediate node with trusted repeaters. Also, several wavelength channels in existing WDM optical networks should be planned as QChs and PChs. In practice, different number of nodes and QChs/PChs may produce different costs and performance for QKD over SDONs. Accordingly, how to optimize the cost of deploying QKD over SDONs while satisfying the performance requirements is another open issue.

5.3 Key on demand (KoD) for QKD over SDONs

The secret key rate (i.e., the generation of secret keys in bits per second) in current advanced QKD systems is extremely low compared with the gigabit data transmission over each wavelength in WDM optical networks. Increasing the number of nodes and QChs/PChs can further increase the secret key rate, but it will also drastically increase the system complexity and power consumption. Thus, the use of an efficient key on demand (KoD) scheme to achieve efficient secret key resource usage while satisfying security requirements of CChs and DChs is also essential for QKD over SDONs.

6. Conclusions

This chapter provides a brief introduction to the basic principles and enabling technologies of QKD. Based on the QKD-enabling technologies, an architecture of QKD over SDONs is presented. Resource allocation problem is elaborated in detail and is classified into wavelength allocation, time-slot allocation, and secret key allocation problems in QKD over SDONs. Finally, several open issues and challenges are discussed.

Author details

Yongli Zhao*, Yuan Cao, Xiaosong Yu and Jie Zhang
State Key Laboratory of Information Photonics and Optical Communications,
Beijing University of Posts and Telecommunications, Beijing, China

*Address all correspondence to: yonglizhao@bupt.edu.cn

IntechOpen

References

[1] Winzer PJ. Scaling optical fiber networks: Challenges and solutions. Optics & Photonics News. 2015;**26**(3):28-35. DOI: 10.1364/OPN.26.3.000028

[2] Fok MP, Wang Z, Deng Y, Prucnal PR. Optical layer security in fiber-optic networks. IEEE Transactions on Information Forensics and Security. 2011;**6**(3):725-736. DOI: 10.1109/TIFS.2011.2141990

[3] Skorin-Kapov N, Furdek M, Zsigmond S, Wosinska L. Physical-layer security in evolving optical networks. IEEE Communications Magazine. 2016;**54**(8):110-117. DOI: 10.1109/MCOM.2016.7537185

[4] Rawat DB, Reddy SR. Software defined networking architecture, security and energy efficiency: A survey. IEEE Communication Surveys and Tutorials. 2017; **19**(1):325-346. DOI: 10.1109/COMST.2016.2618874

[5] Zhao Y, He R, Chen H, Zhang J, Ji Y, et al. Experimental performance evaluation of software defined networking (SDN) based data communication networks for large scale flexi-grid optical networks. Optics Express. 2014;**22**(8):9538-9547. DOI: 10.1364/OE.22.009538

[6] Cao Y, Zhao Y, Colman-Meixner C, Yu X, Zhang J. Key on demand (KoD) for software-defined optical networks secured by quantum key distribution (QKD). Optics Express. 2017;**25**(22):26453-26467. DOI: 10.1364/OE.25.026453

[7] Schreiber LR, Bluhm H. Toward a silicon-based quantum computer. Science. 2018;**359**(6374):393-394. DOI: 10.1126/science.aar6209

[8] Lo HK, Curty M, Tamaki K. Secure quantum key distribution. Nature Photonics. 2014;**8**:595-604. DOI: 10.1038/nphoton.2014.149

[9] Maeda W, Tanaka A, Takahashi S, Tajima A, Tomita A. Technologies for quantum key distribution networks integrated with optical communication networks. IEEE Journal of Selected Topics in Quantum Electronics. 2009;**15**(6):1591-1601. DOI: 10.1109/JSTQE.2009.2032664

[10] Lo HK, Chau HF. Unconditional security of quantum key distribution over arbitrarily long distances. Science. 1999;**283**:2050-2056. DOI: 10.1126/science.283.5410.2050

[11] Cao Y, Zhao Y, Yu X, Wu Y. Resource assignment strategy in optical networks integrated with quantum key distribution. Journal of Optical Communications and Networking. 2017;**9**(11):995-1004. DOI: 10.1364/JOCN.9.000995

[12] Mao Y, Wang B-X, Zhao C, Wang G, Wang R, et al. Integrating quantum key distribution with classical communications in backbone fiber network. Optics Express. 2018;**26**(5):6010-6020. DOI: 10.1364/OE.26.006010

[13] Karinou F, Brunner HH, Fung C-HF, Comandar LC, Bettelli S, et al. Toward the integration of CV quantum key distribution in deployed optical networks. IEEE Photonics Technology Letters. 2018;**30**(7):650-653. DOI: 10.1109/LPT.2018.2810334

[14] Patel KA, Dynes JF, Lucamarini M, Choi I, Sharpe AW, et al. Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks. Applied Physics Letters. 2014;**104**(5):051123. DOI: 10.1063/1.4864398

[15] Zhao Y, Cao Y, Wang W, Wang H, Yu X, et al. Resource allocation in

optical networks secured by quantum key distribution. IEEE Communications Magazine. 2018;**56**(8):130-137. DOI: 10.1109/MCOM.2018.1700656

[16] Cao Y, Zhao Y, Wu Y, Yu X, Zhang J. Time-scheduled quantum key distribution (QKD) over WDM networks. Journal of Lightwave Technology. 2018;**36**(16):3382-3395. DOI: 10.1109/JLT.2018.2834949

[17] Peters NA, Toliver P, Chapuran TE, Runser RJ, McNown SR, et al. Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments. New Journal of Physics. 2009;**11**(4):045012. DOI: 10.1088/1367-2630/11/4/045012

[18] Qi B, Zhu W, Qian L, Lo HK. Feasibility of quantum key distribution through a dense wavelength division multiplexing network. New Journal of Physics. 2010;**12**(10):103042. DOI: 10.1088/1367-2630/12/10/103042

[19] Bennett CH, Brassard G. Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing; Bangalore, India; 1984

[20] QuantumCTek [Internet]. Available from: http://www.quantum-info.com/English/

[21] Toshiba QKD system [Internet]. Available from: https://www.toshiba.eu/eu/Cambridge-Research-Laboratory/Quantum-Information/Quantum-Key-Distribution/Toshiba-QKD-system/

[22] Elkouss D, Martinez-Mateo J, Ciurana A, Martin V. Secure optical networks based on quantum key distribution and weakly trusted repeaters. Journal of Optical Communications and Networking. 2013;**5**(4):316-328. DOI: 10.1364/JOCN.5.000316

[23] Peev M, Pacher C, Alléaume R, Barreiro C, Bouda J, et al. The SECOQC quantum key distribution network in Vienna. New Journal of Physics. 2009;**11**(7):075001. DOI: 10.1088/1367-2630/11/7/075001

[24] Sasaki M, Fujiwara M, Ishizuka H, Klaus W, Wakui K, et al. Field test of quantum key distribution in the Tokyo QKD network. Optics Express. 2011;**19**(11):10387-10409. DOI: 10.1364/OE.19.010387

[25] Wang S, Chen W, Yin Z-Q, Li H-W, He D-Y, et al. Field and long-term demonstration of a wide area quantum key distribution network. Optics Express. 2014;**22**(18):21739-21756. DOI: 10.1364/OE.22.021739

[26] Shannon CE. Communication theory of secrecy systems. Bell Labs Technical Journal. 1949;**28**(4):656-715

[27] Gleim AV, Egorov VI, Nazarov YV, Smirnov SV, Chistyakov VV, et al. Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference. Optics Express. 2016;**24**(3):2619-2633. DOI: 10.1364/OE.24.002619

[28] Aguado A, Hugues-Salas E, Haigh PA, Marhuenda J, Price AB, et al. Secure NFV orchestration over an SDN-controlled optical network with time-shared quantum key distribution resources. Journal of Lightwave Technology. 2017;**35**(8):1357-1362. DOI: 10.1109/JLT.2016.2646921

[29] Runser RJ, Chapuran TE, Toliver P, Goodman MS, Jackel J, et al. Demonstration of 1.3 μm quantum key distribution (QKD) compatibility with 1.5 μm metropolitan wavelength division multiplexed (WDM) systems." In: Proceedings of OFC/NFOEC; March 2005; Anaheim, California, United States. DOI: 10.1109/OFC.2005.192752. p. OWI2

[30] Nweke NI, Runser RJ, McNown SR, Khurgin JB, Chapuran TE, et al. EDFA bypass and filtering architecture enabling QKD+WDM coexistence on mid-span amplified links. In: Proceedings of CLEO/QELS; May 2006; Long Beach, California, United States. DOI: 10.1109/CLEO.2006.4628431. p. CWQ7

[31] Kawahara H, Medhipour A, Inoue K. Effect of spontaneous Raman scattering on quantum channel wavelength-multiplexed with classical channel. Optics Communications. 2011;**284**:691-696. DOI: 10.1016/j. optcom.2010.09.051

[32] Wang LJ, Chen LK, Ju L, Xu ML, Zhao Y, et al. Experimental multiplexing of quantum key distribution with classical optical communication. Applied Physics Letters. 2015;**106**(8):081108. DOI: 10.1063/1.4913483

[33] Aleksic S, Winkler D, Hipp F, Poppe A, Franzl G, Schrenk B. Towards a smooth integration of quantum key distribution in metro networks. In: Proceedings of ICTON; July 2014; Graz, Austria. DOI: 10.1109/ICTON.2014.6876369

[34] Wen B, Sivalingam KM. Routing, wavelength and time-slot assignment in time division multiplexed wavelength-routed optical WDM networks. In: Proceedings of INFOCOM; June 2002; New York, USA. pp. 1442-1450. DOI: 10.1109/INFCOM.2002.1019395

[35] National Institute of Standards and Technology (NIST). Advanced Encryption Standard (AES). Federal Information Processing Standard (FIPS) 197. Nov. 2001

[36] Taha M, Schaumont P. Key-updating for leakage resiliency with application to AES modes of operation. IEEE Transactions on Information Forensics and Security. 2015;**10**(3):519-528. DOI: 10.1109/TIFS.2014.2383359

[37] Jouguet P, Kunz-Jacques S, Debuisschert T, Fossier S, Diamanti E, et al. Field test of classical symmetric encryption with continuous variables quantum key distribution. Optics Express. 2012;**20**(13):14030-14041. DOI: 10.1364/OE.20.014030

[38] Eraerds P, Walenta N, Legr'e M, Gisin N, Zbinden H. Quantum key distribution and 1 Gbit/s data encryption over a single fibre. New Journal of Physics. 2010;**12**(6):063027. DOI: 10.1088/1367-2630/12/6/063027

[39] Sharma G, Kalra S. A novel scheme for data security in cloud computing using quantum cryptography. In: Proceedings of AICTC 2016; August 2016; Bikaner, India. DOI: 10.1145/2979779.2979816

[40] Assche GV. Quantum Cryptography and Secret-Key Distillation. Cambridge University; 2006

[41] Derbez P, Fouque PA, Jean J. Improved key recovery attacks on reduced-round AES in the single-key setting. In: Proceedings of EUROCRYPT 2013; May 2013; Athens, Greece. DOI: 10.1007/978-3-642-38348-9_23