Research Article | Vol. 29, No. 2 / 18 January 2021 / Optics Express 1578

Optics EXPRESS

Dynamic secret-key provisioning in quantum-secured passive optical networks (PONs)

HUA WANG,[1] YONGLI ZHAO,[1,*] MASSIMO TORNATORE,[2] XIAOSONG YU,[1] AND JIE ZHANG[1]

[1] *State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China*

[2] *Department of Electronics, Information, and Bioengineering, Politecnico di Milano, Milano 20133, Italy*

[*] *yonglizhao@bupt.edu.cn*

Abstract: Quantum cryptography (QC) is currently under investigation to build highly secure optical communication networks. QC requires distribution of quantum keys (also called "secret" keys) on separate wavelength channels than those used to transmit the encrypted data. Hence, we propose a quantum-secured passive optical network (QS-PON) that supports both i) the traditional wavelength channels for secured data transmission, and ii) a quantum key distribution network (QKDN) running on separate dedicated wavelengths. The QKDN generates and stores secret keys that are then assigned to users' demands served on traditional PON channels. To generate secret keys, quantum transmitters at the optical network units (ONUs) exchange qubits with a quantum receiver at the optical line terminal (OLT). Then, the generated secret keys are stored in quantum key pools (QKPs) installed at both OLT and the ONUs and assigned to users' demands. Point-to-multipoint QKD systems have been experimentally demonstrated over various forms of quantum access networks (QANs), showing that an efficient mechanism to generate and assign quantum keys based on traffic requests is a critical component of QANs. In this study, we present a new QS-PON architecture, and we propose a dynamic secret-key provisioning (DSKP) algorithm that effectively generates and assigns secret keys from users' demands. Our proposed DSKP algorithm features two phases, the lowest-first secret-key generation (LF-SKG) phase and the hierarchical-clustering secret-key consumption (HC-SKC) phase. In this study, we also provide an analytical model that describes how secret keys are generated and consumed in QKPs. In our illustrative numerical evaluation, we compare our algorithm for secret-key provisioning with a baseline IPACT-based solution in terms of service-rejection ratio, time-slot utilization, and guard- and relay-time saving. Results show that DSKP reduces service-rejection ratio and guard- and relay-time of about 16% and 39.54%, respectively.

© 2021 Optical Society of America under the terms of the OSA Open Access Publishing Agreement

1. Introduction

Data transmission in optical networks supports various types of network services, among which several are requiring a highly-secured communication substrate, such as online banking/trading, personal privacy, military applications, etc [1]. However, conventional encryption technologies used in optical communications are potentially challenged by emerging computing methods that might soon become capable to crack keys based on complex mathematical calculation (e.g., important results toward quantum supremacy have been recently announced by Google [2]). To guarantee secure transmission of sensitive data, quantum cryptography (QC) is emerging as an attractive technology that can generate truly random and secure keys. The security of quantum keys derives from the fundamental laws of quantum mechanics like the "no-cloning theorem" and "Heisenberg's uncertainty principle" [3]. This kind of secret-key provisioning is being introduced in optical networks to provide probabilistically-secure communication. To enable QC over

#412188 https://doi.org/10.1364/OE.412188
Journal © 2021 Received 19 Oct 2020; revised 2 Dec 2020; accepted 20 Dec 2020; published 11 Jan 2021

Optics EXPRESS

optical networks, quantum key distribution (QKD) is regarded as a common way to share secret keys between each pair of end-points of a communication. Also, optical networks can provide optic fibers as transmission carriers to distribute quantum keys. By leveraging dedicated or multiplexed optical fibers, a QKDN generates and delivers secret keys (i.e., performs "secret-key provisioning (SKP)") for adjacent, as well as non-adjacent, nodes. With the development of practical development QKD, QKDNs have gradually become a promising and feasible solution.

"Last-mile" secure connection has also been considered in QKDN, and it is referred as Quantum Access Network (QAN), to provide secret-key access to final users. The idea of QAN has attracted a lot of attention (see, e.g., [4,5]), and demonstrated to be capable of guaranteeing security of "last-mile" communication through secure key distribution among a central node (e.g., the network operator's central office) and several end users. Still, QAN design poses several challenges, spanning from theoretical modeling, to resource allocation algorithms, to testbed experimentation. In the past decades, QANs have been prototyped with different device deployments and channel settings. In [6], the concept of using QC was proposed for the first time to provide secure communication in optical access networks. Since then, various demonstrations of QS-PONs have been experimented and simulated with different QKD configurations (i.e., multiple QKD receivers (Qrec) shared with one QKD transmitter (Qtra) [7–9], multiple Qtras shared with one Qrec [10–12], and multiple Qtras shared with multiple Qrecs [5]). Also, QKD in QAN can be achieved by using wavelength division multiplexing (WDM) [4,13] and time division multiplexing (TDM) [14,15], to share fiber wavelength with classical data channels. These proposals demonstrate QAN physical feasibility, but the problem of how to dynamically allocate QKD wavelengths to generate secure keys for final users has not yet been investigated.

In this paper, we focus on a specific embodiment of QAN, which is Quantum Secured Passive Optical Networks (QS-PONs). In QS-PON, secured data transmission occurs on the standard wavelength channels of a PON, as e.g., in Ref. [16] (note we refer in the following to wavelengths used to transmit secured data as data channels), while SKP is performed over a separate set of wavelengths referred as QKD channels (see Section 2.A for more details). Two basic problems are addressed: *i)* how to effectively design a QS-PON architecture to arrange secret-key distribution for final users, and *ii)* how to dynamically allocate QS-PON resources to multiple users based on their requests. For the first one, as QKD transceivers are very expensive, we consider sharing of a single centralized Qrec among several Qtras using time division multiplexing, as proposed in [6]. Then, secret-key distribution can be implemented in a way similar to the scheduling of user requests between the ONUs and the OLT. For the second one, we employ Dynamic Bandwidth Assignment (DBA) to improve the bandwidth utilization (as done in traditional PONs (non-QS)). In this regard, a similar DBA scheme for effective secret-key provisioning must be developed in QS-PON, considering the combination of different constraints driven by QKD like unidirectional secret-key generation assigned for bidirectional data encryption. Hence, even though existing protocols for traditional PONs such as interleaved polling algorithm (IPACT) [17–19] could still be applied to manage time-slot allocation for the QKD, in such existing approaches the generated secret keys will then need to be arranged for non-adjacent nodes by the cache devices like quantum key pool (QKP) [20–22]. To generate and assign secret keys for multiple users, we propose in this paper a dynamic secret-key provisioning (DSKP) algorithm in QS-PON to allocate time slots.

Our proposed DSKP algorithm can effectively generate and assign secret keys according to users' demands. DKSP devises time-slot allocations to support two separate processes, namely secret key generation (SKG) and secret key consumption (SKC). The algorithm aims at improving the successful provisioning of keys to users (effectively scheduling the SKG and SKC processes). To jointly address these two processes, our proposed DSKP algorithm features two phases, the lowest-first secret-key generation (LF-SKG) phase, and hierarchical-clustering secret-key assignment (HC-SKC) phase. After having presented the DKSP algorithm, in this study we

Optics EXPRESS

provide also an analytical model that describes how secret keys are generated and consumed in QKPs over time. The model is useful to gain some generic insights on the behavior of QKP occupation and on its impact of the SKP process results obtained. Finally, in our illustrative numerical evaluation, we simulatively compare our algorithm to a baseline IPACT-based solution for SKP in terms of service-rejection ratio (SR) and guard-time saving (GTS) among other metrics. Results show that DSKP reduces SR and GTS of about 16% and 39.54%, respectively, compared to a baseline IPACT-based approach.

The remainder of this paper is organized as follows. Section 2 discusses our proposed QS-PON architecture. In Section 3, we clarify the time-slot allocation problem for QKD and we introduce network and requests models. In Section 4, we introduce our DSKP algorithm to generate and assign secret keys based on secure requests. In Section 5, we formulate a QKP model to describe how secret-key volume changes over time. In Section 6, we show some illustrative numerical results to evaluate the effectiveness of the proposed algorithm. Section 7 concludes the paper.

2. Related works of QKD networking

QKD is derivated from QC, and regarded as a critical technology that can provide secret keys for two separated users. Unlike tradition encryption methods, the security of secret keys relies on the fundamental laws of quantum physics, like Heisenberg uncertainty principle and None-cloning theorem. Based on such fundament, QKD has the advantage of allowing two users to share keys while also being aware of the existence of eavesdropper. To explore the feasibility of QKD for practical application, testbeds of QKD integrated in practical optical networks are being currently investigated [23–27]. The latest demonstration of secret-key rate and transmission distance in QKDN have achieved up to 1.26 megabits per second key rates over 50 kilometers of standard optical fiber [28] and 1.16 bits per hour over 404 kilometers of ultra-low-loss fiber [29]. Building on the top of these communication trials, advanced forms of SDN-controlled networking [30–32] and resource allocation [33–35] in QKDN are also being investigated to improve the efficiency and flexibility. Regarding QKD integration in edge network, a quantum-secured, inter-domain 5G service orchestration over optical networks have been recently experimentally demonstrated [32].

3. Illustration of the QS-PON

3.1. QS-PON architecture

A possible architecture of QS-PON is shown in Fig. 1, which is a QAN built over a Time and Wavelength Division Multiplexed PON (TWDM-PON) infrastructure. Within this architecture, Qtras are installed at the ONU side while a Qrec is installed at the OLT side, to jointly perform QKD. A pair of Qtra and Qrec can implement the transmission of quantum signal and the selection of measurement basis [6]. The wavelength channels operating in a QS-PON consist of quantum wavelengths (QWs), optical wavelengths (OWs), and user data wavelengths (UWs). Among them, QW, OW and UW are respectively used for the transmission of quantum bits, optical (not quantum) signals that supports the QKD process (e.g., measurement basis, time synchronization data), users' data as in traditional PONs (or more advanced forms of TWDM-PON). QWs are placed at approximately 1310 nm [4], OWs and UWs are placed at approximately 1550 nm [4]. They are multiplexed on single fiber by a passive optical splitter (POS). To increase resource efficiency, QWs can be further divided into time slots by using TDM [34,35], thus Qrec can perform QKD with various Qtras during different time slots. Secret keys generated between each pair of Qtra and Qrec are stored in the quantum key pool (QKP) prepared for the subsequent security requests [20–22]. In summary, SKP between OLT and ONUs is achieved by point-to-multi-point QKD and OTDM technologies between Qtras and Qrecs.

Optics EXPRESS

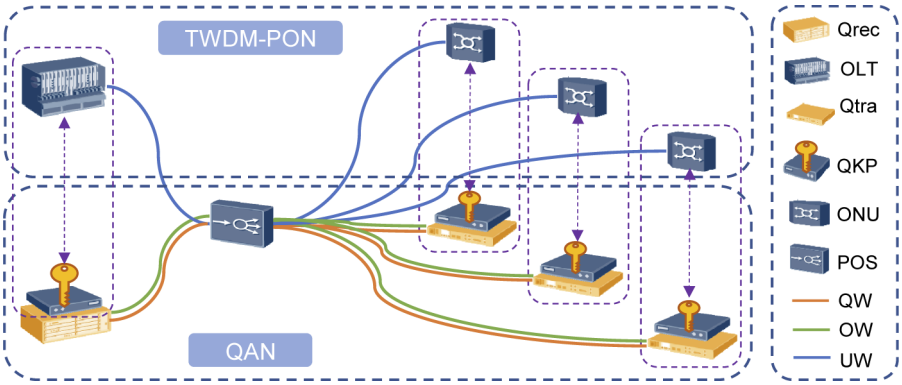

Fig. 1. The architecture of QS-PON.

3.2. *Secret key generation (SKG) and secret key consumption (SKC) in the QS-PON*

As already mention, SKP includes SKG process and SKC process.

- SKG process is triggered when the volume of secret keys in QKP is less than a certain threshold. This trigger of SKG will release a "supplement request" which is sent from ONU to OLT to obtain the required key volume in QKP. The interaction between Qrec and Qtras for SKG is shown with a simple example in Fig. 2(a). In our example, three Qtras share one single Qrec and send quantum signals in sequence by occupying different time slots to generate secret keys and refill the QKP. Once the SKG is terminated, the keys are stored in the QKPs located on both sides.
- SKC process is triggered by a "security request" that can be requested in three modalities: *i)* OLT to ONU, *ii)* ONU to OLT, *iii)* ONU to ONU. Figure 2(b) depicts the three SKC modalities. For the modality *i)* and *ii)*, OLT and ONU can use secret keys taken from their QKPs to directly encrypt the information. For the modality *iii)*, OLT needs to perform intermediate exchange ("relay") of the keys through a "key repeater". As of today, quantum keys can be relayed through quantum repeater [36] which exploits entanglement distribution, or through a trusted repeater [36] which encrypts one key with another key. As the quantum-relay technology is still in its infancy, we consider in this study key relay via a trusted repeater.

3.3. *SKG workflow in the QS-PON*

A workflow clarifies the interaction required to perform on-demand QKD among Qtra, Qrec, OLT, and ONU, as shown in Fig. 3. To start, OLT sends instructions to collect security requests from ONUs. If some ONU's QKP has a low volume, the ONUs send supplement requests to OLT. At the same time, the ONU checks the status of Qtra to see if the Qtras can be activated to generate new keys. After that, the OLT checks the status of Qrec and the key volume in QKP to verify whether SKG and SKC can be performed (key volume in QKP must be sufficient tos atisfy the security requests as much as possible). After these steps, the OLT formulates a schedule based on the received request to specify time intervals for various ONUs (see Section 3). Finally, the schedule is communicated to all ONUs.

Optics EXPRESS

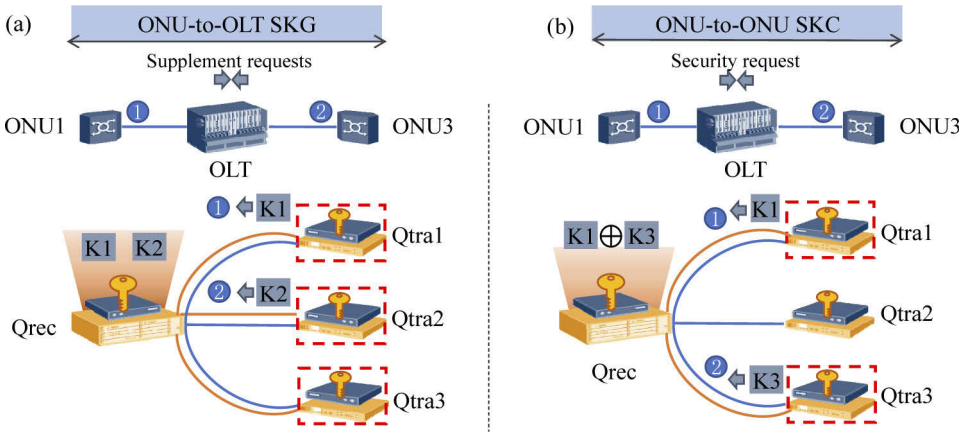

Fig. 2. The ONU-to-ONT SKG and ONU-to-ONU SKC diagram, (a) the process of SKG for ONU-to-OLT, (b) the process of SKC for ONU-to-ONU.

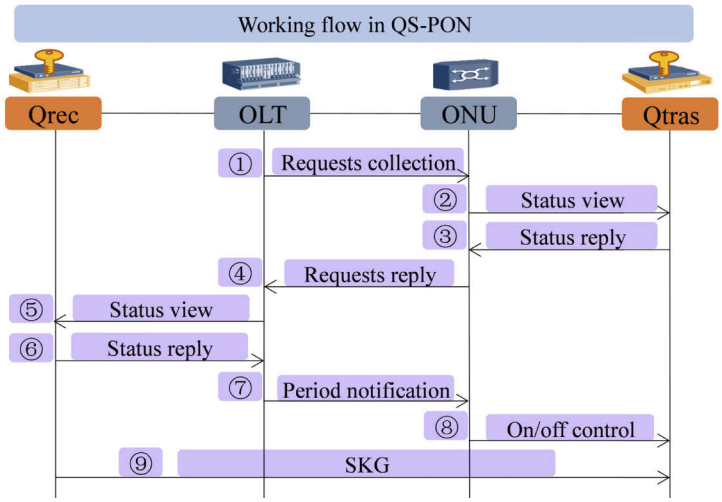

Fig. 3. The SKG work flow in QS-PON.

4. DSKP in the QS-PON

4.1. Problem description

Let us now describe the problem of time-slot allocation for SKP in QS-PON. We separate SKP into two sub-phases: SKG and SKC. For the SKG phase, when a supplement request arrives, OLT needs to specify time slots for Qtras to perform QKD and supplement keys in the QKP. As we are suing OTDM, a schedule for SKG must be identified such that only one Qtra at a time is served. The other Qtras need to wait for their SKG slot to come, but they can still proceed with normal SKC until key volume in their QKP gets to 0, when SKP requests cannot be served and will be rejected. Thus, our proposed DKSP algorithm initially selects the QKP with lowest key volume as the one to be supplemented first and assigns available time slots to it, as shown in Fig. 4(a). For the SKC phase, (triggered by security requests from ONUs for data encryption), OLT first determines the modality of security requests, then performs key relay for ONU-to-ONU requests (if needed), and finally sends the keys to the requesting ONU. As shown in Fig. 4(b), the

Optics EXPRESS

processing order follows the arrivals of requests, and a guard time is imposed between each SKC request. When the destination ONU for consecutive SKC requests is the same one, the guard time between these SKC requests is unnecessary and may lead to bandwidth waste. Thus, the objective of DSKP during the SKC phase is to reduce the unnecessary guard time occupation by grouping requests from the same ONU. Focusing on these two phases, our proposed DSKP algorithm, which is described in the next section, aims at scheduling SKC and SKG requests to jointly minimize scheduling delay and service rejection.

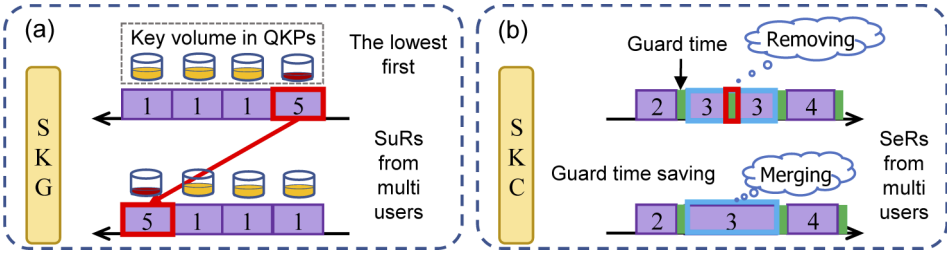

Fig. 4. Diagram of two sub-problems, (a) SKG, and (b) SKC.

4.2. Network model

The physical topology of a QS-PON can be modeled as a graph $G(V,\ W_c,\ W_{QKD}, QKP\ (K_{curr}, K_{threshold},\ K_{full})\ )$, where V denotes the network nodes, and W_c and W_{QKD} refer to the sets of wavelengths used for normal optical communication and QKD, respectively; and the triplet QKP contains K_{curr}, that represents current value of secret-key volume in QKP, $K_{threshold}$ that is threshold above which SKG is triggered, and K_{full} that is the capacity of the QKP. Note that, in this paper, we only focus on the assignment of wavelengths used for QKD, and the assignment of classical communication in TWDM-PON can be performed as in any of several previous studies [16–18]. Since we are considering TDM, W_{QKD} is divided into several uniform time slots (t_{slot}), assigned to different users and spaced with a guard time (t_g).

4.3. Request model

Parameter K_{rate} indicates as the average secret-key volume generated in a time slot in the network. For the SKG and SKC, two types of requests, i.e., supplement request and security request, are denoted as $r_{su}(s,\ d, K_{req})$ and $r_{se}(s,\ d,\ K_{req})$, respectively. s and d are the source and destination nodes, and K_{req} represents the secret-key volume required by ONUs. s and d in different requests can refer to different elements, e.g., OLT and ONU, or ONU and ONU. The number of t_{slot}s to support a supplement request or security request can be described as:

$$n = \lceil K_{req}/K_{rate} \rceil \tag{1}$$

and thus, the total time of available t_{slot}s required for a user (T) is:

$$T = nt_{slot} + t_g \tag{2}$$

assuming that all the slots associated to the same user are scheduled consecutively.

5. Two DSKP components: LF-SKG and HC-SKC

After the illustration of LF-SKG and HC-SKC, we now will elaborate on how the time-slot allocation is performed by the proposed in DSKP algorithm. The DSKP algorithm is correspondingly divided into two sub-algorithms: LF-SKG algorithm and HC-SKC algorithm.

Optics EXPRESS

5.1. LF-SKG algorithm

Lowest-first secret-key generation (LF-SKG) is the policy chosen for the time-slot allocation of secret-key generation. The intuitive logic behind this policy is that, the longer time a QKP has to wait to be refilled, the more likely it is deplete its key reserve, which will more likely lead to rejection of subsequent SKP requests. To solve this problem, we designed a LF-SKG algorithm to select the Qtra with the lowest key volume in QKP among various Qtras.

As shown in Table 1, LF-SKG algorithm aims to arrange time slots for supplement requests (r^i_{su}s). Let us assume that r^i_{su} arrives dynamically from ONUs to OLT during the current time period (that is referred as time window "$Window_{T\_SKG}$"). After each $Window_{T\_SKG}$, OLT initially collects r^i_{su} from ONUs into the set R_{su} and checks the W_{QKD}s to find whether there is an available capacity to perform QKD. Then, we look the volume of secret keys in the QKPs in which includes both of source and destination nodes in each r^i_{su} to identify the order of r^i_{su}s in R_{su} for the SKG. The order of r^i_{su}s follows the LF-SKG principle, that means the r^i_{su} with the lowest secret-key volume is arranged as the first one to be allocated with time slots and perform SKG. Next, we calculate and allocate available W_{QKD}s for each r^i_{su} in the R_{su}. To achieve it, we first count the number of time slots that is required a r^i_{su} for the SKG. The required number (n) of time slots is calculated by the ratio of K_{req} of the r^i_{su} and the K_{rate} (as shown in Eq. (1)). OLT allocates the corresponding n consecutive t_slots to the r^i_{su}, and the series of allocated t_slots for various r^i_{su} within a $Window_{T\_SKG}$ can form a SKG cycle. Finally, OLT broadcasts the SKG cycle to all ONUs, and the ONUs control the on/off states of Qtras.

Table 1. LF-SKG algorithm

Algorithm 1: LF-SKG algorithm	
Input: $G(V,\ W_c,\ W_{QKD}, QKP(K_{curr}, K_{threshold},\ K_{full})\ ), K_{rate},\ \ r^i_{su} \in R_{su}(s,\ K_{req})$, $Window_{T\_SKG}$, t_slot, n. Output: C_{SKG}.	
1	**if** *the time is during the* $Window_{T\_SKG}$ **then**
2	Add r^i_{su}s in the R_{su}
3	**end if**
4	**if** *the time is after the* $Window_{T\_SKG}$
5	*Update the occupation status of* W_{QKD}
6	**for all** $r^i_{su} \in R_{su}$ **do**
7	*Check the volume of secret keys of the scr. and des. in* r^i_{su}
8	*Record the volume of secret keys in the* r^i_{su}
9	*Compare the volume of secret keys with the last one*
10	*Replace the lowest volume of secret keys in the* r^i_{su}
11	*The order of* r^i_{su} *follows the key volume form low to high in* R_{su}
12	**end for**
13	**for all** $r^i_{su} \in R_{su}$ **do**
14	*Calculate the number of time slots required by* r^i_{su}
15	*Assign the time slots to the* r^i_{su}
16	**end for**
17	**end if**

5.2. Hierarchical-clustering in SKC

HC is a statistical method that clusters various samples into different groups with similar features [37–38]. To reduce the unnecessary guard-time occupation in SKC process, HC is used to cluster

Optics EXPRESS

SKP requests with the same destination nodes. The clustering process depends on similarity degree between two different samples (i.e., destination nodes). The similarity degree can be, e.g., represented by the calculation of using distances like Minkowski and Euclidean Distance, etc. To simplify the calculation, we adopt a simple clustering distance, i.e., the Absolute Value Distance. The distance under absolute value d for two nodes w_i and w_j in total requests $k = \{1, \cdots, p\}$ can be calculate as in Eq. (3).

$$\mathrm{d}(w_i, w_j) = \sum_{k=1}^{p} |w_i - w_j| \tag{3}$$

When the number of requests becomes large, the distance value of each pair of requests is better to be presented in the form of a matrix W, as shown in Eq. (4) (n.b.: the distance of a node to itself is the case of $d = 0$ in the diagonal). The difference between the max and min distances in matrix W calculated by Eq. (5) is referred as a distance gap d_{gap}.

$$\mathrm{W} = \begin{array}{c} \\ w_1 \\ \cdots \\ w_n \end{array} \begin{array}{c} \begin{array}{ccc} w_1 \cdots & & w_n \end{array} \\ \begin{bmatrix} 0 & \cdots & d(w_1, w_n) \\ & 0 & \cdots \\ & & 0 \end{bmatrix} \end{array} \tag{4}$$

$$d_{gap} = d_{max}(w_1, w_n) - d_{min}(w_1, w_n) \tag{5}$$

After the calculation of W, the clustering process can start. We exploit height to constantly select and merge the requests with same distance in the matrix. First, all elements in W are grouped together in a set H_1 with a height 0. If we assume the number of clusters is c, then the height is constructed by d_{gap}/c as a constant value. As shown in Eqs. (6)–9, several groups in the set H_1 with the same height can be merged a common sub-set h_1. Sub-set h_1 is as one factor put in a new set H_2 with the other factors that have different height in sub-set h_1. Also, set H_3 with height $2 \times d_{gap}/c$ can be constructed by composing h_2, w_{i+3}, and w_{i+4}. Analogously, elements and sub-sets can be constantly composed until one sub-set remained in ($H_n H_n = d_{gap}$). The grouped clusters are shown in each step of composing with different heights.

$$H_1 = \{w_i, w_{i+2}, \cdots, w_{i+6}\} \tag{6}$$

$$H_2 = \{h_1, \cdots, w_{i+3}, w_{i+4}, w_{i+5}, w_{i+6}\} \tag{7}$$

$$H_3 = \{h_2, \cdots, w_{i+5}, w_{i+6}\} \tag{8}$$

$$\cdots$$

$$H_n = \{h_{n-1}\} \tag{9}$$

5.3. HC-SKC algorithm

As shown in Table 2, HC-SKC is for the situation where OLT receives security request (r^i_{se}) from ONUs and relays secret keys from the source node to the destination node. Since SKC process occurs in parallel to SKG, we suppose they have different time window for the generation and assignment of secret keys. Analogously, the sets of W_c and R_{se} will be updated at the beginning of each $Window_{T\_SKC}$. Then, we consider two possible cases, based on the key volume of QKP: $K_{curr} = 0$ and $K_{curr} > 0$. For $K_{curr} = 0$, SKC cannot be performed since there are no keys in QKP to be provided for the requests. For $K_{curr} > 0$, as mentioned in Section 2. B, SKC can be achieved by the relaying function that is directly performed in the OLT side and the transmission of the secret keys from OLT to ONU. Next, we apply the clustering of r^i_{se}s according to the algorithm in Section 4.B to reduce the guard time in SKC process. By calculating the absolute distance d_{d_i,d_j} between r^i_{se}s, the r^i_{se}s generated between ONUs will be grouped to a set S_{d_i} if they have the same

Optics EXPRESS

destination node. The other r^i_{se}s with different d_{d_i,d_j} values will be put into set $S_{d_{ir}}$. r^i_{se}. r^i_{se} in set $S_{d_{ir}}$ can be grouped as $S_{d_{ir}}\{\{r^i_{se}, r^j_{se}\}, \{\cdots\}\cdots\}$ according to d_{P_i,p_j} following the HC process described in section4.B. Next, r^i_{se}s in the sets S_{d_i}, and S_{dir} will also be dealt one by one according to HC process, and the output order will be set as SKC cycle (C_{SKC}). Finally, the time-slot allocation for each r^i_{se} is included in C_{SKC}, and the number of C_{SKC} will be Max($N^{r_{su}}_{slot}$)/n if there are n *t_slot*s of each r^i_{se} in C_{SKC}.

Table 2. HC-SKC algorithm

Algorithm 2: HC-SKC algorithm	
Input: $G(V,\ W_c,\ W_{QKD}, K_{rate}, QKP(K_{curr}, K_{threshold},\ K_{full})$), $r^i_{se} \in R_{se}(s,\ d,\ k_{req})$, $Window_{T\_SKC}$, *t_slot*, *m*. Output: C_{SKC}.	
1	**if** t>$Window_{T\_SKC}$ **then**
2	*update the occupation states of* W_c *in* G
3	*update* R_{se} *set for each* r_{se}
4	*update* K_{curr} *in QKP*
5	**if** $K_{curr} = 0$ **then**
6	*reject the* r_{se} *and wait until* K_{curr}>0
7	**end if**
8	**for all** $r^i_{se} \in R_{se}(s,\ d,\ k_{req})$ **do**
9	*calculate* d_{d_i,d_j} *between* r^i_{se} *and* r^j_{se}
10	**if** $d_{d_i,d_j} = 0$ **then**
11	*cluster* r^i_{se}*s in set* $S_{d_{ir}}\{r^i_{se}, r^j_{se}, \cdots\}$
12	**end if**
13	*calculate* d_{P_i,p_j} *between* r^i_{se} *and* r^j_{se} *in set* $S_{d_{ir}}\{r^i_{se}, r^j_{se}, \cdots\}$
14	**if** $d_{P_i,p_j} = 0$ **then**
15	*cluster* r^i_{se}*s with* $d_{P_i,p_j} = 0$ *in front of set* $S_{d_i}\{\{r^i_{se}, r^j_{se}\}, \{\cdots\}\cdots\}$
16	**end if**
17	*cluster the* r^i_{se}*s in* $S_{d_{ir}}$
18	**if** *s or d = OLT* **then**
19	*set* $s_i = 1$ *for each* r^i_{se}
20	*put* d_{d_i,d_j}, d_{P_i,p_j} *and* s_i *with in HC process*
21	**end if end for end if**
22	*set n t_slot for each* r^i_{se} *in a* C_{SKC}
23	*the numbers of* $C_{SKC} \rightarrow Max(N^{r_{su}}_{slot})/n$
24	*the order of* $C_{SKC} \rightarrow$ *the order of* r^i_{se} *after HC process*
25	**end if**

5.4. Analysis of DKSP complexity

Time complexity of DSKP algorithm comprises two parts, respectively for LF-SKG and HC-SKC. LF-SKG complexity depends on the 'for' loops (line 3 to 6 in Algorithm 1) related to the number of r^i_{su}s. Higher number of r^i_{su}s ($V \uparrow$) will bring higher complexity (O($K + V$) $\uparrow$). HC SKC complexity mainly is contributed by HC process, that can be estimated as O($t \times \alpha^2$) [39], where t is the number of iterations and α is sample quantity. Thus, the overall complexity is O($K + V + t \times \alpha^2$).

Optics EXPRESS

6. QKP modeling and verifying in the QS-PON

6.1. QKP modeling

QKP is an important component in QS-PON and there is no QKP in traditional PONs. It is used for the storage of secret keys for supplement requests and the continuous fulfillment for security requests, thereby introducing a balance between SKG and SKC processes on the key volume. In this section, we construct a mathematical model of QKP, analyze the relationship between SKG and SKC, and quantify their influence on secret-key volume in QKP as a function of time. The symbols used in our mathematical model are listed in Table 3.

(a) Relationship between SKG and SKC

Table 3. Parameters

Symbol	Definition
M	Numbers of requests.
P	A random value from a random distribution, 0<P<1.
N	Key volume required for a request.
$S_c(t)$	SKC rate at a time.
$S_{c\_slot}(t_{slot})$	SKC volume per t_{slot}.
$S_{g\_slot}(t_{slot})$	SKG volume per t_{slot}.
K_{full}	Capacity of QKP, i.e., a fixed value.
$K_{threshold}$	Threshold of QKP for key supplement.
$K_{curr}(t_{slot})$	Key volume in QKP in current t_{slot}.
$K_{inve}(t_{slot})$	Key stock volume per t_{slot} in QKP.
N_{slot}	Numbers of t_{slot} used for the supplement.

SKG and SKC directly influence secret-key volume in QKP, which will, in turn, also influence SKP for users. Here, we construct mathematical formulations respectively for SKG and SKC.

$$S_{c\_slot}(t_{slot}) = M \times \left[1 - \left(\frac{k}{t_{slot}}\right)^{a}\right] \times P \times N \quad t_{slot} \geq \mathrm{k};\ a{>}0 \tag{10}$$

Equation (10) describes the consumption volume of secret keys within a t_{slot}. Arrival of security requests follows heavy-tailed distribution which can describe the network data traffic realistically. Suppose that the average number of the requests at t_{slot} is M, required key volume is N, and P is a constant value where key volume required by users can be represented by $P \times N$ (0<P<1). The probability density function is $\frac{\mathrm{a}}{\mathrm{k}}\left(\frac{\mathrm{k}}{t_{slot}}\right)^{\mathrm{a}+1}$, where a and k are constants and $\mathrm{a} \geq \mathrm{k},\ k{>}0$.

$$S_{g\_slot}(t_{slot}) = K_{rate} \tag{11}$$

Equation (11) describes the generation volume of secret keys within a t_{slot}. It can be seen as a fixed value within a certain time.

$$S_{c\_slot}(nt_{slot}) = M \times N \times P \times \left\{1 - \left(\frac{k}{nt_{slot}}\right)^{a}\right\} \tag{12}$$

$$0 \leq S_{c\_slot}(nt_{slot}) \leq K_{full}\ \mathrm{k} \leq t_{slot} \leq \frac{k}{n}\left(\frac{MNP}{MNP - K_{full}}\right)^{\frac{1}{a}} \tag{13}$$

Equation (12) describes the volume of consumed keys within n continuous t_{slot}s in QKP. In addition, to ensure the subsequent secret-key provision capacity, the volume of consumed keys in

Optics EXPRESS

QKP should be bigger than 0 and smaller than K_{full}. Correspondingly, Eq. (13) shows the size of a t_{slot} should be satisfied.

$$S_{g\_slot}(nt_{slot}) = nt_{slot}K_{rate} \tag{14}$$

$$0 \le S_{g\_slot}(nt_{slot}) \le K_{full} \tag{15}$$

Equation (14) describes the volume of generated keys in nt_{slot}s. It has the same restriction with consumed value as shown in Eq. (15), and that is the generated volume in nt_{slot}s should be bigger than 0 and smaller than K_{full}.

b) Changing of secret-key volume in QKP

Based on the above equations of SKG and SKC, the key volume stored or consumed per time slot in a QKP can be judged by the rates of SKG and SKC.

$$K_{inve}(nt_{slot}) = S_{g\_slot}(nt_{slot}) - S_{c\_slot}(nt_{slot}) = nt_{slot}K_{rate} - M \times N \times \left[1 - \left(n\frac{k}{t_{slot}}\right)^a\right] \tag{16}$$

Equation (16) evaluates the key volume to be generated or consumed in a t_{slot}.

$$K_{inve}(nt_{slot}) \ge 0, S_{g\_slot}(nt_{slot}) > S_{c\_slot}(nt_{slot})\,(\frac{MNk^a}{MN - K_{rate}})^{\frac{1}{a}} > nt_{slot} \tag{17}$$

When $S_{g\_slot}(t_{slot}) > S_{c\_slot}(t_{slot})$, Eq. (17) represents an excess key volume that can be stored in QKP. Put $K_{inve}(t_{slot}) \ge 0$ into Eq. (16), we can get $nt_{slot} < (\frac{MNk^a}{MN-K_{rate}})^{\frac{1}{a}}$ which means that key supplement can not only satisfy consumption, but also have the ability to store keys within a certain time period.

$$K_{inve}(nt_{slot}) < 0, S_{g\_slot}(nt_{slot}) < S_{c\_slot}(nt_{slot})\, nt_{slot} > (\frac{MNk^a}{MN - K_{rate}})^{\frac{1}{a}} \tag{18}$$

When $S_{g\_slot}(t_{slot}) < S_{c\_slot}(t_{slot})$, Eq. (18) represents the needed key volume and the key shortage can be supplemented by the keys remained in previous time slots in QKP. Also, if we put $K_{inve}(t_{slot}) < 0$ into Eq. (16), we can get $nt_{slot} > (\frac{MNk^a}{MN-K_{rate}})^{\frac{1}{a}}$.

$$\frac{dK_{curr}(t_{slot})}{dt_{slot}} = -S_{c\_slot}(t_{slot}) \tag{19}$$

Equation (19) describes the real-time-slot key volume in QKP.

$$K_{curr}(t_{slot}) = C_1 - M \times N \times P \times \left[t_{slot} + \frac{k}{a-1}\left(\frac{k}{t_{slot}}\right)^{a-1}\right] \quad C_1 > K_{full} \tag{20}$$

$$K_{full} > K_{curr}(t_{slot}) > K_{threshold} \qquad t_{slot1} > t_{slot} > k$$

$$K_{threshold} \ge K_{curr}(t_{slot}) > 0 \qquad t_{slot2} > t_{slot} > t_{slot1}$$

$$K_{curr}(t_{slot}) \le 0 \qquad T > t_{slot} > t_{slot2}$$

Equation (20) is the integral results of Eq. (19), representing the current secret-key volume in QKP changing over t_{slot}. C_1. is a positive constant. In order to guarantee successful SKP, two parameters, full volume and threshold volume, are set in QKP. According to the capacity of providing keys, the current secret-key volume in QKP can be divided into three phases. If $K_{full} > K_{curr}(t_{slot}) > K_{threshold}$, this means secret keys in the QKP can fully support the SKC of users. If $K_{threshold} \ge K_{curr}(t_{slot}) > 0$, this means secret keys in the QKP will be totally consumed and a key supplement is needed in the QKP. If $K_{curr}(t_{slot}) \le 0$, this means secret keys in the

Optics EXPRESS

QKP cannot serve security requests and this is the case when the LF-SKG algorithm must be performed. Moreover, as the t_{slot} increases, $K_{curr}(t_{slot})$ in QKP will decrease from full to a value below $K_{threshold}$.

$$K_{req} = (1-\alpha)(K_{full} - K_{curr}(t_{slot}))$$
$$= (1-\alpha)\left(K_{full} - C_1 + M \times N \times P \times \left[t_{slot} + \frac{k}{a-1}\left(\frac{k}{t_{slot}}\right)^{a-1}\right]\right) \quad (21)$$

Equation (21) represents the key volume to be supplemented. Consider the key consumption involved in this process, α is set as a surplus-dependent parameter of consumption rate ($0 \leq \alpha \leq 1$).

$$N_{slot} = \frac{K_{req}}{K_{rate}} \quad (22)$$

Equation (22) calculates the numbers of t_{slot}s used for a request.

$$K_{full} > K_{curr}(t_{slot}) > K_{threshold}\ t_{slot1} > t_{slot} > 0$$

$$\frac{dK_{curr}(t_{slot})}{dt_{slot}} = -S_{c\_slot}(t_{slot}) \quad (23)$$

$$K_{curr}(t_{slot}) = C_1 - M \times N \times P \times \left[t_{slot} + \frac{k}{a-1}\left(\frac{k}{t_{slot}}\right)^{a-1}\right] \quad (24)$$

$$K_{threshold} \geq K_{curr}(t_{slot}) > 0 \quad T > t_{slot} > t_{slot1}$$

$$\frac{dK_{curr}(t_{slot})}{dt_{slot}} = -(S_{c\_slot}(t_{slot}) - S_{g\_slot}(t_{slot})) \quad (25)$$

$$K_{curr}(t_{slot}) = C_2 + K_{rate} \times t_{slot} - M \times N \times P \times \left[t_{slot} + \frac{k}{a-1}\left(\frac{k}{t_{slot}}\right)^{a-1}\right] \quad (26)$$

Limited by $K_{full} > K_{curr}(t_{slot}) > K_{threshold}$ and $K_{threshold} \geq K_{curr}(t_{slot}) > 0$, Eqs. (23) to (26) show two phases of secret-key volume changing over t_{slot} in QKP. When $K_{threshold} \geq K_{curr}(t_{slot}) > 0$, it will trigger the supplement of secret keys. C_1 and C_2 are positive constants.

6.2. Performance analysis of QKP modeling

After having introduced our mathematical model for SKG and SKC in QS-PON, in this subsection we explore the influence of several parameters on SKG and SKC behavior. We run the proposed mathematical model in static setting (in Matlab) and also a dynamic network simulation (developed in C++) as a comparison. In these simulations, we consider a 32-ONU PON where Qtras and Qrec are located at OLT and ONUs. Arrival of security requests follows heavy-tailed Pareto distribution, and the source and destination nodes are randomly selected. Required key volume in the security requests is randomly selected from different ranges, which can be set as variables. SKG and SKC rates are then selected as a function of the required key value within a certain range. Simulations show how the volume of secret keys changes in QKP influenced by SKG and SKC. We conduct the simulation using the parameters listed in Table 4, but the parameter settings are not limited to these values.

Figure 5 shows the trend of key volume in QKP based on our model. It includes two sub-phases to show how secret-key volume in QKP changes over time under the situations with and without SKG. In the first sub-phase, as we can see, secret keys in QKP are gradually consumed to a value below $K_{threshold}$. This part only contains the consumption of secret keys until key volume is below the threshold, and then SKG will be triggered to supplement keys in QKP. The key volume gradually increases since the secret-key supplement works to enhance SKP capacity of QKP.

Optics EXPRESS

Table 4. Parameters

Symbol	Value	Symbol	Value
M	20000	α	0
P	[0, 1]	$K_{threshold}$	4000
N	200	K_{full}	400000

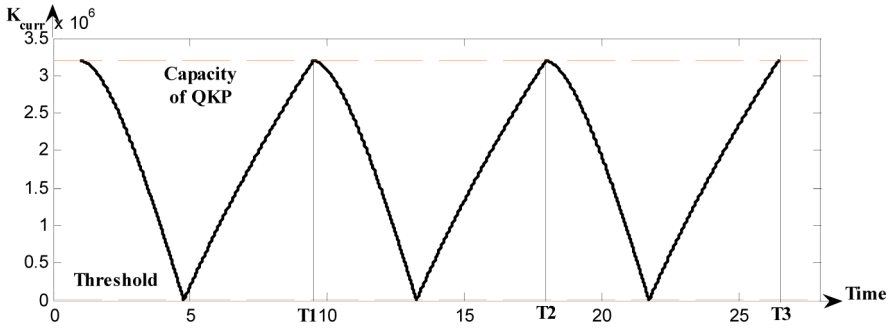

Fig. 5. QKP model shows how secret-key volume changes over time in QKP with SKC and SKG (SKG rate = 60 and SKC rate selected from range [0, 400]).

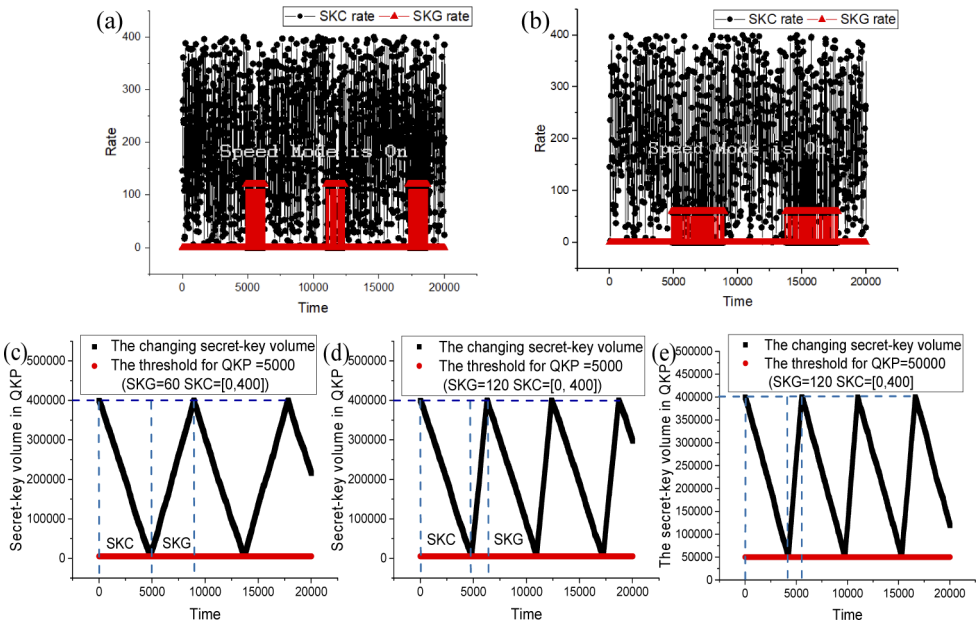

Fig. 6. Simulation results showing how SKG and SKC rates affects secret-key volume in QKP. (a) and (b) show the SKC rate versus different SKG rates (SKC rate selected from range [0, 400], SKG rate=60 and 120 respectively). (c) and (d) show secret-key volume in QKP changing over time with different SKG rates (SKG rate=60 and 120 respectively). (e) shows how key volume in QKP changes with different $K_{threshold}$ values (i.e., $K_{threshold}$=50000, respectively), and the SKC and SKG rates are set to fixed values in this case.

Optics EXPRESS

Figure 6 shows, using dynamic simulation, how SKG and SKC rates affects secret-key volume in QKP. In Figs. 6(a) and (b)we plot the SKC and SKG rate, considering that SKC occurs during the whole process, while SKG (in red) is triggered only when key volume goes below a threshold. Note that SKG lasts as long as it is needed to fill up the QKP. It can be observed, comparing the two figures, that higher SKG takes shorter time to fill up the QKP. Figures 6(c) and (d) show the secret-key volume changing over time with different SKG rates. Also, comparing Figs. 6(c)-(e) with Fig. 5 we can observe that higher SKG rate enables shorter time to fill up the QKP (also called "supplementing time"). Note that a similar temporal trend for key volume in QKP has been presented in Ref. [40], which supports the correctness of our QKP model. Figure 6(e) show the secret-key volume changing over time with different $K_{threshold}$s. Bigger $K_{threshold}$ can shorten the time consumed by SKG and thus causing shorter time period. In addition, similar to Fig. 6, the changing trend of secret-key volume is periodic.

6.3. Summary

In this section, we constructed a mathematical model representing the key volume in the QKP and analyzed the performance obtained from the model with simulation. We can observe that the change of SKG and SKC rates will influence the key volume in QKP. This shows the setting of threshold value for the supplement has a strong impact on the performance of SKP. In addition, the simulation results of the trend of key volume changing over time have a similar trend performance with that in Ref. [40].

7. Illustrative numerical results and discussion

To evaluate the effectiveness of the DSKP algorithm, we extended the dynamic network simulation discussed above to evaluate more performance metrics. With the parameters described in Section 5.B, the DSKP algorithm is simulated and compared to a baseline IPACT-based SKP that supports SKG and SKC according to the order of user arrivals. The $K_{threshold}$ of QKPs, K_{rate} in different links, $Window_{T\_SKG}$, and the offered load of requests (OL) are set as variable parameters for the comparisons. The guard time between different ONUs is set to 800 ns according to [41]. K_{req} in each security request is a random value selected from the range [0, 400]. We consider 1 quantum channel to transmit quantum signals (|QW|=1) (it is also assumed that 2 other optical channels transmit measurement basis and sync signals respectively (|OW|=2), but their resource assignment simply follows resource assignment it the QKD wavelength). Note that the number of QKD wavelengths must be set proportionally to the number of QKD devices (so, in our setting for 32 ONUs, each hosting one Qtra, we estimated that 1 QW is enough). Based on the above simulation settings, the performance of our proposed algorithms is evaluated in terms of service-rejection ratio (SR), time-slot utilization (TU), guard time saving (GTS), and clustering tree diagram (CTD). Namely:

- SR is the probability of rejecting a security request (ratio between rejected and total security requests). Rejection of a security request occurs when no secret keys can be provided for the request.
- TU is the probability of occupying time slots for secure connection (ratio between occupied and total time slots). Calculation of time-slot occupation includes both SKG and SKC process.
- GTS is a percentage of guard-time-saving during SKC process (i.e., the percentual difference in guard time between using HC and not using HC).
- CTD is a metric used to provide a graphical presentation of how security requests are clustered in a time window. The clusters are obtained grouping the requests with the same destination nodes.

Optics EXPRESS

7.1. Service-rejection ratio (SR)

As shown in Fig. 7, we present SR under the combined impact of three variable factors (i.e., *OL*, $Window_{T\_SKG}$, $K_{threshold}$) plotted in the form of bar graphs. The figure is divided by a red dashed line, which shows the IPACT-based SKP on the left side and the DSKP on the right side. In general, DSKP significantly reduces SR compared to the IPACT-based SKP. This is because DSKP (specifically, during the LF-SKG phase) generates keys starting from the ONU with lowest number of keys in the QKP, hence alleviating the SR. Also, SR decreases for higher K_{rate}, since higher K_{rate} increases the generation of secret keys. As for varying *OF* (as shown in Fig. 7(a)), SR increases with bigger *OL*, because bigger *OL* accelerates the consumption of secret keys. For the changing of $Window_{T\_SKG}$ and $K_{threshold}$ shown in Figs. 7(b) and 7(c), the two figures show that $Window_{T\_SKG}$ has no influence on SR, and SR decreases for higher $K_{threshold}$, since higher $K_{threshold}$ can always guarantee a certain number of secret keys in QKP to satisfy security requests.

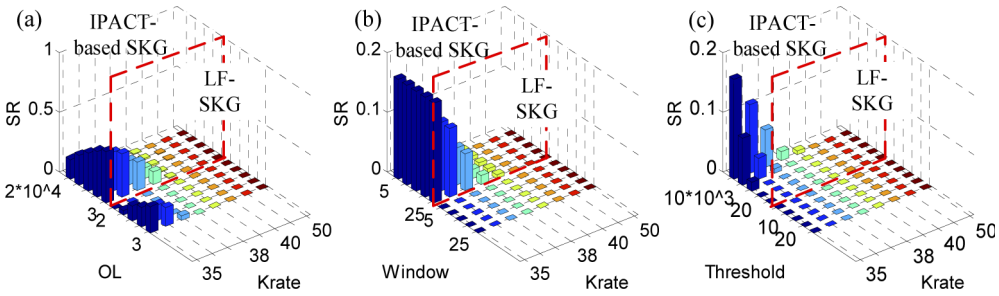

Fig. 7. Plots of SR under the combined impact of three factors (i.e., *OL*, $Window_{T\_SKG}$, $K_{threshold}$). Note that K_{rate} is varied from 35 to 50 with two unequal spacings (i.e., 1 and 5), and SKC rate is a value selected from a fixed range [0, 400]. (a), (b) and (c) are changing with three different variable parameters, i.e., *OL*, $K_{threshold}$, and $Window_{T\_SKG}$. Specifically, in (a) we assume $K_{threshold}$=5000 and $Window_{T\_SKG}$=5, in (b) we assume *OL*=20000 and $K_{threshold}$=5000, and in (c) we assume *OL*=20000 and $Window_{T\_SKG}$=5.

7.2. Time-slot utilization (TU)

Figure 8 shows the TU changing with different variable parameters, i.e., K_{rate} vs K_{req}, $K_{threshold}$ vs *OL*, $Window_{T\_SKC}$ vs *OL*. In Fig. 8(a), we can see bigger K_{req} and smaller K_{rate} can increase TU, since higher consumption rate requires higher time slots, and more SKG will enable QKP to support more SKC, thus occupying more time slots. As shown in Figs. 8(b) and 8(c), $K_{threshold}$ and $Window_{T\_SKC}$ almost have no influence on TU, as TU depends on the key volume contained in each security request (which is not affected by $K_{threshold}$ or $Window_{T\_SKC}$), while bigger *OL* can increase TU as more time slots will be occupied by increasing number of secret-key requests in a window. Note that the proposed algorithms are not compared with the benchmark, as the proposed algorithms and the IPACT benchmark have no different influence on TU which merely depends on key-volume requirements.

7.3. Guard time saving (GTS)

Figure 9 shows the impact of several system parameters GTS. Note that positive values of GTS mean HC SKC can save guard time, and the GTSs are always positive values under different parameter settings. For K_{rate}=180, $Window_{T\_SKC}$=20 and $K_{threshold}$ = 40000, GTS can be up to almost 40%. Specifically, Fig. 9(a) shows that K_{rate} and K_{req} have no influence on GTS, instead Fig. 9(b) shows that increase in *OL* and $Window_{T\_SKC}$ result in an increased GTS. This is because larger $Window_{T\_SKC}$ can allow more arrival of request to increase the probability of having same

Optics EXPRESS

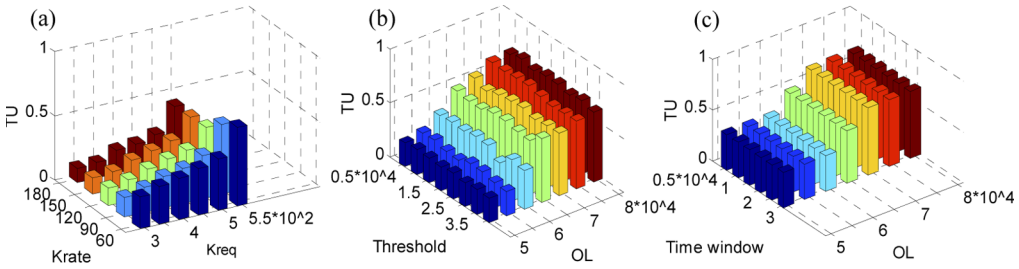

Fig. 8. The time-slot utilization (TU) under different variable parameters. (a) TU variation for different K_{rate} and K_{req}, (b) and (c) TU variations, for fixed K_{rate} and K_{req} (i.e., K_{rate}=60 and K_{req} in the range [0, 400]), but changing OF, $K_{threshold}$, and $Window_{T\_SKC}$.

destination nodes to save time. In Fig. 9(c), $K_{threshold}$ also shows no influence on GTS, but bigger OL can slightly increase GTS for the same reason seen in Fig. 8(b).

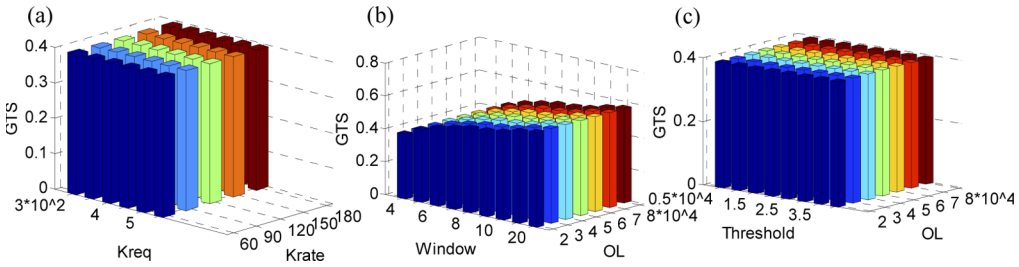

Fig. 9. The GTS under different variable parameters. The specific parameter settings are the same as in Fig. 8.

7.4. Service-rejection ratio (SR)

In Fig. 10, the CTDs graphically represent the clustering process of security requests during four time windows. The x- and y-axis represents the sample requests and the H of each time clustering (see Section 4.B), respectively. We randomly select the sample requests in a common time window to present their clustering tree diagram. At the beginning, every request is located in a common, and then we merge the two closest clusters to form a new sub-cluster according to H. As the cluster height increases, samples are decomposed into more classes. In addition, initial merging processes help increasing time saving, as it has been discussed in Section 5.D.

Optics EXPRESS

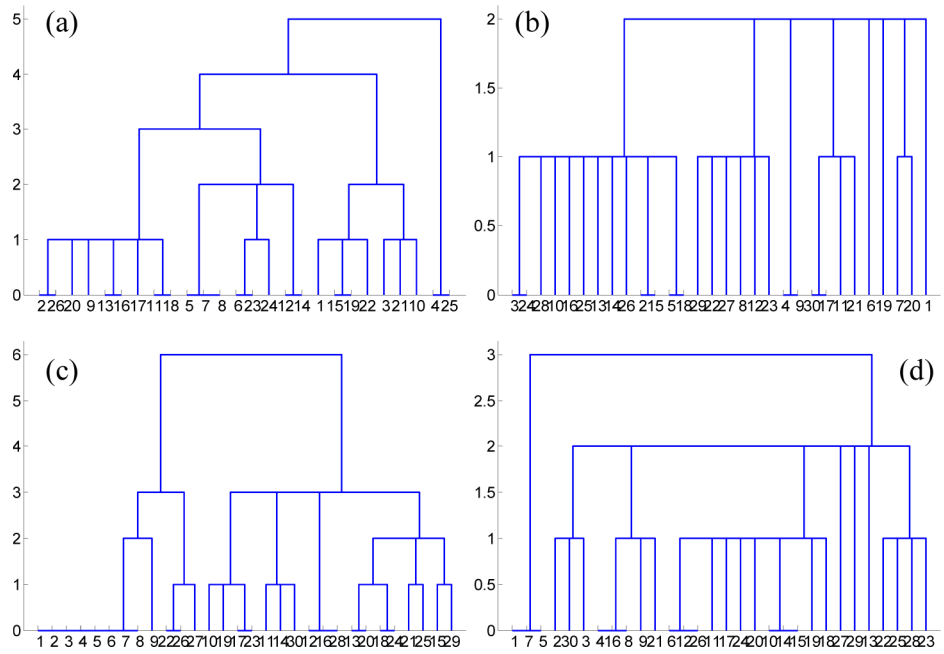

Fig. 10. Diagrams of clustering tree during four $Window_{T_SKC}$s in SKC process.

8. Conclusions

This paper investigates a QS-PON architecture to secure data transmission in PON via SKP, driven by point-to-multi-point QKD. By deploying QKD in PON, the QS-PON architecture shows how QKP can be used to efficiently distribute secret keys in QS-PON. After discussing the problems related to the processes of generation and consumption of secret keys, an algorithm, called DSKP, is devised to generate and assign secret keys on demand. Two targets are sought by DSKP, namely, to reduce service-rejection ratio and to avoid wastage of guard time as much as possible. To verify the effectiveness of our simulation settings, we construct a general QKP model that has similar performance with results presented in Ref. [40]. Then, we analyze the behavior of this model under both static and dynamic network settings. Finally, using dynamic simulation, we illustrate the effectiveness of DSKP algorithm in comparison with an IPACT-based baseline dynamic bandwidth assignment algorithm. We analyze four main metrics, SR, CTD, TU, and ITS, and we show that DSKP can reduce SR and ITS by about 16% and 39%, respectively. As future work, we plan to investigate aspects related to survivability of SKP in QS-PON.

Funding. National Key Research and Development Program of China (2020YFE0200600); National Natural Science Foundation of China (62021005, 61822105, 61971068); Fundamental Research Funds for the Central Universities (2019XD-A05); BUPT Postgraduates Innovation and Entrepreneurship Project (2020-YC-A420); BUPT Excellent Ph.D. Students Foundation (CX2019215).

Disclosures. The authors declare no conflicts of interest.

References

1. N. Skorin-Kapov, M. Furdek, S. Zsigmond, and L. Wosinska, "Physical-layer security in evolving optical networks," IEEE Commun. Mag. **54**(8), 110–117 (2016).
2. F. Arute, K. Arya, and R. Babbush, *et al.*, "Quantum supremacy using a programmable superconducting processor," Nature **574**(7779), 505–510 (2019).
3. P. A. M. Dirac, "The Principles of Quantum Mechanics," 3rd edn. Clarendon Press, Oxford, (1947).
4. P. D. Kumavor, A. C. Beal, S. Yelin, E. Donkor, and B. C. Wang, "Comparison of four multi-user quantum key distribution schemes over passive optical networks," J. Lightwave Technol. **23**(1), 268–276 (2005).

Optics EXPRESS

5. B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, "A quantum access network," Nature **501**(7465), 69–72 (2013).
6. P. D. Townsend, S. J. D. Phoenix, K. J. Blow, and S. M. Barnett, "Design of quantum cryptography systems for passive optical networks," Electron. Lett. **30**(22), 1875–1877 (1994).
7. L. H. Gong, Y. Liu, and N. R. Zhou, "Novel quantum virtual private network scheme for PON via quantum secure direct communication," Int. J. Theor. Phys. **52**(9), 3260–3268 (2013).
8. W. Chen, Z.-F. Han, T. Zhang, H. Wen, Z.-Q. Yin, F.-X. Xu, Q.-L. Wu, Y. Liu, Y. Zhang, X.-F Mo, Y.-Z. Gui, G. Wei, and G.-C. Guo, "Field experiment on a "star type" metropolitan quantum key distribution network," IEEE Photonics Technol. Lett. **21**(9), 575–577 (2009).
9. V. Fernandez, R. J. Collins, K. J. Gordon, P. D. Townsend, and G. S. Buller, "Passive optical network approach to gigahertz-clocked multiuser quantum key distribution," IEEE J. Quantum Electron. **43**(2), 130–138 (2007).
10. B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, S. W.-B. Tam, Z. L. Yuan, and A. J. Shields, "Quantum secured gigabit optical access networks," Sci. Rep. **5**(1), 18121 (2016).
11. I. Choi, R. J. Young, and P. D. Townsend, "Quantum key distribution on a 10Gb/s WDM-PON," Opt. Express **18**(9), 9600–9612 (2010).
12. A. Ciurana, J. Martínez-Mateo, M. Peev, A. Poppe, N. Walenta, H. Zbinden, and V. Martin, "Quantum metropolitan optical network based on wavelength division multiplexing," Opt. Express **22**(2), 1576–1593 (2014).
13. J. Martinez-Mateo, A. Ciurana, and V. Martin, "Quantum key distribution based on selective post-processing in passive optical networks," IEEE Photonics Technol. Lett. **26**(9), 881–884 (2014).
14. I. Choi, R. J. Young, and P. D. Townsend, "Quantum information to the home," New J. Phys. **13**(6), 063039 (2011).
15. G.989.1: 40-Gigabit-capable passive optical networks (NG-PON2): General requirements, ITU-T, G Series: G.989.1.
16. G. Kramer, B. Mukherjee, and G. Pesavento, "IPACT a dynamic protocol for an Ethernet PON (EPON)," IEEE Commun. Mag. **40**(2), 74–80 (2002).
17. B. Lannoo, L. Verslegers, D. Colle, M. Pickavet, M. Gagnaire, and P. Demeester, "Analytical model for the IPACT dynamic bandwidth allocation algorithm for EPONs," J. Opt. Netw. **6**(6), 677–688 (2007).
18. G. Kramer, B. Mukherjee, and G. Pesavento, "Interleaved polling with adaptive cycle time (IPACT): a dynamic bandwidth distribution scheme in an optical access network," Photonic Netw. Commun. **4**(1), 89–107 (2002).
19. Y. Cao, Y. Zhao, Y. Wu, X. Yu, and J. Zhang, "Time-scheduled quantum key distribution (QKD) over WDM networks," J. Lightwave Technol. **36**(16), 3382 (2018).
20. H. Wang, Y. Zhao, X. Yu, A. Nag, Z. Ma, J. Wang, L. Yan, and J. Zhang, "Resilient quantum key distribution (QKD)-integrated optical networks with secret-key recovery strategy," IEEE Access **7**, 60079–60090 (2019).
21. Y. Cao, Y. Zhao, C. Colman-Meixner, X. Yu, and J. Zhang, "Key on demand (KoD) for software-defined optical networks secured by quantum key distribution (QKD)," Opt. Express **25**(22), 26453–26467 (2017).
22. S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," Science **362**(6412), eaam9288 (2018).
23. S. Wang, W. Chen, Z.-Q. Yin, H.-W. Li, D.-Y. He, Y.-H. Li, Z. Zhou, X.-T. Song, F.-Y. Li, D. Wang, H. Chen, Y.-G. Han, J.-Z. Huang, J.-F. Guo, P.-L. Hao, M. Li, C.-M. Zhang, D. Liu, W.-Y. Liang, C.-H. Miao, P. Wu, G.-C. Guo, and Z.-F. Han, "Field and long-term demonstration of a wide area quantum key distribution network," Opt. Express **22**(18), 21739–21756 (2014).
24. M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, "Field test of quantum key distribution in the Tokyo QKD Network," Opt. Express **19**(11), 10387–10409 (2011).
25. D. Stucki, M. Legre, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat, J.-B. Page, D. Perroud, G. Ribordy, A. Rochas, S. Robyr, J. Tavares, R. Thew, P. Trinkler, S. Ventura, R. Voirol, N. Walenta, and H. Zbinden, "Long-term performance of the Swiss quantum key distribution network in a field environment," New J. Phys. **13**(12), 123001 (2011).
26. C. Elliott, "The DARPA quantum network," *Quantum Communications and cryptography*, CRC Press, 91–110 (2018).
27. A. Poppe, M. Peev, and O. Maurhart, "Outline of the SECOQC quantum-key-distribution network in Vienna," Int. J. Quantum Inform. **06**(02), 209–218 (2008).
28. L. C. Comandar, B. Fröhlich, M. Lucamarini, K. A. Patel, A. W. Sharpe, J. F. Dynes, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Room temperature single-photon detectors for high bit rate quantum key distribution," Appl. Phys. Lett. **104**(2), 021101 (2014).
29. H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," Phys. Rev. Lett. **117**(19), 190501 (2016).
30. A. Aguado, V. Lopez, D. Lopez, M. Peev, A. Poppe, A. Pastor, J. Folgueira, and V. Martin, "The Engineering of Software-Defined Quantum Key Distribution Networks," IEEE Commun. Mag. **57**(7), 20–26 (2019).

Optics EXPRESS

31. Y. Cao, Y. Zhao, X. Yu, and J. Zhang, "Multi-tenant provisioning over software defined networking enabled metropolitan area quantum key distribution networks," J. Opt. Soc. Am. B **36**(3), B31–B40 (2019).
32. R. Wang, R. S. Tessinari, E. H. Salas, A. Bravalheri, N. Uniyal, A. S. Muqaddas, R. S. Guimaraes, T. Diallo, S. Moazzeni, Q. Wang, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "End-to-end Quantum Secured Inter-Domain 5G Service Orchestration Over Dynamically Switched Flex-Grid Optical Networks Enabled by a q-ROADM," J. Lightwave Technol. **38**(1), 139–149 (2020).
33. Y. Cao, Y. Zhao, J. Wang, X. Yu, Z. Ma, and J. Zhang, "KaaS: Key as a Service over Quantum Key Distribution Integrated Optical Networks," IEEE Commun. Mag. **57**(5), 152–159 (2019).
34. Y. Zhao, Y. Cao, W. Wang, H. Wang, X. Yu, J. Zhang, M. Tornatore, Y. Wu, and B. Mukherjee, "Resource Allocation in Optical Networks Secured by Quantum Key Distribution," IEEE Commun. Mag. **56**(8), 130–137 (2018).
35. X. Tang, A. Wonfor, R. Kumar, R. V. Penty, and I. H. White, "Quantum-safe metro network with low-latency reconfigurable quantum key distribution," J. Lightwave Technol. **36**(22), 5230–5236 (2018).
36. F. Murtagh and P. Contreras, "Algorithms for hierarchical clustering: an overview, II," WIREs Data Mining Knowl. Discov. **7**(6), e1219 (2017).
37. A. Bouguettaya, Q. Yu, X. Liu, X. Zhou, and A. Song, "Efficient agglomerative hierarchical clustering," Expert Syst. Appl. **42**(5), 2785–2797 (2015).
38. N. Pang, J. Zhang, C. Zhang, and X. Qin, "Parallel Hierarchical Subspace Clustering of Categorical Data," IEEE Trans. Comput. **68**(4), 542–555 (2019).
39. A. Banerjee, Y. Park, F. Clarke, H. Song, S. Yang, G. Kramer, K. Kim, and B. Mukherjee, "Wavelength-division-multiplexed passive optical network (WDM-PON) technologies for broadband access: a review," J. Opt. Netw. **4**(11), 737–758 (2005).
40. H. Song, B. W. Kim, and B. Mukherjee, "Long-reach optical access networks: A survey of research challenges, demonstrations, and bandwidth assignment mechanisms," IEEE Commun. Surv. Tutorials **12**(1), 112–123 (2010).
41. L. G. Kazovsky, W.-T. Shaw, D. Gutierrez, N. Cheng, and S.-W. Wong, "Next-generation optical access networks," J. Lightwave Technol. **25**(11), 3428–3442 (2007).

83.48.185.44 on 2021-01-12 12:54:11