Flexible Encryption Tunnel with Limited Quantum Key Distribution over Classical Optical Networks

Yuhang Liu
State Key Lab of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications
Beijing, 100876 China
yuhangliu@bupt.edu.cn

Xiaosong Yu
State Key Lab of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications
Beijing, 100876 China
xiaosongyu@bupt.edu.cn

Yongli Zhao
State Key Lab of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications
Beijing, 100876 China
yonglizhao@bupt.edu.cn

***Abstract*—The increasing threat posed by quantum computing to traditional encryption methods necessitates the development of advanced cryptographic solutions. Quantum key distribution (QKD), with its ability to generate secure symmetric keys, offers a promising approach. However, QKD faces significant challenges in practical deployment, especially in multi-point interconnected networks. This work introduces a flexible encryption tunnel (FET) designed to address these challenges by dynamically adjusting cryptographic strength and key supply strategies based on network conditions and secret key rate fluctuations. The proposed mechanism ensures seamless integration of QKD within classical optical networks, optimizing key utilization through multi-path routing and adaptive encryption. We compare the performance of FET-based QKD (FET-QKD) with rigid encryption tunnel-based QKD (RET-QKD) across various network topologies, including ring, tree, and mesh. Simulation results demonstrate that FET-QKD achieves a peak QKD service success ratio of 98.4% in ring topology under high traffic loads and a key throughput of 2.43 Mbits, outperforming RET-QKD by over 3.1 times. However, performance gains are limited in complex mesh networks due to increased interference and resource contention. This study highlights the potential of FET-QKD to facilitate the widespread adoption of QKD by enhancing the synergy between quantum and classical networks.**

Keywords—Quantum key distribution, flexible encryption tunnel, optical network

I. Introduction

Quantum computing is increasingly posing a threat to traditional encryption methods that rely on computational complexity, bringing security risks to sensitive data communications [1]. This includes sectors such as financial services and government communications. Quantum key distribution (QKD), based on the principles of quantum mechanics, can detect eavesdropping on communication channels and generate symmetric keys that are secure over the long term. These keys can replace the key exchange mechanisms used in protocols like transport layer security and internet protocol security, providing enhanced data communication security [2]. However, due to the fragile nature of quantum states and the current immaturity of quantum repeaters, QKD requires parallel deployment alongside existing data communication infrastructure. This forms an independent key provisioning infrastructure. Considering cost constraints, network operators aim to enable plug-and-play functionality for QKD devices at classical optical communication nodes [3]. Additionally, they seek to support quantum channels using wavelength division multiplexing, eliminating the need for additional fibre deployment [4].

Despite these efforts, the practical deployment of QKD still faces theoretical limitations. These constraints hinder its large-scale application in multi-point interconnected networks. One significant challenge is the rate-distance trade-off: the secret key rate (SKR) in QKD decreases significantly with distance [5]. As a result, QKD struggles to generate sufficient keys to meet the security demands of high-capacity communications over long distances. This limitation creates a mismatch between the available key resources and the growing demand for secure, high-capacity communication in modern networks. Another challenge arises from the low intensity of quantum channels, which makes them vulnerable to noise when coexisting with classical optical communication [6]. Quantum channels operate at extremely low power, while classical data channels, particularly high-power signals, can introduce noise through phenomena such as Raman scattering. This interference degrades the transmission quality of quantum bits and reduces the SKR of QKD. Additionally, in networks where high-power signals are dynamically configured, the power levels and routes of classical signals frequently change. These changes cause unpredictable fluctuations in SKR, further complicating the integration of QKD into practical network environments [7].

Given these challenges, designing an encryption tunnel based on QKD that can adjust dynamically is critical. The tunnel must respond to changes in network traffic, real-time encryption requirements, and quality of service demands. Developing a flexible encryption tunnel that can intelligently manage key resources and adapt to dynamic network conditions is essential for the widespread adoption of QKD. In this work, we propose a flexible encryption tunnel mechanism considering the limited QKD capability. This mechanism adjusts encryption strategies according to the key rate fluctuations, variations in network traffic, and diverse encryption needs. It ensures optimal allocation and utilization of QKD key resources in multi-point interconnected networks.

II. Limited QKD over Classical Optical Networks

In a multi-point interconnected QKD network, key supply serves as a fundamental function. The process can be divided into two main stages: QKD-key supply and key supply agent (KSA)-key supply. As shown in Fig. 1(a), the QKD-key supply refers to the transmission of keys generated by the point-to-point QKD system to the key manager (KM). The capacity of this process is measured by the SKR, which is

979-8-3315-2096-0/25/$31.00 ©2025 IEEE

constrained by the rate-distance limitation of the QKD system. As distance increases, the SKR decreases accordingly. Furthermore, SKR can be influenced by noise, particularly in scenarios where QKD and classical optical communication coexist. In such cases, classical signals may interfere with quantum channels via effects like Raman scattering, further reducing the SKR.

On the other hand, as shown in Fig. 1(b), KSA-key supply involves the distribution of keys from the KSA to the end users. For the end-to-end cryptographic application (CA), the overall key supply is built upon the QKD-keys. The end-to-end key supply is based on trusted relay, and according to the principles of the one-time pad, the global key can only be securely supplied when every segment of the relay successfully generates keys. The rate at which this global key supply is constructed is defined as the key supply rate (KSR). KSR represents the network's ability to provide keys in an end-to-end manner. Since KSR depends on the minimum SKR across multiple relay segments, it is constrained by a bottleneck effect, where the segment with lowest SKR limits the overall KSR. Together, these two processes enable continuous key supply for multi-point communications. However, due to the challenges for QKD over classical optical networks, effectively managing and improving KSR remains a critical issue in QKD network design.

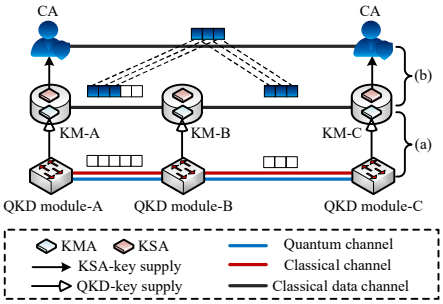

Fig. 1. (a) Illustration of point-to-point QKD-key supply amd (b) end-to-end KSA-key supply.

A. *Limitation on QKD-key Supply with Classical Optical Interference*

Leveraging existing classical optical network infrastructure for the deployment of QKD significantly enhances the practical application prospects of QKD. However, classical data channels inherently interfere with quantum channels, especially in wavelength division multiplexing systems where quantum and classical channels coexist within the same optical fibre. This interference primarily occurs in two forms. The first is Raman scattering, where high-power classical optical signals traveling through the fibre introduce noise into nearby quantum signals through the Raman effect. This noise reduces the reception efficiency of single-photon states. The second form is crosstalk from adjacent channels. Due to the non-ideal performance of devices, classical channels can interfere with quantum channels through spectral leakage and other interactions. Both forms of interference can significantly degrade the SKR in QKD systems.

Moreover, the dynamic configuration of classical optical communications can induce fluctuations in quantum channels. For example, adjusting the power, routing, or wavelength of classical signals within the network can cause instantaneous or sustained interference to quantum channels, leading to unpredictable fluctuations in the SKR of QKD systems. Thus, while QKD systems already experience jitter due to environmental noise and device stability during transmission, the dynamic changes in classical optical communications further exacerbate this uncertainty. As shown in Fig. 2, under ideal conditions represented by the blocks, the QKD system between nodes C and D can generate five key units per time unit. However, when dynamic adjustments occur in classical signal power, routing, or wavelength, interference from Raman scattering and crosstalk from adjacent channels leads to a reduction in the SKR, which is illustrated by the grey blocks. In this case, the QKD system over link C-D can only produce four key units per time unit, highlighting a degradation in the SKR. This reduction in key generation not only disrupts the stability of key supply but also imposes constraints on the overall network's security performance. In scenarios where large volumes of keys are required, this SKR degradation introduces a bottleneck that could compromise the system's ability to maintain secure communication. This makes the fluctuation of SKR one of the key issues affecting QKD performance in practical deployments.

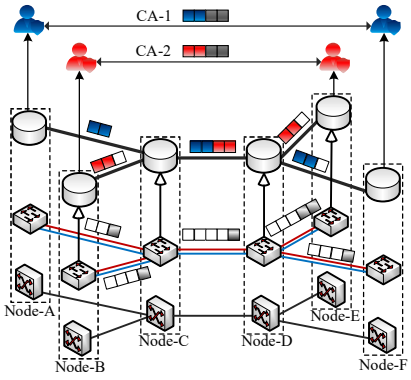

Fig. 2. Illustration of limited QKD over classical optical networks

B. *Limitation on KSA-key Supply with Uneven SKR Distribution and Resource Competition*

In a multi-point interconnected QKD network, the key supply capacity at the KSA level is tightly coupled with the SKR of individual QKD system segments. However, due to inherent fluctuations in the SKR across different QKD links, the network often experiences uneven SKR distribution. This uneven distribution causes variability in the KSR, as the overall key supply for end-to-end communication is constrained by the segment with the lowest SKR. When one segment has a lower SKR, it creates a bottleneck that limits the key supply capacity across the entire QKD network. Furthermore, dynamic SKR fluctuations across different links exacerbate this instability, making it challenging to support large-scale key distribution. Addressing this fluctuation and ensuring consistent key supply at the KSA-key supply level is critical for maintaining optimal QKD network performance.

Another limiting factor is resource competition in key relay routes. As illustrated in Fig. 2, the QKD link C-D simultaneously serves as a middle segment for both the A-F and B-E key relay routes, leading to resource competition. In this case, the SKR of the C-D link is not only limited by its

inherent conditions but also by the need to meet the key supply demands of multiple relay routes. When resources on the C-D link are constrained, this competition directly affects the overall KSR of both relay routes. Since both the A-F and B-E routes rely on the C-D link, the bottleneck created by the C-D link could reduce the KSR for both CA-1 and CA-2, thereby affecting the key distribution capacity across the network. Particularly under high-load scenarios, the C-D link may need to dynamically allocate key resources between multiple relay routes, further increasing system complexity and uncertainty.

To address this issue, scheduling mechanisms can be employed to dynamically optimize resource allocation on the C-D link based on the key demands and the status of each route. By constructing flexible encryption tunnels for the two cryptographic applications, the network can adaptively allocate key resources and adjust tunnel configurations according to the actual key requirements and link conditions. This dynamic approach allows the network to mitigate resource competition, and enhance the overall performance and scalability of the QKD system.

III. Flexible Encryption Tunnel with Limited QKD

In addressing the aforementioned challenges, the flexible encryption tunnel-based QKD (FET-QKD) is an encryption mechanism designed to dynamically adjust cryptographic strength and key supply strategies based on the real-time state of the network and fluctuations in SKR. This mechanism is particularly effective in addressing the challenges faced by QKD systems, especially in classical optical networks where issues such as interference from Raman scattering and SKR fluctuations are more pronounced. It enables QKD and classical optical communications to operate in synergy, providing continuous secure communication services through dynamic encryption adjustments, even when resources are limited or key supply is insufficient. The core features of the flexible encryption tunnel include the following:

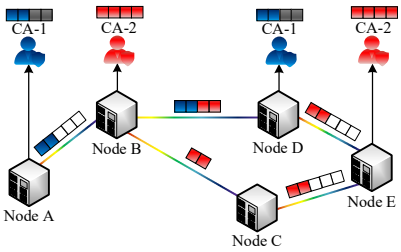

Fig. 3. Illustration of flexible encryption tunnel-based QKD strategy

Adaptability: The flexible encryption tunnel can dynamically adjust cryptographic strength based on the real-time SKR of the QKD system. When SKR fluctuates or decreases, the system can opt for alternative the encryption algorithm or reduce the key update frequency to maintain communication security, even in situations of insufficient key supply. When the KSR stabilizes, the encryption tunnel can increase the key supply frequency to enhance overall encryption strength. As shown in Fig. 3, this adaptability is illustrated by CA-1, where the encryption algorithm switches according to SKR fluctuations. Initially, CA-1 requests four key units for encryption, but when SKR decreases, the flexible encryption tunnel adapts by reducing the key supply to two units, ensuring communication continuity. Although the number of keys is reduced, the flexible encryption tunnel maintains encryption security by adjusting the encryption algorithm or lowering the update frequency to accommodate the limited key supply.

Resource Optimization: Based on the controller's global resource optimization capability, the flexible encryption mechanism is enabled to search for and maximize the use of available QKD key resources in resource-constrained scenarios. The tunnel can coordinate key resources across multiple routes, establishing a multi-route key supply mechanism to improve resource utilization efficiency and alleviate resource competition caused by concurrent service demands. Fig. 3 demonstrates this resource optimization through the multi-route key supply construction for CA-2. To meet the needs of CA-2, the system uses both the key relay routes B-D-E and B-C-E to simultaneously construct end-to-end KSA-keys, achieving the requested key supply. This optimization effectively leverages the key generation capacity of multiple QKD links, improving the overall KSR and preventing resource competition on a single path.

TABLE I. Pseudocode of FET-QKD Strategy

FET-QKD Strategy

Input: $G(V, E, W)$, R.
Output: F_R, π_R, the FET-QKD result for each user request, and updated network status.

Initialize $F_R \leftarrow \emptyset$;
for each service request $r(s_r, d_r, b_r, k_x) \in R$ **do**
  routing computation for $r(s_r, d_r, b_r, k_x)$ with K-shortest-path (KSP), store the result as $\pi_r(p_r, \lambda_r)$;
  routing for the data communication request $r_d(s_r, d_r, b_r)$ with first-fit algorithm, store the result as $\pi_{rd}(p_{rd}, \lambda_{rd})$;
  if $(\pi_{rd}(p_{rd}, \lambda_{rd}) = \emptyset)$
    mark $F_r = FAILED$;
    break;
  end if
  Initialize $\eta_{max} \leftarrow \infty$, $KSR\_total \leftarrow 0$;
  for each available routing p_{ri} in $\pi_r(p_r, k_x)$
    Initialize $KSR\_candidate \leftarrow \infty$;
    for each traversed links (s_i, d_j) in p_{ri}
      record SKR and $KSR\_occupied$ for ongoing services;
      $KSR\_remain \leftarrow SKR - KSR\_occupied$;
      if $(KSR\_remain < KSR\_candidate)$
        $KSR\_candidate \leftarrow KSR\_remain$;
      end if
    end for
    if $(KSR\_candidate > k_x)$
      add (p_{ri}, k_x) to the routing result π_r;
      mark $F_r = SUCCEED$;
      break;
    else if $(KSR\_candidate > k_{compromized})$
      mark $F_r = Compromised$;
      break;
    else if $(KSR\_candidate > 0)$
      add $(p_{ri}, KSR\_candidate)$ to the routing result π_r;
      $KSR\_total \leftarrow KSR\_total + KSR\_candidate$;
      if $(KSR\_total > k_{compromized})$
        $KSR\_replace \leftarrow KSR\_candidate - (KSR\_total - k_{compromized})$;
        add $(p_{ri}, KSR\_replace)$ to the routing result π_r;
        mark $F_r = Compromised$;
        break;
      end if
    end if
  end for
end for
return the route table π_R, success flag F_R, and updated network status.

The FET-QKD algorithm implements the flexible encryption tunnel by dynamically managing QKD-key and KSA-key supply, and optimizing multi-route to adapt to real-time SKR fluctuations and resource constraints. As outlined in the pseudocode in Table 1, the algorithm begins by initializing the result set and iterating over each service request to compute viable routes for both QKD and classical data communication. The algorithm's core adaptive mechanism lies in its ability to calculate and update the available KSR for each traversed link. As each candidate route is evaluated, the algorithm retrieves real-time SKR and KSR status from the network (Line 13) and adjusts the candidate path's available KSR accordingly (Lines 14–17). If the remaining KSR along any segment is lower than expected, the system reduces the requested key supply to fit within the available resources, maintaining communication continuity by switching to a degraded encryption algorithm if needed.

When multiple key relay routes are available, the algorithm performs incremental key allocation to optimize resource usage. It distributes key demands across multiple routes (e.g., using both B-D-E and B-C-E paths in Fig. 3) to prevent bottlenecks on any single path. If a route cannot meet the key request, the algorithm aggregates partial keys from multiple routes (Lines 26–28) until the total demand is satisfied, at which point any excess allocation is trimmed (Lines 29–32) to avoid resource wastage. This multi-route key supply strategy ensures that QKD and classical optical networks can function in synergy, even when the available SKR is limited or unevenly distributed. By the end of each iteration, the algorithm updates the routing table and network status (Line 38), providing feedback for future adjustments. Based on the above, the FET-QKD algorithm realizes the flexible encryption tunnel, ensuring that both security and efficiency are maintained even in the case of constrained resources and fluctuating network conditions.

IV. Simulation Results

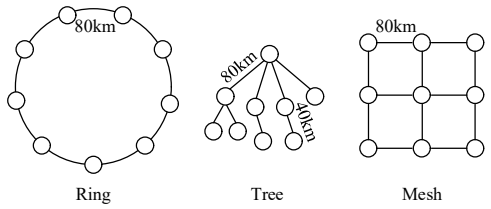

Fig. 4. 9-node ring, tree, and mesh network topologies.

For the proposed strategy, simulations were conducted using three common metro-scale topologies: ring, tree, and mesh, each consisting of 9 nodes. The link distance was fixed at 80 km in ring and mesh topologies, and each classical data service operated at a bit rate of 100 Gbps. In the tree topology, the first layer links were set to 80km, while the second layer links were configured to 40km to simulate the access side. Each link was equipped with a DV-QKD system to serve 105 service requests, arriving according to a Poisson distribution. The simulations were implemented using Java 1.8. The quantum channels for QKD systems were assigned to the optimal wavelength at real time and co-propagated with 100 Gbps data channels across 40 wavelength channels, ranging from 1530 nm to 1562 nm, with a 0.8 nm spacing. As recommended by NIST for AES key renewal, each 64 GB data block requires one 256-bit AES key for encryption [8]. The use of AES-128 was considered a compromised QKD service. All simulation results were averaged over 100 runs to ensure statistical reliability. The detailed parameter settings for the DV-QKD system are provided in Table 2 [9].

TABLE II. Parameters Setting of The DV-QKD System

Parameter	Value
Average number of photons per signal pulse, μ	0.48
Phase-distortion error probability, e_d	0.015
Quantum efficiency of detectors, η_d	0.2
Channel loss coefficient, α	0.046km^{-1}
Receiver dark count rate, γ_{dc}	1E-7ns^{-1}
Time gate interval, T_d	100ps
Pulse repetition frequency, f_s	1GHz
Optical transmit power for data communication	0dBm

Figs. 5, 6, and 7 compare rigid encryption tunnel-based QKD (RET-QKD) and FET-QKD in terms of QKD service success ratio (QSSR) and total key utilization (TKU) across 9-node ring, tree, and mesh topologies. In these comparisons, QSSR reflects the proportion of successfully completed QKD services, while TKU refers to the total throughput of keys used during communication. In Fig. 5, under a traffic load of approximately 200 erlangs, RET-QKD achieves a QSSR of 32.5%. In contrast, FET-QKD leverages flexible encryption tunnels to achieve a QSSR of 98.4%, demonstrating its robustness against network load variations. Furthermore, FET-QKD significantly TKU, with a value of 2.43 Mbits compared to 0.79 Mbits for RET-QKD, representing an improvement of approximately 3.1 times. This indicates that FET-QKD not only ensures service continuity under heavy network traffic but also optimizes resource usage through key relay route selection and key management strategies.

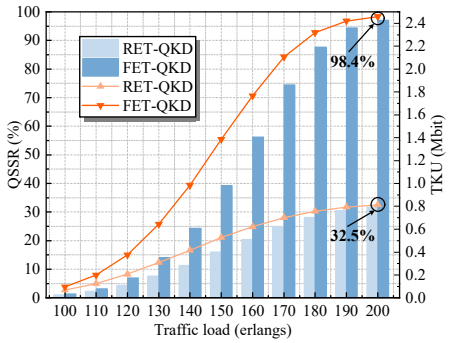

Fig. 5. Comparison of RET-QKD and FET-QKD in terms of QSSR and TKU in ring topology.

As shown in Fig. 6, in the tree topology, the hierarchical structure and multi-hop communication introduce challenges for key distribution. With a traffic load of approximately 200 erlangs, the comparison between RET-QKD and FET-QKD highlights significant differences in QSSR and TKU. The QSSR for RET-QKD remains low due to limited key supply, while FET-QKD achieves a higher QSSR of approximately 97.1%. This results from the adaptive encryption mechanism that dynamically adjusts the encryption strength and efficiently allocates keys across multiple key relay routes. Moreover, the TKU for FET-QKD reaches 2.38 Mbits under

the same conditions, a significant improvement over RET-QKD. This increase ensures that key resources are utilized optimally, reducing the impact of resource contention in a tree-based network. The ability to maintain higher QSSR and TKU demonstrates the effectiveness of FET-QKD in overcoming the inherent limitations of tree topologies, where bottlenecks are common due to traffic concentration at intermediate nodes.

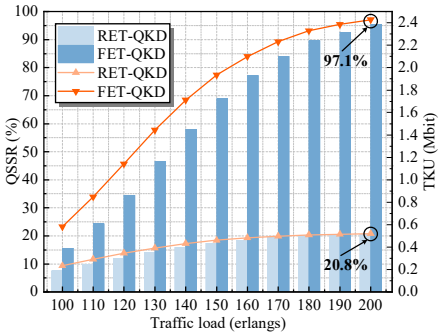

Fig. 6. Comparison of RET-QKD and FET-QKD in terms of QSSR and TKU in tree topology.

In the mesh topology, we compared the performance of RET-QKD and FET-QKD under different traffic loads. At a traffic load of 200 erlangs, the QSSR for RET-QKD and FET-QKD reaches 15.5% and 38.9%, respectively. Although FET-QKD shows a slight reduction in QSSR under high-load conditions, it demonstrates a significant advantage in terms of TKU. Specifically, at 200 erlangs, the TKU for RET-QKD is 0.31 Mbits, while FET-QKD achieved a TKU of 0.68 Mbits, representing a 2.19-fold increase in key throughput. However, the performance optimization of FET-QKD in the mesh topology is limited compared to other topologies, as indicated by the QSSR peaking at only 38.9% under certain conditions. This limitation can be explained by the complexity of routing in mesh networks, where the increased number of interconnected nodes results in higher resource contention and interference among key relay routes. Even with flexible encryption, the overlapping routings may create bottlenecks that restrict further improvement in QSSR. Additionally, the dynamic nature of key demand in mesh topologies requires more frequent adjustments to encryption tunnels, which may further impact service stability and reduce QSSR at higher traffic loads.

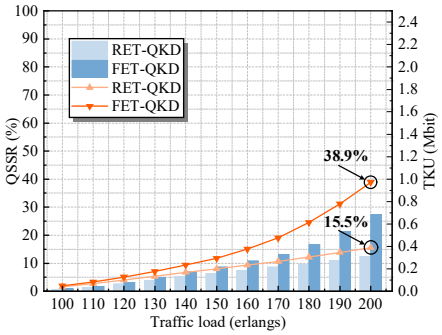

Fig. 7. Comparison of RET-QKD and FET-QKD in terms of QSSR and TKU in mesh topology.

V. Conclusions

This work presents a flexible encryption tunnel mechanism that enables the efficient deployment of QKD over classical optical networks. The proposed FET-QKD strategy dynamically adapts to network fluctuations, ensuring optimal key distribution and service continuity, even under constrained resource conditions. Through simulations across ring, tree, and mesh topologies, FET-QKD demonstrated a QSSR of 98.4% in ring topology, ensuring uninterrupted QKD service, even under heavy traffic loads. In tree topology, FET-QKD improved TKU to 2.38 Mbits compared to RET-QKD, showcasing its ability to manage hierarchical structures with multi-hop communication. In mesh topology, FET-QKD achieved a TKU of 0.68 Mbits at 200 erlangs, representing a 2.19-fold improvement over RET-QKD, though QSSR only reached 38.9% due to increased path interference and resource contention. These findings underscore the importance of adaptive encryption strategies in overcoming the inherent limitations of QKD systems and maximizing their utility across diverse network environments. The performance limitations in mesh networks highlight the need for further research. Future work will focus on advanced scheduling algorithms and key relay architectures to enhance scalability, reduce interference, and further optimize key utilization, promoting the large-scale adoption of QKD.

Acknowledgment

This work was supported by Innovation Program for Quantum Science and Technology (2021ZD0300704), NSFC project (62350001, U22B2026), the Funds for Creative Research Groups of China (62021005), the Fundamental Research Funds for the Central Universities (2023PY08), and BUPT Excellent Ph.D. Students Foundation under Grant CX2023140. (Corresponding author: Xiaosong Yu)

References

[1] F. Hu, et al., "Quantum computing cryptography: Finding cryptographic Boolean functions with quantum annealing by a 2000 qubit D-wave quantum computer," Physics Letters A, vol. 384, no. 10, pp. 126214, April 2020.

[2] Y. Cao, et al., "The evolution of quantum key distribution networks: On the road to the qinternet," IEEE Communications Surveys & Tutorials, vol. 24, no. 2, pp. 839-894, January 2022.

[3] X. Yu et al., "Secret-Key Provisioning With Collaborative Routing in Partially-Trusted-Relay-based Quantum-Key-Distribution-Secured Optical Networks," J. Lightwave Technol., vol. 40, no. 12, pp. 3530-3545, February 2022.

[4] F. Honz et al., "First Demonstration of 25λ× 10 Gb/s C+ L Band Classical/DV-QKD Co-Existence Over Single Bidirectional Fiber Link," J. Lightwave Technol., vol. 41, no. 11, pp. 3587-3593, June 2023.

[5] M. Lucamarini, et al., "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," Nature, vol. 557, no. 7705, pp. 400-403, May 2018.

[6] J. N. Niu, et al., "Optimized channel allocation scheme for jointly reducing four-wave mixing and Raman scattering in the DWDM-QKD system," Appl. Optics, vol. 57, no. 27, pp. 7987-7996, September 2018.

[7] X. Yu et al., "Multi-path-based quasi-real-time key provisioning in quantum-key-distribution enabled optical networks (QKD-ON)," Opt. Express, vol. 29, no. 14, pp. 21225-21239, June 2021.

[8] E. Barker, et al., "Recommendation for pair-wise key-establishment schemes using discrete logarithm cryptography," National Institute of Standards and Technology, Gaithersburg, Maryland, USA, No. NIST Special Publication (SP) 800-56A Rev. 3 (Draft), 2018, DOI: 10.6028/NIST.SP.800-56Ar3.

[9] S. Bahrani, M. Razavi, and J. A. Salehi, "Wavelength assignment in hybrid quantum-classical networks," Scientific reports, vol. 8, no. 1, pp. 3456, 2018, DOI: 10.1038/s41598-018-21418-6.