IC-QKD: An Information-Centric Quantum Key Distribution Network

Qiaolun Zhang, Omran Ayoub, Jun Wu, Xi Lin, Massimo Tornatore

***Abstract*—Current and next-generation networks are threatened by emerging attacks from quantum computers. To protect these services against quantum threat, quantum key distribution (QKD) using optical networks is being investigated and tested as a safe countermeasure to provide information-theoretic security. Although recent studies confirm the feasibility of QKD over optical networks, two main technical challenges, among others, remain unaddressed: i) the limited rate of generating keys requires efficient key distribution to secure the numerous applications, and ii) as key requests from applications can be characterized by different importance, QKD networks need a key distribution platform that accounts for such diversity. To address these challenges, we propose to incorporate the paradigm of Information-Centric Networking (ICN) within the QKD process, and we describe a novel information-centric quantum key distribution (IC-QKD) network for efficient and differentiated key distribution. We first design a semantic-based key distribution scheme, which leverages ICN to incorporate the knowledge of application importance in QKD and to enhance the resource efficiency of QKD by decoupling the sender from its receiver. We then propose an in-network key-caching scheme, which is especially advantageous for multicast applications, as keys can be cached and reused for multiple users of a multicast group to accelerate key distribution. Finally, we design a semantic-based application analysis for semantic-based key caching and distribution, which serves various applications with different priorities. Simulation results show that the proposed QKD network can reach up to about 16% increase in the capability of serving key requests with respect to the existing QKD network.**

***Index Terms*—Quantum key distribution, Information-Centric Networking, key caching.**

I. Introduction

Current and next-generation networks, such as Fifth Generation (5G) and Sixth Generation (6G) networks will serve as the communication infrastructure for a new digital world, where a wide range of new network applications will be offered as, e.g., autonomous driving and remote medicine. These new applications require to transmit over the network very sensitive users' information [1], and any breach in network security can compromise users' privacy and, in turn, societal well-being. To cope with new emerging security threats, approaches guaranteeing network security need to continuously evolve.

Network security, including data integrity and privacy, is currently ensured through cryptographic-based network security protocols such as Secure Shell Protocol and Secure Sockets Layer. Such protocols are designed with well-established encryption techniques, such as public-key cryptography and symmetric-key cryptography. However, as quantum computing rapidly evolves, traditional cryptographic techniques risk being compromised by attacks from large-scale quantum computers. Hence, operators are looking into novel security frameworks, as traditional encryption methods can no longer offer the security level required in especially next-generation networks [2].

Two main quantum-safe security technologies are being currently investigated, namely, post-quantum cryptography (PQC), aiming at designing new algorithms that are resilient against a quantum computer, such as lattice-based cryptography [2], and Quantum Key Distribution (QKD), which instead aims at creating a secure communication channel by exploiting fundamental principles of quantum mechanics, such as no-cloning theorem. Specifically, QKD substitutes public-key cryptography by securely distributing keys. Among these two techniques, PQC is only secure against known quantum attacks [2], while QKD is proved to be information-theoretic secure. In addition, QKD has already been investigated and tested in optical networks. Moreover, its standardization is ongoing by the ITU Telecommunication Standardization Sector and by the Industry Specification Group on QKD for Users of the European Telecommunications Standards Institute.

Recent technical progress in QKD is threefold. First, QKD is being implemented over optical networks to overcome the restrictions of the point-to-point nature of QKD links [3], [4], hence allowing QKD to secure networked users with trusted nodes. Specifically, a trusted node converts a quantum signal to a classical signal and generates a new quantum signal to distribute the keys to the next nodes. Although trusted node introduces weak points, a recent study proves that with current technology, long-range QKD is not feasible without trusted nodes [5]. Second, the record point-to-point transmission distance of QKD in optical fiber [6] and total distance for satellite-to-ground QKD [7] can now reach up to 830 kilometers and 4,600 kilometers, respectively, making it possible to deploy a global QKD network. Third, QKD has been demonstrated in an optical network over already-deployed fibers, which reduces the time and cost to deploy QKD systems, hence facilitating its adoption [8]. All these recent advances in QKD confirm the feasibility of a real integration of QKD within current and next-generation networks. Recent works already set the initial vision on how to secure 5G/6G with QKD [1], but they do not specifically

Qiaolun Zhang and Massimo Tornatore are with the Department of Electronics, Information and Bioengineering, Politecnico di Milano, 20133 Milano, Italy.

Omran Ayoub is with the Department of Innovative Technologies, University of Applied Sciences of Southern Switzerland, 6928 Lugano, Switzerland.

Jun Wu (corresponding author) is with the Graduate School of Information, Production and Systems, Waseda University, Fukuoka 808-0135, Japan (e-mail: jun.wu@ieee.org).

Xi Lin are with School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, China and Shanghai Key Laboratory of Integrated Administration Technologies for Information Security, China.

offer solutions to two important challenges facing the practical deployment of QKD networks, namely, the *limited amount of distributed secret keys* and *highly dynamic and diverse key requirements of different applications*.

Limited Amount of Distributed Secret Keys: The secret key rate (defined as the speed at which keys are generated between network nodes) achievable in today's QKD networks is still relatively low, which requires new schemes to accelerate key distribution. For instance, the maximum secret key rate of a metropolitan area deployment [4] is less than 100 kbps, i.e., it can only provide 400 keys per second (assuming AES-256 protocol), which is a low key rate considering the large number of requests expected in 5G/6G networks. These limitations are aggravated in wide-area networks, as key rate significantly decreases with distance (less than 1 kbps with transmission distance longer than 500 km as in Ref. [6]) due to absorption and noise affecting the quantum signals [3]. A possible approach to meet the high demand for secret keys is to store (cache) unused keys generated during low-request periods in key repositories, called Quantum Key Pools (QKPs) [3], maintained in each node for later use to improve resource efficiency, and hence accelerating key distribution.

Highly Dynamic and Diverse Key Requirements of Different Applications: The current networks (5G as an example) have three categories of services, namely, Enhanced Mobile Broadband, Ultra-reliable and Low-latency Communications, and Massive Machine Type Communications, which represent a variety of applications with different requirements, in terms of, e.g., as latency, security level, importance, etc. Future 6G networks are envisioned to support even more revolutionary applications affecting experiences of humans and machines with diverse key requirements [1]. To guarantee the security of these applications, QKD schemes over optical networks need to adapt swiftly to dynamic and diverse key requests for current and next-generation networks.

In this study, we investigate how Information-Centric Networking (ICN) can provide desirable features in terms of effective content distribution [9] that can be of utmost benefit in QKD networks. Firstly, ICN decouples the sender from its receiver, which allows to efficiently distribute keys from nodes that cached keys rather than the sender, by leveraging ICN routing paradigm. Secondly, an ICN in-network key-caching scheme provides a natural framework to effectively store and assign secret keys that have been generated, but not immediately used. This ICN caching system (that is an extension of QKP and we rename, in the QKD context, as *key store*) is especially useful for securing multicast applications, as keys can be cached and reused for multiple users of a multicast group, hence accelerating key distribution. Thirdly, the content name for ICN packets is designed to contain rich semantic features, which can be exploited for distributing keys to diverse applications in the network. Note that an ICN can be built on top of an existing network using ICN overlay solutions [10], which do not require additional dedicated hardware.

To the best of our knowledge, the integration of ICN features in QKD networks has not been previously explored. Ref. [11] investigated how to secure ICN with QKD, but it does not consider the reversed problem, i.e., how to use ICN principles to improve the efficiency of QKD. Our proposed IC-QKD network can be used to secure any type of network (e.g., future network use cases in 5G/6G) and not only ICN. Moreover, in our proposed architecture, key distribution is also allowed between non-adjacent nodes. Our work is not limited to static resource assignment for key generation, but it also covers the dynamic resource allocation scenario. Although other approaches such as semantic-based information retrieval may also provide, similarly to our proposal, semantic-based key distribution, the main reason that motivated us to use ICN is that ICN can jointly provide in-network key caching scheme and semantic-based key distribution, offering an effective and new interpretation of the quantum key pools as "key stores" in ICN. Thus, in this article, we propose an information-centric quantum key distribution (IC-QKD) network that efficiently distributes keys for current and next-generation networks.

The contributions of our work can be summarized as follows:

- We propose a novel information-centric quantum key distribution scheme called IC-QKD over optical networks, which integrates ICN and QKD to manage the key distribution for applications with diverse requirements.
- We design an information-centric cache mechanism to provide in-network key-caching. This mechanism is particularly advantageous for multicast applications as keys can be cached and reused for different multicast users to accelerate key distribution.
- We propose a semantic-based key analysis scheme for IC-QKD. This scheme can analyze application importance based on the rich semantic features to provide differentiated key caching and distribution for diverse applications.

The remaining sections are organized as follows. Sec. II provides an overview of the proposed IC-QKD network. Sec. III discusses the details of the proposed IC-QKD scheme. In Sec. IV we provide a numerical evaluation of the proposed IC-QKD scheme. In Sec. V we conclude the paper and discuss future work for IC-QKD.

II. IC-QKD Network Ecosystem and Architecture Overview

We first overview the overall IC-QKD network ecosystem used to efficiently generate, distribute, and assign keys.

A. IC-QKD Network Ecosystem

The ecosystem for an IC-QKD network consists of four main elements: network applications, QKD network infrastructure, key requests, and a key-management system. Fig. 1 shows the relation between these four elements.

- Network applications: these applications need to be secured using the keys generated in the IC-QKD network. Network applications can be multicast or unicast.
- QKD network infrastructure: this infrastructure is used to generate the keys, and it consists of quantum nodes (QNs) and QKD links. Each node is equipped with QKD modules (transceivers) and each link has multiple

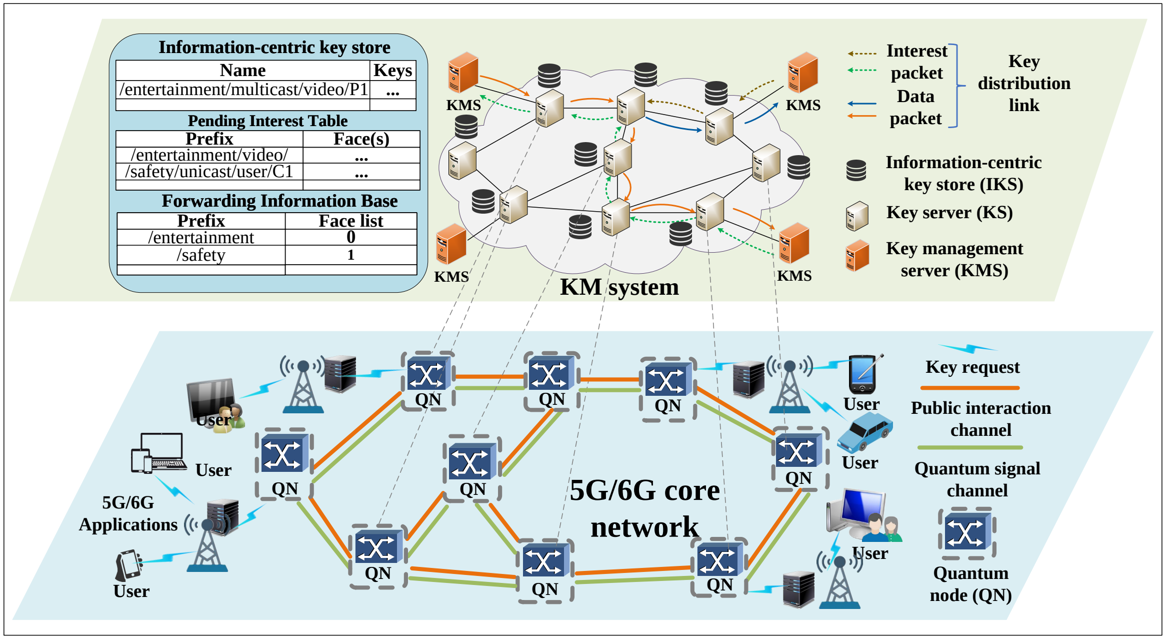

Fig. 1. Overview of the proposed IC-QKD network ecosystem.

quantum channels where qubits are transmitted. The QKD infrastructure stays on top of the physical layer and can adopt different QKD protocols. How to tolerate noise and reduce quantum bit error rates are not the focus of this work. Fig. 1 adopts Bennett-Brassard-1984 (BB84) protocol, which generates keys with public interaction channel and quantum signal channel.

- Key requests: a key request by an application user includes the application identifier, application importance, key type, and the number of required keys. Different users requesting keys within the same multicast group share the same key, while different key requests for a unicast application use different keys.
- Key management (KM) system: the KM system consists of key servers (KSs), key distribution links, and key management servers (KMSs). The key distribution link shares keys in the upper layer with keys already generated using quantum signals with traditional channels. The KS maintains a cache, referred to as *information-centric key store (IKS)*, located in the QN, which stores keys and can exchange keys with other KSs using the key distribution links. The KMS gets the generated keys from the KS, and then assigns keys for different applications.

The keys generated in the QKD infrastructure are managed by the KMS to secure the network applications as follows. To request keys for an application, the user sends a key request to a KMS for the requested application. The key management layer distributes keys based on ICN. Specifically, each KS can work as ICN *publisher* or *consumer* for keys or as an intermediate node (a node along the path between the *publisher* and the *consumer*). The *consumer* requests keys using *interest packets*, and the *publisher* publishes the keys and returns the requested keys with *data packets* after receiving the *interest packet*. Keys can be distributed from intermediate nodes that cache keys rather than the publisher.

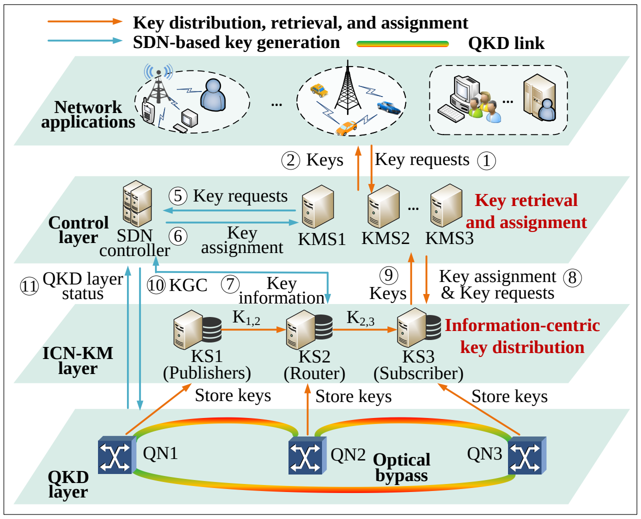

Fig. 2. Proposed IC-QKD network architecture.

The key-distribution process is controlled by three tables maintained in each KS, namely, IKS, pending interest table (PIT), and forwarding information base (FIB). The IKS is a key store designed for caching keys, based on the concept of content store (CS) in ICN. The PIT stores all the interest packets for keys that an intermediate node has forwarded and has not yet satisfied. Once an interest packet is satisfied, the intermediate node can forward the corresponding data packet according to the PIT and remove the information of the interest packet from the PIT. The intermediate node forwards interest packets based on FIB by matching the prefix of the content name. The FIB is generated with adapted conventional routing protocols such as Open Shortest Path First protocol.

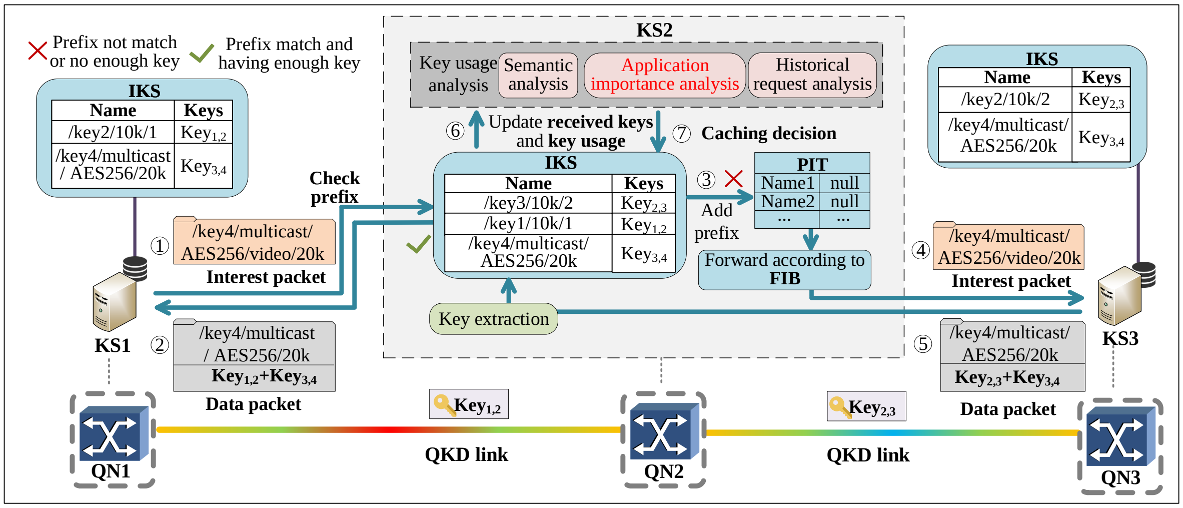
✗ Prefix not match or no enough key
✓ Prefix match and having enough key
IKS
Name | Keys
/key2/10k/1 | $Key_{1,2}$
/key4/multicast / AES256/20k | $Key_{3,4}$
Check prefix
① /key4/multicast/ AES256/video/20k
Interest packet
KS1
② /key4/multicast / AES256/20k
$Key_{1,2}$+$Key_{3,4}$
Data packet
KS2
Key usage analysis
Semantic analysis
Application importance analysis
Historical request analysis
⑥ Update received keys and key usage
⑦ Caching decision
IKS
Name | Keys
/key3/10k/2 | $Key_{2,3}$
/key1/10k/1 | $Key_{1,2}$
/key4/multicast/ AES256/20k | $Key_{3,4}$
③ ✗
Add prefix
PIT
Name1 null
Name2 null
... ...
Forward according to FIB
Key extraction
IKS
Name | Keys
/key2/10k/2 | $Key_{2,3}$
/key4/multicast/ AES256/20k | $Key_{3,4}$
④ /key4/multicast/ AES256/video/20k
Interest packet
KS3
⑤ /key4/multicast/ AES256/20k
$Key_{2,3}$+$Key_{3,4}$
Data packet
$Key_{1,2}$
$Key_{2,3}$
QKD link
QKD link
QN1
QN2
QN3

Fig. 3. Key caching and distribution scheme for IC-QKD network in ICN-KM layer.

B. IC-QKD Network Architecture

Starting from the ecosystem above, we propose a four-layer architecture for the IC-QKD network, as shown in Fig. 2. This architecture consists of an application layer (i.e., the 5G/6G users), a control layer, an ICN key management (ICN-KM) layer, and a QKD layer. Note that the ICN-KM layer corresponds to the grey part in Fig. 1.

The control layer governs the key generation through a centralized Software-Defined Networking (SDN) controller, which is the current state-of-the-art technology to control QKD networks [12]. Note that any other centralized system with the capability to control the key generation in the QKD layer could also be considered. The control layer governs the key generation through an SDN controller as follows. First, the SDN controller gets the key requests from KSs. Then, it analyzes the resources (e.g., available quantum modules and cached keys) in the QKD layer and releases a key-generation command (KGC), which is sent to the QKD layer to generate keys. The KGC will initiate point-to-point QKD connections. The point-to-point QKD may use optical bypass controlled by the SDN controller to bypass intermediate nodes and generate keys for non-adjacent nodes, which can improve the resource efficiency of the network [13]. In addition, the SDN controller also interacts with KMS to send key requests to the ICN-KM layer, which decides the key distribution between non-adjacent nodes and reduces the computational complexity of the SDN controller.

The key distribution and assignment are as follows:

- Users need to secure their transmissions using keys generated in the QKD network. These users send the key requests to a nearby KMS. The KMS returns an identical key to users of the same application.
- KMS aggregates and send the keys requests to the SDN controller, which assigns the already cached keys to these requests. If the no available keys are cached, the KS will send interest packets to other KSs in the ICN-KM layer for keys. Besides, the KMS will also send key generation requests to the SDN controller, which controls the generation of keys in the QKD layer.
- Key-distribution process distributes keys across the ICN-KM layer, which is secured by encrypting the distributed keys with the keys generated in the QKD network.
- KS stores the received keys in the IKS in the ICN-KM layer. For multicast applications, keys distributed in the IKS of different KSs can also be reused.
- Key retrieval and assignment are performed in the KMS, which extracts the keys from the connected KS and assigns them to users for various applications.

III. An Information-Centric QKD Scheme

In this section, we present the details of the proposed semantic-based IC-QKD scheme to solve the abovementioned two challenges facing practical deployment. We first propose an information-centric cache mechanism to accelerate key distribution. Then, to provide differentiated key distribution for diverse applications, we design a semantic-based trusted key-distribution process to utilize information such as application importance.

A. Information-Centric Cache Mechanism

In ICN, all the contents have a content name which is used to identify and distribute a specific content. The content name is a string, which can provide rich information that describes the content. To leverage this rich semantic feature for QKD, we design an information-centric caching mechanism, called IKS, which caches the keys according to the information provided by the content name associated with the keys. The IKS is located in the KS of the ICN-KM layer. The cache mechanism differs for unicast vs. multicast applications. A key for a unicast application can only be used for one user. Once the key is used, it is removed from the IKS. For multicast applications, different users share the same key. Even if a key is used, it may still be cached in the IKS.

The caching process is shown in Fig. 3. At the bottom of Fig. 3, there are three QNs, namely, QN1, QN2, and QN3. QN1 and QN2 generate $key_{1,2}$, and QN2 and QN3 generate

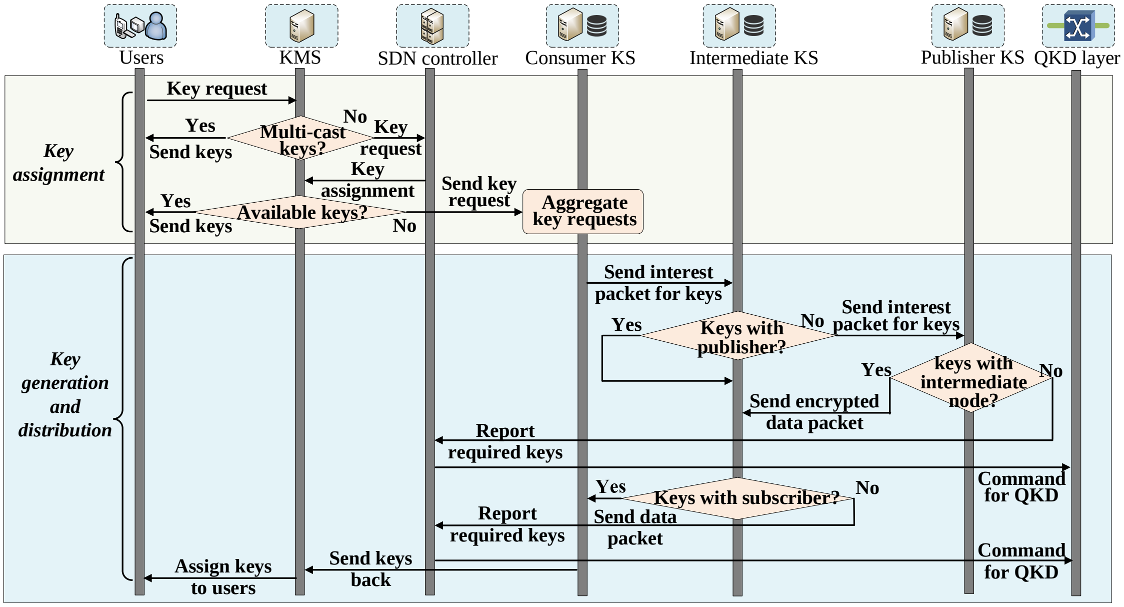

Fig. 4. Workflow of the proposed IC-QKD.

$key_{2,3}$ between them. Three key servers, namely, KS1, KS2, and KS3 are embedded to QN1, QN2, and QN3, respectively. The keys generated in the QNs are cached in the corresponding KSs. The key cache process is shown with an example of KS2 in Fig. 3 as follows. Once KS2 receives an interest packet for keys, it will first check whether keys are cached by matching prefixes in the IKS. If the required keys are already cached in the IKS, the KS will return the keys with a data packet. If the prefix does not match the keys in the IKS or keys are not used for the current applications, the prefix of the interest packet will be added to the PIT, and the interest packet is forwarded according to the FIB (note that the entries in FIB are prioritized according to historical requests). For instance, if KS2 receives an interest packet with content name */key4/multicast/AES256/20k*, it will forward the interest packet to KS3 by matching prefixes in FIB. When the interest packet reaches a KS (KS3 in this example) that contains the requested keys, the KS will send back a data packet containing the requested keys, which decouples the sender from the receiver because keys can be sent directly from an intermediate node between the sender and receiver. When KS2 receives the data packet, it will forward the data packet according to the PIT.

After receiving data packets with keys, KS extracts and caches keys based on key usage analysis with ICN features, which prioritizes key caching based on application importance and historical requests as in Fig. 3. The key usage analysis includes three components as follows. 1) The semantic analysis analyzes the ICN semantic features in the content name, which obtains information about the applications that require the keys. 2) The application importance analysis gets the importance of different applications based on the semantic analysis. 3) The historical request analysis uses the previous key requests to predict the applications that will require keys. After performing key usage analysis, the KS obtains caching decision and then updates IKS. Specifically, if one key is likely to be requested by an important application in the following short time period, the key will be cached in the IKS.

B. Semantic-Based Trusted Key-Distribution Process

To securely distribute keys between KSs, we designed a semantic-based key distribution scheme for IC-QKD network. The semantic information includes information about the content and hence poses privacy issues, which can be mitigated with the PrivICN scheme [14]. As summarized in Fig. 3, we show how keys are securely distributed with the ICN routing paradigm with an example as follows. When KS1 requests keys with content name */key4/multicast/AES256/20k*, it first sends an interest packet to KS2 according to FIB, which contains the forwarding information. Since KS2 does not have the required keys, it forwards the interest packet to KS3. KS3 sends back the data packet with the required keys encrypted with $key_{2,3}$. After receiving the keys, KS2 decrypts the keys with $key_{2,3}$, and sends the data packet to KS1, which is encrypted with $key_{1,2}$. Note that the key-distribution process is trusted since all the transmitted keys are encrypted with the keys generated in the QKD network using One-Time Pad to ensure theoretically perfect secrecy. If multiple applications request the same key between two QNs, the intermediate QN obtains the importance of these key requests based on the semantic analysis, and chooses the key requests to serve based on this semantic analysis. The intermediate KS deals with data packets for multicast applications and unicast applications in different ways. For multicast applications, if multiple users require a key for the service of the application, one key can be distributed to all users. For unicast applications, different users must have different keys to secure the service of the application.

The information-centric cache and key distribution mechanism address two main issues of the existing QKD networks.

- The key cache accelerates key distribution and improves the resource efficiency of the network. For instance, in Fig. 3, assume that the QKD links between (QN1, QN2) and (QN2, QN3) offer key rates of 20 kbps and 10 kbps, respectively, then the achievable key rate between (QN1, QN3) is only 10 kbps. However, if (QN2, QN3) already cached keys, the key cache can be used with the additional key rate between (QN1, QN2) to distribute keys between (QN1, QN3), which accelerates key distribution. Moreover, if another node requests the same keys, the keys are sent directly from the key cache in QN2 rather than QN1, reducing redundant key distribution between (QN1, QN2). Hence, an effective ICN-based key distribution can improve utilization of the keys stored in QKP to save the quantum network resources.
- Since different applications have diverse key requirements, capabilities for differentiated key distribution must be supported. In the proposed IC-QKD, the intermediate KS can analyze the importance of different applications with semantic features of ICN, and then give higher priority to distribute keys for more important applications.

The workflow of IC-QKD is shown in Fig. 4. If the user asks for multicast keys assigned by the KMS to other users, the KMS can directly return the key. If not, the KMS sends requests to the SDN controller for key assignments. If the keys are not cached, the keys will be generated and obtained from the QKD layer according to the following process.

- Firstly, a KS serving the user will work as a consumer, which sends an interest packet for the keys.
- When an intermediate KS receives the interest packet for keys, it will forward the interest packet if keys are already cached. If not. Otherwise, the request will be forwarded to the publisher KS.
- Then the SDN controller will send commands to the QKD layer to generate keys. The generated keys will be sent back as data packets (note that these keys need to be encrypted as shown in Fig. 3).
- If the intermediate node does not have keys to encrypt the data packet, it will report to the SDN controller, which will send commands to the QKD layer to generate the keys using QKD infrastructures.
- Finally, after generating the required keys, KS sends back keys to KMS, which assign keys to users.

IV. Illustrative Numerical Results

In this section, we simulatively compare the effectiveness of key distribution in our proposed IC-QKD network compared to that of an existing QKD network [15].

A. Simulation Settings

We implemented a discrete-event IC-QKD network simulator using an ICN overlay simulator [10] developed in Python 3.8. The simulation is run on a server with Intel(R) Core(TM) i7-10510U CPU processor and 16GB of memory. In the simulation, users' request keys to secure content dynamically, and several applications transmit content to users. The key requests are generated with Zipf law (real traffic traces of QKD networks are not yet available, and Zipf law is widely used to characterize distribution of content requests). We assume that each key request from users requires exactly one key and one KS receives 50 requests on average every second. The QKD layer generates and distributes keys in QKD layer to serve key requests for applications. The applications can be either multicast or unicast. For multicast applications, the same content is sent to different users, who require the same key. We also assume that different applications have different importance (quantified by a weight, e.g., the weight of an emergency application is higher than that of an online gaming application). System performance is evaluated in terms of i) *weighted success probability* of key requests (defined as the ratio of the weighted number of key requests that are successfully served to the total number of the weighted number of key requests) and ii) *cache hit ratio* of keys (defined as the ratio of the key requests served with caches over the total number of key requests). We consider that the existing QKD network is able to distribute and cache the keys with the least recently used (LRU) cache strategy. In addition, to utilize the rich semantic features of the IC-QKD network, we consider that IC-QKD network is capable of caching keys with the importance of different applications by performing semantic analysis on the content name of ICN. More specifically, the content name of ICN is used to determine the importance of different applications, and the historical requests are leveraged to predict popularity of key requests. The application importance and predicted popularity are combined to cache keys. The results are averaged from 10 different instances.

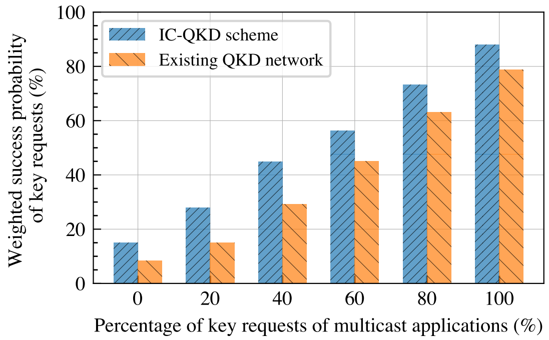

Fig. 5. Evaluation of weighted success probability.

B. Success Probability and Hit Ratio

To evaluate the resource efficiency of the proposed IC-QKD network, we compare the weighted success probability of key requests of the proposed IC-QKD network vs. an existing QKD network while increasing the percentage of key requests of multicast applications in Fig. 5 (note that, while we vary the percentage of multicast applications, the total number of key requests and their weights are kept the same to have a fair comparison). Results show that IC-QKD achieves a higher weighted success probability than the existing QKD network in all cases, ranging from 5% higher success probability, when there are no multicast applications, to 16% when increasing the percentage of multicast services. Even though the benefits of ICN-QKD are mostly expected with multicast applications, our results show that advantage over the existing QKD network is achieved also when all applications are unicast, as IC-QKD distributes keys based on semantic features, giving priority to more important applications. Specifically, the application importance is weighted with the predicted popularity such that a larger amount of keys are cached for more important applications, which increases the weighted success probability even when only unicast applications exist.

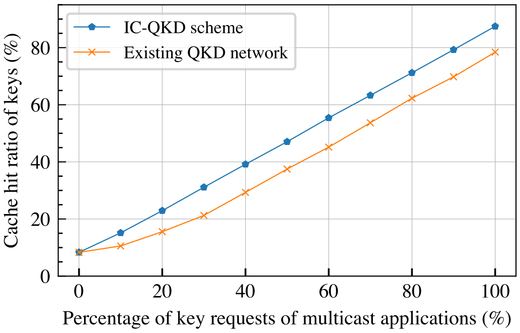

Fig. 6. Evaluation of cache hit ratio of keys.

Fig. 6 shows the cache hit ratio of keys for an increasing percentage of key requests of multicast applications to evaluate the proposed IKS. With only unicast applications, cache hit ratios in the two schemes are the same. Note that even though the two schemes have the same cache hit ratio, the IC-QKD scheme is capable of caching more important applications, resulting in a higher weighted success probability as in Fig. 5. When the percentage of multicast applications increases, the difference in the cache hit ratio of keys between the two schemes can be as high as 10%. The cache hit ratio of keys in the IKS in the IC-QKD scheme is higher than the existing QKD network, because the existing QKD network only caches keys in the end nodes while the proposed IC-QKD network manages to cache and use keys in the intermediate nodes.

V. Conclusion

In this article, we start by discussing some of the challenges of QKD in current and next-generation networks, and then propose and evaluate a new QDK network scheme based on Information-Centric Networking to meet these challenges. The proposed IC-QKD can secure network applications with efficient and differentiated key distribution leveraging ICN properties. Specifically, an information-centric key store is designed for IC-QKD to perform in-network caching of keys, which can be especially useful for multicast applications. Additionally, by analyzing the semantic features in IC-QKD network, the key caching and distribution scheme can provide semantic-based key distribution for key requests coming from applications with different importance. Our simulation results provide an initial quantification of the effectiveness of our proposed scheme in terms of weighted success probability of key requests and cache hit ratio of keys. As a future work, we aim to implement and design a testbed to verify the proposed scheme in case of practical deployment in real-life scenarios.

Acknowledgment

This work was funded by the National Operative Program (PON) "Research and Innovation" of the Italian Ministry of University and Research. It was also partly supported by the National Natural Science Foundation of China under Grants U21B2019 and 61972255 together with Program of Shanghai Academic Young Research Leader under grant 20XD1422000.

References

[1] Z. Wei *et al.*, "Toward multi-functional 6g wireless networks: Integrating sensing, communication, and security," *IEEE Communications Magazine*, vol. 60, no. 4, pp. 65–71, 2022.

[2] L. Chen *et al.*, *Report on post-quantum cryptography*. US Department of Commerce, National Institute of Standards and Technology, 2016.

[3] 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, 2022.

[4] T.-Y. Chen *et al.*, "Implementation of a 46-node quantum metropolitan area network," *npj Quantum Information*, vol. 7, no. 1, p. 134, 2021.

[5] B. Huttner *et al.*, "Long-range qkd without trusted nodes is not possible with current technology," *npj Quantum Information*, vol. 8, no. 1, p. 108, 2022.

[6] S. Wang *et al.*, "Twin-field quantum key distribution over 830-km fibre," *Nature Photonics*, vol. 16, no. 2, pp. 154–161, 2022.

[7] Y.-A. Chen *et al.*, "An integrated space-to-ground quantum communication network over 4,600 kilometres," *Nature*, vol. 589, no. 7841, pp. 214–219, 2021.

[8] A. Gatto *et al.*, "A BB84 QKD Field-Trial in the Turin Metropolitan Area," in *Photonics in Switching and Computing*, 2021, pp. Tu1A–2.

[9] L. Zhang *et al.*, "Named data networking," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 3, pp. 66–73, 2014.

[10] Q. Zhang *et al.*, "Sema-iiovt: Emergent semantic-based trustworthy information-centric fog system and testbed for intelligent internet of vehicles," *IEEE Consumer Electronics Magazine*, vol. 12, no. 1, pp. 70–79, 2023.

[11] K. Matsuzono *et al.*, "Qkdn meets icn: Efficient secure in-network data acquisition," in *IEEE Global Communications Conference (GLOBECOM)*, 2021, pp. 1–7.

[12] H. Wang *et al.*, "Quantum-key-distribution (qkd) networks enabled by software-defined networks (sdn)," *Applied Sciences*, vol. 9, no. 10, p. 2081, 2019.

[13] Q. Zhang *et al.*, "Routing, channel, key-rate and time-slot assignment for qkd in optical networks," *IEEE Transactions on Network and Service Management*, 2023, early access.

[14] C. Bernardini *et al.*, "Privicn: Privacy-preserving content retrieval in information-centric networking," *Computer Networks*, vol. 149, pp. 13–28, 2019.

[15] Q. Zhu, X. Yu, Y. Zhao, A. Nag, and J. Zhang, "Resource allocation in quantum-key-distribution- secured datacenter networks with cloud–edge collaboration," *IEEE Internet of Things Journal*, vol. 10, no. 12, pp. 10 916–10 932, 2023.

Qiaolun Zhang is currently a Ph.D. student in Politecnico di Milano. His current research interests are in the fields of quantum key distribution network, information-centric networks, 6G, etc.

Omran Ayoub is currently a researcher at University of Applied Sciences of Southern Switzerland. His research interests are in the field of machine learning for communication networks and explainable artificial intelligence.

Jun Wu (S'08-M'12-SM'22) is currently a professor in Waseda University, Japan. His research interests include security and intelligence for IoT, 5G/6G, digital twin, etc.

Xi Lin is an Assistant Professor in Shanghai Jiao Tong University, Shanghai, China. His research interests include Blockchain, multi-access edge computing, Internet of Things, and so on.

Massimo Tornatore (S'03–M'06–SM'13–F'23) is currently a Professor in Politecnico di Milano. He also holds an appointment as Adjunct Professor at University of California, Davis, USA and as visiting professor at University of Waterloo, Canada. His research interests include performance evaluation, optimization, and design of communication networks.