Quantum Network: Security Assessment and Key Management

Hongyi Zhou, Kefan Lv, Longbo Huang, *Senior Member, IEEE*, and Xiongfeng Ma

***Abstract*— As an extension of quantum key distribution, secure communication among multiple users is a basic task in a quantum network. When the quantum network structure becomes complicated with a large number of users, it is important to investigate network issues, including security, key management, latency, reliability, scalability, and cost. In this work, we utilize the classical network theory and graph theory to address two critical issues in a quantum network, security and key management. First, we design a communication scheme with the highest security level that trusts a minimum number of intermediate nodes. Second, when the quantum key is a limited resource, we design key management and data scheduling schemes to optimize the utility of data transmission. Our results can be directly applied to the current metropolitan and free-space quantum network implementations and can potentially be a standard approach for future quantum network designs.**

***Index Terms*— Quantum key distribution, Lyapunov analysis, queueing.**

I. Introduction

As a principal part of quantum cryptography, quantum key distribution (QKD) allows remote communication parties to share identical and private keys for encryption and decryption [1], [2], whose information-theoretical security is guaranteed by the fundamental principles of quantum mechanics [3], [4]. The practical implementation of QKD has a booming development since the beginning of this century. For the most popularly applied photon source — highly attenuated weak coherent state light, the decoy state method [5]–[7] addresses security issues caused by the information leakage of multi-photon components. Since then, many long-distance QKD experiments have been demonstrated around the world [8]–[13]. In the mean time, the measurement-device-independent quantum key distribution (MDI-QKD) protocol has been proposed to address the detection loophole problems [14], which has been demonstrated both in the lab [15]–[19] and in field [20], [21]. Recently, theoretical development on MDI-QKD shows that one can further double the secure communication distance [22], [23]. All these developments suggest that point-to-point QKD over hundreds of kilometers is ready for real-life implementation.

The initial proposal of QKD deals with a two-user communication scenario. In practice, one needs to extend point-to-point links to a network. There are in principle two types of quantum networks according to the way of connection [24]: one is optically switched quantum networks realized by classical optical functions; the other is repeater-based networks. The quantum-repeater-based networks are fully quantum networks enabling multi-partite entanglement distribution [25]–[27]. While in practical implementations, restricted by the current technology, it is the classical repeaters, i.e., trusted intermediate nodes together with optical switches that composites different topological network structures. To this day, there have been a number of experimental demonstrations on the field test of quantum networks. Several testing implementations of quantum networks have been realized in the China, Europe, Japan, and USA [28]–[32]. Today, the topological structures of QKD networks have become more complex than the early ones [28], [29], [31], such as the mesh structure in 46-node Hefei network, and the star-type structure in MDI-QKD network [33]. Besides these fiber-based quantum networks, a satellite-relayed quantum network has been realized recently [34], in which a secret key was exchanged between intercontinental communication partners. In the mean time, researchers explore the feasibility of hybridizing discrete variable schemes with continuous variable ones [35], [36] in a quantum network and integrating QKD into classical networks, such as utilizing wavelength division multiplexing technique [37], [38].

The ultimate goal of quantum communication is to realize large scale quantum networks. There are a few major challenges that a quantum network faces, including (i) designing the proper topological structure, (ii) assessing the security levels, and (iii) managing secure keys. Recently, an engineering framework of a scalable multi-site quantum network has been established [39], in which a QKD system is divided into multiple layers: host layer, key management layer, QKD network layer, and quantum link layer. The core of designing and operating a quantum network lies in the key management layer and QKD network layer, where the issues of security, key management [40], data routing [41] and stability should

Manuscript received June 12, 2020; revised April 22, 2021 and June 22, 2021; accepted December 14, 2021; approved by IEEE/ACM Transactions on Networking Editor Y. Chen. Date of publication January 10, 2022; date of current version June 16, 2022. This work was supported in part by the National Natural Science Foundation of China under Grant 11875173 and Grant 11674193, in part by the National Key Research and Development Program of China under Grant 2017YFA0303900 and Grant 2017YFA0304004, and in part by the Zhongguancun Haihua Institute for Frontier Information Technology. *(Corresponding authors: Hongyi Zhou; Longbo Huang; Xiongfeng Ma.)*

Hongyi Zhou is with the Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China, and also with the Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190, China (e-mail: zhouhongyi@ict.ac.cn).

Kefan Lv, Longbo Huang, and Xiongfeng Ma are with the Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China (e-mail: lvkf14@mails.tsinghua.edu.cn; longbohuang@tsinghua.edu.cn; xma@tsinghua.edu.cn).

Digital Object Identifier 10.1109/TNET.2021.3136943

be dealt with to realize the optimal transmission performance at a low cost.

In a quantum network, communication between two users, Alice and Bob, are often relayed by intermediate nodes. These nodes can be divided into two types, trusted nodes and untrusted nodes, depending on whether or not the security of communication relies on the security of the nodes, respectively. A trusted node executes full QKD process with adjacent nodes and announces the parities of the two key bit strings such that end users can share secret keys. For example, Alice and Bob establish keys, denoted by k_a and k_b, with an intermediate trusted node. The trusted node announces $k_a \oplus k_b$, and eventually, Alice and Bob share a key k_a. Whereas, an untrusted node can be as simple as an optical switch, or it can be an untrusted measurement site used in MDI-QKD schemes. In a simple network structure, such as the MDI-QKD network [33], users can communicate without trusting any intermediate nodes. Since the security of communication does not depend on untrusted nodes, we can only consider the trusted nodes in the following discussions on security assessment. In this paper, we assume all users in the network are connected with insecure classical communication channels, which are treated as a free resource. We focus on the case where quantum keys are consumed for private communication.

Security is a crucial issue in a quantum network, which may be compromised if an adversary, Eve, can manipulate or crack intermediate trusted nodes. In reality, it is important to evaluate security if Eve can at least compromise one of the nodes. In the extreme case where Eve can hack all the intermediate nodes, no secure communication can be established. Thus, we first consider the interesting problem of security assessment when a certain amount of the nodes are compromised. In particular, for a general network structure, we find an optimal communication scheme using the graph representation of a quantum network [42], [43]. With the highest security level, the communication is secure unless the nodes that eavesdropper compromises form a cut in the graph of the quantum network, which is the ultimate solution of an efficient attack strategy by the adversary.

Another issue addressed in this work is the data routing and key management in the network. In private key systems such as QKD, the encoding process may consumes keys with the same length as the message. With the current quantum technology, the key generation speed (10 Mbps) is far below the speed of classical data transmission (1 Tbps). Thus, the key is a limited resource in a network for most communication tasks. In a network with multiple communication tasks, the lack of key management will lead to instability and inefficiency. To address this issue and optimize network management, we adopt techniques addressing similar problems in the classical network research. Specifically, we formulate the problem of QKD-based network communication as a flow scheduling problem in resource-constrained networks, such as processing networks [44], [45] and energy-harvesting networks [46], [47]. In this formulation, each data transmission consumes supporting resources (in our case, quantum key bits), and the network operator needs to jointly optimize resource usage, data routing, and scheduling. Then, to solve the problem of key-constrained data transmission, we adopt the Lyapunov network optimization technique [48] and design a key management and data scheduling algorithm that has low-implementation complexity. We also rigorously show that our algorithm achieves near-optimal performance in terms of data transmission utility.

II. Security Assessment

The security in a quantum network lies in two aspects: quantum channel and intermediate nodes. The former has been well studied in the security analysis of QKD; while the latter is a new problem emerging in quantum networks. Trusted nodes can extend communication distances, keeping a relatively high key rate at the mean time. At a cost, the security of communication can be compromised by the trustworthiness of intermediate relay nodes. In practice, an important task is to design a key exchange procedure, so that it can tolerate the maximal number of compromised nodes. We define the tolerance of the compromised nodes as security level. Our target is to find a communication scheme that can tolerate as many compromised node as possible, i.e., with the highest security level.

In this section, we first present our network model. Then, we consider several simple communication schemes and provide the corresponding attack strategies. After that, we propose the strongest attacks that can hack all possible communication schemes. We find a communication strategy with the highest security level that is secure unless Eve performs the strongest attack.

A. Network Model

In our model, we consider two networks. One is a classical network for data transmission, and the other is a quantum network for key generation. When two users Alice and Bob want to establish a communication, they first distribute secret keys via the quantum network and then encrypt the message and transmit it by the classical network. A quantum network can be represented by a graph $G = (\mathcal{N}, \mathcal{L})$, where $\mathcal{N}$ and $\mathcal{L}$ are the sets of vertices and edges, respectively. Here a vertex $c \in \mathcal{N}$ represents a basic unit in a quantum network, which can be a node or a QKD sub-network whose internal structure is unrelated to the security assessment. An edge in the graph represents a QKD link used to distribute secure key strings between connected nodes. While a classical network is represented by another graph $G' = (\mathcal{N}, \mathcal{L}')$ sharing the same vertices with the quantum one. Edges in the graph G' represent classical links, which may be different from the QKD links. In this section, we assume the classical links can be freely used and hence neglect the classical communication efficiency in the following discussions.

We focus on the security of nodes and trust the security of QKD links, i.e., we assume the QKD process has been completed and secret keys have been generated. For example, in this model, the untrusted measurement site in MDI-QKD is merged into the QKD links in as an edge in the graph G. We have the following assumptions for the adversary Eve.

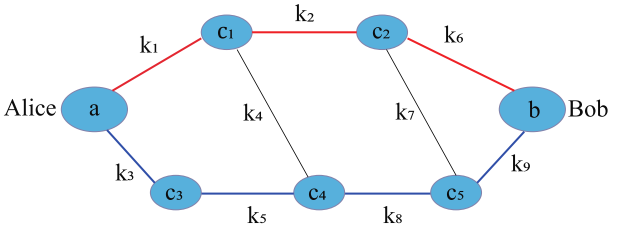


Fig. 1. Graph representation of a quantum network. Alice and Bob are the two communicating parties denoted by a and b, respectively. There are 5 intermediate nodes between them, denoted by $c_1 \sim c_5$. Each edge represents a quantum channel or quantum key strings generated between the connected nodes, denoted by $k_1 \sim k_9$.

TABLE I

Two-Path Communication Scheme. The Two Paths Are the Red Line $a \rightarrow c_1 \rightarrow c_2 \rightarrow b$ and the Blue Line $a \rightarrow c_3 \rightarrow c_4 \rightarrow c_5 \rightarrow b$ Shown in Figure 1

1) Alice holds the message x and generates a random bit string y locally with the same length $|x| = |y|$.
2) Alice sends the message $x \oplus y$ to her neighbor node c_1 and y to c_3, encrypted by quantum keys.
3) The node c_1 sends $x \oplus y$ through the red path to c_2, and eventually to Bob. Similarly, c_3 sends y through the blue path to c_4, to c_5, and eventually to Bob.
4) Finally, Bob receives y and $x \oplus y$ from the two different paths. He obtains the message x by applying an XOR operation, $x = x \oplus y \oplus y$.

a) Eve has access to all classical channels. b) Eve has no information about the quantum key of an edge if she does not compromise either of the connected nodes. c) Eve learns everything of the quantum key if she compromises at least one of the connected nodes. We present a toy quantum network G in Fig. 1, where Alice and Bob are two communicating parties. There are 5 intermediate nodes between them denoted by $c_1 \sim c_5$, and 9 edges $k_1 \sim k_9$, each representing a quantum channel or quantum key strings generated between the connected nodes.

Here, we use the path concept in the graph theory to describe the sequence of nodes used in message transmission. We only consider simple paths here since any loop of the message transmission is useless in a network. Take the red line in Figure 1 as an example. Once Alice and Bob pick a path, all intermediate nodes are fixed, $a \rightarrow c_1 \rightarrow c_2 \rightarrow b$. There are two means for key sharing. One is that Alice and Bob ask all the intermediate nodes (c_1 and c_2 in this example) to announce the parities from the exclusive-or (XOR) operations on the key bit strings with their two neighbors in the path. In the example, c_1 announces $k_1 \oplus k_2$ and c_2 announces $k_2 \oplus k_6$. Then Bob can share the same key with Alice by calculating the parities. Alternatively, c_2 will first calculate Alice's key with the parity announced by c_1, encrypt Alice's key with k_6, and sends it to Bob. In this method, Alice's key can be regarded as a message. In theory, both ways of private communication are equally secure. The first method uses fewer encryptions and decryptions. Also, the intermediate nodes do not obtain the final key directly. However, in practice, the first method will lead to low communication efficiency since all the intermediate nodes should publicly announce their parity bits for the key exchange of end-users. The second method is similar to the data transmission in a realistic network, i.e., a node will receive an encrypted message from one of its neighbors and a request to convey the message to another neighbor privately. The difference between the two methods will vanish if we neglect classical communication efficiency. Therefore, we do not distinguish these two methods in the following discussions.

B. Multi-Path Communication Scheme and Strongest Attack

Let us begin with a simple case with only one single-line path, which is represented by the red line $a \rightarrow c_1 \rightarrow c_2 \rightarrow b$ in Figure 1. Alice sends the message to her neighbour relay node encrypted with the quantum key. The message is decrypted and re-encrypted by intermediate nodes and finally received by Bob. This is a strategy that consumes the least amount of keys. In terms of security, this scheme can be weak because once Eve cracked any node on the path, she gets the message.

In order to strengthen the single-path strategy, one can introduce an additional disjoint path, the blue line $a \rightarrow c_3 \rightarrow c_4 \rightarrow c_5 \rightarrow b$ shown in Figure 1, to defend the single-point eavesdropping attack. The second path is used to transmit another independent random bit string. The final message is the XOR result of the two strings transmitted via the two paths. The details of the communication scheme is shown in Table I.

Suppose Eve can only successfully hack one of the intermediate nodes, she can only learn y or $x \oplus y$, and hence the transmission of x is still secure. In fact, if Eve can only hack the nodes in one of the two paths (red or blue), the transmission is secure. Only when Eve can hack nodes from both paths, say c_2 and c_3, she can eavesdrop the message. Obviously, the two-path scheme is securer than the single-path one in practice.

Generally, we can increase the number of paths to increase communication security. The two-path scheme shown in Box I can be generalized to a multi-path scheme. In an n-path scheme, Alice sends $x \oplus y_1 \oplus y_2 \cdots \oplus y_{n-1}, y_1, y_2, \ldots, y_{n-1}$ by n paths. Then it follows step 2, 3 and 4 in Table I. Finally, Bob can recover the message x. Sometimes, adding a path may not increase security. For example, in the aforementioned two-path strategy, adding the third path, $a \rightarrow c_1 \rightarrow c_4 \rightarrow c_5 \rightarrow b$, cannot enhance security since any hacking strategy that can successfully break the security of the two-path scheme will also break this three-path scheme. Our target is to design a robust communication scheme against as many compromised nodes as possible.

Now, we model communication schemes and define the security levels regarding a quantum network formally. In a quantum network represented by a graph $G = (\mathcal{N}, \mathcal{L})$, we denote $\mathcal{M}$ to be the set of paths used in a communication scheme, which has one-to-one correspondence to the communication scheme, and denote $\mathcal{A} \subseteq \mathcal{N} \setminus \{a, b\}$ the set of compromised nodes, which uniquely determines Eve's hacking strategy. We introduce a Boolean function $sec(\mathcal{A}, \mathcal{M})$ of a communication scheme and hacking strategy, which is defined as follows.

Definition 1: For a communication scheme $\mathcal{M}$ and Eve's strategy $\mathcal{A}$, if $\mathcal{M}$ is secure against compromised nodes in $\mathcal{A}$, then $sec(\mathcal{A}, \mathcal{M}) = 1$. Otherwise, $sec(\mathcal{A}, \mathcal{M}) = 0$.

We can see that $sec(\mathcal{A}, \mathcal{M}) = 0$ if and only if each path in $\mathcal{M}$ goes through at least one nodes in $\mathcal{A}$. In other words, $sec(\mathcal{A}, \mathcal{M}) = 1$ if and only if there is at least one path in $\mathcal{M}$ which does not go through any nodes in $\mathcal{A}$. We define the security level as follows.

Definition 2: Given a network G, the source and sink nodes a and b, and the communication scheme $\mathcal{M}$, the security level of $\mathcal{M}$ is the optimal value of the following maximization problem,

$$\begin{aligned} &\max_{\mathcal{A}} \ |\mathcal{A}| \\ &\text{s.t. } sec(\mathcal{A}, \mathcal{M}) = 1. \end{aligned} \tag{1}$$

We also define a strongest attack to be the most powerful attack that can successfully hack all possible communication schemes.

Definition 3: A strongest attack $\mathcal{A}^{st}$ can successfully hack all possible communication schemes,

$$\forall \mathcal{M}, \quad sec(\mathcal{A}^{st}, \mathcal{M}) = 0. \tag{2}$$

By definition, we see that a strongest attack should contain at least one node of each possible path between Alice and Bob. When Eve compromises a node, we assume that she knows all the keys distributed from (and to) this node. From a security point of view, one can think of Eve making those connecting edges insecure. Given an attack $\mathcal{A}$, define $\mathcal{L}_A \subseteq \mathcal{L}$ as the set of insecure edges caused by this attack. If Alice and Bob cannot be connected by a path without using any edges in $\mathcal{L}_A$, no secure path can be found under this attack and such attack is strongest. Thus, we have the following theorem.

Theorem 1: Attack $\mathcal{A}$ is strongest if and only if Alice and Bob belongs to different disjoint subsets partitioned by a cut-set contained in $\mathcal{L}_A$.

Proof: Proof of "if": a cut in the graph theory is a partition of the nodes into two disjoint subsets. It determines a cut-set, the set of edges whose two end nodes belongs to different subsets of the partition. Alice and Bob belongs to different subsets. Hence any path connecting Alice and Bob must have at least one edge that connect two nodes of different subset. From the definition, this edge belongs to the cut-set. That is, any path connecting them must contain at least one edge in the cut-set. Then, no secure communication is possible. The attack is strongest.

Proof of "only if": we need to prove that if $\mathcal{L}_A$ contains no cut-set, there must be a secure path between Alice and Bob. Consider the set of nodes that have secure paths to Alice, if Bob belongs to this set, the proof is done by finding the secure path. If Bob does not belong to it, this set and its compliment set are two disjoint subsets. This partition is a cut. The cut-set must be contained in $\mathcal{L}_A$ and hence $\mathcal{A}$ is strongest.

From the theorem, we can have the following corollary.

Corollary 1: If an attack is not strongest, there exists a secure path connecting Alice and Bob.

1) Communication Scheme of the Highest Security Level: Now, we want to study the most secure communication scheme. That is, such a scheme can tolerate any attacks that other schemes can tolerate. Denote the set of strongest attacks to be $\mathcal{A}^{st}$.

Definition 4: A communication scheme, $\mathcal{M}^h$, has the highest security level if

$$\mathcal{M}^h : sec(\mathcal{A}, \mathcal{M}^h) = \begin{cases} 0 & \mathcal{A} \in \{\mathcal{A}^{st}\} \\ 1 & otherwise \end{cases} \tag{3}$$

Here we propose a scheme $\mathcal{M}_0$ with the highest security level.

Definition 5: In the communication scheme $\mathcal{M}_0$, each node in the network except Alice and Bob broadcasts the parity (XOR result of all the keys from the neighbor). Bob receives all the parity information via unencrypted channels (available to Eve). By calculating the parity information, he can share a secret key with Alice.

We take the network in Figure 1 as an example. Here c_1 will announce $k_1 \oplus k_2 \oplus k_4$, c_2 will announce $k_2 \oplus k_6 \oplus k_7$, etc. Of course, Alice's and Bob's positions are symmetric. All the parity information can be sent to Alice. The scheme still works.

Theorem 2: Scheme $\mathcal{M}_0$, defined in Definition 5, is of the highest security level.

Proof: First, we need to show that this scheme can yield an identical key between Alice and Bob. On Alice's side, she performs the XOR operation to all the keys connected to her and obtains k_A. Upon receiving all the parity information from the network, Bob performs XOR operation on all the parity bit string along with his keys connected to his neighbors. Then, all the keys in this network appear in this XOR operation twice except those of the nodes connected directly with Alice. Thus, Bob's XOR result gives k_A and all others are canceled out. In the end, they can achieve an identical key.

Then, we show that the generated key is secure for any attacks that are not strongest. If an attack is not strongest, from Corollary 1, we can find a secure path between Alice and Bob. For the scheme $\mathcal{M}_0$, one can think of k_A a secure random key bit string being transmitted from Alice to Bob with one-time pad encryption [49] and being XOR with some extra random bit strings that might known to Eve. Specifically, suppose the secure path is $a \to c_1 \to c_2 \to \cdots \to b$. Then Alice can send her random bit string via this path to Bob. In this case, she adds more unrelated random bit strings, which will not affect the security of the transmission.

Finally, it is obvious that $\mathcal{M}_0$ is insecure under a strongest attack, since it forms a cut between Alice and Bob.

At the end of this part, we have the following remarks. We notice that similar problems have been investigated in both classical [50] and quantum networks [24], where the relation between the maximum tolerable compromised nodes and the network connectivity is given. There is also a communication scheme proposed in [51] with probabilistic information-theoretical security. In contrast, our results are independent of the connectivity and not probabilistic, i.e., our communication scheme is secure unless Eve performs the strongest attack. Another remark is that we assume the classical channel is free between any two nodes. Thus, there is no need to consider the efficiency of classical data transmission in the analysis.

In practical cases, we need to consider the trade-off between network efficiency and security level. We leave this problem for future works.

III. Utility Optimization and Key Management

When maximizing the security of the network in the previous section, we essentially assume that the key from QKD is sufficient for encryption. While in a practical quantum network, the amount of key is usually limited since QKD is normally far slower than classical communication. In this section, we consider the scenario where the quantum key is a limited source for multiple communication tasks. The problem becomes how to optimize certain network metrics through key management, data scheduling, and routing. For instance, we need to evaluate the encrypted data transmission capacity of a quantum network, i.e., how much data can be transmitted within a unit of time. Here, we borrow techniques in a classical energy harvesting network [46]. The main difference is that the key (corresponding to the energy in an energy harvesting network) is defined over channels rather than nodes, which leads to different target functions and constraints in our optimization problem. In this section, we formulate a utility optimization problem to deal with the key management and data routing problem in a QKD network and find an efficient solution based on Lyapunov optimization techniques.

Again, we follow the graph theory expression $G = (\mathcal{N}, \mathcal{L})$ to represent the network. Specifically, $a, b \in \mathcal{N}$ represent nodes and $l_{[a,b]}$ represents the link between a and b. The time is discretized in the following discussions and t is the index of the time slot. We summarize the notations in Table II and make the following remarks. The working condition of QKD $S_{[a,c]}(t)$ is a Boolean function and the key management strategy lies in the balance between $S_{[a,c]}(t)K_{[a,c]}$ and $P_{[a,c]}(t)$, representing the key generation and consumption, respectively. During data transmission, we only care about their destinations and classify the data accordingly. For example, we call the data flow with the final destination to node b as type-b data. Data scheduling is determined by $R_a^b(t)$, type-b data admitted to a at time t. Since secure data transmission needs encryption, it is given by a function of the key consumption, i.e., $\mu_{[a,c]}(t) = \mu_{[a,c]}(P_{[a,c]}(t))$. In particular, for the case of one-time pad encryption, $\mu_{[a,c]}(t) = P_{[a,c]}(t)$. The total data transmission on an edge $l_{[a,c]}$ is the sum of all types of data transmission, i.e., $\mu_{[a,c]}(t) = \sum_b \mu_{[a,c]}^b(t)$. The key generation rate $K_{[a,c]}$ is determined by the QKD setting between two adjacent nodes, a and c. The key is stored in the edge with a storage upper bound $\theta_{[a,c]}$. When the amount of key stored in the edge $l_{[a,c]} \in \mathcal{L}$ is larger than $\theta_{[a,c]}$ at time slot t, QKD in this edge becomes inactive, i.e., $S_{[a,c]}(t) = 0$. Compared with the energy harvesting network in literature, we neglect the interaction of different paths due to the optical fiber communications applied in the network.

A. Utility Optimization Problem

The data transmission capacity problem is a special case of the utility optimization problems. The utility is defined on each data flow, i.e., $U_a^b(R_a^b(t))$, which quantifies how much one can benefit from achieving a data rate $R_a^b(t)$. The concrete expression of the utility function can be defined according to practical applications. A common utility function is concave with the data transmission flow, for example, $U_a^b(R_a^b(t)) = k\log_2(R_a^b(t))$, where the coefficient k can be as simple as a constant. In particular, when $U_a^b(R_a^b(t)) = R_a^b(t)$, the utility optimization problem reduces to the data transmission capacity problem.

TABLE II

Notations. The Subscript $[a,c]$ Refers to a Quantity Defined Between the Adjacent Nodes a and c. Denote the Data Transmitted to b as Type-b Data

Symbol	Interpretation
N	Number of nodes in the network, $\lvert\mathcal{N}\rvert$
L	Number of edges in the network, $\lvert\mathcal{L}\rvert$
$\mathcal{N}_a^{in(out)}$	Set of nodes connected to (from) node a
$Q_a^b(t)$	Total type-b data queue at node a
$E_{[a,c]}(t)$	Amount of key stored
$K_{[a,c]}$	Amount of key generated per time slot
$S_{[a,c]}(t)$	Working condition of QKD
$\theta_{[a,c]}$	Saturation of key storage
$\mu_{[a,c]}(t)$	Total data transmission
$\mu_{[a,c]}^b(t)$	Type-b data transmission
$P_{[a,c]}(t)$	Key consumption
$R_a^b(t)$	New type-b data transmission request at node a

The objective of the problem is to optimize the network utility obtained from serving data traffic. Specifically, we consider the following network utility,

$$U_{tot}(\vec{r}) = \sum_{a,b\in\mathcal{N}} U_a^b(r_a^b), \tag{4}$$

where the average type-b data transmission rate at node a is given by

$$r_a^b \equiv \liminf_{t\to\infty} \frac{1}{t}\sum_{\tau=0}^{t-1} R_a^b(\tau), \tag{5}$$

and $\vec{r}$ is the matrix with elements of r_a^b. In order to evaluate the data transmission capacity for a quantum network, we need to optimize Eq. (4) with certain dynamics and constraints.

B. Dynamics and Constraints in a Quantum Network

Now, we model the dynamics, shown in Fig. 2, and the constraints in the network model. First, we have the key storage dynamics,

$$E_{[a,c]}(t+1) = E_{[a,c]}(t) - P_{[a,c]}(t) + S_{[a,c]}(t)K_{[a,c]}, \tag{6}$$

where the increase of the key volume $S_{[a,c]}(t)K_{[a,c]}$ comes from QKD and the decrease $-P_{[a,c]}(t)$ is caused by key consumption for encryption. Note that in Eq. (6), the key storage should be non-negative, $\forall\, t, l_{[a,c]} \in \mathcal{L}$,

$$E_{[a,c]}(t) \geq P_{[a,c]}(t). \tag{7}$$

This key availability constraint, Eq. (7), is a complicated constraint as it couples the key consumption actions across time, i.e., a current $P_{[a,c]}(t)$ decision can affect future actions.

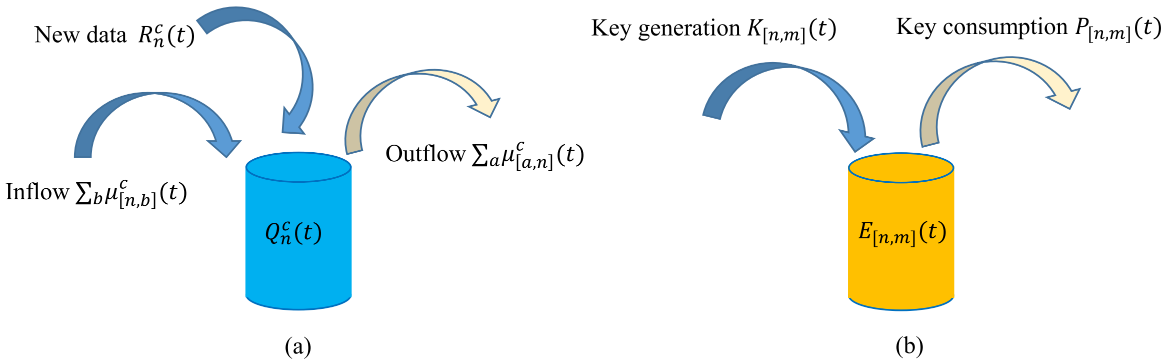

New data $R_n^c(t)$
Inflow $\sum_b \mu_{[n,b]}^c(t)$
$Q_n^c(t)$
Outflow $\sum_a \mu_{[a,n]}^c(t)$
(a)
Key generation $K_{[n,m]}(t)$
Key consumption $P_{[n,m]}(t)$
$E_{[n,m]}(t)$
(b)

Fig. 2. Dynamics in a quantum network. (a) Dynamics of the data queue, as formulated in Eq. (8). (b) Dynamics of the key storage, as formulated in Eq. (6).

Similarly, we have the data transmission dynamics,

$$Q_a^b(t+1) \leq Q_a^b(t) + R_a^b(t) + \sum_{c\in\mathcal{N}_a^{in}} \mu_{[c,a]}^b(t) - \sum_{c\in\mathcal{N}_n^{out}} \mu_{[a,c]}^b(t). \quad (8)$$

The amount of type-b data to be transmitted at node a come from two sources: data flow from other nodes to node a, $\sum_{c\in\mathcal{N}_a^{in}} \mu_{[c,a]}^b(t)$; and new data admitted to a for b, $R_a^b(t)$. Meanwhile, the queue will decrease if data is transmitted from a to other adjacent nodes $\sum_{c\in\mathcal{N}_n^{out}} \mu_{[a,c]}^b(t)$. The inequality is due to the possibility that neighbor nodes may not have enough data to fulfill the allocated rate. In the following discussions, we just take it as an equality, as when the rate is over-allocated, one can just send some dummy data. Finally, we take account of the stability of the network. That is, the data queue backlog of the whole network needs to be convergent with time,

$$\bar{Q} \equiv \limsup_{t\to\infty} \frac{1}{t} \sum_{\tau=0}^{t-1} \sum_{a,b} Q_a^b(\tau) < \infty. \quad (9)$$

The stability condition makes sure that all packets admitted into the network are eventually delivered.

C. Algorithm Design

To solve the utility optimization problem defined in Section III-A, we design an algorithm based on the Lyapunov optimization technique [52], which has found wide applications in different network scenarios [53]–[55]. Define the Lyapunov function,

$$L(t) \equiv \frac{1}{2} \sum_{a,b\in\mathcal{N}} [Q_a^b(t)]^2 + \frac{1}{2} \sum_{l_{[a,c]}\in\mathcal{L}} [E_{[a,c]}(t) - \theta_{[a,c]}]^2, \quad (10)$$

where the storage saturation values $\theta_{[a,c]}$ should be chosen carefully in the algorithm as discussed later in this section. Define the following *drift-plus-penalty* [52] for our algorithm design, so as to optimize utility while ensuring network stability,

$$\Delta_V(t) \equiv \Delta(t) - V \sum_{a,b\in\mathcal{N}} U(R_a^b(t)), \quad (11)$$

where V is a tunable positive constant and

$$\Delta(t) = L(t+1) - L(t). \quad (12)$$

The construction of the target function, Eq. (11), is similar to the Lagrange multiplier method.

Then, we choose the control action to minimize the drift-plus-penalty given in Eq. (11). Using the queueing dynamics in Eqs. (6) and (8), after some algebras, we decouple the key management and data transmission, so that we can optimize them separately. In the end, the target function Eq. (11) can be rewritten as

$$\begin{aligned}\Delta_V(t) \leq B &+ \sum_{l_{[a,c]}\in\mathcal{L}} (E_{[a,c]}(t) - \theta_{[a,c]}) S_{[a,c]}(t) K_{[a,c]} \\ &- \sum_{a,b\in\mathcal{N}} [V U_a^b(R_a^b(t)) - Q_a^b(t) R_a^b(t)] \\ &- \sum_{a,b\in\mathcal{N}} \sum_{c\in\mathcal{N}_a^{out}} \mu_{[a,c]}^b(t) [Q_a^b(t) - Q_c^b(t)] \\ &- \sum_{l_{[a,c]}\in\mathcal{L}} (E_{[a,c]}(t) - \theta_{[a,c]}) P_{[a,c]}(t). \quad (13)\end{aligned}$$

Here the constant B is given by

$$B \equiv N^2 (\frac{3}{2} d_{max}^2 \mu_{max}^2 + R_{max}^2) + \frac{L}{2} (P_{max} + K_{max})^2, \quad (14)$$

where the subscript max means the maximal possible values in the strategies and $d_{max} = \max_a(|\mathcal{N}_a^{in}|, |\mathcal{N}_a^{out}|)$. The detailed derivations of Eq. (13) is presented in Appendix A.

Before we give the utility optimization algorithm, we need to introduce the following network technical terms. The saturation of the key storage, $\theta_{[a,c]}$, is defined as

$$\theta_{[a,c]} \equiv \delta\beta V + P_{max}, \quad (15)$$

where δ is a positive constant satisfying $\mu_{[a,c]}(P_{[a,c]}(t)) \leq \delta P_{[a,c]}(t)$ and β is the largest first derivative of the utility functions, $\beta = \max_{a,b} \beta_{a,b} = \max_{n,c} (U_a^b)'(0)$. Here, we only consider $(U_a^b)'(0)$ since the utility function is concave. The operational meaning of $\theta_{[a,c]}$ is to let key storage be saturated to a positive constant $\theta_{[a,c]}$ rather than zero since we often need a positive key storage to handle urgent data transmission tasks.

TABLE III

UTILITY OPTIMIZATION ALGORITHM

1) Input of the algorithm. Initialize $\theta_{[a,c]}$. At every time slot t, observe $Q_a^b(t)$ and $E_{[a,c]}(t)$.
2) Key generation. If $E_{[a,c]}(t) - \theta_{[a,c]} < 0$, perform key generation, i.e., let $S_{[a,c]}(t) = 1$; otherwise, let $S_{[a,c]}(t) = 0$. Note that this decision minimizes the second term on the right-hand side of Eq. (13).
3) Data transmission. Make a local optimization on the third term of the right-hand side of Eq. (13),

$$\max_{R_a^b(t)} \quad VU_a^b(R_a^b(t)) - Q_a^b(t)R_a^b(t), \tag{18}$$

with the constraint of $0 < R_a^b(t) < R_{max}$.

4) Key management. Optimize the key consumption over all edges, $\vec{P}(t)$, by solving the following maximization

$$\begin{aligned}\max_{\vec{P}(t)} G(\vec{P}(t)) &= \sum_{n\in\mathcal{N}}\sum_{c\in\mathcal{N}_a^{out}} \mu_{[a,c]}(t)W_{[a,c]}(t) \\ &\quad + \sum_{l_{[a,c]}\in\mathcal{L}} (E_{[a,c]}(t) - \theta_{[a,c]})P_{[a,c]}(t) \\ &= \sum_{l_{[a,c]}\in\mathcal{L}} \left\{\mu_{[a,c]}(t)W_{[a,c]}(t) + (E_{[a,c]}(t) - \theta_{[a,c]})P_{[a,c]}(t)\right\},\end{aligned} \tag{19}$$

subject to the key availability constraint Eq. (7).

5) Routing and scheduling. Find $b^* \in argmax_b W_{[a,c]}^b(t)$. If $W_{[a,c]}^{b^*}(t) > 0$, set $\mu_{[a,c]}^{b^*}(t) = \mu_{[a,c]}(t)$, i.e., allocate the full rate over the link $l_{[a,c]}$ to any commodity achieving the maximum positive weight.
6) Queue update. Update $Q_a^b(t)$ and $E_{[a,c]}(t)$ according to their dynamics Eqs. (6) and (8), respectively.

Then, we define the weight of the type-b data over the link $l_{[a,c]}$ as

$$W_{[a,c]}^b(t) = Q_a^b(t) - Q_c^b(t) - \gamma. \tag{16}$$

The link weight is given by $W_{[a,c]}(t) = \max_b W_{[a,c]}^b(t)$. Here, γ is defined as

$$\gamma \equiv R_{max} + d_{max}\mu_{max}, \tag{17}$$

which means the maximum possible increase of the data queue in a node in a single time slot, including the maximum endogenous increase $d_{max}\mu_{max}$ and exogenous increase R_{max}. We consider a data transmission task by some link $l_{[a,c]}$ to be important only when the data queue difference between two nodes, $Q_a^b(t) - Q_c^b(t)$, is large enough (larger than γ).

The main idea of the algorithm is to optimize the data transmission, $R_a^b(t)$ ($\forall a, b \in \mathcal{N}$), and key management, $P_{[a,c]}(t)$ ($\forall l_{[a,c]} \in \mathcal{L}$), by minimizing the target function, Eq. (13), subject to Eqs. (7) and (8). In Eq. (13) we can see that the optimization of $R_a^b(t)$ and $P_{[a,c]}(t)$ can be done separately. Note that the network stability constraint Eq. (9) is automatically satisfied under the Lyapunov drift approaches Eq. (12). The total utility Eq. (4) is not optimized directly, but the optimization result can be arbitrarily close to maximum utility of Eq. (4), which will be discussed in details in Sec. III-D.

Now, we present the main optimization algorithm given in Table III, inspired by the energy-limited scheduling algorithm [46].

D. Analysis of the Algorithm and Its Performance

Here, we explain how the algorithm works and analyze its performance. We make some remarks on the details of the algorithm. First, the key availability constraint given in Eq. (7) is actually redundant, i.e., we can directly optimize Eq. (19) without any constraint and obtain the same key management action. To prove this, we have the following lemma and leave the proof in Appendix B

Lemma 1: The data queue and key storage have the following deterministic bounds, $\forall a, b, t, l_{[a,c]} \in \mathcal{L}$,

$$\begin{aligned}0 &\le Q_a^b(t) \le \beta V + R_{max}, \\ 0 &\le E_{[a,c]}(t) \le \theta_{[a,c]} + K_{max}.\end{aligned} \tag{20}$$

Suppose the optimized key consumption vector obtained by Eq. (19) is $\vec{P^*}(t)$. Then we consider a new key consumption vector $\vec{P_0}(t)$ by setting $P_{[a,c]}^*(t)$ in $\vec{P^*}(t)$ to be 0, i.e., the only difference between $\vec{P^*}(t)$ and $\vec{P_0}(t)$ is the key consumption in the link $l_{[a,c]}$. If the constraint Eq. (7) is violated, i.e., $E_{[a,c]} < P_{[a,c]}$, then

$$\begin{aligned}&G(\vec{P^*}(t)) - G(\vec{P_0}(t)) \\ &= \mu_{[a,c]}(P_{[a,c]}^*(t))W_{[a,c]}(t) + \left(E_{[a,c]}(t) - \theta_{[a,c]}\right)P_{[a,c]}^*(t) \\ &\le \delta P_{[a,c]}^*(t)(\beta V - d_{max}\mu_{max}) - \delta\beta V P_{[a,c]}^*(t) \\ &< 0,\end{aligned} \tag{21}$$

which leads to a contradiction that $\vec{P^*}(t)$ is not the optimized strategy. The first inequality is obtained by Lemma 1 and $\mu_{[a,c]}(P_{[a,c]}^*(t)) \le \delta P_{[a,c]}^*(t)$ is due to the definition of δ of Eq. (15). Especially, for one-time-pad encryption, we have $\mu_{[a,c]}(P_{[a,c]}^*(t)) = P_{[a,c]}^*(t)$ and we can take $\delta \ge 1$.

Second, in steps *key management* and *routing and scheduling*, we make an optimization on the destination b, i.e., we only consider the destination b^* with the maximum link weight, because

$$\begin{aligned}\sum_b \mu_{[a,c]}^b(t)W_{[a,c]}^b(t) &\le \sum_b \mu_{[a,c]}^b(t)W_{[a,c]}(t) \\ &= \mu_{[a,c]}(t)W_{[a,c]}(t)\end{aligned} \tag{22}$$

Therefore, it is optimal to allocate the full rate over the link $l_{[a,c]}$ to any commodity achieving the maximum positive weight. If there are multiple destinations b^* achieving the maximum link weight, we can randomly choose one of them to allocate the full rate.

Third, one can see that the optimized target function in the algorithm is different from the original utility function given in Eq. (4). We want to show that the optimization result of the algorithm can be arbitrary close to the optimal utility U_{tot}, i.e., the performance of the algorithm is given by the following theorem and leave its proof in Appendix C.

Theorem 3: The utility optimization result of the algorithm can be arbitrarily close to the optimal utility U_{tot},

$$\begin{aligned}\liminf_{\tau\to\infty} U_{tot}(\vec{r}(\tau)) &= \liminf_{\tau\to\infty}\sum_{n,c} U_a^b(r_a^b(\tau))\\ &\geq U_{tot}(\vec{r^*}) - \frac{\tilde{B}}{V},\end{aligned} \tag{23}$$

where $r_a^b(\tau) = \frac{1}{\tau}\sum_{t=0}^{\tau-1} R_a^b(t)$ is the average data flow, $\tilde{B} = B + N^2\gamma d_{max}\mu_{max}$ is a constant, and $\vec{r^*}$ is an optimal solution for Eq. (4).

Finally, compared to the original algorithm given in [46], we can optimize the key management in Eq. (19) locally for each edge rather than each node. This is a particularly useful feature for practical implementation.

E. Simulation

To test our algorithm, we make a simulation of the toy network model given in Fig. 1. Here we consider a simple task where the data are transmitted from Alice to Bob, i.e., $R_a^b(t) = 0$ for all nodes a except Alice's node. From the network structure in Fig. 1 we can see that $d_{max} = 2$. We set the values of other parameters as $\beta = 1$, $\delta = 2$, $P_{max} = \mu_{max} = 2$, $R_{max} = 3$, $K_{[a,c]} = 0.1, \forall l_{[a,c]}$, $\gamma = d_{max}\mu_{max} + R_{max} = 7$ and $\theta_{[a,c]} = \delta\beta V + P_{max} = 2V + 2$. These values are just taken for simplicity and we do not consider their units. The utility function is taken as $U(r) = \ln(1 + r)$. The optimization of such a utility function is actually also a maximization of data transmission. We simulate the utility of the whole network versus $V \in \{5, 10, 15, 20, 25, 30, 35, 40, 45\}$ to see convergence behavior when V goes larger.

The simulation of the total utility is given in Fig. 3. It turns out that the utility converges quickly to the optimal value of 0.1815, which shows our algorithm is quite efficient. We also show the evolution of the total data queue and key storage in Fig. 4 with $V = 40$. We can observe that the network become stable after $t = 10^3$. and the data queue grows slowly during $t \in [10^2, 10^3]$, which is because the amount of data queue exceeds the key storage in the previous time period. After the stability of the network, the gap between the key storage and data queue is determined by the parameter settings, which can be optimized and is left for future works. The evolution of the utility is shown in Fig. 5. The drop at the beginning comes from the initialization of the network. The data transimission at the beginning is high since the data and key storage is initialized to be zero, which leads to a high utility. The convergence speed is similar to the original algorithm [46].

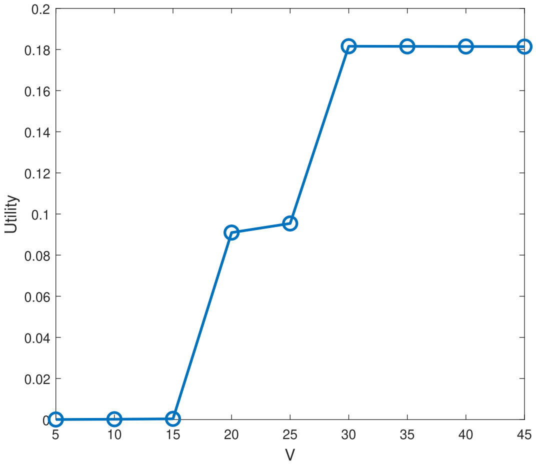


Fig. 3. Simulation result of a toy network model. The optimized utility (also maximized data transmission) converges quickly to the optimal value.

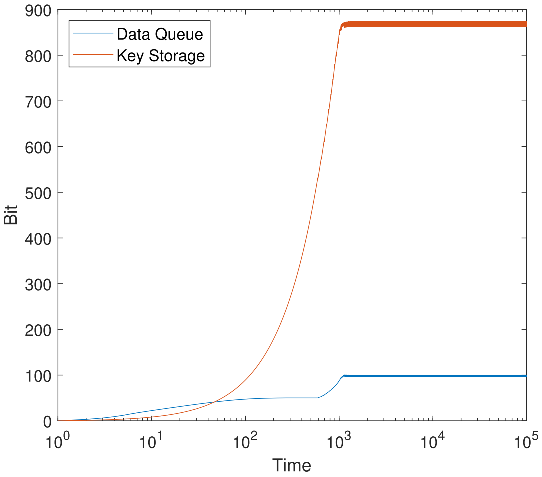


Fig. 4. Evolution of the total data queue and key storage of the toy network with $V = 40$. We can see that the network become stable after $t = 10^3$. The width of both curves shows the data fluctuations.

In our simulation of the toy model, we choose typical values for the parameters β, δ, P_{max}, μ_{max}, R_{max}, and $K_{[a,c]}$ and assume that the key rates in different links are the same, $K_{[a,c]} = 0.1, \forall l_{[a,c]}$. While in a practical field test we can substitute some real values into the simulation, such as the QKD key rates in each link and the classical channel capacity. We can obtain useful results with the real values, for example, the convergence time of data queue and key storage, the saturation of the data queue and key storage, and the data transmission capacity of the network.

We make comparisons with some other routing protocols in the literature. Some protocols are proposed for different targets in a QKD network. For example, in ref. [56], the authors apply a multi-path routing scheme to maximize the key rate between two remote end-users in a network with both quantum repeaters and trusted nodes. While in ref. [57], the authors consider a routing protocol based on current key storage. It applies a modified Open Shortest Path Fast routing

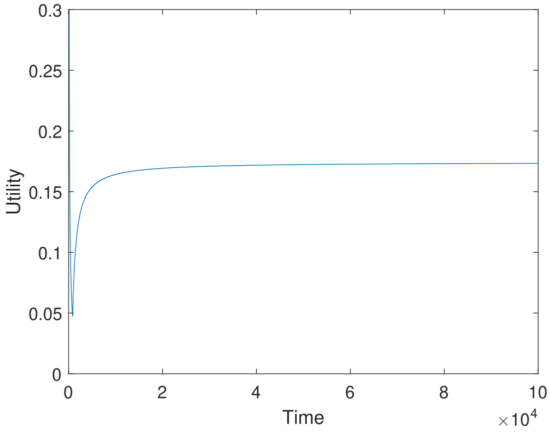


Fig. 5. Evolution of the utility of the toy network with $V = 40$.

algorithm to minimize the path length between end-users and reduce the key consumption in the meantime. There are also some routing protocols in energy harvesting networks, aiming at optimizing the utility function of the data flow. In [58], the utility optimization has been formulated as a standard convex optimization problem without Lyapunov optimization techniques, however, it requires future knowledge on the energy harvesting that is hardly available. Another protocol based on a convex optimization problem without Lyapunov optimization techniques is proposed in ref. [47], which gives rise to an asymptotic optimal solution. By simulating the simplest network with one source and one destination, it shows a better performance on utility compared with the optimizations based on Lyapunov optimization techniques.

IV. Discussion and Conclusion

In this work, we propose solutions to two typical and crucial issues in quantum networks, namely security and key management. We tackle the security issue with graph theory and design a communication scheme of the highest security level, where each intermediate node broadcasts the XOR result of all its keys. To optimize the utility of the data. These two problems are closely connected in some special situations. Suppose the key is free and data cannot be stored in each node. Then our optimization problem will reduce to the maximum flow problem in a directed graph. If we further assume the capacities of the classical links are the same, this maximum flow will be proportional to the security level according to the max-flow min-cut theorem.

In this paper, we consider two networks, a classical network for data transmission and a QKD network for key generation. The latter can be naturally extended to an entanglement distribution network in the future, where the key distribution and XOR operation correspond to the Einstein–Podolsky–Rosen (EPR) pair distribution and entanglement swapping. It is interesting to apply the techniques used in this work to an entanglement distribution network.

For future works, one can substitute the data communication requests and key rate of an actual quantum network (such as the Hefei 46-node network) to our simulations and make a field test of our results. One can also consider more complex topological structures and other practical issues such as latency and scalability.

Finally, a trusted node does not need to perform full QKD with users, i.e., the privacy amplification process can be omitted first and raw keys can be directly exchanged [59]. We call such a node an honest but curious node. In this case, the intermediate nodes lie between trusted and untrusted. The security assessment needs more complicated analysis.

Appendix A
Derivations of Eq. (13)

By the definition of $\Delta(t)$ in Eq. (12), we divide $\Delta(t)$ into two parts. The first part comes from the data queue term,

$$\begin{aligned}&\frac{1}{2}\sum_{a,b\in\mathcal{N}}[Q_a^b(t+1)]^2-\frac{1}{2}[Q_a^b(t)]^2\\ &=\sum_{a,b\in\mathcal{N}}Q_a^b(t)\left(-\sum_{c\in\mathcal{N}_a^{out}}\mu_{[a,c]}^b(t)+\sum_{c\in\mathcal{N}_a^{in}}\mu_{[c,a]}^b(t)+R_a^b(t)\right)\\ &\quad+\frac{1}{2}\left(-\sum_{c\in\mathcal{N}_a^{out}}\mu_{[a,c]}^b(t)+\sum_{c\in\mathcal{N}_a^{in}}\mu_{[c,a]}^b(t)+R_a^b(t)\right)^2.\end{aligned}\tag{24}$$

For the first term in the rhs. of Eq. (24), we want to show that

$$\begin{aligned}&\sum_{a,b}Q_a^b(t)\left(-\sum_{c\in\mathcal{N}_a^{out}}\mu_{[a,c]}^b(t)+\sum_{c\in\mathcal{N}_a^{in}}\mu_{[c,a]}^b(t)\right)\\ &\qquad=-\sum_{a,b\in\mathcal{N}}\sum_{c\in\mathcal{N}_a^{out}}\mu_{[a,c]}^b(t)[Q_a^b(t)-Q_c^b(t)].\end{aligned}\tag{25}$$

Consider an arbitrary term, $Q_a^b(t)\left(-\mu_{[a,c]}^b(t)+\mu_{[a',a]}^b(t)\right)$, there will always be another term in the summation $Q_c^b(t)\left(-\mu_{[c,c']}^b(t)+\mu_{[a,c]}^b(t)\right)$. We can regroup these terms and obtain $-\mu_{[a,c]}^b(t)[Q_a^b(t)-Q_c^b(t)]$. Similarly, we can do this for all other terms in the summation and get the rhs. of Eq. (25).

For the second term in the rhs. of Eq. (24), we have

$$\begin{aligned}&\left(-\sum_{c\in\mathcal{N}_a^{out}}\mu_{[a,c]}^b(t)+\sum_{c\in\mathcal{N}_a^{in}}\mu_{[c,a]}^b(t)+R_a^b(t)\right)^2\\ &\leq\left(\sum_{c\in\mathcal{N}_a^{out}}\mu_{[a,c]}^b(t)\right)^2+\left(\sum_{c\in\mathcal{N}_a^{in}}\mu_{[c,a]}^b(t)+R_a^b(t)\right)^2\\ &\leq d_{max}^2\mu_{max}^2+(d_{max}\mu_{max}+R_{max})^2\\ &\leq d_{max}^2\mu_{max}^2+\frac{1}{2}(d_{max}^2\mu_{max}^2+R_{max}^2)\\ &=3d_{max}^2\mu_{max}^2+2R_{max}^2.\end{aligned}\tag{26}$$

Similar calculations can be done for the second part of $\Delta(t)$ which comes from the key storage term. Finally we can get Eq. (13) by some algebras.

APPENDIX B
PROOF OF LEMMA 1

We prove this lemma with mathematical induction. First we can easily see that the bound holds for $t = 0$, since $Q_a^b(0) = 0$ and $E_{[a,c]}(0) = 0$.

Then we prove that if $0 \leq Q_a^b(t) \leq \beta V + R_{max}$, then $0 \leq Q_a^b(t+1) \leq \beta V + R_{max}$. According to the dynamics of data queue Eq. (8), we can see that the increase of the data queue comes from two aspects: endogenous data $\sum_{c\in\mathcal{N}_a^{in}} \mu_{[c,a]}^b(t)$ and exogenous data $R_a^b(t)$. We consider the following two exclusive cases: first, if there are endogenous data, then they must come from at least one other node, say c. From Eq. (16), if there is a data flow from c to a at time t, their data queues at time t must satisfy,

$$Q_a^b(t) \leq Q_c^b(t) - \gamma \leq \beta V + R_{max} - \gamma. \tag{27}$$

From time slot t to $t+1$, the maximum possible data queue increase of one node is γ. Then we have $Q_a^b(t+1) \leq \beta V + R_{max}$; second, there are no endogenous data, which means there are only exogenous data or there are no data queue increase at all. From Eq. (18), the existence of a valid optimization result $R_a^b(t)$ requires $Q_a^b(t) \leq \beta_{a,b} V \leq \beta V$. From time slot t to $t+1$, the maximum possible exogenous data queue increase is R_{max}. Then we also have $Q_a^b(t+1) \leq \beta V + R_{max}$. If there are no data queue increase from t to $t+1$, it is straightforward that $Q_a^b(t+1) \leq Q_a^b(t) \leq \beta V + R_{max}$.

Finally we prove if $0 \leq E_{[a,c]}(t) \leq \theta_{[a,c]} + K_{max}$, then $0 \leq E_{[a,c]}(t+1) \leq \theta_{[a,c]} + K_{max}$. We also consider the following two exclusive cases: according to the second step of the algorithm, if $E_{[a,c]}(t) < \theta_{[a,c]}$, there will be key generation with a maximum key of K_{max}, then $E_{[a,c]}(t+1) < \theta_{[a,c]} + K_{max}$; if $E_{[a,c]}(t) \geq \theta_{[a,c]}$, there will be no key generation and $E_{[a,c]}(t+1) \leq E_{[a,c]}(t) \leq \theta_{[a,c]} + K_{max}$.

APPENDIX C
PROOF OF THEOREM 3

In the algorithm we minimize the following function at time t

$$\begin{aligned} D(t) = &\sum_{l_{[a,c]}\in\mathcal{L}} (E_{[a,c]}(t) - \theta_{[a,c]}) S_{[a,c]}(t) K_{[a,c]} \\ &- \sum_{a,b\in\mathcal{N}} [V U_a^b(R_a^b(t)) - Q_a^b(t) R_a^b(t)] \\ &- \sum_{a,b\in\mathcal{N}} \sum_{c\in\mathcal{N}_a^{out}} \mu_{[a,c]}^b(t) [Q_a^b(t) - Q_c^b(t) - \gamma] \\ &- \sum_{l_{[a,c]}\in\mathcal{L}} (E_{[a,c]}(t) - \theta_{[a,c]}) P_{[a,c]}(t), \end{aligned} \tag{28}$$

and get an optimized set of strategies $\mathcal{S} = \{R_a^b(t), P_{[a,c]}(t)\}$. Now we consider another function

$$\begin{aligned} \tilde{D}(t) = &\sum_{l_{[a,c]}\in\mathcal{L}} (E_{[a,c]}(t) - \theta_{[a,c]}) S_{[a,c]}(t) K_{[a,c]} \\ &- \sum_{a,b\in\mathcal{N}} [V U_a^b(R_a^b(t)) - Q_a^b(t) R_a^b(t)] \\ &- \sum_{a,b\in\mathcal{N}} \sum_{c\in\mathcal{N}_a^{out}} \mu_{[a,c]}^b(t) [Q_a^b(t) - Q_b^c(t)] \\ &- \sum_{l_{[a,c]}\in\mathcal{L}} (E_{[a,c]}(t) - \theta_{[a,c]}) P_{[a,c]}(t) \\ = &D(t) - \sum_{a,b\in\mathcal{N}} \sum_{c\in\mathcal{N}_a^{out}} \mu_{[a,c]}^b(t) \gamma. \end{aligned} \tag{29}$$

We can see that the only difference between Eq. (28) and Eq. (29) is that in Eq. (29) γ is not introduced. Suppose the optimized strategy to minimize Eq. (29) is $\tilde{\mathcal{S}} = \{\tilde{R}_a^b(t), \tilde{P}_{[a,c]}(t)\}$. We have the following relation,

$$\begin{aligned} D^{\mathcal{S}}(t) &\leq D^{\tilde{\mathcal{S}}}(t) \\ \tilde{D}^{\tilde{\mathcal{S}}}(t) &\leq \tilde{D}^{\mathcal{S}}(t). \end{aligned} \tag{30}$$

From the first inequality of Eq. (30) we quickly get

$$\tilde{D}^{\mathcal{S}}(t) \leq \tilde{D}^{\tilde{\mathcal{S}}}(t) + N^2 \gamma d_{max} \mu_{max}. \tag{31}$$

Then we substitute Eq. (31) to Eq. (13),

$$\Delta(t) - V \sum_{a,b\in\mathcal{N}} U_a^b(R_a^b(t)) \leq B + \tilde{D}^{\mathcal{S}}(t) \leq \tilde{B} + \tilde{D}^{\tilde{\mathcal{S}}}(t), \tag{32}$$

where $\tilde{B} = B + N^2 \gamma d_{max} \mu_{max}$. Since the strategy $\tilde{\mathcal{S}} = \{\tilde{R}_a^b(t), \tilde{P}_{[a,c]}(t)\}$ can take continuous values, we apply the relation $-\tilde{D}^{\tilde{\mathcal{S}}}(t) \geq V U_{tot}(\vec{r^*})$ given in Theorem 1 of [46] and Claim 1 of [60]. This means the maximization of the total utility in a single time slot will be larger than that in time average,

$$\Delta(t) - V \sum_{a,b\in\mathcal{N}} U_a^b(R_a^b(t)) \leq \tilde{B} - V U_{tot}(\vec{r^*}). \tag{33}$$

Then we sum over Eq. (33) from $t = 0$ to $t = \tau - 1$,

$$L(\tau) - L(0) - V \sum_{t=0}^{\tau-1} \sum_{a,b\in\mathcal{N}} U_a^b(R_a^b(t)) \leq \tau\tilde{B} - \tau V U_{tot}(\vec{r^*}). \tag{34}$$

Divide $V\tau$ in both sides and use $L(\tau) \geq 0$ and $L(0) = 0$,

$$\begin{aligned} \sum_{a,b\in\mathcal{N}} U_a^b\Big(\frac{1}{\tau}\sum_{t=0}^{\tau-1} R_a^b(t)\Big) &\geq \frac{1}{\tau}\sum_{t=0}^{\tau-1}\sum_{a,b\in\mathcal{N}} U_a^b(R_a^b(t)) \\ &\geq U_{tot}(\vec{r^*}) - \frac{\tilde{B}}{V}, \end{aligned} \tag{35}$$

where the first inequality is because the utility function is concave. Then we take a $\liminf$ as $\tau \to \infty$ and have

$$\liminf_{\tau\to\infty} \sum_{a,b} U_a^b(r_a^b(\tau)) \geq U_{tot}(\vec{r^*}) - \frac{\tilde{B}}{V}. \tag{36}$$

ACKNOWLEDGMENT

The authors would like to thank T. Chen, Y. Liu, and S. Yao for enlightening discussions, and also would like to thank the anonymous reviewers for their constructive comments.

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst. Signal Process.*, New York, NY, USA: IEEE Press, Dec. 1984, pp. 175–179, doi: 10.1016/j.tcs.2014.05.025.

[2] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, Aug. 1991, doi: 10.1103/PhysRevLett.67.661.

[3] H. K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *Science*, vol. 283, no. 5410, p. 2050, 1999. [Online]. Available: http://science.sciencemag.org/content/283/5410/2050

[4] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, no. 2, pp. 441–444, 2000, doi: 10.1103/PhysRevLett.85.441.

[5] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.*, vol. 91, no. 5, Aug. 2003, Art. no. 057901, doi: 10.1103/PhysRevLett.91.057901.

[6] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 94, no. 23, Jun. 2005, Art. no. 230504, doi: 10.1103/PhysRevLett.94.230504.

[7] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," *Phys. Rev. Lett.*, vol. 94, no. 23, Jun. 2005, Art. no. 230503, doi: 10.1103/PhysRevLett.94.230503.

[8] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, "Experimental quantum key distribution with decoy states," *Phys. Rev. Lett.*, vol. 96, no. 7, Feb. 2006, Art. no. 070502, doi: 10.1103/PhysRevLett.96.070502.

[9] D. Rosenberg *et al.*, "Long-distance decoy-state quantum key distribution in optical fiber," *Phys. Rev. Lett.*, vol. 98, no. 1, Jan. 2007, Art. no. 010503, doi: 10.1103/PhysRevLett.98.010503.

[10] T. Schmitt-Manderbach *et al.*, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Phys. Rev. Lett.*, vol. 98, no. 1, Jan. 2007, Art. no. 010504, doi: 10.1103/PhysRevLett.98.010504.

[11] C.-Z. Peng *et al.*, "Experimental long-distance decoy-state quantum key distribution based on polarization encoding," *Phys. Rev. Lett.*, vol. 98, no. 1, Jan. 2007, Art. no. 010505, doi: 10.1103/PhysRevLett.98.010505.

[12] Y. Liu *et al.*, "Decoy-state quantum key distribution with polarized photons over 200 km," *Opt. Exp.*, vol. 18, no. 8, pp. 8587–8594, Apr. 2010. [Online]. Available: http://www.opticsexpress.org/abstract.cfm?URI=oe-18-8-8587

[13] A. Boaron *et al.*, "Secure quantum key distribution over 421 km of optical fiber," *Phys. Rev. Lett.*, vol. 121, no. 19, Nov. 2018, Art. no. 190502, doi: 10.1103/PhysRevLett.121.190502.

[14] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, Mar. 2012, Art. no. 130503, doi: 10.1103/PhysRevLett.108.130503.

[15] Y. Liu *et al.*, "Experimental measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 111, no. 13, Sep. 2013, Art. no. 130502, doi: 10.1103/PhysRevLett.111.130502.

[16] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, "Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 112, no. 19, May 2014, Art. no. 190503, doi: 10.1103/PhysRevLett.112.190503.

[17] T. F. da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid, "Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits," *Phys. Rev. A, Gen. Phys.*, vol. 88, no. 5, Nov. 2013, Art. no. 052303, doi: 10.1103/PhysRevA.88.052303.

[18] Y.-L. Tang *et al.*, "Measurement-device-independent quantum key distribution over 200 km," *Phys. Rev. Lett.*, vol. 113, no. 19, Nov. 2014, Art. no. 190501, doi: 10.1103/PhysRevLett.113.190501.

[19] H.-L. Yin *et al.*, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Phys. Rev. Lett.*, vol. 117, no. 19, Nov. 2016, Art. no. 190501, doi: 10.1103/PhysRevLett.117.190501.

[20] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, "Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks," *Phys. Rev. Lett.*, vol. 111, no. 13, Sep. 2013, Art. no. 130501, doi: 10.1103/PhysRevLett.111.130501.

[21] Y. L. Tang *et al.*, "Field test of measurement-device-independent quantum key distribution," *IEEE J. Sel. Topics Quantum Electron.*, vol. 21, no. 3, pp. 116–122, May 2015.

[22] X. Ma, P. Zeng, and H. Zhou, "Phase-matching quantum key distribution," *Phys. Rev. X*, vol. 8, no. 3, Aug. 2018, Art. no. 031043, doi: 10.1103/PhysRevX.8.031043.

[23] J. Lin and N. Lütkenhaus, "Simple security analysis of phase-matching measurement-device-independent quantum key distribution," *Phys. Rev. A, Gen. Phys.*, vol. 98, no. 4, Oct. 2018, Art. no. 042332, doi: 10.1103/PhysRevA.98.042332.

[24] L. Salvail, M. Peev, E. Diamanti, R. Alléaume, N. Lütkenhaus, and T. Länger, "Security of trusted repeater quantum key distribution networks," *J. Comput. Secur.*, vol. 18, no. 1, pp. 61–87, Jan. 2010.

[25] M. Epping, H. Kampermann, C. Macchiavello, and D. Bruß, "Multi-partite entanglement can speed up quantum key distribution in networks," *New J. Phys.*, vol. 19, no. 9, Sep. 2017, Art. no. 093012.

[26] M. Takeoka, E. Kaur, W. Roga, and M. M. Wilde, "Multipartite entanglement and secret key distribution in quantum networks," 2019, *arXiv:1912.10658*.

[27] S. Das, S. Bäuml, M. Winczewski, and K. Horodecki, "Universal limitations on quantum key distribution over a network," 2019, *arXiv:1912.03646*.

[28] C. Elliott, "The darpa quantum network," in *Quantum Communications and Cryptography*. Boca Raton, FL, USA: CRC Press, 2005, pp. 91–110.

[29] M. Peev *et al.*, "The SECOQC quantum key distribution network in Vienna," *New J. Phys.*, vol. 11, no. 7, 2009, Art. no. 075001.

[30] W. Chen *et al.*, "Field experiment on a 'star type' metropolitan quantum key distribution network," *IEEE Photon. Technol. Lett.*, vol. 9, no. 21, pp. 575–577, May 1, 2009.

[31] M. Sasaki *et al.*, "Field test of quantum key distribution in the Tokyo QKD network," *Opt. Exp.*, vol. 19, no. 11, pp. 10387–10409, 2011.

[32] S. Wang *et al.*, "Field and long-term demonstration of a wide area quantum key distribution network," *Opt. Exp.*, vol. 22, no. 18, pp. 21739–21756, 2014.

[33] Y.-L. Tang *et al.*, "Measurement-device-independent quantum key distribution over untrustful metropolitan network," *Phys. Rev. X*, vol. 6, no. 1, Mar. 2016, Art. no. 011024, doi: 10.1103/PhysRevX.6.011024.

[34] S.-K. Liao *et al.*, "Satellite-relayed intercontinental quantum network," *Phys. Rev. Lett.*, vol. 120, no. 3, Jan. 2018, Art. no. 030501, doi: 10.1103/PhysRevLett.120.030501.

[35] B. Qi, "Simultaneous classical communication and quantum key distribution using continuous variables," *Phys. Rev. A, Gen. Phys.*, vol. 94, no. 4, Oct. 2016, Art. no. 042340, doi: 10.1103/PhysRevA.94.042340.

[36] O. Elmabrok, M. Ghalaii, and M. Razavi, "Quantum-classical access networks with embedded optical wireless links," *J. Opt. Soc. Amer. B, Opt. Phys., Opt. Phys.*, vol. 35, no. 3, pp. 487–499, 2018.

[37] T. Chapuran *et al.*, "Optical networking for quantum key distribution and quantum communications," *New J. Phys.*, vol. 11, no. 10, 2009, Art. no. 105001.

[38] B. Qi, W. Zhu, L. Qian, and H.-K. Lo, "Feasibility of quantum key distribution through a dense wavelength division multiplexing network," *New J. Phys.*, vol. 12, no. 10, Oct. 2010, Art. no. 103042.

[39] P. K. Tysowski, X. Ling, N. Lütkenhaus, and M. Mosca, "The engineering of a scalable multi-site communications system utilizing quantum key distribution (QKD)," *Quantum Sci. Technol.*, vol. 3, no. 2, Nov. 2017, Art. no. 024001.

[40] M. Pattaranantakul, A. Janthong, K. Sanguannam, P. Sangwongngam, and K. Sripimanwat, "Secure and efficient key management technique in quantum cryptography network," in *Proc. 4th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Jul. 2012, pp. 280–285.

[41] C. Yang, H. Zhang, and J. Su, "The QKD network: Model and routing scheme," *J. Modern Opt.*, vol. 64, no. 21, pp. 2350–2362, Nov. 2017.

[42] M. Pant, H. Krovi, D. Englund, and S. Guha, "Rate-distance tradeoff and resource costs for all-optical quantum repeaters," *Phys. Rev. A, Gen. Phys.*, vol. 95, no. 1, Jan. 2017, Art. no. 012304, doi: 10.1103/PhysRevA.95.012304.

[43] S. Pirandola, "End-to-end capacities of a quantum communication network," *Commun. Phys.*, vol. 2, p. 51, May 2019.

[44] L. Jiang and J. Walrand, "Scheduling and congestion control for wireless and processing networks," *Synth. Lectures Commun. Netw.*, vol. 3, no. 1, p. 156, 2010.

[45] J. G. Dai and W. Lin, "Asymptotic optimality of maximum pressure policies in stochastic processing networks," *Ann. Appl. Probab.*, vol. 18, no. 6, pp. 2239–2299, Dec. 2008.

[46] L. Huang and M. J. Neely, "Utility optimal scheduling in energy-harvesting networks," *IEEE/ACM Trans. Netw.*, vol. 21, no. 4, pp. 1117–1130, Aug. 2013.

[47] S. Chen, P. Sinha, N. B. Shroff, and C. Joo, "A simple asymptotically optimal joint energy allocation and routing scheme in rechargeable sensor networks," *IEEE/ACM Trans. Netw.*, vol. 22, no. 4, pp. 1325–1336, Aug. 2014.

[48] L. Georgiadis, M. J. Neely, and L. Tassiulas, *Resource Allocation and Cross-Layer Control in Wireless Networks*. Norwell, MA, USA: Now Publishers, 2006.

[49] G. S. Vernam, "Cipher printing telegraph systems: For secret wire and radio telegraphic communications," *Trans. Amer. Inst. Electr. Eng.*, vol. 45, no. 2, pp. 109–115, Feb. 1926.

[50] D. Dolev, C. Dwork, O. Waarts, and M. Yung, "Perfectly secure message transmission," *J. ACM*, vol. 40, no. 1, pp. 17–47, Jan. 1993.

[51] T. R. Beals and B. C. Sanders, "Distributed relay protocol for probabilistic information-theoretic security in a randomly-compromised network," in *Proc. Int. Conf. Inf. Theoretic Secur.* Berlin, Germany: Springer, 2008, pp. 29–39.

[52] L. Georgiadis, M. J. Neely, and L. Tassiulas, "Resource allocation and cross-layer control in wireless networks," *Found. Trends Netw.*, vol. 1, no. 1, pp. 1–144, 2006.

[53] L. Huang, "Intelligence of smart systems: Model, bounds and algorithms," *IEEE/ACM Trans. Netw.*, vol. 25, no. 5, pp. 2960–2973, Oct. 2017.

[54] B. Li, R. Li, and A. Eryilmaz, "On the optimal convergence speed of wireless scheduling for fair resource allocation," *IEEE/ACM Trans. Netw.*, vol. 23, no. 2, pp. 631–643, Apr. 2015.

[55] R. Urgaonkar, B. Urgaonkar, M. J. Neely, and A. Sivasubramaniam, "Optimal power cost management using stored energy in data centers," in *Proc. ACM Sigmetrics*, Jun. 2011, pp. 221–232.

[56] O. Amer, W. O. Krawec, and B. Wang, "Efficient routing for quantum key distribution networks," in *Proc. IEEE Int. Conf. Quantum Comput. Eng. (QCE)*, Oct. 2020, pp. 137–147.

[57] Y. Tanizawa, R. Takahashi, and A. R. Dixon, "A routing method designed for a quantum key distribution network," in *Proc. 8th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Jul. 2016, pp. 208–214.

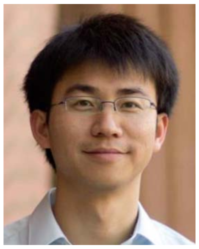
[58] S. Chen, P. Sinha, N. B. Shroff, and C. Joo, "Finite-horizon energy allocation and routing scheme in rechargeable sensor networks," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 2273–2281.

[59] W. Stacey, R. Annabestani, X. Ma, and N. Lütkenhaus, "Security of quantum key distribution using a simplified trusted relay," *Phys. Rev. A, Gen. Phys.*, vol. 91, no. 1, Jan. 2015, Art. no. 012338, doi: 10.1103/PhysRevA.91.012338.

[60] M. J. Neely, "Energy optimal control for time-varying wireless networks," *IEEE Trans. Inf. Theory*, vol. 52, no. 7, pp. 2915–2934, Jul. 2006.

Hongyi Zhou received the bachelor's degree in theoretical physics from Peking University in 2014 and the Ph.D. degree from Tsinghua University in 2019. He is currently an Assistant Professor with the Institute of Computing Technology, Chinese Academy of Sciences. From 2019 to 2021, he did his Post-Doctoral Researcher with the University of Tokyo. In 2021, he joined the Institute of Computing Technology, Chinese Academy of Sciences. His current research are focused on quantum cryptography and quantum optics.

Kefan Lv received the bachelor's degree in computer science and technology from the Institute for Interdisciplinary Information Sciences (IIIS), Tsinghua University, in 2018. He is an Alumni of IIIS, Tsinghua University.



Longbo Huang (Senior Member, IEEE) is currently an Associate Professor (with tenure) with the Institute for Interdisciplinary Information Sciences (IIIS), Tsinghua University, Beijing, China. He has held visiting positions with the LIDS Laboratory, MIT, The Chinese University of Hong Kong, Bell-labs France, Microsoft Research Asia (MSRA), and the Simons Institute for the Theory of Computing, UC Berkeley. He serves/served on the TPCs and Organizing Committees for IEEE/ACM/AI conferences, including ACM Sigmetrics 2021 (the General Chair), ITC 2022 (the TPC Co-Chair) and WiOpt 2020 (the TPC Co-Chair). He currently serves on the editorial board for ACM TRANSACTIONS ON MODELING AND PERFORMANCE EVALUATION OF COMPUTING SYSTEMS (ToMPECS) and IEEE/ACM TRANSACTIONS ON NETWORKING (ToN). He received the Outstanding Teaching Award from Tsinghua University in 2014, the Google Research Award and the Microsoft Research Asia Collaborative Research Award in 2014, and was selected into the MSRA StarTrack Program in 2015. He won the ACM SIGMETRICS Rising Star Research Award in 2018.

Xiongfeng Ma received the B.Sc. degree from Peking University in 2003 and the Ph.D. degree from the University of Toronto. He is currently an Associate Professor with Tsinghua University. From 2008 to 2011, he did his post-doctoral researcher and visiting positions with the University of Waterloo, the University of Toronto, and the University of Leeds. In 2012, he joined Tsinghua University. His main research interest lies in quantum information and quantum optics, particularly in quantum cryptography and quantum foundation.