Title:

Key relay protocol for quantum key distribution

Industrial Partner:

Mitsubishi Electric Corporation, Information Technology R&D Center

Mitsubishi Electric Corp. is a world leader in the manufacture and sale of electrical and electronic products and systems used in a broad range of fields and applications. As a global leader among green companies, our technologies are being applied to contribute to and support society and daily life around the world. The Information Technology R&D Center is actively creating new businesses through basic research and development in the fields of information technology, media intelligence, electro-optics microwaves, and communication technologies. We seek technologies that reinforce our position at the leading edge of progress, with work to renew existing businesses through the fruits of our R&D in the field of IT.

Industry Mentor

Toyohiro Tsurumaru, Ph.D., Senior Expert, Advanced Basic Research Dept.

Background and the problem

The Quantum Key Distribution (QKD, also often called quantum cryptography) encryption method is guaranteed to be unbreakable, as described in the literature [1–3]. Unlike currently widely used cryptographic methods, this method relies on the physical laws of quantum mechanics for its security. It has been proven that it cannot be broken, despite technological progress (note 1).

This encryption method is quantum technology, but unlike quantum computers, it has already been commercialized. Startups have been selling products since the 2000s. Today, large companies such as Toshiba and NEC are also selling related products.

Nevertheless, for several reasons, QKD has not yet been adopted widely throughout society. One reason is the short communication distance (note 2). The key relay (KR) is often applied to alleviate this weakness. With this project, we aim at improving the KR, increase the communication distance of QKD, and contribute to its widespread adoption.

Description of the situation

Actual situation

In QKD, as in normal communication devices, the sender and receiver (hereinafter designated respectively as Alice and Bob) each possess a communication device, connected using a communication channel such as optical fiber. When Alice and Bob turn on their devices, a secret key for encryption is distributed to both (Fig. 1(a), step 1). Using the secret key thus obtained for that of

an existing encryption method (e.g., AES or one-time pad [8]), Alice and Bob can achieve secure communication (Fig. 1(a), step 2)

However, as described already, the current communication distance of QKD is short: typically around 50 km.

Abstract situation

We can simplify the situation described above to facilitate mathematical consideration.

First, regarding the two steps in Fig. 1(a), we assume that only step 1 is our responsibility. In other words, we are responsible only for providing the secret key. We do not care which encryption method the users use it for. Second, we disregard the internal workings of the QKD devices, and simply regard them as a black box that distributes secret a key to two distinct points. Third, we call QKD's typical communication distance (50 km) the unit length.

Then the QKD device can be regarded as a black box that (Fig. 1(b))

- consists of an edge of the unit length, and
- distributes the same random bits r to (players at) the end nodes
- in such a way that the value of r is unknown to any other player.

Below, we consider only what can be done using this black box. From this standpoint, the black box described above need no longer be implemented with actual QKD devices. For example, even if it were implemented as a trusted courier (with which a user would locally generate a random number, store it in a storage device, and ask a trusted person to carry it physically), the logical consequences would be the same. Therefore, the user has no need to know about the internal workings of the QKD devices involving quantum phenomena.

Key relay protocol

In reality, because strong demand exists for communication beyond the unit length, a method called the key relay (KR) is often used ([4,5], note 3). By this simple method, multiple channels are connected in series. The sender's secret key is decrypted and re-encrypted at relay nodes (joints of edges) repeatedly (Figs. 1(c) and (d)). However, as might be readily apparent, this method has the following weakness:

- (Weakness) Once one relay node (i.e., a node other than Alice or Bob) is taken over, the security of the entire system collapses.

Methods for overcoming this weakness have been investigated in several earlier studies [4,5], but no conclusive solution has been reported.

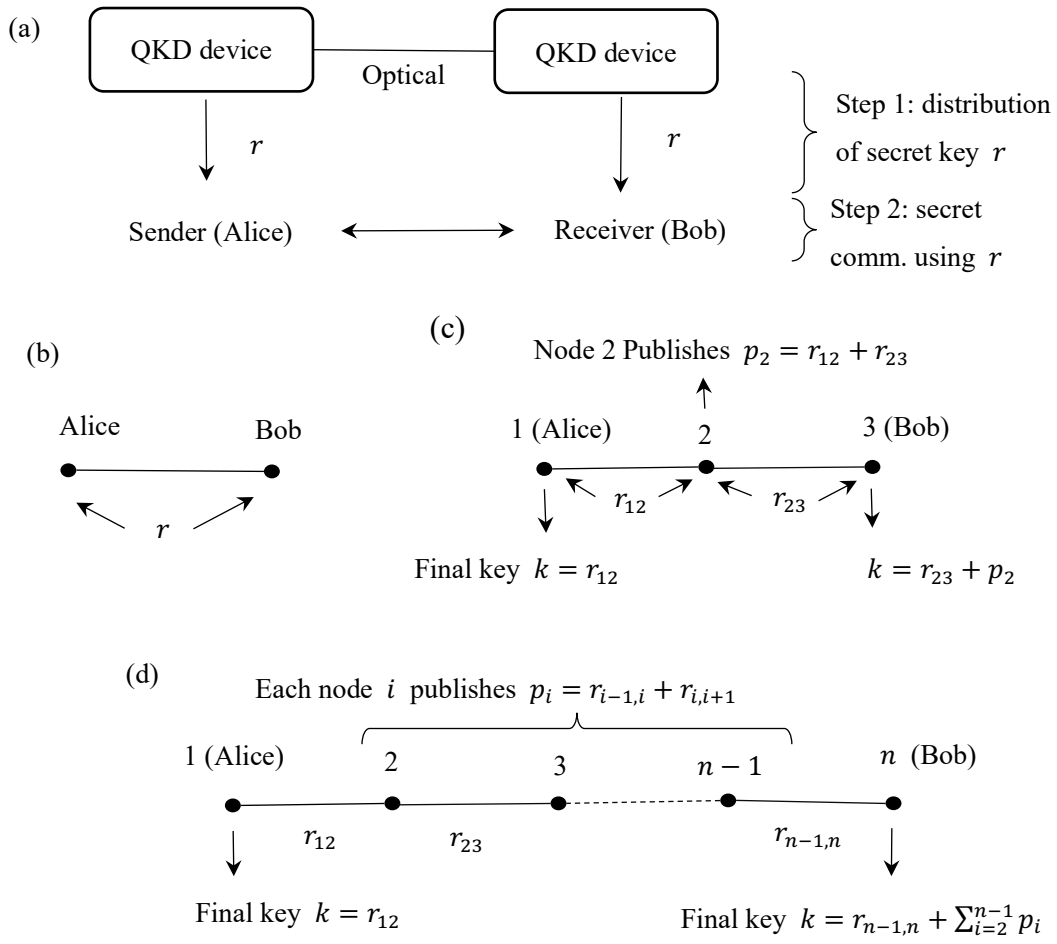

Figure 1. Conceptual diagram of QKD and a simple example of a key relay (KR).
(a) Typical usage of QKD equipment. Step 1: The QKD equipment distributes a random number r to the sender and receiver (the value of r is known only to the sender and receiver). Step 2: The sender and receiver use r as a secret key to encrypt classical communication, e.g., over the internet. (b) An abstract description of step 1 in (a). (c) The simplest case of key relay (KR). Two communication channels are arranged in series. The goal is for users 1 (Alice) and 3 (Bob) to share the final key $k = r_{12}$. To achieve this, node 2 publishes p_2. Then user 3 obtains the final key k from this and the local key r_{23}. It is noteworthy that $p_2 = r_{12} + r_{23}$ can be regarded as the ciphertext of message k, one-time pad encrypted with key r_{23}. (d) A straightforward generalization of (c) with multiple relay nodes (i.e., nodes other than Alice and Bob).

Goal

This project goal is the creation of methods to overcome the weakness described above.

Perhaps this goal sounds too abstract. To make it more accessible, we present two example problems

of specific interests below. One need not limit oneself to these two directions: any other direction would be fine as long as it overcomes the weakness described above. Alternatively, by borrowing ideas from these problems, one might create and solve new and interesting mathematical problems, which can even be unrelated to KR.

Irrespective of which direction is adopted, the mathematical approach is expected for solving the problem, i.e., any new assumption should be stated explicitly. Claims of the validity of the proposed method, such as the security, should be made with logically sound reasoning, as described elsewhere herein (note 1).

Problem 1

As described already, quantum mechanics conforms to the laws of physics; QKD uses it to realize secure communication. In a similar sense, the property that

- (Causality) one cannot transmit information faster than the speed of light, i.e., faster than 300,000 km/s,

is also accepted as a law of physics (based on the theory of relativity). Several cryptographic methods using it have been proposed [6].

Can the weakness of the KR be overcome by this idea, i.e., using causality? Or, if that is not possible, can one prove its impossibility?

Problem 2

A simple way to mitigate the weaknesses of KR is to use it in parallel (Fig. 2(a)). In this case, the eavesdropper must take over multiple nodes to ascertain the secret key.

It is also straightforward to generalize this configuration to an arbitrary network (Fig. 2(b); [4,5]). Henceforth, we designate this as the generalized form of the KR protocol (KRP).

The KRP turns out to be very similar to *secure network coding* (SNC, [6] and Fig. 2(c)), which have been studied extensively for years in information theory. Moreover, it can be proved easily that it actually includes SNC in terms of functionality [5]: a SNC scheme can always be simulated using a KRP on the same graph. Consequently, our question is: Does the reverse inclusion relation hold? If not, then what are examples of useful KRPs, i.e., those KRP protocols which cannot be realized using SNC?

This problem is important for the following reasons.

Research investigating KRP, a new research topic, has progressed very slowly and with few investigations described in the literature. By contrast, SNC has a longer history and a huge accumulated body of research results. If the KRP and SNC turn out to be equivalent, then one would

no longer need to study the KRP; it would be sufficient to translate the known results of SNC for use in the KRP.

However, if these two techniques are not equivalent, then there might be KRPs that cannot be realized with SNC, which might be useful for applications such as QKD.

It is noteworthy that recent research has shown that, at least under limited conditions (each edge transmits only one bit), the KRP is strictly larger [4]. Therefore, our question can be rephrased more precisely as "Can one show that SNC and the KRP are not equivalent under the general condition?"

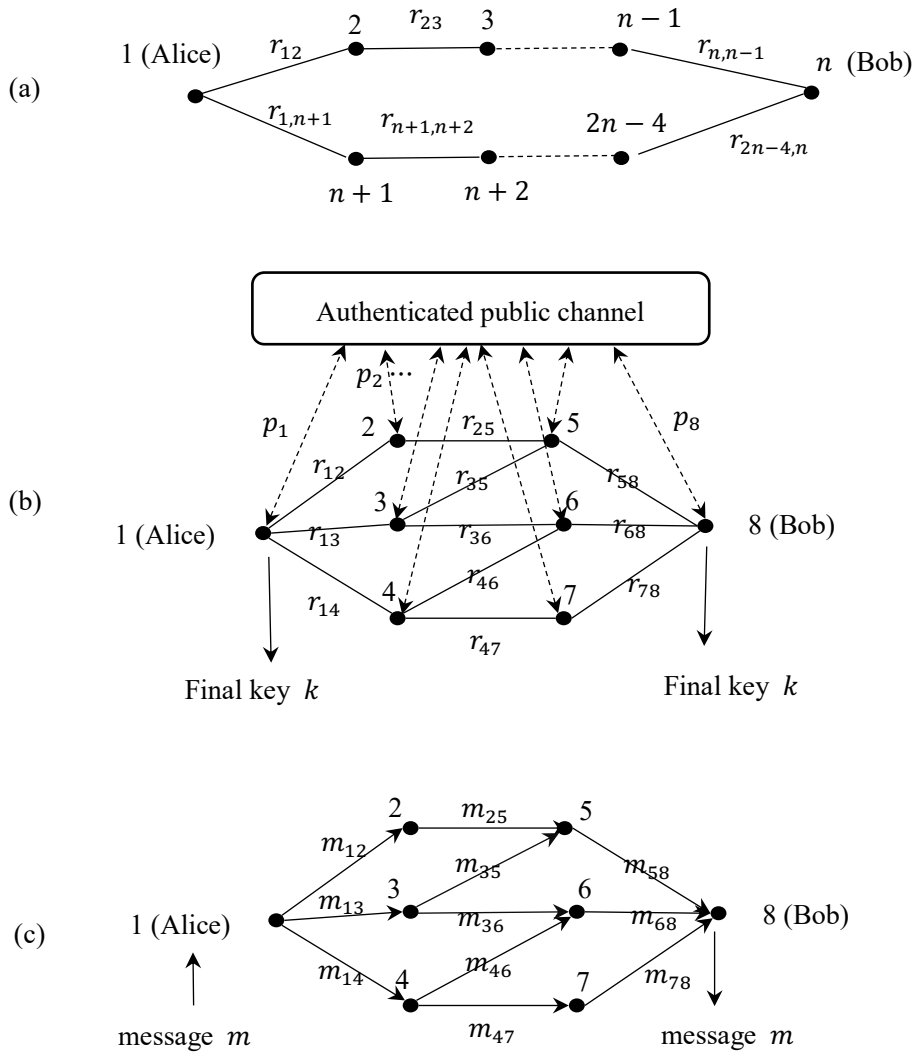

Figure 2. Key relay protocol (KRP) and secure network coding (SNC).

(a) A parallel extension of Fig. 1(d). Relay nodes (nodes $2..,n-1,n+1,\ldots,2n$) publish the XOR of secret keys r_{ij} of their adjacent edges. Alice (Bob) calculates the secret key $k_1 = r_{12} +$

$r_{1,n+1}, (k_n = r_{n,n-1} + r_{2n-4,n} + \sum_i p\_i)$. In this case, k remains unknown, even when one of the relay nodes is taken. (b) One can also generalize (a) to any network. We designate this as a generalized form of the key relay protocol (KRP). Here a random number r_{ij} is distributed to both ends of each edge (i,j); it is unknown to anyone other than nodes i and j. Each node i calculates and publishes public information p_i based on r_{ij} of adjacent edges. Alice and Bob calculate the secret key k from p_i and from r_{ij} of adjacent edges. A good KRP is one in which k remains secret, even when many relay nodes are taken. (c) Secure network coding closely resembles the KRP in (b) and has been studied for years. Here, information m_{ij} can be transmitted securely on each edge (i,j), but public communication channels are not available. Alice sends a message m to Bob. A good SNC scheme is one in which message m remains secret, even when many intermediate nodes are taken.

Caveat

In solving the problems described above, one should not use cryptographic primitives based on computational assumptions as components, which are already widely used today. Those methods include post-quantum cryptography. Such methods must be avoided because the security of such primitives is explicitly inferior to that of QKD, which holds without computational assumptions. In general, the overall cryptosystem security is dependent on its weakest link. If any one component relies on computational assumption, then so does the entire system, making the use of QKD meaningless in the first place. Additional details are presented in note 1.

Basic knowledge:

Information theory (preferable), graph theory (preferable), quantum information theory (preferable)

Notes

- Note 1:Accurate meaning of “guaranteed to be unbreakable”

  The property of being "guaranteed to be unbreakable" is technically known as *information-theoretic security*, which means that the security of the cryptographic method can be proven with no assumptions, and only through probabilistic considerations [8]. By this terminology, QKD is described more accurately as a cryptographic method that achieves information-theoretic security based on quantum mechanics [1,2].

  Widely used cryptographic methods have a weaker property designated as *computational security* [8], where 1) one assumes that “a certain mathematical problem is difficult to solve by computer” (computational assumption), and 2) prove the security of the method at hand based on that assumption. A famous example is the RSA cryptosystem, which is based on the difficulty of a problem similar to prime factorization [8].

In other words, in quantum cryptography, the security is proven mathematically considering the laws of quantum mechanics as assumptions. By contrast, in modern cryptography, the security is proven mathematically under computational assumptions. Logically, both quantum mechanics and computational assumptions are assumptions. The difference is that quantum mechanics is a physical law, whereas computational assumptions are conjectures without a proof.

Indeed, quantum mechanics, which was discovered 100 years ago, has been repeatedly verified through experimentation. By contrast, computational assumptions are opinions based on circumstantial evidence for which no effective solution algorithm has been reported to date. In fact, in several cases, cryptographic methods once deemed secure turned out to be insecure as research progressed ([8], Section 7.2.3).

- Note 2: Another reason is that it is more expensive than existing encryption methods.
- Note 3: A technology called *quantum repeater* ([2], Section III.E) is also being assessed to address the same issue, but will not be considered for this project because it has not yet been realized.

References

[1] Nielsen, M. A., & Chuang, I. L. (2010). Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge: Cambridge University Press.

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. 74, 145 (2002), DOI: https://doi.org/10.1103/RevModPhys.74.145.

[3] F. Xu, X.-F. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan "Secure quantum key distribution with realistic devices," Rev. Mod. Phys. 92, 025002 – Published 26 May, 2020, DOI: https://doi.org/10.1103/RevModPhys.92.025002.

[4] L. Salvail, M. Peev, E. Diamanti, R. Alléaume, N. Lütkenhaus, and T. Länger, "Security of trusted repeater quantum key distribution networks," Journal of Computer Security, vol. 18, no. 1, pp. 61-87, 2010, DOI: 10.3233/JCS-2010-0373; https://arxiv.org/abs/0904.4072.

[5] G. Kato, M. Fujiwara and T. Tsurumaru, "Advantage of the Key Relay Protocol Over Secure Network Coding," in IEEE Transactions on Quantum Engineering, vol. 4, pp. 1-17, 2023, Art no. 4100517, DOI: 10.1109/TQE.2023.3309590.

[6] A. Kent, "Unconditionally Secure Bit Commitment," Phys. Rev. Lett. 83, 1447 (1999); DOI: https://doi.org/10.1103/PhysRevLett.83.1447.

[7] N. Cai and R. W. Yeung, "Secure network coding," Proceedings IEEE International Symposium on Information Theory, Lausanne, Switzerland, 2002, pp. 323, DOI: 10.1109/ISIT.2002.1023595.

[8] J. Katz and Y. Lindell. 2014. Introduction to Modern Cryptography, Second Edition (2nd. ed.). Chapman & Hall – CRC.