IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 14 August 2024, accepted 23 September 2024, date of publication 26 September 2024, date of current version 7 October 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3468442

RESEARCH ARTICLE

Information Theoretically Secure Data Relay Using QKD Network

MIKIO FUJIWARA, GO KATO, AND MASAHIDE SASAKI
National Institute of Information and Communications Technology, Koganei, Tokyo 184-8795, Japan

Corresponding author: Mikio Fujiwara (fujiwara@nict.go.jp)

This work was supported in part by the Ministry of Internal Affairs and Communications, Japan, through the ICT Priority Technology Research and Development Project, under Grant JPMI00316.

ABSTRACT For information that requires long-term confidentiality (e.g. national security, military security, genomic data etc.), the threat of eavesdropping must be seriously considered. The leakage of such information would not only cause temporary confusion but would also have serious repercussions for future generations. Part of such important data are already being exchanged over the Internet using cryptography that is not resistant to quantum computers. Considering the possibility of harvest attacks on information that must be kept secret for centuries, developing a technology that can immediately eliminate the risk of eavesdropping in principle is desirable. In response to these demands, we previously developed a system called the quantum secure cloud, which realizes an information-theoretically secure data transmission, storage, reconstruction, and authentication with a single password, using an established technology of quantum key distribution network. We now apply this technology to develop an information-theoretically secure long-distance data-relay function and succeed in developing a distributed data-relay simulator that is compatible with current quantum key distribution networks. The throughput of this protocol is more than 10 Mbps for 10 MB data, so it can be applied to practical use.

INDEX TERMS Quantum key distribution, Tokyo QKD network, secret sharing, information-theoretically secure authentication with a single password, data relay.

I. INTRODUCTION

Recent advances of quantum computing technologies are faster than expected in the past years. The latest roadmap predicts the realization of a quantum computer with quantum error-correction capability by approximately 2030 [1]. Therefore, cryptography resistant against quantum computers are highly demanded. Critical information such as national security and military security related data, and genomic data need to be securely protected over a time scale of centuries, using cryptography resistant against quantum computers [2]. The leakage of such information would not only cause temporary confusion but would also have serious repercussions for future generations. For example, leakage of genomic data incurs the risk of an abuse of a personal information [3] as well as the risk of trans-generational effects.

Likely threats against such critical data include store-now-decrypt-later, i.e., a harvest attack, by future high-performance computers including quantum computers [4]. Ensuring the three essential requirements of information security: confidentiality, integrity and availability against the store-now-decrypt later attacks is an urgent task.

In July 2022, the National Institute of Standards and Technology standardized four cryptographic protocols as post quantum cryptography and further evaluated the four protocols in Round 4 [5]. Of the protocols that advanced to Round 4, supersingular isogeny key encapsulation was immediately considered flawed [6]. This case implies that regardless of how good mathematical cryptography is, appearance of new attack methods cannot be excluded. In contrast, physical-layer cryptography, particularly quantum key distribution (QKD), can guarantee information-theoretical security because security is guaranteed by physical laws [7], [8]. That is, the threat of decryption does not exist in principle,

The associate editor coordinating the review of this manuscript and approving it for publication was Lukasz Wisniewski.

although threats of decryption due to device imperfections in the system still exists [9]. A QKD is also superior in terms of forward security [10], making it suitable for the transmission of data that needs to be kept secret long term.

In the QKD scheme represented by the BB84 protocol [11], a single photon is used as a transmission medium to share a random number, and the scheme's performance is significantly affected by transmission-line losses. Even the fastest commercialized QKD system achieves 1 Mbps at a fiber transmission loss of 10dB (50 km with a standard fiber loss of 0.2 dB/km) [12], and wavelength multiplexing and other measures are required to achieve higher speeds [13].

To distribute keys over longer distances, QKD networks currently in operation in many countries [14], [15] employ a key-relay method via trusted nodes to expand the usage distance and number of users [16]. Moreover, by combining with post-quantum cryptography (PQC), high secure long-distance QKD technology has been studied [17].

In order to realize information-theoretically secure data transmission and storage satisfying confidentiality and availability, the National Institute of Information and Communications Technology implemented a secret-sharing protocol [18] on a QKD network, whose system is referred to as the quantum secure cloud [19], [20], [21].

Needless to say, user authentication is essential for the secure operation of QKD networks for data confidentiality and integrity. For secure user authentication, methods using PQC [22] or group authentication [23] have been proposed. Furthermore, a protocol has been proposed that uses group authentication to implement secure key relay even if some nodes are compromised [24]. Unlike computationally secure PQC and group authentication that requires multiple nodes, we have developed information-theoretically secure user authentication and data-integrity verification simultaneously with a single password using the secret computation function of secret sharing scheme [19], [20]. In particular, our protocol can achieve information-theoretical security with a single password. The data volume of a single password is considerably smaller than those of other data shares. Additionally, the password must be a piece of information that only the user knows. Therefore, the password is the most important dataset in this protocol. In our previous studies, a data owner used this secret-sharing system from one specific location. Therefore, the locations at which the data were registered/reconstructed were identical.

However, data reconstruction by a data owner is, in principle, possible anywhere, as long as the share holders required for reconstruction are connected by QKD. If a password that is known only to the data owner can be securely passed only to a specific person on the QKD network without a key relay by trusted nodes, and if that specific person can communicate with the share holder with information-theoretical security, this protocol can be applied to secure data storage and relay without undue reliance on the security levels of trusted nodes. In other words, the secret sharing is a scheme that enables long-term secure data storage. Even if some shares would be leaked, the confidentiality of the original secret data is not breached if the number of leaked shares is below a threshold. This property can be applied to relax the security requirements for trusted nodes in secure communication by key relay through quantum key distribution networks. The problem lies in securely transmitting the password. In addition, during a key relay for share transmission, the threshold assumption and risk of information leakage at trusted nodes in each route must be minimized by prohibiting the key supply from the same trusted node to multiple key-relay routes for share transmission.

In this study, we demonstrate an information-theoretically secure data-relay system that has minimal impact on key-information leakage from a trusted node by applying a key-relay route-selection rule: a trusted node can only participate in one relay route for each share transmission and the password can only be transmitted to a specific person with one QKD link.

This protocol enables information-theoretically secure authentication using a single password. By transmitting the password using a key from a QKD link (in which a high key generation rate is not necessarily required), user authentication can be realized without depending on the security level of the trusted node. Therefore, in this protocol, the ability to search for key-relay routes to transmit passwords and shares is important.

We integrated the secure data relay system with a QKD network controller (QKDNC) [25] for the key-relay route control in an actual QKD network to verify its practicality. Furthermore, compared with our previous system [19], we achieved a throughput improvement of more than 10 times, which implies that our system can be used as a real communication method. Additionally, the terminals used in the simulation experiments were equipped with secure personal authentication technology using multi-factor authentication, creating an environment where many users can use the same system in peace.

An overview of the protocol and simulation configuration are presented in Section II. The simulation environment and experimental results are presented in Section III. Finally, we discuss and summarize the results in Sections IV and V, respectively.

II. PROTOCOL AND SIMULATION CONFIGURATION

The basic protocol follows our previously proposed protocol [19], [20]. This protocol enables a totally information-theoretically secure distributed storage system based on a user-friendly single-password-authenticated secret-sharing scheme. In previous protocols, data were handled by the data owner alone. In this scheme, the data owner and data user are physically located in different places, and the data-relay system is centrally managed by the QKDNC [25]. QKDNC has the role of deciding the key relay route. In the protocol proposed this time, it is necessary to prepare multiple key-relay routes in advance, and since one trusted node does not participate in two or more key-relays. Even if the security of the trusted node is compromised, it is necessary to minimize deterioration of the secret sharing threshold assumption. This time, we have implemented a function in QKDNC that can determine multiple key-relay routes that meet the above conditions. Details are described below.

A. PLAYERS AND THEIR ROLES IN THIS PROTOCOL

This protocol comprises elements with the following five roles.

1) DATA OWNER (DATA SENDER)

The data owner (data sender) is the owner of the data and sets the password (PW) for data reconstruction. Data and password shares are generated by the data owner.

2) DATA USER (DATA RECIPIENT)

The Data user (data recipient) is the recipient of the data, who receives the PW from the data owner and reconstructs the data using this protocol. The data user collects shares and performs calculations to reconstruct the data from the shares.

3) QKDNC

The QKDNC manages the entire QKDN and relays data at the request of the data owner and user. The QKDNC decides the key-relay route.

4) SHARE HOLDER

The share holder stores the shares, exchanges shares between share holders, and generates and transmits shares according to QKDNC's instructions. The share holder is set in the same location as the key-management system of the trusted node.

5) TRUSTED NODE

The trusted node stores and manages keys from the QKD link and performs Vernam's one-time-pad (OTP) encryption [26] using keys from the QKD links for key relay and share-data transmission according to the instructions of the QKDNC.

To simplify the boundaries of responsibilities, we define the trusted node to also function as a share holder. The QKDNC is responsible for the data-relay service. This is because the route setting during key relay is closely related to the security of information in this protocol. Notably, the QKDNC and supervisor of this protocol do not need to have the same identity.

B. OUTLINE OF THE PROPOSED PROTOCOL

The following is an outline of the protocol procedure.

1. The QKDNC receives a request for distributed data storage and the relay of data from the data owner and determines the share holder and data-relay route. At this time, the data user does not necessarily need to make decisions.
2. The data user requests the data to the data owner and the QKDNC through an authenticated public communication channel.
3. The QKDNC determines the key-relay route from the data owner to the data user, considering the relationship between the locations of the share holder and data user at this point. If there is no suitable route at this point, the QKDNC either start from the route search or choose to deny the service.
4. If the QKDNC succeeds in determining the key-relay route, data relay is performed (If the QKDNC cannot determine a suitable key-relay route for the data relay, it notifies the data owner that the data-relay service has been aborted).
5. The data owner sends the PW to the data user using key from the single QKD links, and the data user receives the PW for data reconstruction from the data owner. *(Note: This process may be performed at the beginning of the data relay protocol.)*
6. The PW received in Step 5 is used to reconstruct the relayed data, which have been made secret through secret sharing.
7. After confirming the integrity of the data using the PW, the protocol is completed.

C. DETAILS OF THE PROPOSED PROTOCOL

The protocol we have implemented this time is based on that of the previous literature [19], [20], and updated with new steps for the data relay. In the following, the data relay protocol is presented along the line of [19] with newly added steps highlighted in *italic* font. A conceptual view of the data-relay configuration is shown in Fig. 1, being compared with the previous scheme in [19] and [20].

We introduce notations for Shamir's secret sharing (SS) (k, n)-threshold scheme we use. Secret data D are divided into n shares $f_{\mathrm{D}}(a_1), f_{\mathrm{D}}(a_2), \ldots, f_{\mathrm{D}}(a_n)$, where f_{D} is a randomly chosen polynomial of degree $k-1$ at most with a constant term $f_{\mathrm{D}}(0)$, which represents the secret data D itself, and $a_1, a_2, \ldots, a_n$ are public values. Then, the knowledge of any k or more pieces of $f_{\mathrm{D}}(a_i)$ makes D easily computable through a Lagrange interpolation. However, the knowledge of any $k-1$ or fewer pieces of $f_{\mathrm{D}}(a_i)$ leaves D completely undetermined (in the sense that all possible values are equally likely). In other words, the attacker cannot recover the original data from less than the threshold k of the shares, even when using unlimited computational resources. This enables secret calculations (addition and multiplication [18]). In fact, $f_{\mathrm{D}^{(1)}}(a_i) + f_{\mathrm{D}^{(2)}}(a_i)$ becomes a share of the addition of two secret datasets $D^{(1)}$ and $D^{(2)}$. Similarly, $f_{\mathrm{D}^{(1)}}(a_i) \times f_{\mathrm{D}^{(2)}}(a_i)$ is used as the share of $D^{(1)} \times D^{(2)}$. However, in the multiplication process, the degree of the polynomial $f_{\mathrm{D}^{(1)}}(x) \times f_{\mathrm{D}^{(2)}}(x)$ is $2k-2$. Thus, $2k-1$ of shares are necessary to reconstruct $D^{(1)} \times D^{(2)}$.

Here, we describe our password-authenticated secret-sharing scheme. It comprises four phases in which all communications between the data owner machine and storage servers, and among the storage servers, are OTP encrypted by the keys supplied from the QKD network. Thus, information-theoretical security during data transmission can be ensured. Calculations can be performed over an arbitrary finite field, and Mersenne primes are typically used as the finite field to achieve high calculation speeds.

A detailed procedure is exemplified below in the case where there are four share holders ($n = 4$) denoted as 1, 2, 3, and 4, and we assume that an attacker can corrupt at most one storage server. A detailed conceptual diagram of this protocol is shown in Fig. 2.

(0) Password transmission phase

The data owner sends the password P to the specified end user through a direct connection OTP-encrypted with a key from the QKD link. This process can also be performed between Phase (2) and (3), as described below.

1) DATA REGISTRATION PHASE

The data owner implements the following process for secure data rely:

(1-1)

The data owner calculates the shares of the data and passwords. Because each calculation in the finite field with prime order $q = 2^m - 1$ can only handle blocks of length $m - 1$ bits at most, secret data D, which generally has a considerably longer length, needs to be divided into pieces of $(m-1)$-bit blocks, say l pieces; $D = D_l \,|D_{l-1}| \cdots |D_1$. The data owner sets an $(m-1)$-bit password P, which should have sufficient entropy against the on-line dictionary attack, then computes a message-authentication code, $MAC = D_l P^l + D_{l-1} P^{l-1} + \cdots + D_1 P$, which is denoted as D_{l+1}, and finally appends it to the data for subsequent message authentication.

(1-2)

For each data block, data shares $f_{\mathrm{D}_i}(1)$, $f_{\mathrm{D}_i}(2)$, $f_{\mathrm{D}_i}(3)$, and $f_{\mathrm{D}_i}(4)$ are created for storage servers 1, 2, 3, and 4, respectively, using a polynomial f_{D_i} with a degree of 2 at most, where $i = 1, \ldots, l + 1$. Password shares $f_{\mathrm{P}}(1), f_{\mathrm{P}}(2), f_{\mathrm{P}}(3)$, and $f_{\mathrm{P}}(4)$ are created using a polynomial f_{P} with a degree of 1 at most.

(1-3)

These shares are then sent to the corresponding share holders.

Each share holder server stores the set of shares.

2) COMPUTATION AND COMMUNICATION AMONG SHARE HOLDERS PHASE

This process is performed to prevent the leakage of information other than the fact that the password was incorrect, even if an incorrect password is entered during data reconstruction.

(2-1)

Each share holder server generates a random number, denoted as R_j for the j-th storage server, and makes its shares $f_{\mathrm{R}_{ij'}}(1), f_{\mathrm{R}_{ij'}}(2), f_{\mathrm{R}_{ij'}}(3), f_{\mathrm{R}_{ij'}}(4)$ using a polynomial $f_{\mathrm{R}_{ij'}}$ with a degree of 1 at most. Furthermore each server generates shares of the "0" $f_{\mathrm{Z}_{ij'}}(1), f_{\mathrm{Z}_{ij'}}(2), f_{\mathrm{Z}_{ij'}}(3), f_{\mathrm{Z}_{ij'}}(4)$ using polynomial $f_{\mathrm{Z}_{ij'}}$ with a degree of 2 at most, such that $f_{\mathrm{Z}_{ij'}}(0) = 0$ should hold so as to keep the confidentiality of the share in the data-reconstruction phase without changing the value of the data share. Share of the "0" is essential to ensure uniformity of shares, because $(f_{\mathrm{P}}(j) - f_{\mathrm{P}'}(j))\, R_i(j)$ term causes discontinuity and non-uniformity in shares.

(2-2)

The share holders send shares which are calculated in **(2-1)** to each other. Each share holder receives three shares of three random numbers and three shares of the "0," and stores them together with the ones produced by itself. For information-theoretical security, the above procedure must be iterated $l + 1$ times before each data reconstruction of l blocks secret data. That is, the j-th share holder has to keep $l + 1$ sets of $(f_{\mathrm{R}_{i1}}(j), f_{\mathrm{R}_{i2}}(j), f_{\mathrm{R}_{i3}}(j), f_{\mathrm{R}_{i4}}(j), f_{\mathrm{Z}_{i1}}(j), f_{\mathrm{Z}_{i2}}(j), f_{\mathrm{Z}_{i3}}(j), f_{\mathrm{Z}_{i4}}(j))$.

3) DATA RELAY AND RECONSTRUCTION PHASE

At process (0), the data user receives password P from the data owner using the key of the QKD link without the trusted node key relay. When the user needs to restore data, the data user recalls and uses the password when reconstructing the data. We denote this password as P’.

(3-1)

The data user chooses three types of j-line-share holders that are geographically close and have shared keys for the OTP. Without loss of generality, we may assume that they are one, two, and three-line-share holders, denoting them as a set $L = \{1, 2, 3\}$.

(3-2)

The data user generates shares of P,’ $f_{\mathrm{P}'}(1)$, $f_{\mathrm{P}'}(2)$, *and* $f_{\mathrm{P}'}(3)$ *using a polynomial* $f_{\mathrm{P}'}$ *with degree at most one.*

(3-3)

Each set$(L, f_{\mathrm{P}'}(j))$ is sent to each corresponding share holder. (request)

(3-4)

If $|L| \neq 3$, the request is rejected regarding it as an improper request. Otherwise, for each data block, each share holder, say j-th one, computes $R_i(j) = f_{\mathrm{R}_{i1}}(j) + f_{\mathrm{R}_{i2}}(j) + f_{\mathrm{R}_{i3}}(j)$, $Z_i(j) = f_{\mathrm{Z}_{i1}}(j) + f_{\mathrm{Z}_{i2}}(j) + f_{\mathrm{Z}_{i3}}(j)$ and

$$F_i(j) = (f_{\mathrm{P}}(j) - f_{\mathrm{P}'}(j))\, R_i(j) + Z_i(j) + f_{\mathrm{D}_i}(j)\,.$$

$F_i(j)$ $(i = 1, \ldots, l + 1)$ are then sent to the data user (response). Here R_i and Z_i should be discarded at each request-response for information-theoretical security. And Z_i is added to ensure the uniformity of $F_i(j)$.

(3-5)

For each data block, the data user finds polynomial $F_i(x)$ *with a degree of two.*$F_i(0)$ *is the reconstructed block.*

(3-6)

The data user calculates the Message Authentication Code (MAC) from $F_1(0), \ldots, F_l(0)$ *as in the first phase. If* $F_{l+1}(0)$ *is equal to the calculated MAC, the data owner successfully reconstructs secret data D.*

In general, the number of share holders n and (expected) maximum number of corrupted share holders t, can be set arbitrarily provided that $n \geq 2t + 1$ is met ($k = 2t + 1$). Although the data user decodes the secret data D by using responses from $2t + 1$ of n servers, the responses do never leak any information about D if $P' \neq P$ (see next subsection for the details). The number of servers should be set considering the cost and risk of information leakage for each share holder. As for the related polynomial orders, see [19].

D. SECURITY CRITERIA

In the above settings, the same three kind of security criteria as those in [19] can be fulfilled, with the update of players, i.e., not only the data owner but also the data user, which was restated as follows for reader's convenience. (Security proof of them given in Supplementary Information of [19] is also redescribed in APPENDIX.)

(i) If t corrupted share holders jointly try to forge the reconstructed data by active attacks on the protocol, the data user can detect it with probability $(1 - l/q)$ if P is chosen randomly, or equivalently, the MAC can be forged with a probability of l/q,

(ii) The total information that t corrupted share holders can see in the protocol is independent from the data owner's (or the data user's) password P and stored secret data D, if the other share holders, data owner, and data user are honest.

(iii) Even if an attacker first corrupts t share holders and then participates in the data-reconstruction phase pretending to be a data end by utilizing the corrupted share holders, the total information that the attacker can obtain is zero, other than whether the guessed password P' is equal to the correct password P.

III. SIMULATED RESULT

We confirmed the normal operation of our protocol on an actual QKD network using an early version of our system and achieved throughputs of several kbps.

To improve the throughput, we revised the software that was originally used. The simulation results described below were obtained in a simulated environment, for simplicity, assuming that every QKD link accumulates a sufficient amount of keys for the data relay. The network simulator was connected to a secret decentralized network (called a quantum secure cloud) formed on the Tokyo QKD Network [27]. For the verification of its use on the actual network, the actual keys generated on the Tokyo QKD Network were also used for cryptographic transmission. Figure 3 shows the conceptual view of the data relay experiment corresponding to Fig.2. This system can be used multiple users.

We have implemented the following functions to improve security of this system during actual use.

➢ A key-relay route for data transmission between the sender and receiver of data by the QKDNC is determined. To clarify the correspondence between the trusted-node compromise and threshold assumption of secret sharing during a data relay, each trusted node is assumed to joint key relay on a single route, as shown in Figs. 1 and 3.

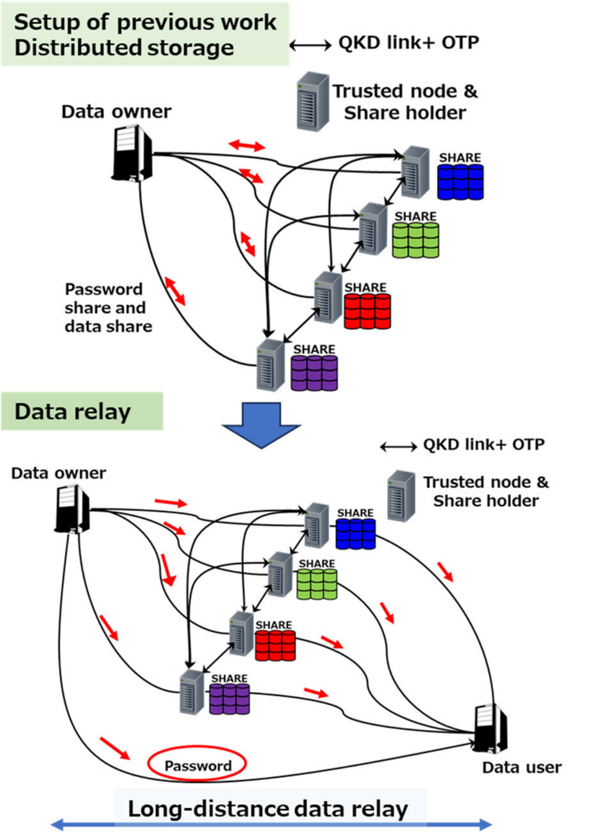


FIGURE 1. Conceptual configuration of information theoretically secure distributed storage and data relay.

➢ At the data user's terminal, the password and reconstructed data received are stored on a USB that is successfully authenticated through Wegmann–Carter authentication [28] using the terminal equipment. This makes information leakage difficult, even if the super user of the terminal server is a different person.

➢ Data from the USB were also encrypted. Therefore, decrypting the data is difficult, even if the USB is lost.

Figure 4 shows the Mersenne prime size dependence of the throughput of data registration, computation and communication among share holders, and the data relay and reconstruction phases for the cases of 1 MB, 10 MB, and 100 MB of data.

No significant effect was observed on the size of the Mersenne primes. In the previous study [19], the data blocks and number of communications depended on the size of the Mersenne prime, resulting in throughput degradation when the Mersenne prime was small. This time, the data blocks are transmitted in batches and the dependence on the size of the Mersenne primes is almost eliminated.

However, the fastest data size is 10 MB, which achieved more than twice the throughput of the case of 1 MB

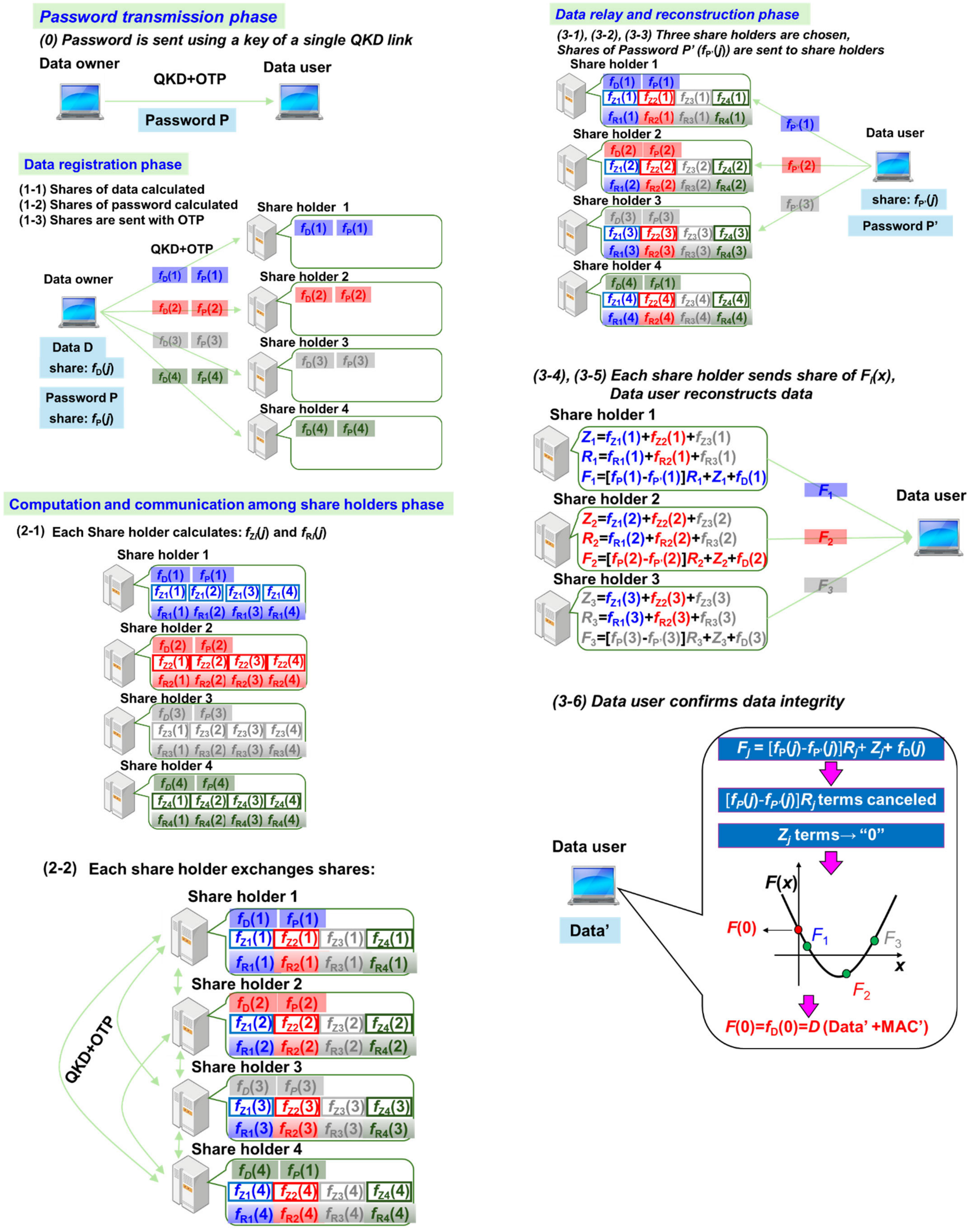

Password transmission phase
(0) Password is sent using a key of a single QKD link
Data owner
QKD+OTP
Data user
Password P
Data registration phase
(1-1) Shares of data calculated
(1-2) Shares of password calculated
(1-3) Shares are sent with OTP
QKD+OTP
Data owner
Data D
share: $f_D(j)$
Password P
share: $f_P(j)$
$f_D(1)$ $f_P(1)$
$f_D(2)$ $f_P(2)$
$f_D(3)$ $f_P(3)$
$f_D(4)$ $f_P(4)$
Share holder 1
Share holder 2
Share holder 3
Share holder 4
Computation and communication among share holders phase
(2-1) Each Share holder calculates: $f_{Zi}(j)$ and $f_{Ri}(j)$
$f_{Z1}(1)$ $f_{Z1}(2)$ $f_{Z1}(3)$ $f_{Z1}(4)$
$f_{R1}(1)$ $f_{R1}(2)$ $f_{R1}(3)$ $f_{R1}(4)$
$f_{Z2}(1)$ $f_{Z2}(2)$ $f_{Z2}(3)$ $f_{Z2}(4)$
$f_{R2}(1)$ $f_{R2}(2)$ $f_{R2}(3)$ $f_{R2}(4)$
$f_{Z3}(1)$ $f_{Z3}(2)$ $f_{Z3}(3)$ $f_{Z3}(4)$
$f_{R3}(1)$ $f_{R3}(2)$ $f_{R3}(3)$ $f_{R3}(4)$
$f_{Z4}(1)$ $f_{Z4}(2)$ $f_{Z4}(3)$ $f_{Z4}(4)$
$f_{R4}(1)$ $f_{R4}(2)$ $f_{R4}(3)$ $f_{R4}(4)$
(2-2) Each share holder exchanges shares:
QKD+OTP
$f_{Z1}(1)$ $f_{Z2}(1)$ $f_{Z3}(1)$ $f_{Z4}(1)$
$f_{R1}(1)$ $f_{R2}(1)$ $f_{R3}(1)$ $f_{R4}(1)$
Data relay and reconstruction phase
(3-1), (3-2), (3-3) Three share holders are chosen,
Shares of Password P' ($f_{P'}(j)$) are sent to share holders
Data user
share: $f_{P'}(j)$
Password P'
$f_{P'}(1)$
$f_{P'}(2)$
$f_{P'}(3)$
(3-4), (3-5) Each share holder sends share of $F_i(x)$,
Data user reconstructs data
$Z_1=f_{Z1}(1)+f_{Z2}(1)+f_{Z3}(1)$
$R_1=f_{R1}(1)+f_{R2}(1)+f_{R3}(1)$
$F_1=[f_P(1)-f_{P'}(1)]R_1+Z_1+f_D(1)$
$Z_2=f_{Z1}(2)+f_{Z2}(2)+f_{Z3}(2)$
$R_2=f_{R1}(2)+f_{R2}(2)+f_{R3}(2)$
$F_2=[f_P(2)-f_{P'}(2)]R_2+Z_2+f_D(2)$
$Z_3=f_{Z1}(3)+f_{Z2}(3)+f_{Z3}(3)$
$R_3=f_{R1}(3)+f_{R2}(3)+f_{R3}(3)$
$F_3=[f_P(3)-f_{P'}(3)]R_3+Z_3+f_D(3)$
F_1
F_2
F_3
(3-6) Data user confirms data integrity
Data'
$F_j = [f_P(j)-f_{P'}(j)]R_j+ Z_j+ f_D(j)$
$[f_P(j)-f_{P'}(j)]R_j$ terms canceled
Z_j terms→ "0"
$F(x)$
$F(0)$
x
$F(0)=f_D(0)=D$ (Data' +MAC')

FIGURE 2. Conceptual view of information-theoretically secure data-relay protocol based on password sharing scheme. Here, $f_D(j)$ denotes a series $\left(f_{D_1}(j), f_{D_2}(j), \cdots, f_{D_{l+1}}(j)\right)$; the same rule also applies to $f_{R_{j'}}(j)$, $f_{Z_{j'}}(j)$. For ease of reading, we denoted $f_{R_{j'}}(j)$, $f_{Z_{j'}}(j)$ as $f_{Rj'}(j)$, $f_{Zj'}(j)$.

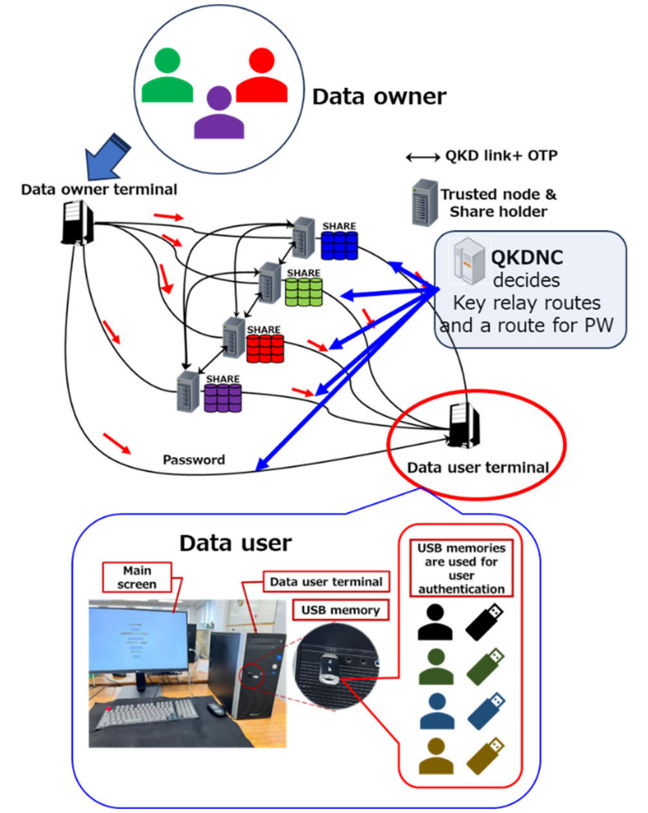


FIGURE 3. Conceptual configuration of the data relay system with multi-user compatibility. The picture with the speech bubble in the figure is a multi-user compatible terminal. By using USB memories, this terminal can support multi-users. Processors in this system are CPU 4 core with 16 GB RAM memory.

or 100 MB data size. The 1 MB case resulted in sparser packets, and the accumulation of data-independent processing such as splitting share data, which resulted in a lower throughput than the 10 MB case. When handling 100 MB of data, performance deteriorated significantly during computation and communication in the share holder phase. In this phase, each share holder sends shares of "0" and random number "R" to other three share holders. These shares have the same data size (100 MB) respectively. Thus, in total, 600 MB data are sent to other share holder servers. Moreover, each share holder server receives 600 MB data. This results in total of 1200 MB (9.6 Gbits) of process for sending and receiving during the computation and communication among share holders phase, which was approximately 10 times the theoretical limit of the network interface card (NIC). This is assumed to have caused communication congestion, resulting in throughput degradation.

Figure 5 shows the data-size dependence of the throughput using Mersenne prime 2^{44497}-1 in the data registration, computation and communication among share holders, and data relay and reconstruction phases. This figure also shows that the rate of increase in the processing time was higher when the file size increased from 10 to 100 MB than when it increased from 1 to 10 MB. This phenomenon can be observed when a large file size is used compared to the network throughput. In the future, the throughput is expected to be improved by increasing the performance of NICs and network devices.

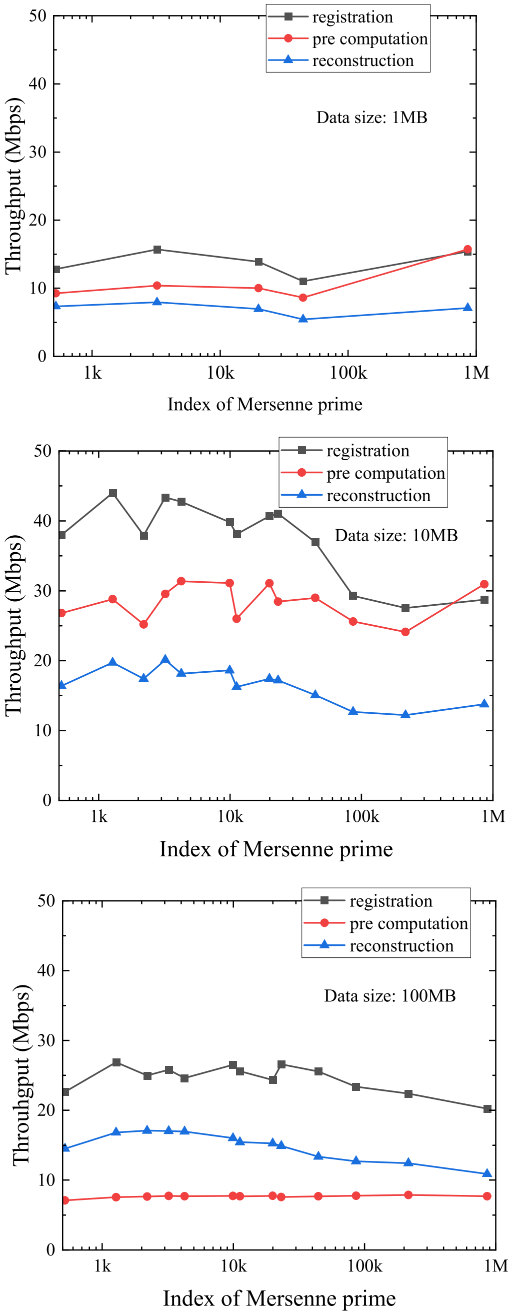


FIGURE 4. Throughput of our protocol as functions of the Mersenne prime size in data registration, computation and communication among share holders, and data relay and reconstruction phases for the case of 1 MB, 10 MB, and 100 MB data.

In these experiments, the OTP encryption [26] was not the cause of throughput degradation. In the OTP encryption/decryption process, we achieved a throughput of 2 Gbps or higher using a commercial high-performance server by optimizing the network processing acceleration application development kit (i.e., data plane development kit; DPDK) and

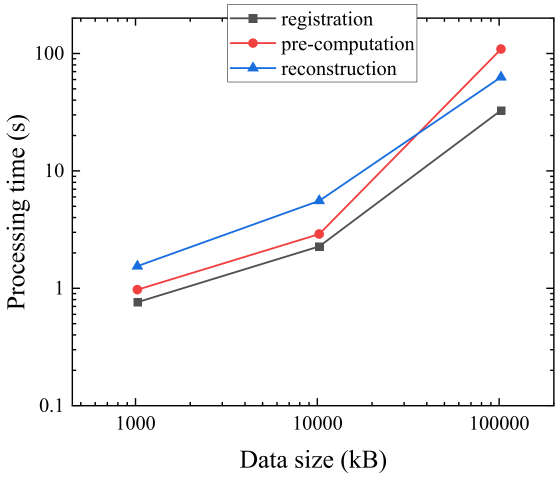


FIGURE 5. The data size dependence of throughput using Mersenne prime 2^{44497}-1 in data registration, computation and communication among share holders, and data relay and reconstruction phases.

a NIC that supports the DPDK. The delay time was less than 100 μs for the OTP encryption transmission over the 90 km Koganei-Otemachi-Koganei loopback.

To summarize the experimental results, using the Mersenne prime 2^{19937}-1, the throughputs of the data-registration phase, computation and communication among share holders, and data-reconstruction phase were 24.3 Mbps, 7.75 Mbps, and 15.2 Mbps for 100 MB of data, respectively. The total processing time for this data-relay protocol was 197 s for all phases. Our simulation equipment can be installed in the Tokyo QKD Network because it has a standard interface with the QKDN. Furthermore, we successfully demonstrated a key-acquisition function from the real QKDN.

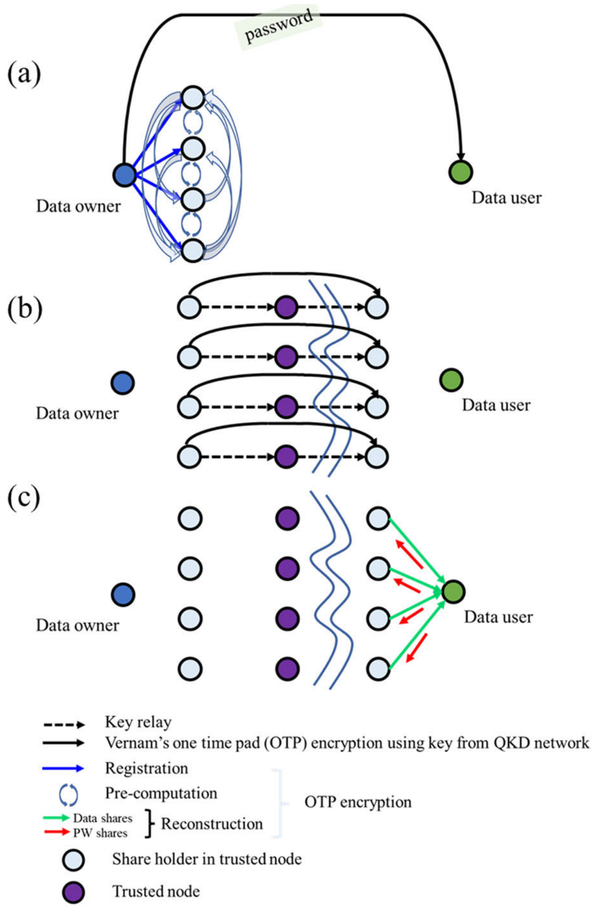


FIGURE 6. A conceptual view of secure data relay using our secret sharing protocol with multi trusted nodes key relay; (a) password transmission phase, data registration phase and computation and communication among share holders phase; (b) shares transfer by key relay though trusted nodes; (c) data reconstruction phase.

IV. LONG-DISTANCE DATA RELAY SCENARIO OF THIS PROTOCOL

The key-generation rate R of the BB84 type QKD link is a linear function of the channel transmittance η, and η is a function of exp(-αl) in which α is 0.2 dB/km with a normal single-mode fiber and l is the length of the fiber. In the simple model, the key-rate ratio of the same distance l with n link key relays and one link is ($1/n$)· exp(-$\alpha l/n$) to exp(-αl). For example, the key-generation rate at a distance of 100 km with a two-link key relay was more than five times higher than that with one link. Therefore, a key relay based on trusted nodes is efficient for large data transfer. In the simulation described in Section III, the share transfer was achieved using one relay node in each route; in principle, however, the number of key relay nodes is not limited. Instead, our protocol requires that one trusted node be controlled to participate in only one shared transmission route to minimize the impact on the compromise-threshold assumption.

As far as the password transmission is concerned, which is used for identity authentication and is the most important information for this protocol, it only requires a considerably smaller data-transfer size than the transmission of shares. Furthermore, the password must be transmitted without a key relay to avoid compromising the trusted nodes. Therefore, the password should be transmitted via OTP encryption using a key shared by the long-distance QKD of a direct link, such as twin-field QKD [29], [30] or a satellite-based QKD [31]. In such cases, key distribution may be performed at the level of several 100 km without going through a trusted node. Using such a long-distance QKD link, information-theoretically secure data relay and personal authentication may be achieved at the scale of QKD networks. Figure 6 shows a conceptual view of a secure data relay using our protocol with a multi trusted node key-relay.

If a real-time data relay is required, the throughput of the multiple key relays must also be considered. This is because our scheme requires at least the same number of routes as the threshold value for the secret-sharing protocol. The performance of this scheme was limited by the route with the lowest throughput. Therefore, to develop an effective approach, the key-relay route search function of the QKD network must be improved.

V. SUMMARY

We developed an information-theoretically secure data relay and authentication (identify verification) based on our secret-sharing protocol by prohibiting the participation of key relays in more than one route when selecting the route of the key relay. The throughput of the data-registration phase, computation and communication among share holders, and data-reconstruction phase were 24.3, 7.75, and 15.2 Mbps for 100 MB of data, respectively. However, if the data is divided into 10 MB units, throughput exceeding 10 Mbps can be achieved in all phases. This throughput is more than ten times higher than that of previous our works. These throughputs were similar to those of normal secret-sharing services that use Shamir's protocol. This implies that the proposed system can be used in real services. For example, human whole genome data is approximately 8-10 GB in size. By dividing the whole genomic data to 10 MB, it can be transferred within several hours with information-theoretical security. This scheme is based on our password-sharing protocol, in which information-theoretical secure authentication is achieved by applying a secret computation function for secret sharing. In other words, our data-relay scheme is a fusion of a QKDN and secure coding scheme that includes secret sharing. Such technology fusion can expand the areas in which quantum-communication technologies can play an active role in the communication infrastructure. The newly developed system also incorporates network control technology in accordance with ITU-T recommendations and can be directly applied to QKDNs for secure distributed data storage and long-distance relay. Moreover, our scheme can relax the security requirements for trusted nodes in QKDN, reduce the risk of information leakage when conducting confidential data transmission services, and contribute to lower costs when providing QKDN business.

In the future, it will be necessary to improve the central management functions of the QKDN. The introduction of a central management system is expected to optimize key relay routes, visualize the trade-off between security requirements and key consumption, and improve the efficiency of security management of each trusted node. In addition, the modularization of the software and implementation framework is expected to simplify system management.

APPENDIX

The security proof of our protocol was described in Supplementary Information of [19]. To facilitate understanding of this paper, the proof is redescribed in the appendix.

Sketch of security proof of the password-authenticated secret sharing

The scheme has the following three properties.

Theorem 1: If t corrupted storage servers try together to change the reconstructed data by deviating from the protocol, the data owner can detect it with probability of $(1 - l/q)$ if password P is randomly chosen.

(Proof) Manipulating 0's shares sent to honest servers in Computation and communication among share holders phase and the responses sent back to the data owner in Data Reconstruction phase, t corrupted storage servers make the data owner reconstruct forged data blocks $\tilde{F}_i \neq F_i(0)$. The probability that MAC of forged data blocks $(\tilde{F}_l, \ldots, \tilde{F}_1)$ equals to $\tilde{F}_{l+1}$ is l/q, because MAC is calculated by using an l-degree polynomial that has (at most) l solutions. This means that such malicious behavior can be detected with probability of $(1 - l/q)$.

Theorem 2: The total information which t corrupted storage servers can see in the protocol is independent from the data owner's password p and stored secret data D, if the other servers and the data owner follow the protocol.

(Proof) We consider an attacker who corrupts t servers. The information that the attacker can see in Registration phase is t shares of password P and secret data D, which are generated by using t-degree polynomials. Therefore, they are independent from P and D as in Shamir's SS. The information that the attacker can see in Computation and communication among share holders phase is t shares of random numbers and "0" computed by honest servers, which are clearly independent from P and D.

The information that the attacker can see in Data reconstruction phase is t shares of P.' Even if $P' = P$, the shares are independent from P and D.

Note that this situation does not change even if the corrupted servers send fake shares to honest servers.

Theorem 3: Even if an attacker first corrupts t of storage servers, then participates in Data reconstruction phase pretending to be a data owner by utilizing the corrupted servers, the total information which the attacker can obtain is no information other than whether the guessed password P' is equal to the correct password P or not.

(Proof) Here we describe the proof in the case where there is only one data block. The generalization to the case of multiple data blocks is straightforward.

We consider an attacker who corrupts at most t servers $C = \{c_1, \ldots, c_t\} \subseteq \{1, \ldots, n\}$ and tries to get some information on password P and/or secret data D by pretending the data owner in Data reconstruction phase. In Data reconstruction phase, the attacker chooses a set of $2t+1$ servers, L, in which all corrupted servers are included. Then, $\tilde{H} = \{1, \ldots, n\} \setminus C$ is the set of honest servers, $H = L \cap \tilde{H} = \{h_1, \ldots, h_{t+1}\}$ is the set of the honest servers that join the request-response process. The attacker can obtain all information in the corrupted servers and all information what those servers can observe in all phases. Furthermore, the attacker and the corrupted servers C can generate messages in arbitrary way and send them to honest servers $\tilde{H}$. Without loss of generality, we assume $c_1 < \ldots < c_t$ and $h_1 < \ldots < h_{t+1}$.

First, we list up all information the attacker views. In Registration phase, the attacker obtains the shares of P and D generated by the data owner using random polynomials f_{P} and f_{D} of degrees at most t and $2t$, respectively. In each Computation and communication among share holders phase, the attacker obtains the shares of a random number R_h and "0" generated by honest server h using random polynomials

f_{R_h} and f_{z_h} of degrees at most t and $2t$, respectively. In each Data reconstruction phase (3-4), the attacker obtains F_h as response which is computed by honest server h according to the scheme procedure. Thus, the information the attacker views through this attack is as follows:

$$\begin{aligned}
V_1 &= \{f_{\mathrm{P}}(c) \mid c \in C\}, \\
V_2 &= \{f_{\mathrm{D}}(c) \mid c \in C\}, \\
V_3 &= \left\{f_{\mathrm{R}_h}(c) \mid h \in H, c \in C\right\}, \\
V'_3 &= \left\{f_{\mathrm{R}_h}(c) \mid h \in \tilde{H} \setminus H, c \in C\right\}, \\
V_4 &= \left\{f_{0_h}(c) \mid h \in H, c \in C\right\}, \\
V'_4 &= \left\{f_{0_h}(c) \mid h \in \tilde{H} \setminus H, c \in C\right\}, \\
V_5 &= \{F_h \mid h \in H\}.
\end{aligned}$$

Clearly, V_1, V_2 themselves do not leak any information about password P and secret data D. Also, V'_3, V'_4 give no information to the attacker, because they are not used in Data reconstruction phase. On the other hand, V_3 and V_4 have the possibility to leak some additional information because they are related to the response V_5 through f_{R_h} and f_{z_h}. So, we consider (V_3, V_4, V_5).

Let $R_c^{(h)}$ and $Z_c^{(h)}$ be the values sent from corrupted server c to honest server h as a share of random number and "0", respectively, in Computation and communication among share holders phase. Let $P'^{(h)}$ be the value that the attacker, at the beginning of Data reconstruction phase, sends to honest server h as a request. Note that these values may not be determined from polynomials, but there exists a unique polynomial $f_{\mathrm{P}'}(x)$ of degree t which satisfies $f_{\mathrm{P}'}(h) = P'^{(h)}$ for all $h \in H$. Hereafter, we show that V_3, V_4, V_5 has no additional information, unless $P \neq f_{\mathrm{P}'}(0)$ holds.

Each F_h in V_5 is computed by honest server h as follows:

$$F_h = \left(f_{\mathrm{P}}(h) - P'^{(h)}\right)\left(\sum_{h' \in H} f_{\mathrm{R}_{h'}}(h) + \sum_{c \in C} R_c^{(h)}\right) + \sum_{h' \in H} f_{z_{h'}}(h) + \sum_{c \in C} Z_c^{(h)} + f_{\mathrm{D}}(h). \tag{A.1}$$

Defining

$$\begin{aligned}
\Delta_h &= f_{\mathrm{P}}(h) - P'^{(h)} = f_{\mathrm{P}}(h) - f_{\mathrm{P}'}(h), \\
f_{\mathrm{R}}(x) &= \sum_{h \in H} f_{\mathrm{R}_h}(x) = \sum_{i=0}^{t} \rho_i x^i, \\
f_{\mathrm{Z}}(x) &= \sum_{h \in H} f_{z_h}(x) = \sum_{i=1}^{2t} z_i x^i,
\end{aligned}$$

Eq. (A.1) is written as

$$F_h = \Delta_h\left(f_{\mathrm{R}}(h) + \sum_{c \in C} R_c^{(h)}\right) + f_{\mathrm{Z}}(h) + \sum_{c \in C} Z_c^{(h)} + f_{\mathrm{D}}(h).$$

Then, all values in V_3, V_4, V_5 are represented by the following linear equation:

$$\begin{pmatrix}
\sum_{h \in H} f_{\mathrm{R}_h}(c_1) \\
\vdots \\
\sum_{h \in H} f_{\mathrm{R}_h}(c_t) \\
F_{h_1} \\
\vdots \\
F_{h_{t+1}} \\
\sum_{h \in H} f_{z_h}(c_1) \\
\vdots \\
\sum_{h \in H} f_{z_h}(c_t)
\end{pmatrix}
= \begin{pmatrix}
0 \\
\vdots \\
0 \\
\Delta_{h_1} \sum_{c \in C} R_c^{(h_1)} + \sum_{c \in C} Z_c^{(h_1)} + f_{\mathrm{D}}(h_1) \\
\vdots \\
\Delta_{h_{t+1}} \sum_{c \in C} R_c^{(h_{t+1})} + \sum_{c \in C} Z_c^{(h_{t+1})} + f_{\mathrm{D}}(h_{t+1}) \\
0 \\
\vdots \\
0
\end{pmatrix}
+ M \begin{pmatrix}
\rho_0 \\
\vdots \\
\rho_t \\
z_1 \\
\vdots \\
z_{2t}
\end{pmatrix}, \tag{A.2}$$

where

$$M = \begin{pmatrix} A & 0 \\ E & K \\ 0 & B \end{pmatrix},$$

and

$$A = \begin{pmatrix} 1 & c_1 & c_1^2 & \cdots & c_1^t \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & c_t & c_t^2 & \cdots & c_t^t \end{pmatrix}, B = \begin{pmatrix} c_1 & c_1^2 & \cdots & c_1^{2t} \\ \vdots & \vdots & \ddots & \vdots \\ c_t & c_t^2 & \cdots & c_t^{2t} \end{pmatrix},$$

$$E = \begin{pmatrix} \Delta_{h_1} & \Delta_{h_1} h_1 & \Delta_{h_1} h_1^2 & \cdots & \Delta_{h_1} h_1^t \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \Delta_{h_{t+1}} & \Delta_{h_{t+1}} h_{t+1} & \Delta_{h_{t+1}} h_{t+1}^2 & \cdots & \Delta_{h_{t+1}} h_{t+1}^t \end{pmatrix},$$

$$K = \begin{pmatrix} h_1 & h_1^2 & \cdots & h_1^{2t} \\ \vdots & \vdots & \ddots & \vdots \\ h_{t+1} & h_{t+1}^2 & \cdots & h_{t+1}^{2t} \end{pmatrix}.$$

Because all values $(\rho_0, \ldots, \rho_t, z_1, \ldots, z_{2t})$ in the last term of Eq. (A.2) are chosen by the honest servers, they have uniform distribution. Thus, if the matrix M is nonsingular, then (V_3, V_4, V_5) as a whole has uniform distribution and is independent from $\Delta_h, f_{\mathrm{D}}, R_c^{(h)}, Z_c^{(h)}$, and the choice of C. The non- singularity of M is evaluated as follows.

Let E_i be the i-th row of the matrix E and K'_i be the matrix obtained by removing the i-th row from the matrix K. Then

$$\det M = \sum_{i=1}^{t+1} \left((-1)^{i-1} \det \begin{bmatrix} A \\ E_i \end{bmatrix} \cdot \det \begin{bmatrix} K'_i \\ B \end{bmatrix} \right), \det \begin{bmatrix} A \\ E_i \end{bmatrix}$$

$$= \Delta_{h_i} \det \begin{bmatrix} & A & \\ 1 \; h_i & \cdots & h_i^t \end{bmatrix},$$

$$= (-1)^t \, \Delta_{h_i} \left(\prod_{c \in C} (c - h_i) \right) \left(\prod_{\substack{c' > c \\ c, c' \in C}} (c' - c) \right),$$

and

$$\det \begin{bmatrix} K'_i \\ B \end{bmatrix} = \left(\prod_{h \in H \setminus \{h_i\}} h \right) \left(\prod_{c \in C} c \right) \left(\prod_{h \in H \setminus \{h_i\}} \left(\prod_{c \in C} (c - h) \right) \right)$$

$$\times \left(\prod_{\substack{c' > c \\ c, c' \in C}} (c' - c) \right) \left(\prod_{\substack{h' > h \\ h, h' \in H \setminus \{h_i\}}} (h' - h) \right).$$

By noting,

$$f_{\mathrm{P}}(0) - f_{\mathrm{P}'}(0)$$

$$= \sum_{h_i \in H} \Delta_{h_i} \left(\prod_{h \in H \setminus \{h_i\}} h \right) \left(\prod_{h \in H \setminus \{h_i\}} (h - h_i) \right)^{-1},$$

we obtain

$$\det M = (-1)^t \left(\prod_{c \in C} c \right) \left(\prod_{\substack{c' > c \\ c, c' \in C}} (c' - c) \right)^2$$

$$\times \left(\prod_{h \in H} \left(\prod_{c \in C} (c - h) \right) \right)$$

$$\times \left(\prod_{\substack{h' > h \\ h, h' \in H}} (h' - h) \right) (f_{\mathrm{P}}(0) - f_{\mathrm{P}'}(0)).$$

Hence, $\det M \neq 0$ holds if and only if $f_{\mathrm{P}}(0) = P \neq f_{\mathrm{P}'}(0)$. Note that polynomial $f_{\mathrm{P}'}(x)$ is determined by the values $f_{\mathrm{P}'}(h) = P'^{(h)}$ sent from the attacker to the honest servers as password's shares. So, $f_{\mathrm{P}'}(0)$ can be considered as a "guessed" password P'. Consequently, (V_3, V_4, V_5) has no additional information if the guessed password P' is not equal to the registered password P. This means that, no matter how the attacker acts co-operating with the corrupted servers, it cannot get additional information beyond the on-line dictionary attack.

In this attack model, the attacker is assumed to corrupt the t servers in L. If one thinks this assumption not realistic, we can slightly modify the scheme as follows. For every possible set L, Computation and communication among share holders phase is performed by the servers in L (rather than all servers). When L is specified by the data owner in Data reconstruction phase, servers use shares of random numbers and "0" for the specified L. The used shares must be discarded, however, shares for other set $L' (\neq L)$ need not to be discarded. The security of this modified protocol is proven in a similar way to the above proof. Note that if the number of servers n is $2t + 1$, we need not modify the scheme.

ACKNOWLEDGMENT

The authors would like to thank NEC, Toshiba, Gakushuin University, and NTT for their contribution to the operation of Tokyo QKD Network.

REFERENCES

[1] *IBM*. Accessed: Oct. 4, 2024. [Online]. Available: https://www.ibm.com/quantum/roadmap

[2] *AWS*. Accessed: Oct. 4, 2024. [Online]. Available: https://aws.amazon.com/jp/health/genomics/

[3] *Asahi*. Accessed: Oct. 4, 2024. [Online]. Available: https://www.asahi.com/articles/ASR6B570SR67UTFL00N.html

[4] *Freedom Lab*. Accessed: Jul. 15, 2022. [Online]. Available: https://www.freedomlab.com/posts/harvest-now-decrypt-later

[5] *NIST*. Accessed: Oct. 4, 2024. [Online]. Available: https://csrc.nist.gov/Projects/post-quantum-cryptography/round-4-submissions

[6] W. Castryck and T. Decru. *An Efficient Key Recovery Attack on SIDH*. Accessed: Oct. 4, 2024. [Online]. Available: https://eprint.iacr.org/2022/975.pdf

[7] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, Mar. 2002, doi: 10.1103/RevModPhys.74.145.

[8] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993, doi: 10.1109/18.256484.

[9] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, "Trojan-horse attacks on quantum-key-distribution systems," *Phys. Rev. A, Gen. Phys.*, vol. 73, no. 2, Feb. 2006, Art. no. 022320, doi: 10.1103/physreva.73.022320.

[10] M. Mehic, S. Rass, P. Fazio, and M. Voznak, *Quantum Key Distribution Networks: A Quality of Service Perspective*. New York, NY, USA: Springer, 2022, p. 13.

[11] C. H. Bennett and G. Brassard, "Quantum cryptography: Public-key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst. Signal Process.*, Bengaluru, India, 1984, pp. 175–179.

[12] J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, M. Fujiwara, M. Sasaki, and A. J. Shields, "Stability of high bit rate quantum key distribution on installed fiber," *Opt. Exp.*, vol. 20, no. 15, p. 16339, Jul. 2012, doi: 10.1364/oe.20.016339.

[13] K.-I. Yoshino, T. Ochi, M. Fujiwara, M. Sasaki, and A. Tajima, "Maintenance-free operation of WDM quantum key distribution system through a field fiber over 30 days," *Opt. Exp.*, vol. 21, no. 25, pp. 31395–31401, Dec. 2013, doi: 10.1364/oe.21.031395.

[14] *The University of Chicago*. Accessed: Aug. 13, 2024. [Online]. Available: https://news.uchicago.edu/story/chicago-quantum-network-argonne-pritzker-molecular-engineering-toshiba

[15] T.-Y. Chen et al., "Implementation of a 46-node quantum metropolitan area network," *NPJ Quantum Inf.*, vol. 7, no. 1, p. 134, Sep. 2021, doi: 10.1038/s41534-021-00474-3.

[16] *Quantum Key Distribution Networks: Quantum Key Distribution Networks—Key Management*, document ITU-T Y.3803, 2020.

[17] N. Lemons, B. Gelfand, N. Lawrence, A. Thresher, J. L. Tripp, W. P. Gammel, A. Nadiga, K. Meier, and R. Newell, "Extending quantum key distribution through proxy re-encryption," *J. Opt. Commun. Netw.*, vol. 15, no. 7, pp. 457–465, Jul. 2023, doi: 10.1364/JOCN.474487.

[18] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979, doi: 10.1145/359168.359176.

[19] M. Fujiwara, A. Waseda, R. Nojima, S. Moriai, W. Ogata, and M. Sasaki, "Unbreakable distributed storage with quantum key distribution network and password-authenticated secret sharing," *Sci. Rep.*, vol. 6, no. 1, p. 28988, Jul. 2016, doi: 10.1038/srep28988.

[20] M. Fujiwara, R. Nojima, T. Tsurumaru, S. Moriai, M. Takeoka, and M. Sasaki, "Long-term secure distributed storage using quantum key distribution network with third-party verification," *IEEE Trans. Quantum Eng.*, vol. 3, pp. 1–11, 2022, doi: 10.1109/TQE.2021.3135077.

[21] M. Fujiwara, H. Hashimoto, M. Kujiraoka, Y. Tanizawa, Y. Ishida, M. Sasaki, and M. Nagasaki, "Secure secondary utilization system of genomic data using quantum secure cloud," *Sci. Rep.*, vol. 12, Nov. 2022, Art. no. 18530, doi: 10.1038/s41598-022-22804-x.

[22] L.-J. Wang, K.-Y. Zhang, J.-Y. Wang, J. Cheng, Y.-H. Yang, S.-B. Tang, D. Yan, Y.-L. Tang, Z. Liu, Y. Yu, Q. Zhang, and J.-W. Pan, "Experimental authentication of quantum key distribution with post-quantum cryptography," *NPJ Quantum Inf.*, vol. 7, no. 1, May 2021, Art. no. 67, doi: 10.1038/s41534-021-00400-7.

[23] Y. Luo, H.-K. Mao, Q. Li, and N. Chen, "An information-theoretic secure group authentication scheme for quantum key distribution networks," *IEEE Trans. Commun.*, vol. 71, no. 9, pp. 5420–5431, Sep. 2023, doi: 10.1109/TCOMM.2023.3280561.

[24] Y. Luo, Q. Li, and H.-K. Mao, "Distributed information-theoretical secure protocols for quantum key distribution networks against malicious nodes," 2023, *arXiv:2302.07688*.

[25] *Quantum Key Distribution Network: Functional Architecture*, document ITU-T Y3802, 2020.

[26] 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, doi: 10.1109/T-AIEE.1926.5061224.

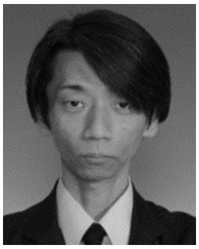
[27] M. Sasaki et al., "Field test of quantum key distribution in the Tokyo QKD network," *Opt. Exp.*, vol. 19, no. 11, pp. 10387–10409, May 2011, doi: 10.1364/oe.19.010387.

[28] M. N. Wegman and J. L. Carter, "New hash functions and their use in authentication and set equality," *J. Comput. Syst. Sci.*, vol. 22, no. 3, pp. 265–279, Jun. 1981, doi: 10.1016/0022-0000(81)90033-7.

[29] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, no. 7705, pp. 400–403, May 2018, doi: 10.1038/s41586-018-0066-6.

[30] Y. Liu, W.-J. Zhang, C. Jiang, J.-P. Chen, C. Zhang, W.-X. Pan, D. Ma, H. Dong, J.-M. Xiong, C.-J. Zhang, H. Li, R.-C. Wang, J. Wu, T.-Y. Chen, L. You, X.-B. Wang, Q. Zhang, and J.-W. Pan, "Experimental twin-field quantum key distribution over 1000 km fiber distance," *Phys. Rev. Lett.*, vol. 130, no. 21, May 2023, Art. no. 210801, doi: 10.1103/physrevlett.130.210801.

[31] J. Yin, Y. Cao, Y. H. Li, S. K. Liao, L. Zhang, J. G. Ren, W. Q. Cai, W. Y. Liu, B. Li, H. Dai, and G. B. Li, "Satellite-based entanglement distribution over 1200 kilometers," *Science*, vol. 356, no. 6343, pp. 1140–1144, Jun. 2017, doi: 10.1126/science.aan3211.



MIKIO FUJIWARA received the B.S. and M.S. degrees in electrical engineering and the Ph.D. degree in physics from Nagoya University, Nagoya, Japan, in 1990, 1992, and 2002, respectively.

He has been involved in research and development activities at NICT (previously called CRL, Ministry of Posts and Telecommunications of Japan), since 1992. His research interests include quantum key distribution and QKD network application.

GO KATO was born in Japan, in 1976. He received the B.S., M.S., and Ph.D. degrees in science from The University of Tokyo, Tokyo, Japan, in 1999, 2001, and 2004, respectively.

In 2004, he joined the NTT Communication Science Laboratories and has been involved in the theoretical investigation of quantum information. In 2022, he moved to the National Institute of Information and Communication Technology, Tokyo. His research interests include emerging mathematical structures in the field of quantum information. He is a member of the Physical Society of Japan.

MASAHIDE SASAKI received the B.S., M.S., and Ph.D. degrees in physics from Tohoku University, Japan, in 1986, 1988, and 1992, respectively. From 1992 to 1996, he worked on the development of semiconductor devices with Nippon-Kokan Company (currently JFE Holdings). In 1996, he joined the Communications Research Laboratory, Ministry of Posts and Telecommunications (since 2004, NICT). His research interests include quantum optics, quantum communication, and quantum cryptography. He is a NICT Fellow.