Park et al. *EPJ Quantum Technology* (2023) 10:48
https://doi.org/10.1140/epjqt/s40507-023-00205-x

EPJ Quantum Technology
a SpringerOpen Journal

RESEARCH Open Access

Mutual entity authentication of quantum key distribution network system using authentication qubits

Hojoong Park[1†], Byung Kwon Park[2,3,4†], Min Ki Woo[2], Min-Sung Kang[5], Ji-Woong Choi[5], Ju-Sung Kang[1], Yongjin Yeom[1] and Sang-Wook Han[2,3*]

*Correspondence: swhan@kist.re.kr
[2]Center for Quantum Information, Korea Institute of Science and Technology, Seoul, South Korea
[3]Division of Nano and Information Technology, Korea Institute of Science and Technology School, Korea University of Science and Technology, Seoul, South Korea
Full list of author information is available at the end of the article
[†]Equal contributors

Abstract

Entity authentication is crucial for ensuring secure quantum communication as it helps confirm the identity of participants before transmitting any confidential information. We propose a practical entity authentication protocol for quantum key distribution (QKD) network systems that utilizes authentication qubits. In this protocol, authentication qubits that are encoded with pre-shared information are generated and exchanged to verify the legitimacy of each entity. By using the authentication qubit, participants can identify each other with enhanced security level through the quantum channel. The proposed protocol can be easily integrated with existing QKD systems without the need for additional hardware. In this study, we demonstrated the efficacy of the proposed scheme using a 1xN QKD network system and verified its stable operation over a deployed fiber network. Additionally, a security analysis of the proposed entity authentication protocol and architecture is provided.

Keywords: Entity authentication; Quantum key distribution network; Deterministic random bit generation

1 Introduction

Quantum key distribution (QKD) ensures secure communication between two remote parties, Alice and Bob, based on quantum phenomena [1–3]. It has already been commercialized as one of the most mature quantum technologies. Since its initial proposal [1], QKD has undergone significant development, including improvements in communication distance [4–7], achieving higher key rates [8, 9], exploring network architectures [10–21], and performing security analyses [22–26]. Nonetheless, several security issues must still be addressed to ensure secure communication, such as key, message, and entity authentication. Specifically, entity authentication is the starting point of secure communication and a process to verify the legitimacy of the communicating parties before sending important secure messages over communication channels. Therefore, it must be conducted before sending any sensitive secure information [27–35]. Traditionally, authentication has been conducted at the concluding stages of the post-processing procedure using authentication tags. In recent times, entity authentication in QKD systems incorporating modern

cryptographic techniques such as post-quantum cryptography based on pre-shared information transmitted through the public channel within the all-pass QKD network [36], has evolved. The QKD uses both a public channel and a quantum channel. However, there have been no reports of entity authentication using the quantum channel due to technical difficulties.

Although there has been no research on entity authentication in QKD through the quantum channel, research on quantum authentication itself continues to be published. The quantum authentication of entities is typically verified by an authorized party, referred to as an arbitrator. They usually use entangled states to confirm the identities of others, which is a fragile technology to maintain and measure the entangled states. Additionally, even under network conditions, the arbitrator uses Greenberger–Horne–Zeilinger (GHZ) states to identify multiple participants [37], which can be challenging given the current technology.

To establish a more practical quantum authentication, a single photon measurement has been proposed and applied in some studies [38–40]. In these methods, legitimate participants share information for identification before communication, and the sender who needs to identify themselves sends photons encoded with pre-shared information. These photons, called authentication qubits, are measured by the identifier. The sender is granted approval if the measurements and pre-shared information are found to match. This approach can be easily implemented in QKD systems without the need to maintain entangled states and perform somewhat tricky experiment such as Bell measurement. However, the use of a single photon still makes the system vulnerable to losses in the quantum channel, requiring the sender to prepare a large number of authentication qubits for reliable identification. This, in turn, increases the consumption of pre-shared information.

In this work, we present a mutual entity authentication of QKD network system through quantum channel. It can be implemented using the conventional QKD system based on BB84 protocol without the need for additional hardware. Our scheme can mutually authenticate each other at the end of the BB84 protocol including both the classical and quantum channels that were used. To mitigate the burden on pre-shared information, we leverage the deterministic random bit generation (DRBG) technique to produce a large quantity of authentication qubits efficiently.

We successfully implemented the authentication system within a 1xN QKD network operating in a real-world environment. This star-type topology is essential for organizing extensive metropolitan QKD networks for end-users. Our authentication scheme was effectively demonstrated, consistently maintaining stable system performance, including a low quantum bit error rate (QBER) for the authentication qubits, for a duration exceeding 40 hours.

The remainder of this paper is organized as follows: In Sect. 2, we explain the entity authentication protocol and the QKD network architecture with the proposed entity authentication scheme. In Sects. 3 and 4, we describe the security analysis and the experimental results of the authentication system on the deployed fiber network, respectively. Finally, in Sect. 5, we summarize and conclude our work.

2 Proposed authentication scheme

2.1 Entity authentication protocol

The overall sequence of the proposed entity authentication protocol is as follows. At first, two entities generate the authentication information from the pre-shared secret informa-

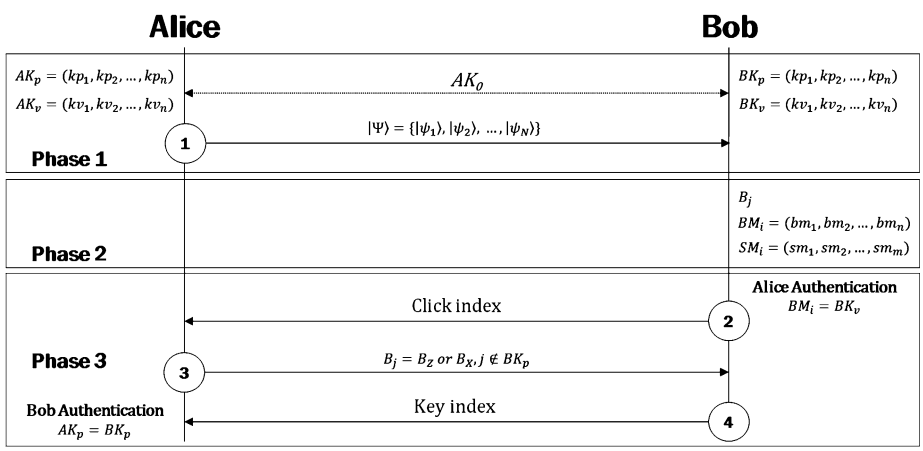

Figure 1 Entity authentication scheme with BB84 protocol for QKD system

tion. The output sequence is then transformed into quantum states. Next, the quantum states are included in the qubit stream and transmitted through the quantum channel. Finally, the two entities authenticate each other based on a comparison of pre-shared information and information transmitted in quantum states. Before describing the detailed protocol, we define two terminologies, an authentication qubit and a signal qubit, to clarify the protocol; the authentication qubit is used for authentication, and the signal qubit is used for key generation.

Figure 1 describes the entire protocol, which integrates the BB84 protocol and the proposed entity authentication method. In the preparation phase (Phase 1), Alice and Bob share a finite size of secret information AK_0. The pre-shared secret information AK_0 and Δt are utilized as input data of the DRBG to generate authentication qubits. It should be noted that Δt is time-synchronization information of each QKD device and gives a freshness to the protocol. In particular, if attackers block the quantum channel and the authentication protocol is performed again, Alice and bob share $\Delta t'$, which is different from Δt. Then, the two entities share distinct authentication qubits due to the characteristic of DRBG. Thus, it is difficult for attackers to predict the pre-shared secret AK_0.

In addition, a cryptographically secure random bit generator should be adopted as DRBG to ensure the security strength of the authentication protocol from the viewpoint of the cryptographic module validation program (CMVP) [41–43]. It is recommended that in the CMVP, the random bits used for cryptographic protocols can be generated from the cryptographically secure random bit generator [44–46]. The cryptographically secure random bit generator involves two steps: a non-deterministic random bit generator known as a true random number generator (TRNG) step and a DRBG step. The non-deterministic random bit generator outputs a seed used as the input value of the DRBG in the first step, and then, the cryptographically secure random bit sequence is finally generated from the DRBG using the seed as input data. Because the final output is processed by the vetted cryptographic algorithm in the DRBG step, it can be protected against vulnerabilities such as the aging effect [47], changing environments [48], and various attacks [49–51] on the TRNG, as well.

$DRBG(AK_0, \Delta t) = \{R_1, R_2, \ldots, R_n\}$ denotes authentication information generated by DRBG, where n is the total number of authentication qubits. R_i is used to derive i-th

authentication qubit and is concatenated by p_i and kv_i, where p_i denotes an interval of i-th authentication qubit and $(i-1)$-th authentication qubit, and kv_i is the value which determines the quantum state. Let d be a maximum interval between adjacent authentication qubits and Alice generates the qubit stream, the length N. Let AK_p denote a set of authentication qubit position inserted in the qubit stream, then $AK_p = \{kp_1, kp_2, \ldots, kp_n\}$ is represented as follows:

$$kp_i = \begin{cases} p_1 \mod d, & i = 1, \\ 1 + kp_{i-1} + (p_i \mod d), & i \leq n. \end{cases}$$

Let AK_v denote a set of the encoding for authentication qubit; AK_v is represented as $AK_v = \{kv_1, kv_2, \ldots, kv_n\}$ where $kv_i \in \{00, 01, 10, 11\}$. Alice generates the quantum state $|AQ_{kp_i}\rangle$ for authentication as follows:

$$|AQ_{kp_i}\rangle = \begin{cases} |0\rangle, & kv_i = 00, \\ |1\rangle, & kv_i = 01, \\ |+\rangle, & kv_i = 10, |-\rangle, kv_i = 11, \end{cases}$$

where $|+\rangle$. denotes as $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle$. denotes as $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Alice transmits the qubit stream to Bob, and each transmitted quantum state is as follows:

$$|\psi_j\rangle = \begin{cases} |S_j\rangle, & j \notin AK_p, \\ |AQ_{j=kp_i}\rangle, & j \in AK_p. \end{cases}$$

Let N be the total number of signal qubits. For $1 \leq j \leq N$, $|S_j\rangle$. is the j-th signal qubit to distribute Alice and Bob the secret key in the QKD system and is represented as $|S_j\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Alice transmits the authentication qubit $|AQ_{kp_i}\rangle$ inserted in the signal qubit stream depending on kp_i to Bob.

In the measurement phase (Phase 2) depicted in Fig. 1, Bob measures $|\Psi\rangle = \{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_N\rangle\}$ transmitted by Alice. Let BK_p denote a set of authentication qubit position and BK_v denote a set of the encoding information of authentication qubit from Bob. Because Bob has the same pre-shared secret information AK_0, time-synchronization information Δt, and the DRBG as Alice, Bob is able to generate the same authentication information as Alice's information, which is described as $BK_p = \{kp_1, kp_2, \ldots, kp_n\}$ and $BK_v = \{kv_1, kv_2, \ldots, kv_n\}$. If the measurement basis of Bob is denoted as $B = \{b_1, b_2, \ldots, b_N\}$, the j–th basis is generated as follows:

$$b_j = \begin{cases} B_Z \text{ or } B_X, & j \notin BK_p, \\ B_{j=kp_i}, & j \in BK_p, \end{cases}$$

$$\text{where } B_{j=kp_i} = \begin{cases} B_Z, & kv_i = 00 \text{ or } 01, \\ B_X, & kv_i = 10 \text{ or } 11, \end{cases} \quad \text{and}$$

B_Z is the $\{|0\rangle, |1\rangle\}$ basis and B_X is $\{|+, |-\rangle\}$ basis.

The measurement phase is terminated after acquiring the authentication qubits, BM, and the signal qubits, SM, using the measurement basis B. It should be noted that BM and SM are the set of the measurement result $j \in BK_p$ and $j \notin BK_p$, respectively.

In authentication phase (Phase 3), Bob could identify Alice by comparing the measurement result, $BM = (bm_1, bm_2, \ldots, bm_n)$ with the output of the DRBG, $BK_v = (kv_1, kv_2, \ldots, kv_n)$. If the measurement basis $B_{kp_i} = B_Z$ is used to measure the authentication qubit, kv_i is 00 or 01. Then, Bob verifies the fact that the least significant bit of kv_i is equal to bm_i. The measurement basis $B_{kp_i} = B_X$ is applied in the same method as before.

By verification in Phase 3, Bob can authenticate a legitimate entity with equal pre-shared secret information AK_0 and time-synchronization information Δt. In addition, the proposed protocol is conducted by considering QBER, which is the error rate in transmitting authentication qubits. Subsequently, Bob transmits the click indices to Alice, then Alice sends $b_{j \notin AK_p}$ which is the basis of the signal qubit among the click indices. Because Bob inspects the modification of authentication qubits through the output of DRBG with pre-shared information, he does not need to provide the basis of authentication qubit, $b_{j \in AK_p}$. Thus, indices used as the key can be sent to Alice with the basis of the signal qubit. In this process, Bob is surely authenticated by Alice because it indicates $AK_p = BK_p$ to inform the indices used as the sifted key by excluding the indices of the authentication qubit AK_p only with the basis of signal qubits. In other words, if Alice and Bob have the identical output sequence of DRBG, it can be considered that Alice has the same pre-shared information as Bob's information.

In summary, the entity authentication protocol can be performed by integrating the traditional QKD based on the BB84 protocol without the need for additional devices or channels, and it is composed of three phases, as shown in Protocol 1. Because Alice and Bob have the same input data AK_0 and Δt as pre-shared secret information, they can generate the same authentication qubit from the DRBG. Therefore, upon successful completion of the authentication protocol, Alice and Bob can simultaneously conduct quantum key distribution and mutual authentication. Furthermore, the QKD device integrated authentication protocol does not cause significant delays in addition to the time required to proceed with a typical QKD protocol, and in the 1:N QKD network system, generally, the time taken to complete the authentication increases linearly as the number of users increases.

Protocol 1 (Entity authentication protocol)

Input: $AK_0, \Delta t$

Output: Success or failure

1. *Preparation phase*
   - 1-1. Alice and Bob generate authentication information using DRBG with $AK_0, \Delta t$.
   - 1-2. Alice and Bob determine a set of authentication qubit position AK_p and BK_p, and a set of the encoding for authentication qubit, AK_v and BK_v, respectively.
   - 1-3. Alice generates a qubit stream $|\Psi\rangle$.
   - 1-4. Alice transmits Bob the authentication qubit inserted in the signal qubit stream $|\Psi\rangle$.
2. *Measurement phase*
   - 2-1. Bob generates a set of the measurement basis $B = \{b_1, b_2, \ldots, b_N\}$.
   - 2-2. Bob measures the transmitted qubit stream $|\Psi\rangle$ using the basis B, and then acquires the authentication qubits, BM, and the signal qubits, SM.

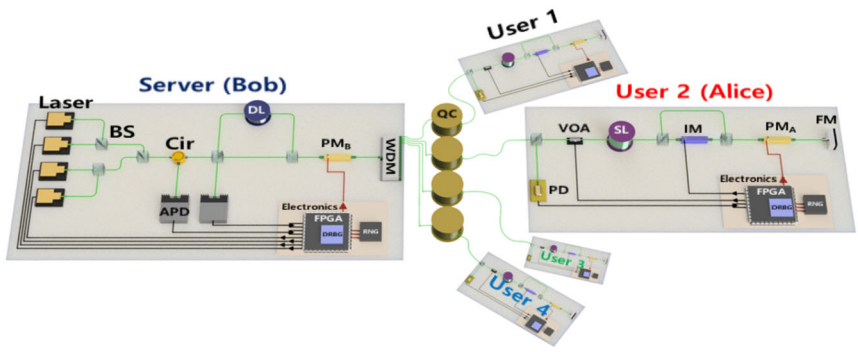

Figure 2 1x4 QKD network system setup for multi-user entity authentication. BS: beam splitter, Cir: circulator, APD: avalanche photo diode, DL: delay line, PBS: polarization beam splitter, PM: phase modulator, WDM: wavelength division multiplexing, QC: quantum channel, PD: photo diode, VOA: variable optical attenuator, SL: storage line, IM: intensity modulator, FM: Faraday mirror, FPGA: field programmable gate array

3. *Authentication phase*
   3-1. Bob verifies Alice's legitimacy by checking whether $BM = BK_v$ or not.
   If $BM \neq BK_v$, then Bob returns failure.
   Else, Bob succeeds to verify Alice, and then transmits the click indices to Alice.
   3-2. Alice sends $b_{j \notin AK_p}$, the basis of the signal qubit among the click indices, to Bob.
   3-3. Bob sends the key indices to Alice.
   3-4. Alice verifies Bob's legitimacy by checking whether $AK_P = BK_P$ or not. If $AK_p \neq BK_p$, then Alice returns failure. Else, Alice succeeds to verify Bob, and then returns success.

2.2 Quantum key distribution network system with entity authentication protocol

Figure 2 shows an entity authentication applicable up to 64 users on the QKD network system setup. The QKD network is based on the plug and play architecture [52–54]. However, it is worth noting that our authentication scheme is not limited to plug and play QKD systems; it can also be applied to one-way QKD systems utilizing the BB84 protocol. The server, Bob, can distribute the secure key to each user, Alice, using wavelength-division multiplexing (WDM). The server used four lasers with different wavelengths to send the users weak coherent light signals. The light signals are transmitted through the quantum channel (QC) and returned by the Faraday mirror (FM) on the user side. The light is attenuated to single photon level by the variable optical attenuator (VOA). The decoy pulse against the photon number splitting attack is generated using an intensity modulator (IM) and two additional polarization beam splitters (PBSs), which is required due to the polarization dependence of the IM. The photon is encoded at the phase modulator (PM_A) and returns to the server. The server chooses the measurement basis of the quantum signal using the phase modulator (PM_B), and the arriving photon interferes at the BS of the interferometer. The photons from four users are organized using time-division multiplexing (TDM) and detected by a pair of avalanche photodiodes (APDs).

For mutual entity authentication between the server and user, the DRBGs were implemented on both sides of an FPGA. The outputs of the DRBG were generated by seeding pre-shared information. At the user side, if $j \in AK_p$, the photon is modulated with AK_v

based on the output of the DRBG. If $j \notin AK_p$, the photon is randomly modulated with $|S_j\rangle$. using a quantum random number generator (QRNG). Further, the server chooses the measurement basis with B_{kp_i} from the output of the DRBG in the case of $j \in BK_p$. In the other case for $j \notin BK_p$, the server chooses a random basis (B_Z or B_X) for measuring the photon. According to the prepared quantum states and measurement basis, the photons interfere at the BS, which causes the detection signals of the APDs. The server compares the measurement results, $BM = \{bm_1, bm_2, \ldots, bm_n\}$, and a part of the DRBG output, $BK_v = \{kv_1, kv_2, \ldots, kv_n\}$, to identify the user. Then, based on the procedure of the protocol, the user can also verify the server is a legitimate entity or not.

3 Security analysis

3.1 Security analysis for authentication information quantity

The proposed mutual entity authentication protocol is performed to validate legitimate entities by pre-shared secret information and the deterministic property of DRBG. In this section, we analyze the security strength of the proposed authentication protocol. The security of our authentication protocol is analyzed from three perspectives; the number of single authentication qubits securely transmitted through the quantum channel, the impersonation attack in this authentication protocol, and the refresh period for managing the authentication protocol securely. In addition, based on the security analysis, we present the security lower bound of the authentication protocol.

The authentication protocol has a structure that determines a legitimate entity when the number of authentication qubits transmitted through the quantum channel is satisfied over the lower bound. The transmission and detection efficiency are considered to analyze the authentication protocol, and it has been well theoretically studied until now [55–58].

Let t_{AB} be the channel transmittance, η_{Bob} be the component losses of Bob's side, and η_D be the detector efficiency. Then, overall transmission efficiency r is denoted as follows:

$$r = t_{AB} \cdot \eta_{\text{Bob}} \cdot \eta_D. \tag{1}$$

It should be noted that if t_{AB} is denoted as loss coefficient α dB/km per $l$km, we can express t_{AB} as $t_{AB} = 10^{-\alpha l/10}$. If η_{Bob} is denoted as βdB, we can state η_{Bob} as $\eta_{\text{Bob}} = 10^{-\beta/10}$. Because the distribution of the transmitted photon follows a Poisson distribution, the overall gain Q_μ is denoted as follows:

$$Q_\mu = \sum_{i=0}^{\infty} Y_i \frac{\mu^i}{i!} e^{-\mu} = Y_0 + 1 - e^{-\mu \cdot r}. \tag{2}$$

Let i be a non-negative integer, Y_i be the yield of an i-photon state, μ be the expected photon numbers transmitted by Alice, and e_{detector} be the error probability in the detector. Then, the overall QBER is calculated as follows:

$$E_\mu Q_\mu = \sum_{i=0}^{\infty} e_i Y_i \frac{\mu^i}{i!} e^{-\mu} = e_0 Y_0 + e_{\text{detector}}\left(1 - e^{-\mu \cdot r}\right), \tag{3}$$

where the error rate of i-photon state, e_i, is calculated as $e_i = \frac{e_0 Y_0 + r_i \cdot e_{\text{detector}}}{Y_i}$ and the transmission rate of i-photon state, r_i, is calculated as $r_i = 1 - (1 - r)^i$. The authentication qubit

is not secure where the multi-photon is detected, and it is valid only when a single authentication qubit is detected by Bob. Thus, Q_1 is derived through the decoy protocol [58]. Let v_1 be the expected photon numbers of the weak decoy state. When the two-decoy state with the vacuum decoy state added, the lower bound of Q_1 is calculated as follows:

$$Q_1^{L,\nu_1} = \frac{\mu^2 e^{-\mu}}{\mu\nu_1 - \nu_1^2}\left(Q_{\nu_1}e^{\nu_1} - Q_\mu e^\mu \frac{\nu_1^2}{\mu^2} - \frac{\mu^2 - \nu_1^2}{\mu^2}Y_0\right). \tag{4}$$

Similarly, e_1^{U,ν_1}, the upper bound of e_1, is calculated as follows:

$$e_1 \le e_1^{U,\nu_1} = \frac{E_{\nu_1}Q_{\nu_1}e^{\nu_1} - e_0 Y_0}{Y_1^{L,\nu_1}\nu_1}. \tag{5}$$

As a result, the lower bound of detection probability of a secure authentication qubit, R_{AQ}, is calculated by multiplying Q_1^{L,ν_1} and $1 - H(e_1^{U,\nu_1})$, where Q_1^{L,ν_1} is the lower bound for a detection rate of a single authentication qubit and $1 - H(e_1^{U,\nu_1})$ means the information quantity except for information loss by error. That is,

$$R_{AQ} \ge Q_1^{L,\nu_1}\left[1 - H\left(e_1^{U,\nu_1}\right)\right]. \tag{6}$$

Note that $H(x)$ is the binary Shannon information function, denoted as $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$.

Let N be the total number of qubits used for the authentication protocol and d be the maximum interval at which authentication qubits are inserted. Because the authentication qubit is inserted at an average $\frac{(d+1)}{2}$ bits interval, the lower bound of the authentication qubits securely transmitted is calculated as follows:

$$N_{AQ} = \frac{2N \cdot R_{AQ}}{d+1}. \tag{7}$$

Because QBER, E_μ, exists in a real QKD system, the number of authentication qubits transmitted to Bob shall be calculated in consideration of E_μ. Let X be a random variable on the number of authentication qubits successfully transmitted through the quantum channel with QBER E_μ. The transmission of the authentication qubit inserted on the qubit stream is an independent trial. Thus, considering the transmission error rate E_μ, the probability that the authentication qubit is successfully transmitted can be $1 - E_\mu$. In addition, let n denote a $n = \lfloor N_{AQ} \rfloor$, then the transmitted authentication qubit follows the binomial distribution with the probability $1 - E_\mu$ and n independent trials, $X \sim B(n, 1 - E_\mu)$. Because n is large enough in the QKD system, X is approximated by the normal distribution with the expectation $n \cdot (1 - E_\mu)$ and the variance $n \cdot (E_\mu - E_\mu^2)$. In other words, we can write as follows:

$$X \sim B(n, 1 - E_\mu) \approx N\left(n \cdot (1 - E_\mu), n \cdot \left(E_\mu - E_\mu^2\right)\right). \tag{8}$$

The lower bound for the number of the transmitted authentication qubits is calculated using the approximation to a normal distribution and the confidence interval, which is one of the interval estimation methods. Hence, the lower bound of the authentication qubit

transmitted by Alice, D, is derived as follows:

$$D \geq n \cdot (1 - E_\mu) - z_{\frac{\alpha}{2}} \sqrt{n \cdot \left(E_\mu - E_\mu^2\right)}. \tag{9}$$

where $z_{\frac{\alpha}{2}}$ is the value that satisfies the formula $\int_{-z_{\frac{\alpha}{2}}}^{z_{\frac{\alpha}{2}}} \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}}\, dx = 1 - \alpha$, which means a significance level for $0 < \alpha < 1$ Consequently, this lower bound D means the security strength of the proposed authentication protocol.

3.2 Security analysis for the authentication protocol

To show that the proposed authentication protocol is secure, we analyze the protocol from the viewpoint of the completeness property and the soundness property [59]; the completeness property denotes that if an honest prover and an honest verifier are given in the authentication protocol, the protocol succeeds with high probability. On the other hand, the soundness property denotes that if there is a dishonest prover, the impersonating probability is negligible.

In the proposed protocol, DRBG is utilized to generate the same authentication information for Alice and Bob. Because the output of DRBG is completely different even if only one bit of the input is altered, the authentication protocol always succeeds when the legitimate entity has the pre-shared secret information. This shows that our authentication protocol satisfies the completeness property.

Next, we analyze our authentication protocol from the viewpoint of the impersonation attack to prove its soundness. The security analysis of the attack is divided into two cases: Eve impersonates Alice in the protocol, and Eve impersonates Bob in the protocol to succeed the authentication protocol, where Eve represents the impersonation attacker. In addition, the analysis is assumed that Eve has succeeded in predicting the time-synchronization information Δt of the QKD system.

Figure 3(a) shows the case where Eve pretends to Alice. Based on the assumption, Eve obtained the time-synchronization information Δt. In order for Eve to perform the authentication protocol successfully by impersonated as Alice, Eve randomly generates R_E imitating the pre-shared secret information AK_0 in the protocol. Then, Eve inputs Δt and R_E into DRBG to make authentication qubits as follows: $\{p_i', kv_i''\}_{i=1}^n \leftarrow \mathrm{DRBG}(R_\epsilon, \Delta t)$. However, since DRBG is a deterministic algorithm, if Eve has inputs different from Alice, Eve obtains entirely different authentication qubits from DRBG than the valid authentication qubits. In order words, except for the case where Eve accidentally chooses $R_E = AK_0$, the following equation is satisfied.

$$\{p_i', kv_i''\}_{i=1}^n \neq \{p_i, kv_i'\}_{i=1}^n \leftarrow \mathrm{DRBG}(AK_0, \Delta t). \tag{10}$$

Although Eve transmits authentication qubits from DRBG by inputting R_E and Δt, Eve almost fails to the impersonation attack in the verification of Bob, except for $R_E = AK_0$. In summary of the case that Eve pretends to Alice, Eve's success probability of the attack is $2^{-|AK_0|}$.

Figure 3(b) depicts the case where Eve pretends to Bob. By assumption, Eve has also obtained the time-synchronization information Δt. There are two scenarios wherein Eve can impersonation attack by pretending to Bob. First, R_E substituted with the pre-shared secret information AK_0 is randomly generated by Eve. Then, Δt and R_E are processed into

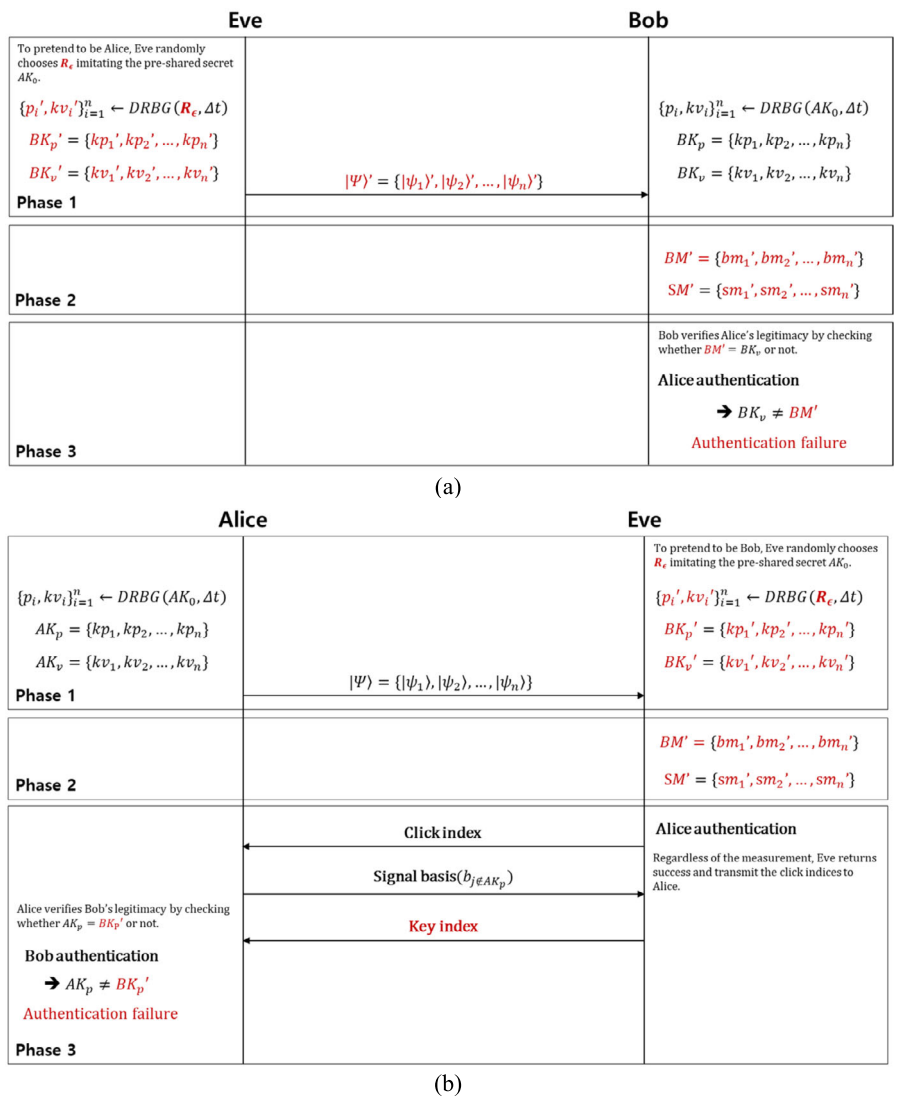

Figure 3 Impersonation attack of the proposed authentication system (a) Eve impersonated as Alice (b) Eve impersonated as Bob. Note that the red text means Eve generates incorrect authentication information since the input data of DRBG has been changed

DRBG to generate authentication qubits as follows: $\{p_i', kv_i''\}_{i=1}^n \leftarrow \mathrm{DRBG}(R_\epsilon, \Delta t)$. Because it is equal to the case that Eve impersonates Alice, Eve's success probability of the attack is $2^{-|AK_0|}$ as well. Second, Eve chooses the correct basis, which is transmitted to Alice. There are two bases: B_Z and B_X, which are randomly generated in the QKD system. Thus, the probability of matching the correct basis of n authentication qubits from N qubits received by Eve is 2^{-n}. In other words, the probability that Eve succeeds in the attack impersonated as Bob is $\mathrm{Max}\{2^{-|AK_0|}, 2^{-n}\}$.

Based on the security analysis from the viewpoint of the impersonation attack, the probability that Eve succeeds the attack is denoted as $\mathrm{Max}\{2^{-|AK_0|}, 2^{-n}\}$. Therefore, the soundness property of this protocol can be satisfied if the pre-shared secret information AK_0 and the number of authentication qubits is sufficiently large.

3.3 Security analysis for refresh period

The usage policy of the DRBG mechanism is considered to design the authentication system securely given that DRBG is employed in our authentication protocol to generate the same authentication information. In particular, the reseed interval, a component of the DRBG mechanism policy, is considered to ensure the security of the proposed authentication protocol. Moreover, it is necessary to calculate the reseed interval of the DRBG mechanism to maximize the randomness of time synchronization information in the QKD system for preventing attacks that block the quantum channel, as well.

For instance, let the DRBG based on the hash function be used in the authentication protocol and the precision of the time-synchronization be 1 ns in our QKD system. To ensure DRBG's security from the viewpoint of the refresh interval, it is referred the DRBG mechanism policy stated in SP 800–90A, which is the NIST's standard for DRBG mechanism [44]. This standard specifies that the maximum number of requests between reseed interval is 2^{48}, and the maximum number of bits per request is 2^{19} bits. Therefore, the reseeding function shall be executed in the DRBG mechanism before the output length is $2^{19} \cdot 2^{48} = 2^{57}$ bits, which is the maximum output length to be assured by the DRBG policy.

From the security analysis, it can be determined that the security strength of the proposed authentication protocol is $\min\{2^D, 2^{|AK_0|}, 2^n\}$ bits. In Sect. 4, we deploy the authentication protocol in the 1xN QKD system and verify its stable operation over a real fiber network.

4 Experimental results

We performed the mutual entity authentication on the 1x4 QKD network system. The proposed protocol was applied to identify the network participants, the user, and server. Each server and user were connected with 25 km of the QC which loss is about 0.21/km. The SHA256 based on DRBG was implemented on an FPGA [44, 60]. The lasers for four users emit weak coherent pulses with 2.5 MHz and 51,200 pulses are transmitted by one session. The photons from the users are detected by the APDs which operation speed is 10 MHz. The timing of the lasers was appropriately modulated for allocating the signals at the designated timing for a certain user. The average photon number of signal and decoy pulse are $\mu = 0.65$ and $\nu_1 = 0.11$, and the proportion of weak and vacuum pulse are 0.1 and 0.01, respectively. The loss of the server is 5.8 dB considering the optical components. The quantum efficiency and background noise of the APDs are 15% and 5,000 cps, respectively.

To satisfy the security of the authentication, the number of detections of the authentication qubits, N_{AQ}, must be enough to recognize the agreement between BM and BK_v. To ensure $N_{AQ} \geq 256$, we calculated the maximum distance of the authentication qubits, d. Because we operate approximately six of QKD session in one second, which is proportional to optical path length, N is 307,200. Here, R_{AQ} can be analyzed under the experimental condition such as the detector, noises, and optical losses. Using (7), $d \leq 4$ is satisfied for identifying each user within every second. Because it is not necessary that the server and users must execute identification shortly, the server and user can adjust the interval of the authentication session which contains the authentication and signal qubits together. We set $d = 4$ and utilized two bits of DRBG output for allowing $p_i \mathrm{mod} d \in \{0, 1, 2, 3\}$. As a result, 270.8 of N_{AQ} was analyzed by carrying out only the authentication session in one second.

The pre-shared information, $AK_0 = 512$ bits, is fed into DRBG as a seed for sharing identical DRBG output. The seed of DRBG should refresh to ensure freshness. A single

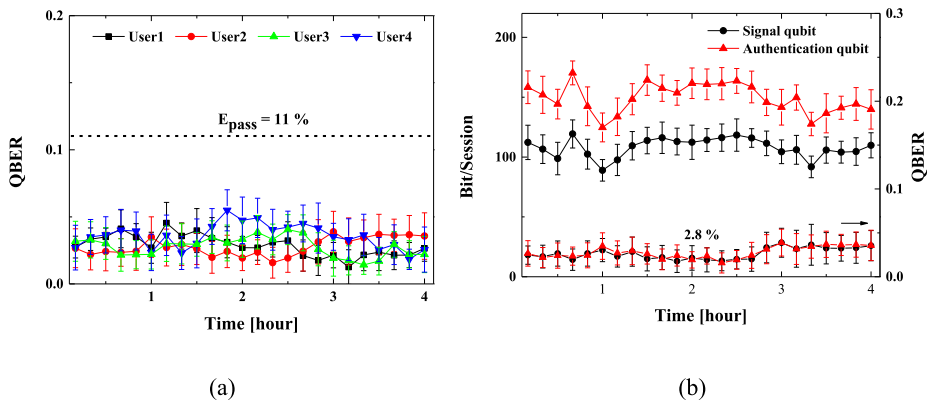

Figure 4 Entity authentication results of 4 users in the QKD network. (a) QBER of authentication qubits about four users. (b) Detection rate and QBER of signal and authentication qubits per session for one of four users

authentication qubit consumes 4 bits, 2 bits each for kp_i and kv_i, so 491, 520 bits are spent in one second regarding to N and d. It is about 2^{19}, which is far below than 2^{57}. In those aspects, if the server and user refresh the seed by the secure key before using 2^{57} of bits, the freshness of the DRBG can be maintained.

Figure 4(a) shows the QBER of the authentication qubits from four users. The server measures the authentication qubits using a measurement basis of $B_{j=kp_i}$ and compares BM and BK_v. The authentication qubits from four users were measured using TDM, and less than 8.9% of QBER occurred over four hours. Considering the security of the QKD, we set the upper bound of the error rate of the authentication qubit, E_{pass}, as 11% [23, 26]. Further, the server was identified as a legitimate entity by monitoring the QBER of the signal qubits, because the server could properly obtain the sifted key using pre-shared information. The key rate and QBER of one user are depicted in Fig. 4(b). As the authentication qubits are generated based on the identical DRBG and pre-shared information, the server certainly selects the right measurement basis, which results in 100% efficiency. Meanwhile, the signal qubits are turned into the sifted key by BB84 protocol with 50% of the efficiency. As a result, the ratio of the key rate between the signal and authentication qubit is about 3:4 by concerning $d = 4$ and efficiency. In the experiment, to identify each participant, 24×10^6 of pulses were transmitted, and the average bit rate per session of the authentication qubit is about 149.5 bit, which is close to the analyzed value of 158.9 bit from Q_μ and Q_{ν_1}. The authentication sessions took place every 30 s. Considering more than 256 bits of the secure authentication bits, N_{AQ} consisting of only single photon measurement, six authentication sessions are required. So, the server and each user identified each other every three minutes while monitoring QBER of the authentication and signal qubit. If the server and users need to conduct entity authentication by every one second, they can replace every session with the authentication session. This means that there is a trade-off in terms of the secure key rate and real-time authentication. The server's capacity to rapidly generate signals and authentication qubits, or its utilization of multi-QKD network links, offers a promising avenue for resolving these challenges.

We demonstrated the proposed authentication protocol in a real environment. 1x3 QKD network system was deployed in the metropolitan area as shown in Fig. 5. The distances from the server to each user are 5.8, 7.7, and 9.9 km, and the fiber losses are 1.29, 1.63, and

Figure 5 Map of the 1 × 3 QKD network. The entity authentication protocol is embedded in each user and server of QKD system

2.23 dB, respectively. The changes in the environment condition lead to fluctuation of the optical path length, which causes degradation of the performance of the QKD network. We automatically compensated it by modulating laser timing in real-time [61]. Figure 6 shows the results of the entity authentication on the 1x3 QKD network in a real-world environment. The authentication and signal qubits from each user were measured, and the key rate and QBER are monitored by the server in real-time. The key rate of the authentication qubit for each user was upper than 250 bit per session, and lower than 5% of QBER was maintained during 40 hours. As mentioned previously, there was a fluctuation of the key rate and QBER due to environmental change. Due to a mismatch of the optimal timing, the key rate was reduced, and relatively more QBER occurred. It was minimized with the compensation algorithm. The key rate and QBER of the signal and authentication qubit showed a similar tendency due to the same experimental condition. However, the qubits from each user suffered from different environmental conditions, which leads to a different variation of the key rate and QBER. The average secure key rates of the authentication qubit from user 1, 2, 3 were 556, 508.6, 433.9 bps, respectively. Further, the server was identified by each user through achieving the secure key and maintaining the QBER of the signal qubits during 40 hours.

5 Conclusion

We demonstrated the proposed mutual entity authentication scheme on 1xN quantum key distribution network system in a real environment. The security analysis and experimental results showed that the protocol can be easily applied to the commercial system and safely identify the network participants in real-time. By using the proposed scheme, the participants can identify each other with the same level of security of the quantum

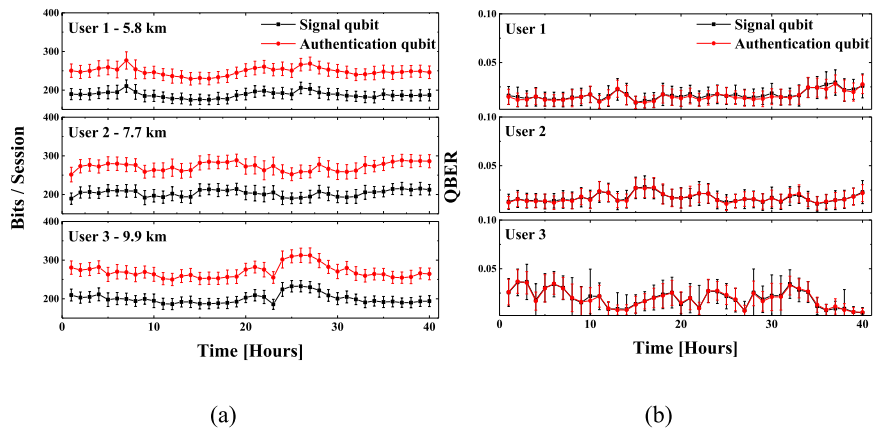

Figure 6 Entity authentication results of the 1x3 QKD network. Entity authentications for users and server were performed in real-world with (a) Bits/session and (b) QBER during 40 hours

key distribution, which covers both public and quantum channels. This scheme can be a promising candidate for verifying the participants of the massive quantum key distribution networks.

Acknowledgements
The authors would like to thank the editor and anonymous reviewers for their valuable suggestions.

Funding
This work was supported by the National Research Foundation of Korea (NRF) (2021M1A2A2043892, 2022M3K4A1097119), Institute for Information and Communications Technology Promotion (IITP) (2020-0-00947, 2020-0-00890), the Commercializations Promotion Agency for R&D Outcomes (2022SCPO_B_0210), KREONET Advanced Research Program Grant from KISTI, and KIST research program (2E31531, 2E32801).

Availability of data and materials
The datasets used and analyzed during the current study are available from the corresponding author on reasonable request.

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
Not applicable.

Competing interests
The authors declare no competing interests.

Author contributions
The protocol design and security analysis were done by Park HJ, Park BK, Kang JS, Yeom YJ, and Han SW. The simulation was done by Park BK, Woo MK, Kang MS, Choi JW, and Han SW. Park HJ and Park BK wrote the draft and all authors reviewed and contributed the final manuscript. The effort was conceived and supervised by Han SW and Yeom YJ.

Author details
[1]Department of Information security, Cryptology and Mathematics, Kookmin University, Seoul, South Korea. [2]Center for Quantum Information, Korea Institute of Science and Technology, Seoul, South Korea. [3]Division of Nano and Information Technology, Korea Institute of Science and Technology School, Korea University of Science and Technology, Seoul, South Korea. [4]Division of Quantum Technology, SDT Inc., Seoul, South Korea. [5]Artificial intelligence & Big Data Examination Division, Korean Intellectual Property Office, Daejeon, South Korea.

Received: 1 July 2023 Accepted: 6 November 2023 Published online: 15 November 2023

References
1. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. Theor Comput Sci. 2014;560:7–11.

2. Ekert AK. Quantum cryptography based on Bell's theorem. Phys Rev Lett. 1991;67(6):661–3.
3. Bennett CH. Quantum cryptography using any two nonorthogonal states. Phys Rev Lett. 1992;68(21):3121–4.
4. Yin H-L, Chen T-Y, Yu Z-W, Liu H, You L-X, Zhou Y-H et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. Phys Rev Lett. 2016;117(19):190501.
5. Lucamarini M, Yuan ZL, Dynes JF, Shields AJ. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. Nature. 2018;557(7705):400–3.
6. Boaron A, Boso G, Rusca D, Vulliez C, Autebert C, Caloz M et al. Secure quantum key distribution over 421 km of optical fiber. Phys Rev Lett. 2018;121(19):190502.
7. Yin J, Li Y-H, Liao S-K, Yang M, Cao Y, Zhang L et al. Entanglement-based secure quantum cryptography over 1,120 kilometres. Nature. 2020;582(7813):501–5.
8. Yuan Z, Plews A, Takahashi R, Doi K, Tam W, Sharpe A et al. 10-Mb/s quantum key distribution. J Lightwave Technol. 2018;36(16):3427–33.
9. Grünenfelder F, Boaron A, Rusca D, Martin A, Zbinden H. Performance and security of 5 GHz repetition rate polarization-based quantum key distribution. Appl Phys Lett. 2020;117(14):144003.
10. Gilles B Felix B Nicolas G Suzanne L, editors. Multiuser quantum key distribution using wavelength division multiplexing. ProcSPIE; 2003
11. Chip E, Alexander C, David P, Oleksiy P, John S, Henry Y, editors. Current status of the DARPA quantum network. ProcSPIE. 2005.
12. Peev M, Pacher C, Alléaume R, Barreiro C, Bouda J, Boxleitner W et al. The SECOQC quantum key distribution network in Vienna. New J Phys. 2009;11(7):075001.
13. Chen T-Y, Liang H, Liu Y, Cai W-Q, Ju L, Liu W-Y et al. Field test of a practical secure communication network with decoy-state quantum cryptography. Opt Express. 2009;17(8):6540–9.
14. Wang S, Chen W, Yin Z-Q, Zhang Y, Zhang T, Li H-W et al. Field test of wavelength-saving quantum key distribution network. Opt Lett. 2010;35(14):2454–6.
15. Sasaki M, Fujiwara M, Ishizuka H, Klaus W, Wakui K, Takeoka M et al. Field test of quantum key distribution in the Tokyo QKD network. Opt Express. 2011;19(11):10387–409.
16. Stucki D, Legré M, Buntschu F, Clausen B, Felber N, Gisin N et al. Long-term performance of the SwissQuantum quantum key distribution network in a field environment. New J Phys. 2011;13(12):123001.
17. Wang S, Chen W, Yin Z-Q, Li H-W, He D-Y, Li Y-H et al. Field and long-term demonstration of a wide area quantum key distribution network. Opt Express. 2014;22(18):21739–56.
18. Tang Y-L, Yin H-L, Zhao Q, Liu H, Sun X-X, Huang M-Q et al. Measurement-device-independent quantum key distribution over untrustful metropolitan network. Phys Rev. 2016;6(1):011024.
19. Liao S-K, Cai W-Q, Handsteiner J, Liu B, Yin J, Zhang L et al. Satellite-relayed intercontinental quantum network. Phys Rev Lett. 2018;120(3):030501.
20. Park BK, Woo MK, Kim Y-S, Cho Y-W, Moon S, Han S-W. User-independent optical path length compensation scheme with sub-nanosecond timing resolution for a 1xN quantum key distribution network system. Photon Res. 2020;8(3):296–302.
21. Chen Y-A, Zhang Q, Chen T-Y, Cai W-Q, Liao S-K, Zhang J et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. Nature. 2021;589(7841):214–9.
22. Lütkenhaus N. Security against individual attacks for realistic quantum key distribution. Phys Rev A. 2000;61(5):052304.
23. Shor PW, Simple PJ. Proof of security of the BB84 quantum key distribution protocol. Phys Rev Lett. 2000;85(2):441–4.
24. Brassard G, Lütkenhaus N, Mor T, Sanders BC. Limitations on practical quantum cryptography. Phys Rev Lett. 2000;85(6):1330–3.
25. Gottesman D, Lo H-K, Lütkenhaus N, Preskill J. Security of quantum key distribution with imperfect devices. Quantum Inf Comput. 2004;4(5):325–60.
26. Pirandola S. Symmetric collective attacks for the eavesdropping of symmetric quantum key distribution. Int J Quantum Inf. 2008;06:765
27. Dušek M, Haderka O, Hendrych M, Myška R. Quantum identification system. Phys Rev A. 1999;60(1):149–56.
28. Zeng G, Keitel CH. Arbitrated quantum-signature scheme. Phys Rev A. 2002;65(4):042312.
29. Mihara T. Quantum identification schemes with entanglements. Phys Rev A. 2002;65(5):052326.
30. Li Q, Chan WH, Long D-Y. Arbitrated quantum signature scheme using Bell states. Phys Rev A. 2009;79(5):054307.
31. Fung C-HF, Ma X, Chau HF. Practical issues in quantum-key-distribution postprocessing. Phys Rev A. 2010;81(1):012318.
32. Zou X, Qiu D. Security analysis and improvements of arbitrated quantum signature schemes. Phys Rev A. 2010;82(4):042325.
33. Kang M-S, Hong C-H, Heo J, Lim J-I, Yang H-J. Controlled mutual quantum entity authentication using entanglement swapping. Chin Phys B. 2015;24(9):090306.
34. Choi J-W, Kang M-S, Heo J, Hong C, Yoon C-S, Han S-W et al. Quantum challenge-response identification using single qubit unitary operators. Phys Scr. 2020;95(10):105104.
35. Choi J-W, Kang M-S, Park CH, Yang H-J, Han S-W. Measurement-device-independent mutual quantum entity authentication. Quantum Inf Process. 2021;20(4):152.
36. Wang L-J, Zhang K-Y, Wang J-Y, Cheng J, Yang Y-H, Tang S-B et al. Experimental authentication of quantum key distribution with post-quantum cryptography. npj Quantum Inf. 2021;7(1):67.
37. Greenberger DM, Horne MA, Shimony A, Zeilinger A. Bell's theorem without inequalities. Am J Phys. 1990;58(12):1131–43.
38. Rass S, König S, Schauer S, editors. BB84 quantum key distribution with intrinsic authentication. In: 9th int. conf. Quantum, nano/bio, micro technol. 2015. p. 41–44.
39. Bae M, Kang H, Kang J-S, Yeom Y, editors. Mutual authentication mechanism using pre-shared key and BB84 quantum key distribution for quantum cryptography communication. Adv Sci Technol Lett 2017. 156–9.
40. Hong C-H, Heo J, Jang JG, Kwon D. Quantum identity authentication with single photon. Quantum Inf Process. 2017;16(10):236.

41. International Organization for Standardization and the International Electrotechnical Commission. Information technology—Security techniques—Random bit generation; 2011 Nov. Report No.: ISO/IEC 18031.s
42. International Organization for Standardization and the International Electrotechnical Commission. Information technology—Security techniques – Test requirements for cryptographic modules; 2017 Mar. Report No.: ISO/IEC 24759.
43. International Organization for Standardization and the International Electrotechnical Commission. Information technology—Security techniques—Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408; 2019 Oct. Report No.: ISO/IEC 20543.
44. National Institute of Standards and Technology. Recommendation for Random Number Generation Using Deterministic Random Bit Generators. Gaithersburg, MD: Special Publication (NIST SP); 2015 Jun. Report No.: 800-90A Rev 1.
45. National Institute of Standards and Technology. Recommendation for the entropy sources used for random bit generation. Gaithersburg, MD: Special Publication (NIST SP); 2018 Jun. Report No.: 800-90B.
46. National Institute of Standards and Technology. Recommendation for Random Bit Generator (RBG) Construction (3rd Draft). Gaithersburg, MD: Special Publication (NIST SP); 2022 Sep. Report No.: 800-90C.
47. Muthukumar A, Sivasankari N, Rampriya K, editors. Anti-aging true random number generator for secured database storage. In: 4th int. conf. Adv. computing, communication syst. 2017. p. 1–7.
48. Barak B, Shaltiel R, Tromer E, editors. True random number generators secure in a changing environment. In: 5th int. workshops. Cryptographic hardware, embedded syst. 2003. p. 166–180.
49. Markettos AT, Moore SW, editors. The frequency injection attack on ring-oscillator- based TRNGs. In: 11th int. workshops. Cryptographic hardware, embedded systems. 2009. p. 317–331.
50. Bayon P, Bossuet L, Aubert A, Fischer V, Poucheret F, Robisson B, Maurine P, editors. Contactless electromagnetic active attack on ring oscillator based TRNG. In: 3rd int. workshops. Constructive side-channel analysis and secure design. 2012. p. 151–166.
51. Ghandali S, Holcomb D, Paar C, editors. Temperature-based hardware Trojan for ring-oscillator-based TRNGs. 2019. arXiv preprint. arXiv:1910.00735.
52. Muller A, Herzog T, Huttner B, Tittel W, Zbinden H, Gisin N. "Plug and play" systems for quantum cryptography. Appl Phys Lett. 1997;70(7):793–5.
53. Ribordy G, Gautier J-D, Gisin N, Guinnard O, Zbinden H. Automated 'plug and play' quantum key distribution. Electron Lett. 1998;34(22):2116–7. https://digital-library.theiet.org/content/journals/10.1049/el_19981473.
54. Stucki D, Gisin N, Guinnard O, Ribordy G, Zbinden H. Quantum key distribution over 67 km with a plug&play system. New J Phys. 2002;4:41.
55. Hwang W-Y. Quantum key distribution with high loss: toward global secure communication. Phys Rev Lett. 2003;91(5):057901.
56. Wang X-B. Beating the photon-number-splitting attack in practical quantum cryptography. Phys Rev Lett. 2005;94(23):230503.
57. Lo H-K, Ma X, Decoy CK. State quantum key distribution. Phys Rev Lett. 2005;94(23):230504.
58. Ma X, Qi B, Zhao Y, Lo H-K. Practical decoy state for quantum key distribution. Phys Rev A. 2005;72(1):012326.
59. Menezes AJ, van Oorschot PC, Vanstone SA. Handbook of applied cryp-tography. Florida: CRC Press; 1996.
60. National Institute of Standards and Technology. Secure Hash Standard (SHS), Gaithersburg, MD: Federal Information Processing Standards Publication; 2015 Aug. Report No.: FIPS 180-3.
61. Park BK, Lee MS, Woo MK, Kim Y-S, Han S-W, Moon S. QKD system with fast active optical path length compensation. Sci China, Phys Mech Astron. 2017;60(6):060311.

Publisher's Note