Quantum Information Processing (2020) 19:18
https://doi.org/10.1007/s11128-019-2510-4

Quantum digital signature in a network

Changho Hong[1] · Jingak Jang[1] · Jino Heo[2] · Hyung-Jin Yang[3]

Received: 1 August 2018 / Accepted: 16 November 2019

Abstract

We propose a quantum digital signature in a network consisting of one signer, multiple verifiers, and a trusted center (TC). The protocol guarantees that messages and signed messages are not counterfeited, and it authenticates the source of the messages. In addition, a signer (or a verifier) cannot, at a later time, deny having signed (received) the message. Theoretically, our quantum digital signature guarantees the security through quantum mechanics.

Keywords Quantum signature · Quantum communication · Quantum cryptography · Communication security

1 Introduction

Digital signature is a mathematical method for validating the integrity and authenticity of a digital document. It is intended to solve the problem of tampering and impersonation in digital communications. Digital signature can provide certification of a signer as well as identity and status of an electronic document. A valid digital signature guarantees that the signed message was created by a genuine signer, the signed message was not altered in transit (integrity or no-forgery), and the signer cannot contradict the signed message he or she has sent (authentication and non-repudiation) [1, 2]. Digital signatures are based on public-key cryptography. Using a public-key protocol, we can generate two types of keys, private and public keys. The public key is publicly available. The private key is known only to the owner or signer and cannot be derived from

✉ Jino Heo
jinoheo80@cbnu.ac.kr

[1] Institute of Electronics and Telecommunications Research Institute, P.O. Box 1, Yuseong, Daejeon 34188, South Korea

[2] College of Electrical and Computer Engineering, Chungbuk National University, Chungdae-ro 1, Seowon-Gu, Cheongju, South Korea

[3] Department of Physics, Korea University, Yeongi 339-700, South Korea

Published online: 26 November 2019

the public key. When a message is encrypted using the public key, only those who know the corresponding private key can decrypt the message. On the other hand, for the RSA digital signature, a message is encrypted using the private key, and all those who know the public key can verify it. All digital signature schemes that base their encryption on assumptions of computational complexity [3] (e.g., the discrete logarithm problem and the factoring problem), are not secure from the quantum point of view [4]. Unfortunately, when quantum computers are factored in, the decryption problem becomes solvable [5, 6]. Quantum digital signature (QDS) has been proposed to remedy this problem.

The first QDS was proposed by Gottesman and Chung [7]. Barnum et al. showed that an unconditionally secure QDS for quantum messages could not be achieved [8]. Zeng and Keitel [9] published an arbitrated quantum signature protocol that could be employed for signing both classical and quantum messages by using the correlation between Greenberger–Horne–Zeilinger (GHZ) states. This protocol was improved in 2008 [10, 11]. Lee et al. [12] and Wang et al. [13] proposed two QDS schemes, with only one of the schemes using a public board. Li et al. [14] proposed a much simpler QDS protocol than Zeng and Keitel's [9]. This protocol was further simplified by Zou et al. [15]. Yoon et al. [16] proposed a QDS based on a quantum search algorithm. Zhang et al. [17] published a QDS scheme by using quantum teleportation technique.

QDSs have been recently realized using linear optics [18, 19]. Robert et al. [20] presented the first experimental realization of QDS that does not require quantum memory.

There are some requirements on digital signature and QDS. These requirements are authenticity, no-forgery, and non-repudiation. Authenticity helps to prevent others from pretending to be the originator of a particular message. Impossibility of forgery of QDS (and digital signature) helps to ensure that the content has not been changed or tampered. Non-repudiation helps to prove that the signer of a message, and not someone else, is its true originator. A signer cannot repudiate the signature on that.

In this paper, we propose a QDS network with Bell states. It is composed of a signer, multi-verifier, and a trusted center (TC). While previous proposals were based on one-to-one relationship between the signer and verifier, our QDS network provides one-to-many relationship, satisfying the digital signature requirement.

The rest of this paper is organized as follows. In the next section, we propose the signature and verification scheme of the QDS network. The security analysis and discussion are presented in Sect. 3. Finally, we conclude our protocol in Sect. 4.

2 QDS network

In digital signature and QDS, even though the signed message should be securely transferred [16], message encryption is not mandatory [11]. For example, when messages (such as employment contract) are published, justification of a signature appearing in the document is far more important than the message itself. The digital signature and QDS, therefore, can be classified according to whether they use a known message or an unknown message [11]. For security purposes, the signer, the verifier, and the TC all announce some information on a public board, which is freely available (intact). In public board, information is not assumed to be blocked or modified, nor additional messages to be added [21, 22].

The QDS network [23] protocol includes three steps: the initialization step, the signature step, and the verification step. During the initialization step, a TC shares entangled qubits with communicators and delivers their keys. During the signature step, Alice signs her message to obtain the signature states. During the verification step, the verifier, Bob(s), verifies Alice's signature assisted by the TC.

2.1 Initialization step

All authentic users share a hash function h, where $h\,:\,(0,1)^* \to (0,1)^{2n}$. One of the characteristics of the hash function h is its fixed length output. This feature provides the message digest. The hash function can be used to verify the message authenticity [24, 25]. Most digital signatures confirm the authenticity of a hashed output of the message. The digital signature method compares the pre-transmitted hashed output to the post-transmitted one.

A TC shares the secret keys K_{TA} and K_{TB} with Alice and Bob, respectively. The bit length of both K_{TA} and K_{TB} is n, where $K_{TA} = K_{TA1}, K_{TA2}, \dots, K_{TAn}$ and $K_{TB} = K_{TB1}, K_{TB2}, \dots, K_{TBn}$.

I-1. A TC generates both n Bell states $|\Phi^+\rangle_{A,T_A}$ and n Bell states $|\Phi^+\rangle_{B,T_B}$.

$$\left|\Phi^+\right\rangle_{j,T_j}^{i} = \frac{1}{\sqrt{2}}\left(|00\rangle_{j,T_j} + |11\rangle_{j,T_j}\right)^{i} \tag{1}$$

where $j \in \{A, B\}$ and $i = \{1, 2, \dots, n\}$.

The TC then divides the entangled states $\otimes_{i=1}^{n}|\Phi^+\rangle_{A,T_A}^{i}$ into an A sequence and T_A sequence, and $\otimes_{i=1}^{n}|\Phi^+\rangle_{B,T_B}^{i}$ into a B sequence and T_B sequence. The sequences are composed of qubits, such that the A sequence is $\left(A_1, A_2, \dots, A_n\right)$, the T_A sequence is $\left(T_{a1}, T_{a2}, \dots, T_{an}\right)$, the B sequence is $\left(B_1, B_2, \dots, B_n\right)$, and the T_B sequence is $\left(T_{b1}, T_{b2}, \dots, T_{bn}\right)$. The TC transmits the A sequence to Alice and the B sequence to Bob. The TC's remaining qubits are the T_A and T_B sequences. During the process of sharing the sequences of qubits, the legitimate users use the following step ST to ensure safe transport of the quantum states.

ST. For the secure transmission of a qubits, the qubit sender randomly mixes decoy photons $|+\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$ or $|-\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)$ with the original qubit sequence. After confirming that the recipient completely received the qubits sequence (it is composed of original qubits and decoy qubits), the sender reveals the individual positions of the decoy photons. The recipient executes X-basis measurements on the decoy photons and reveals the result. The sender of the qubit sequence compares the published result with the initialization states of the decoy qubits and determines whether an attacker was involved [22, 23]. If attackers are revealed, it stops the process and goes back to the initialization step. Otherwise, the procedure will proceed to the next step.

I-2. Alice prepares and announces the message m that she wants to sign on the public board. The message's length $|m|$ is not a constraint.

2.2 Signature step

S-1. Alice computes the hash function $h(m)$:

$$h(m) = \left[h^1(m)||h^2(m)|| \dots ||h^{2n}(m)\right] \tag{2}$$

where $h^l(m) \in \{0,1\}$. $|h(m)| = 2n$ and $l = 1, 2, \dots, 2n$.

Then, she groups $h(m)$ by two bits:

$$h(m) = \left[\left\{h^1(m)||h^2(m)\right\}, \left\{h^3(m)||h^4(m)\right\}, \dots, \left\{h^{2n-1}(m)||h^{2n}(m)\right\}\right]. \tag{3}$$

Therefore, the number of groups of $h(m)$ is n.

S-2. Alice generates the random bit sequence:

$$r_a = \left\{\left(r^1_{a1}||r^2_{a2}\right), \left(r^3_{a1}||r^4_{a2}\right), \dots, \left(r^{2n-1}_{a1}||r^{2n}_{a2}\right)\right\}, \tag{4}$$

where r^{2i-1}_{a1} or $r^{2i}_{a2} \in \{0,1\}$. It is her own secret information.

She calculates α_i as follows:

$$\alpha_i = h^{2i-1}(m)h^{2i}(m) \oplus r^{2i-1}_{a1}r^{2i}_{a2} \in \{00, 01, 10, 11\}, \quad i \in \{1, 2, \dots, n\}, \tag{5}$$

where $h^i h^j \oplus r^i r^j = (h^i \oplus r^i)\|(h^j \oplus r^j)$. Also, the bits α_i refers to one of the four Pauli operators $\left\{I, \sigma_x, i\sigma_y, \sigma_z\right\}$ according to the bit outcomes $\{00, 01, 10, 11\}$, respectively.

S-3. Alice generates the qubit rotation operators $R_y(\theta_{K_{TAi}})$ about the $\hat{y}$ axis,

$$R_y(\theta_{K_{TAi}}) \equiv \exp\left(\frac{-i\theta_{K_{TAi}}\sigma_y}{2}\right) = \cos\frac{\theta_{K_{TAi}}}{2}I - i\sin\frac{\theta_{K_{TAi}}}{2}\sigma_y, \tag{6}$$

by using the secret key K_{TA}. $\theta_{K_{TAi}} \in \left\{\theta_0, \theta_1\right\}$, where θ_0 and θ_1 are preset random angles between the TC and Alice, depending on the value of K_{TA}. There is no correlation between the θ_0 and θ_1, such as in an orthogonal relationship. Users should share a prior rotation angle θ_0 and θ_1 to apply the arbitrary rotation operator to the quantum state. It means θ_0 and θ_1 are not only selected from $\left\{0, \frac{\pi}{2}\right\}$, but from arbitrary angles $\left\{r_o\pi, r_1\pi\right\}$, where $0 \leq r_o\left(r_1\right) \leq 1$ [26].

The purpose of using rotation operators is to authenticate the singer and other legitimate users. The involvement of an attacker who does not know θ_0 and θ_1 (and K_{TA} also) causes an error between the legitimate users and they can detect her. The detailed discussion is explained in Sect. 3.

S-4. Alice creates the signature:

$$\left|sign^A\right\rangle^i = R_y(\theta_{K_{TAi}})\alpha_i|A_i\rangle, \tag{7}$$

where $i = \{1, 2, \dots, n\}$, $\alpha_i \in \{I, \sigma_x, i\sigma_y, \sigma_z\}$, and $|A_i\rangle$ is a element of the A sequence transmitted by TC.

S-5. Alice sends $\left|\mathrm{sign}^A\right\rangle = \left\{\left|\mathrm{sign}^A\right\rangle^1, \left|\mathrm{sign}^A\right\rangle^2, \dots, \left|\mathrm{sign}^A\right\rangle^n\right\}$ to TC by using the step ST. Namely, the transmission of the signature is to send the quantum state using a quantum channels. The TC and Alice check the security of the quantum channel according to the step ST.

S-6. The TC receives the signature sequence $\left|\mathrm{sign}^A\right\rangle$ from Alice and applies the operator $R_y(-\theta_{K_{TAi}})$ generated from the K_{TA} on each $\left|\mathrm{sign}^A\right\rangle^i$. The total state is:

$$\begin{aligned} |\psi\rangle^i_{A,T_a} &= \left(R_y(-\theta_{K_{TAi}}) \otimes I\right)\left|\mathrm{sign}^A\right\rangle \otimes |Ta_i\rangle \\ &= \left(R_y(-\theta_{K_{TAi}}) \otimes I\right)\left(R_y(\theta_{K_{TAi}})\ \ \alpha_i \otimes I\right)\left|\Phi^+\right\rangle^i_{A,T_a} \\ &= \left(\alpha_i \otimes I\right)\left|\Phi^+\right\rangle^i_{A,T_a}, \end{aligned} \tag{8}$$

where $|Ta_i\rangle$ is the component of sequence T_A. The state $|\psi\rangle^i_{A,T_a}$ is one of the four Bell states. After performing the Bell state measurements (BSM) on the A sequence and T_A sequences, the TC obtains Alice's operator α_i from the BSM outcome. If the TC knows all of the α_i, he can infer r_a because he can calculate $h\ (m)$, using the message m published on the public board and the shared hash function h. As stated above, legitimate users share the hash function h, and the message m is publicly announced on the public board in step I-2. The TC obtains r'_a from the BSM and Eq. (8). The rotation operators guarantee user identification, including the authentication of the signer [24, 25].

S-7. For a checking procedure, the TC chooses $n/2$ pairs of numbers $\left(r^{2j-1}_{a1}, r^{2j}_{a2}\right)$ at random and requests Alice to release the bit values of the chosen pair. Once Alice reveals the values, the TC compares Alice's bit values $\left(r^{2j-1}_{a1}, r^{2j}_{a2}\right)$ with TC's own bit values $\left(r^{2j-1'}_{a1}, r^{2j'}_{a2}\right)$, determining whether Alice's signature is correct. This process ensures Alice's non-repudiation because Alice cannot deny that she communicates with the TC. The process of signature is shown in Fig. 1.

2.3 Verification step

V-1. The TC creates his own sequence of random bits:

$$r_t = \left\{\left(r^1_{t1}||r^2_{t2}\right), \left(r^3_{t1}||r^4_{t2}\right), \dots, \left(r^{2n-1}_{t1}||r^{2n}_{t2}\right)\right\}, \tag{9}$$

where r^{2i-1}_{t1} or $r^{2i}_{t2} \in \{0, 1\}$.

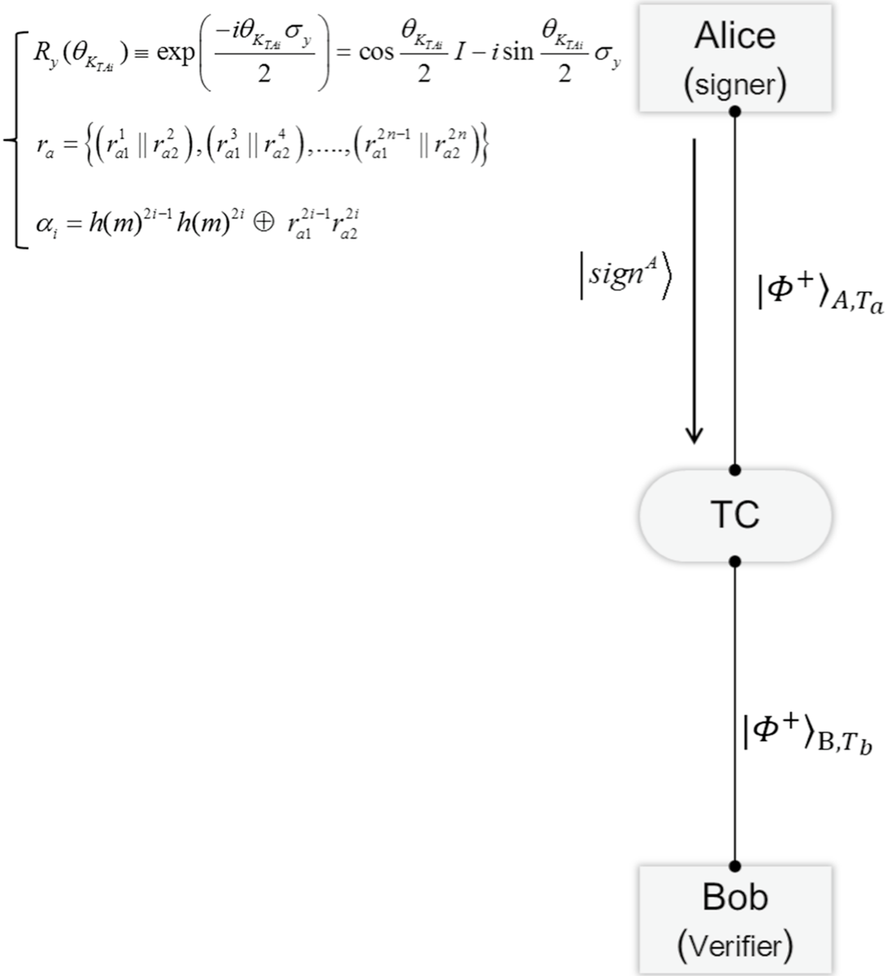
$R_y(\theta_{K_{TAi}}) \equiv \exp\left(\frac{-i\theta_{K_{TAi}}\sigma_y}{2}\right) = \cos\frac{\theta_{K_{TAi}}}{2} I - i\sin\frac{\theta_{K_{TAi}}}{2}\sigma_y$
$r_a = \left\{\left(r_{a1}^1 \| r_{a2}^2\right), \left(r_{a1}^3 \| r_{a2}^4\right), \dots, \left(r_{a1}^{2n-1} \| r_{a2}^{2n}\right)\right\}$
$\alpha_i = h(m)^{2i-1} h(m)^{2i} \oplus r_{a1}^{2i-1} r_{a2}^{2i}$
Alice
(signer)
$\left|sign^A\right\rangle$
$|\Phi^+\rangle_{A,T_a}$
TC
$|\Phi^+\rangle_{\mathrm{B},T_b}$
Bob
(Verifier)

Fig. 1 Process of quantum signature scheme. Alice generates $R_y(\theta_{K_{TAi}})$, r_a, and α by using K_{TA} and hash function h. Finally, she creates a signature $\left|\mathrm{sign}^A\right\rangle$ and sends it to the TC

He calculates β_i as follows:

$$\beta_i = h(m)^{2i-1} h(m)^{2i} \oplus r_{a1}^{2i-1'} r_{a2}^{2i'} \oplus r_{t1}^{2i-1} r_{t2}^{2i} \in \{00, 01, 10, 11\}, \quad i \in \{1, 2, \dots, n\}, \tag{10}$$

where $h^i h^j \oplus r^{i'} r^{j'} \oplus r^i r^j = (h^i \oplus r^{i'} \oplus r^i) \| (h^j \oplus r^{j'} \oplus r^j)$.

As with the α_i, the bit value of β_i refers to one of the four Pauli operators, $\{I, \sigma_x, i\sigma_y, \sigma_z\}$.

V-2. The TC uses the random bits sequence to generate $\left|\mathrm{sign}^{A'}\right\rangle$:

$$\left|\text{sign}^{A'}\right\rangle^{i} = R_y(\theta_{K_{TBi}})\beta_i\left|T_{bi}\right\rangle, \tag{11}$$

where $R_y(\theta_{K_{TBi}})$ is the shared rotation operator between the TC and Bob, similar to the step S-3. So that,

$$R_y(\theta_{K_{TBi}}) \equiv \exp\left(\frac{-i\theta_{K_{TBi}}\sigma_y}{2}\right) = \cos\frac{\theta_{K_{TBi}}}{2}I - i\sin\frac{\theta_{K_{TBi}}}{2}\sigma_y. \tag{12}$$

And $\left|T_{bi}\right\rangle$ in Eq. (11) is a qubit of the T_B sequence that was created in step I-1.

V-3. The TC transmits $\left|\text{sign}^{A'}\right\rangle^{i}$ to Bob securely, using the step ST during which the sender and receiver utilize decoy photons to ensure the security of the communication channel.

Bob applies the operator $R_y\left(-\theta_{K_{TBi}}\right)$ on the received signature states. The total state $|\psi\rangle^{i}_{B,T_b}$ between the TC and Bob is as follows:

$$|\psi\rangle^{i}_{B,T_b} = \left(I \otimes R_y(-\theta_{K_{TBi}})\right)\left|\text{sign}^{A'}\right\rangle^{i} \otimes \left|T_{bi}\right\rangle. \tag{13}$$

V-4. The verifier, Bob, announces that he has received $\left|\text{sign}^{A'}\right\rangle$ by using the public board, and then performs BSM on the B sequence and T_B sequence to obtain γ_i from $\left|\text{sign}^{A'}\right\rangle$:

$$\gamma_i = r_{a1}^{2i-1'} r_{a2}^{2i'} \oplus r_{t1}^{2i-1} r_{t2}^{2i}, \tag{14}$$

where $r_{a1}^{i'} r_{a2}^{i'} \oplus r_{t1}^{i'} r_{t2}^{i'} = (r_{a1}^{i'} \oplus r_{t1}^{i'})\Big\|(r_{a2}^{i'} \oplus r_{t2}^{i'})$.

Because Bob knows the hashed message $h(m)$ and keeps the key K_{TB} shared with the TC, he can decode $\left|\text{sign}^{A'}\right\rangle$. The state $|\psi\rangle^{i}_{B,T_b}$ evolves as:

$$\begin{aligned} |\psi\rangle^{i}_{B,T_b} &= \left(I \otimes R_y(-\theta_{K_{TBi}})\right)\left|\text{sign}^{A'}\right\rangle^{i} \otimes \left|Tb_i\right\rangle \\ &= \left(I \otimes \beta_i\right)\left|\Phi^+\right\rangle_{B,T_b} \\ &= \left[I \otimes \left(h^{2i-1}(m)\, h^{2i}(m) \oplus \gamma_i\right)\right] \ \left|\Phi^+\right\rangle_{B,T_b}, \end{aligned} \tag{15}$$

where the state $|\Phi^+\rangle_{B,T_b}$ was prepared and shared in step I-1. The state $|\psi\rangle'_{B,T_b}$ is one of the Bell states. If Bob performs a BSM on $|\psi\rangle'_{B,T_b}$, he can obtain γ_i from β_i.

V-5. Bob publicly announces γ_i on the public board.

V-6. After Bob's publication of γ_i, Alice announces r_a on the public board. Obtaining r_a from the public board, the TC checks whether γ_i is identical to $r_{a1}^{2i-1} r_{a2}^{2i} \oplus r_{t1}^{2i-1} r_{t2}^{2i}$, where $i = \{1, 2, \ldots, n\}$. If r'_a $\left(= \left\{(r_{a1}^{1'}||r_{a2}^{2'}), (r_{a1}^{3'}||r_{a2}^{4'}), \ldots, (r_{a1}^{2i-1'}||r_{a2}^{2i'})\right\}\right)$ is not identical to r_a, the discrepancy implies that Alice announced the wrong sign information, and further verification is not performed. If r'_a is identical to r_a, the TC announces to Bob that Alice is the legitimate signer and the signature for message m is valid. Alice's signature is only successfully verified if the r_a is rederived by Bob and TC.

Figure 2 shows the verification step.

For multi-user verification, the verification step is accomplished by multiple verifiers. For example, the TC and Bob perform the verification step, while the TC and another verifier, Charlie, perform another verification step for one signer, Alice. Schematic of the QDS network is shown in Fig. 3.

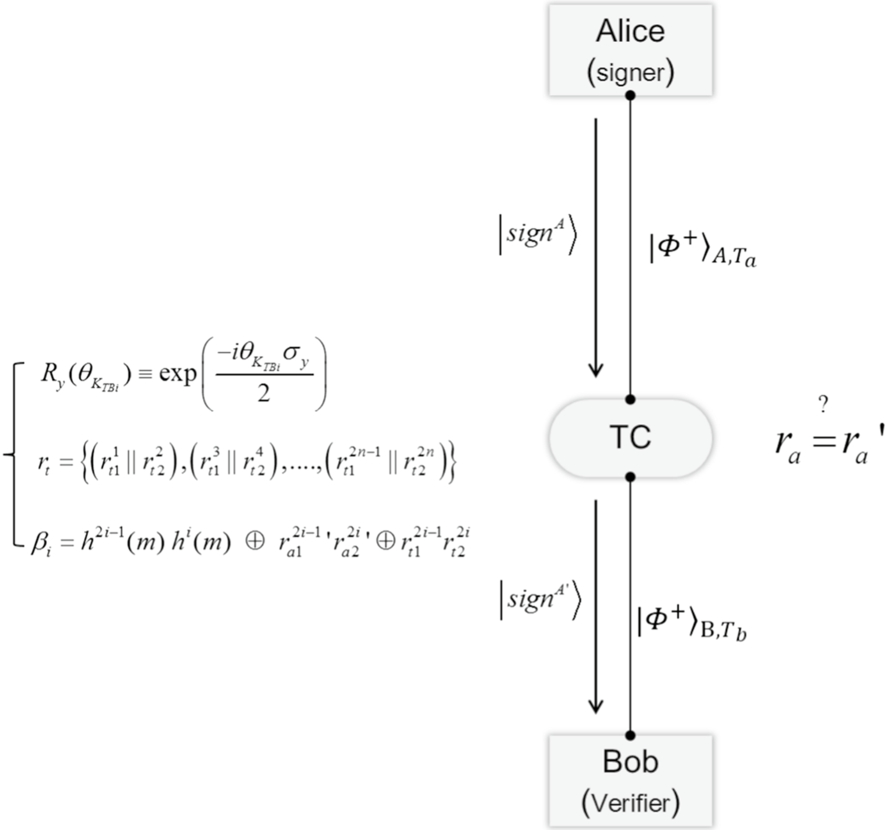
Alice
(signer)
$\left|sign^{A}\right\rangle$
$|\Phi^{+}\rangle_{A,T_a}$
$R_y(\theta_{K_{TBi}}) \equiv \exp\left(\frac{-i\theta_{K_{TBi}}\sigma_y}{2}\right)$
$r_t = \left\{\left(r_{t1}^{1} \| r_{t2}^{2}\right),\left(r_{t1}^{3} \| r_{t2}^{4}\right),\ldots,\left(r_{t1}^{2n-1} \| r_{t2}^{2n}\right)\right\}$
$\beta_i = h^{2i-1}(m)\, h^{i}(m) \oplus r_{a1}^{2i-1}{}' r_{a2}^{2i}{}' \oplus r_{t1}^{2i-1} r_{t2}^{2i}$
TC
$r_a \overset{?}{=} r_a{}'$
$\left|sign^{A'}\right\rangle$
$|\Phi^{+}\rangle_{B,T_b}$
Bob
(Verifier)

Fig. 2 Verification step. The TC verifies Alice's signature by using $|\Phi^{+}\rangle_{A,T_a}$ and K_{TA}. The TC sends $\left|\text{sign}^{A'}\right\rangle$ to the verifier, Bob. Bob performs BSM on $\left|\text{sign}^{A'}\right\rangle$ after applying $R_y\left(\theta_{K_{TB}}\right)$. The TC receives γ from Bob and r_a from Alice. The TC then checks whether r_a is identical to r'_a

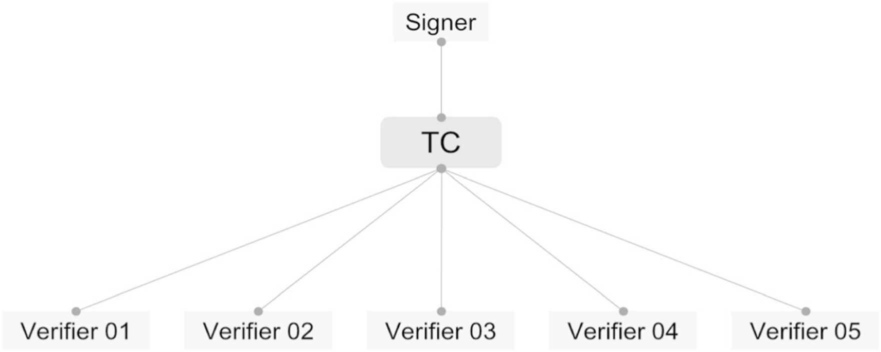

Fig. 3 Our QDS network. It is composed of one signer and multiple verifiers. A bold line represents the Bell state to be shared with the TC

3 Security of our QDS in a network

To validate the security of our QDS protocol, it is necessary to guarantee no-forgery and non-repudiation [9, 12, 14]. No-forgery means that an attacker or the receiver cannot change the signature, and the signature may not be recreated as well. Non-repudiation is that the signatory may not disavow the signed message, and the receiver may not repudiate the receipt of the signature. We now analyze the security of our signature scheme.

Our QDS uses step TC for secure transmission of quantum states. It is important to ensure that this TC procedure is justified in neutralizing known attacks. In particular, as the QDS is based on the ping-pong protocol [27], we will analyze whether it is secure to Wójcik's method [28] and Pavičić attack [29].

Finally, we discuss the security of our QDS in noisy quantum channels.

3.1 Impossibility of forgery in our QDS network

In our QDS, Alice uses her own random bit r_a, shared key K_{TA} with the TC, and initial state $|\Phi^+\rangle_{A,T_a}$ to create the legitimate signature. The TC ultimately verifies the signature and the signer, Alice, by using the key K_{TA} $\left(or \ \ R_y(-\theta_{K_{TA}})\right)$ and the initial state $|\Phi^+\rangle_{A,T_a}$ in step S-6. The key K_{TA} and the state $|\Phi^+\rangle_{A,T_a}$ constitute the information that is known only to Alice and the TC. No one can generate the legitimate sign on $h(m)$ without K_{TA} and $|\Phi^+\rangle_{A,T_a}$. The rotation operator $R_y(\theta_{K_{TA}})$ guarantees the signer's identification. Only the TC can confirm the signer (Alice) by using $R_y(-\theta_{K_{TA}})$ in step S-6. Therefore, our quantum signature scheme guarantees no-forgery property.

For example, suppose that when Alice sends the quantum states $\left|\text{sign}^A\right\rangle$ of the signature in step S-5, the dishonest inner attacker Bob intercepts the string and sends his forgery to the TC. However, it cannot pass the step ST because Bob cannot distinguish the signal photons from the decoy photons. Bob's forgery attack causes errors in the checking procedure (the step ST). Also, Bob does not share Alice's random bit sequence r_a, secret key K_{TA}, and the sequence A, which are the essential information required to create legitimate sign. Therefore, his forgery attempt is futile in our protocol.

Our protocol uses hash function h and public board to guarantee no-forgery property. The announced message m on the public board is open information, but it cannot be changed by an attacker. The information on the public board is not assumed to be blocked or modified [21, 22]. Furthermore, it is almost impossible to find a pair $\left(m, m'\right)$ satisfying $h\ (m) =\ h\ (m'\ )$ due to the properties of hash function h [30, 31]. Thus, if someone (including an inner attacker, such as Bob) alters the open message m to m', it must be checked during the procedure in step V-4 through V-6, because $h(m)$ is not equal to $h(m'\ )$, and the legitimate signer, Alice, did not sign on the $h(m'\ )$. An error occurs if r_a is not identical to r'_a in step V-6 because $h\ (m) \neq h\ (m')$.

3.2 Non-repudiation of our QDS protocol

Repudiation can be done only by the trusted center TC [30, 31]. We, however, suppose that TC is an honest mediator. So we do not assume TC's attacks [30, 31].

Non-repudiation of our QDS is provided by the TC. In our protocol, we supplement the public board [12, 15] to provide more advanced non-repudiation. In addition, to prevent falsification of the qubits sequence in transmission, we randomly mix decoy photons throughout the entire protocol (see the step ST).

Let us consider non-repudiation in more detail.

We now show that the dishonest signer Alice, having sent Bob the signature about the message m, cannot deny her transmission. In steps S-6 and S-7, Alice communicates with TC. That is, for Bob to verify the signature, Alice needs to provide the partial information of r_a to TC. Hence, if Alice later disavows having sent the signature, mediator TC can confirm that she has lied. When Alice announces the false r_a during the step V-6 for repudiation of her sign, the TC can check her malicious acts by comparing r_a and r'_a in step V-6.

We will show that dishonest Bob's disavowal about legitimate signature can be checked by the mediator TC. If Bob lies regarding the value of γ for repudiation of the signature's receipt, the TC can determine that Bob has lied because modulation of γ is impossible in a secure quantum channel. Except for a situation in which noise occurs in the quantum channel during the transmission of $\left|\text{sign}^A\right\rangle$ and $\left|\text{sign}^{A'}\right\rangle$, thus Bob's denial is impossible in ideal quantum channel.

3.3 Discussion of the security against known attack

In the step S-4, the signature states are random and independent pure states. The secret-key sequence $K_{TA}(K_{TB})$ is equally distributed with equal bit 0 and 1, and all signatures are as follows.

$$\left|\text{sign}^A\right\rangle = \otimes_{i=1}^{n}\left|\text{sign}^A\right\rangle^{i} = \otimes_{i=1}^{n} R_y(\theta_{K_{TAi}})\alpha_i\left|A_i\right\rangle \tag{16}$$

To get the information of secret key K_{TA}, an attacker must measure the signature $\left|\text{sign}^A\right\rangle$ using an erratic basis. On the quantum channel, the jth signature state is as follows:

$$\begin{aligned}\rho^j &= \frac{1}{2}\left|\text{sign}^A\right\rangle^j \, {}^j\left\langle\text{sign}^A\right| = \frac{1}{2}R_y\left(\theta_{K_{TAj}}\right)\alpha_j\left|A_j\right\rangle\left\langle A_j\right|\alpha_j^+R_y\left(\theta_{K_{TAj}}\right)^+ \\ &= \frac{I}{2}\end{aligned} \tag{17}$$

It is mixed state. The qubits comprising the signature are independent of each other, and thus the qubit of the entire signature's qubit is given as, $\rho = \frac{I^{\otimes n}}{2^n}$ [24]. This state means that Eve cannot identify the signature on the quantum channels.

Now, we use Holevo's theorem to express the security against Eve's forger attack. It is presented as follows [32, 33]:

$$H(e, K_{TA}) \leq S(\rho) \ll H(K_{TA}) \tag{18}$$

where $H(e, K_{TA})$ is the mutual information between the secret key K_{TA} and the forger e, $S(\rho)$ is the von Neumann entropy of the signature qubit ρ, and $H(K_{TA})$ is the entropy of the secret key K_{TA}. We can find $H(K_{TA}) = I/2$. Although the forger e tries to obtain information about the signature key K_{TA} using quantum measurements on the signature qubit, the amount of information the forger can get is bounded by Eq. (18). It indicates that the amount of information $H(e, K_{TA})$ is much smaller than $H(K_{TA})$, and thus forgery is not possible.

For secure transmission of quantum states, we put to use decoy photons, $|+\rangle$ and $|-\rangle$(X-basis), differently from original qubits sequence using Z-basis in step ST. The decoy state method was first proposed by Hwang [34] to improve the security and performance of practical QKD.

The decoy method is widely used in quantum communications [35–40]. Here, our QDS protocol, which applied the decoy method, shows that it is safe for the following three attacks. The first is that Eve impersonates signer, Alice, the second is that Eve launches the Wójcik's method [28], and the third attack is that she attacks with the Pavičić attack [29].

Firstly, we consider a malicious attacker Eve's impersonation attack. In this attack, Eve intercepts the signature in the middle of the quantum channel and tries to obtain valuable information. In order to impersonation as signer, she sends a newly generated faked signature to TC (and Bob). Eve will pass every decoy photons with the probability, $P_{d-1} = 1/2$. For example, when TC asks signer, Alice (actually Eve), to provide her decoy photons, Eve must send decoy photons that she has no choice but to choose from $\{|+\rangle, |-\rangle\}$. Of course, Bob performs the X-basis measurement according to the measurement regulation of step ST. With probability P_{d-1}, Eve can pass the step ST (security test). When the number of the decoy photons reaches D, the probability that attacker, Eve, succeeds in step ST is $\left(\frac{1}{2}\right)^D$. If D is large enough, the Eve's passing probability is taken to zero. In other words, the detection probability of Eve is

$$P_d = 1 - \left(1 - (1 - P_{d-1})\right)^D = 1 - \left(1 - \frac{1}{2}\right)^D. \tag{19}$$

As D increases, the attacker detection probability converges into 1.

Second, we examine Wójcik's method [28] of eavesdropping in the presence of losses in quantum channels. Here, we briefly describe the Wójcik's method and discuss whether it can affect our QDS. This attack is applicable only to quantum communication protocols that use entangled states (Bell states) and have two transfers. A typical example is the ping-pong protocol [27]. Our QDS is also in the condition that the attack is possible. Figure 4 shows the schematic representation of this attack on the ping-pong protocol.

According to the attack, Eve prepares two auxiliary spatial modes x and y in the state $|\text{vac}\rangle_x|0\rangle_y$. $|\text{vac}\rangle_x$ means the vacuum in the mode x. She performs operator E_{txy} on t-photon (travel photon in the ping-pong protocol), modes x and y. The operation E_{txy} is defined as

$$E_{txy} = \text{SWAP}_{tx}\text{CPBS}_{txy}H_y \tag{20}$$

It is composed of the SWAP gate, Hadamard gate, and the controlled polarization beam splitter (CPBS) gate. CPBS_{Axy} can be expressed as

$$\text{CPBS}_{txy} = \text{CNOT}_{ty}(\text{CNOT}_{tx} \otimes I_y)(I_t \otimes \text{PBS}_{xy})\text{CNOT}_{ty}(\text{CNOT}_{tx} \otimes I_y). \tag{21}$$

The polarization beam splitter (PBS) transmits photons in the state $|0\rangle$ and reflects photons in the state $|1\rangle$. The state of the system is

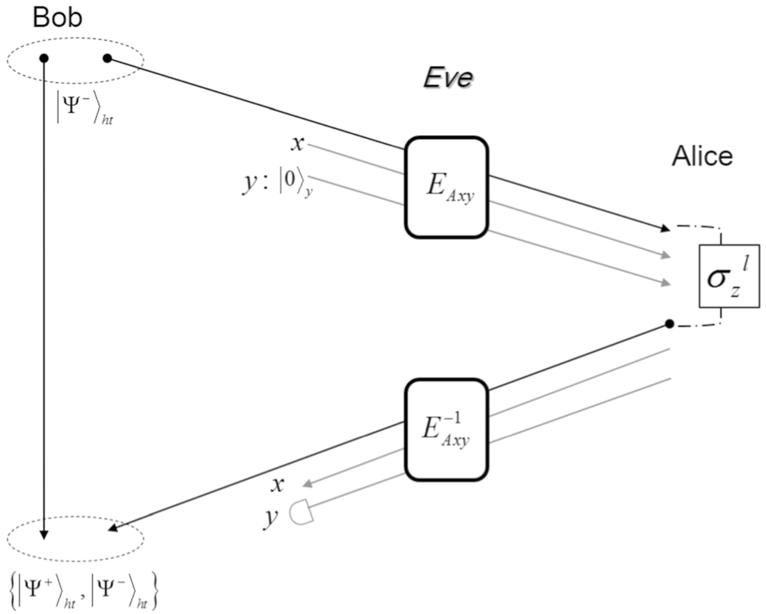

Fig. 4 Wójcik's method on the ping-pong protocol

$$\begin{aligned}|\psi\rangle_{1st} &= E_{txy}\big|\Psi^+\big\rangle_{ht}|\mathrm{vac}\rangle_x|0\rangle_y\\ &= \frac{1}{2}\big[|0\rangle_h\big(|\mathrm{vac}\rangle_t|1\rangle_x|0\rangle_y + |1\rangle_t|1\rangle_x|\mathrm{vac}\rangle_y\big) + |1\rangle_h\big(|\mathrm{vac}\rangle_t|0\rangle_x|1\rangle_y + |0\rangle_t|0\rangle_x|\mathrm{vac}\rangle_y\big)\big].\end{aligned} \tag{22}$$

The t photon is saved in the mode x. Suppose that Alice choose the control mode. According to Eq. (22), Alice detects no photon with a probability 1/2. With the rest of the probability, the photon is detected and its state is anticorrelated with the state of the h photon. Therefore, under this attack, the detection probability of eavesdropper is zero in the control mode of the ping-pong protocol. Eve can hide her existence in the quantum bit error rate (QBER). In the message mode of the protocol, Alice encodes her message with σ_z^l. The encoded t photon comes back from Alice to Bob. Attacker Eve acts E_{txy}^{-1} operator on the t photon and modes x and y in the middle of the channel. After the Eve's second action at the channel, the state of the whole system is

$$|\psi\rangle_{2\mathrm{nd}} = \frac{1}{2}\big[\big|\Psi^+\big\rangle_{ht}\big(|l\rangle_y + |0\rangle_y\big) + |\Psi^-\rangle_{ht}\big(|l\rangle_y - |0\rangle_y\big)\big] \tag{23}$$

Assuming that Alice sends 0 and 1 with the same probability, the mutual information can be calculated [28]. The results are $I_{AB} = I_{AE} = \frac{3}{4}\log_2 3 - 1 \approx 0.189$. We see that mutual information between Alice and Eve is the same as the mutual information between Alice and Bob.

This effective attack on the ping-pong protocol is not the case with our QDS. Eve intervenes in the quantum channel twice, for the first time during the transmission of a qubit of entangled state (T-A attack) and for the second time during the return of the qubit (A-T attack). It is shown in Fig. 4.

In step ST, Trent mixed decoy photons with original qubits and revealed the positions of the decoy photons after Alice receives the qubit sequence. For a decoy photon $|\pm\rangle_t$, the overall state of T-A attack is

$$\begin{aligned}|\phi\rangle_{1\mathrm{st}} &= E_{txy}|\pm\rangle_t|\mathrm{vac}\rangle_x|0\rangle_y\\ &= \frac{1}{2}\big[|0\rangle_t|0\rangle_x|\mathrm{vac}\rangle_y + |\mathrm{vac}\rangle_t|0\rangle_x|1\rangle_y \pm |1\rangle_t|1\rangle_x|\mathrm{vac}\rangle_y \pm |\mathrm{vac}\rangle_t|1\rangle_x|0\rangle_y\big].\end{aligned} \tag{24}$$

Our QDS uses X-basis for decoy photons, compared to the ping-pong protocol. Equation (24) shows that the modes prepared by the attacker are not related to the decoy photon. A decoy photon (h photon) and mode x, which seem to be correlated to each other, are rewritten as follows. In this equation, does not measured terms are excluded.

$$|\phi\rangle_{1\mathrm{st}} \approx \frac{1}{2}\big[\big(|+\rangle_t + |-\rangle_t\big)|0\rangle_x \pm \big(|+\rangle_t - |-\rangle_t\big)|1\rangle_x\big] \tag{25}$$

In step ST, An attacker's intervention with the Wójcik's method make an error with 50% probability per one decoy photon. Then, the detection probability of Eve is the same as the case of Eve's impersonation attack (Eq. 19). That is, as D increases, Eve is definitely detectable. Because the presence of an attacker is revealed in the first attack, the second attack does not continue. Even if this attack passes the step ST and apply E_{txy}^{-1}, the signature state on quantum channel is facing the same situation as Eq. (17) by the rotation operator $R_y\left(\theta_{K_{TA}}\right)$ (Fig. 5).

Finally, in the Pavičić attack [29], an attacker also makes use of Hadamard gate on the mode x compared to the Wójcik's method. It is basically based on the Wójcik's method. Thus, in step ST of our QDS, it can be seen that the presence of an attacker is revealed in a similar way as in the previous analysis of the Wójcik's method. In order to understand, let us apply this attack on a decoy photon of the step ST. An attacker prepares the state $|\mathrm{vac}\rangle_x|0\rangle_y$ and performs operator Q_{txy} on t photon (actually decoy photon, $|\pm\rangle_t$) and modes x and y. The operation Q_{txy} is defined as follows:

$$Q_{txy} = \mathrm{CPBS}_{txy}\left(I_t \otimes H_x \otimes H_y\right) \tag{26}$$

where CPBS is expressed as Eq. (21). In step ST, sender transmits photon $|\pm\rangle_t$. After the first action of the attack, the system state is

$$\begin{aligned} |\gamma\rangle_{1\mathrm{st}} &= Q_{txy}|\pm\rangle_t|\mathrm{vac}\rangle_x|0\rangle_y \\ &= \frac{1}{2}\left[\left(|0\rangle_t|0\rangle_x \pm |1\rangle_t|1\rangle_x\right)|\mathrm{vac}\rangle_y + \left(|0\rangle_t|1\rangle_y \pm |1\rangle_t|0\rangle_y\right)|\mathrm{vac}\rangle_x\right]. \end{aligned} \tag{27}$$

For the security check of the channel, a recipient makes a measurement the decoy photon t with X-basis. We know it from the step ST. Equation (27) is rewritten as follows:

$$\begin{aligned} |\gamma\rangle_{1\mathrm{st}} = \frac{1}{2\sqrt{2}}&\left[\left\{\left(|+\rangle_t + |-\rangle_t\right)|0\rangle_x \pm \left(|+\rangle_t - |-\rangle_t\right)|1\rangle_x\right\}|\mathrm{vac}\rangle_y\right. \\ &\left.+\left\{\left(|+\rangle_t + |-\rangle_t\right)|1\rangle_x \pm \left(|+\rangle_t - |-\rangle_t\right)|0\rangle_x\right\}|\mathrm{vac}\rangle_y\right] \end{aligned} \tag{28}$$

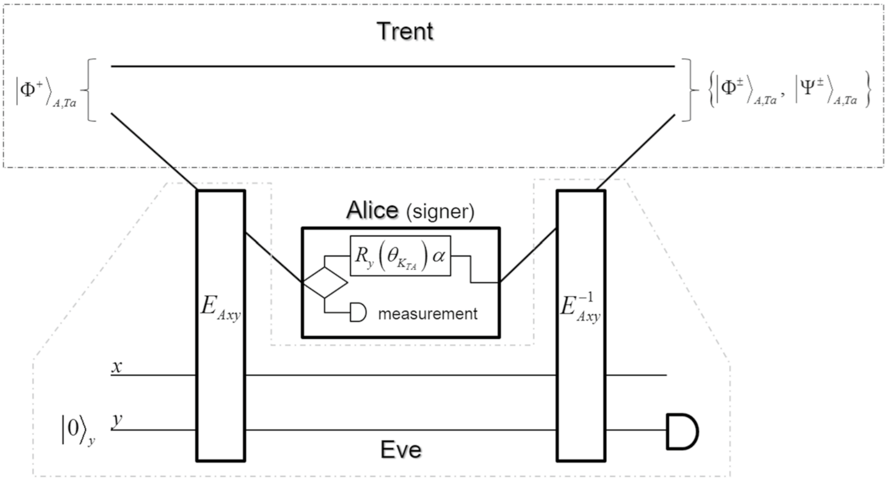

Fig. 5 Wójcik's attack procedure on the QDS

Equation (28) shows that Eve using the Pavičić attack causes an error in step ST. Due to an attacker's intervention, the sender sent $|+\rangle_t$, but the receiver had a 50% probability of receiving $|+\rangle_t$ or $|-\rangle_t$. The error rates are same with the Wójcik's method and the impersonation attack on our QDS. According to Eq. (19), as long as D is large enough, the detection probability of an attacker approaches 1.

What if the attacker is detected in step ST, but ignored it and proceeded to next steps? In fact, M. Pavičić said that an eavesdropper can always distinguish Ψ from Φ states using the Pavičić attack [29]. Therefore, it is necessary to see if this proposition applies to our QDS as well. For analysis, let us assume that $\theta_0 = \frac{\pi}{2}$ and $\theta_1 = \frac{\pi}{4}$. For a particular position u, we assume that $K_{TA(u)} = 1$ and $\alpha_u = I$. The whole states in which the first attack was applied is

$$\begin{aligned} |\gamma\rangle_{1\mathrm{st}} &= Q_{Axy}\big|\Phi^+\big\rangle_{A(u),TA(u)}|\mathrm{vac}\rangle_x|0\rangle_y \\ &= \frac{1}{2}\big[|0\rangle_{A(u)}|0\rangle_x|\mathrm{vac}\rangle_y|0\rangle_{TA(u)} + |0\rangle_{A(u)}|\mathrm{vac}\rangle_x|1\rangle_y|0\rangle_{TA(u)} \\ &\quad +|1\rangle_{A(u)}|\mathrm{vac}\rangle_x|0\rangle_y|1\rangle_{TA(u)} + |1\rangle_{A(u)}|1\rangle_x|\mathrm{vac}\rangle_y|1\rangle_{TA(u)}\big]. \end{aligned} \tag{29}$$

After the signature step of signer and the second attack of the Pavičić attack, the overall state is

$$\begin{aligned} |\gamma\rangle_{2\mathrm{nd}} &= Q_{Axy}^{-1}\left[R\left(\frac{\pi}{4}\right) I\right]_{A(u)}|\gamma\rangle_{1\mathrm{st}} \\ &= \frac{1}{2}\big[|0\rangle_{A(u)}|\mathrm{vac}\rangle_x|0\rangle_y|0\rangle_{TA(u)} + |1\rangle_{A(u)}|0\rangle_x|\mathrm{vac}\rangle_y|0\rangle_{TA(u)} \\ &\quad - |0\rangle_{A(u)}|0\rangle_x|\mathrm{vac}\rangle_y|1\rangle_{TA(u)} + |1\rangle_{A(u)}|\mathrm{vac}\rangle_x|0\rangle_y|1\rangle_{TA(u)}\big] \\ &= \frac{1}{\sqrt{2}}\Big[\big|\Phi^+\big\rangle_{A(u),TA(u)}|\mathrm{vac}\rangle_x|0\rangle_y - |\Psi^-\rangle_{A(u),TA(u)}|0\rangle_x|\mathrm{vac}\rangle_y\Big]. \end{aligned} \tag{30}$$

Table 1 lists the result for possible α_u. It represents that Eve's intervention causes an error rate of 50%. As M. Pavičić's claims, an attacker may be able to distinguish Ψ from Φ, but it is not in our QDS. Even if the attacker's measurement outcome is $|0\rangle_x|\mathrm{vac}\rangle_y$, she cannot determine whether this is $\Psi(|\Psi^-\rangle_{A(u),TA(u)})$. It can be Φ by referring to Table 1. This induced error reveals the presence of an attacker in step S-7. In practice, however, an attacker is revealed by the previous step ST. Because of the secret keys K_{TA}, K_{TB} and the rotation operator $R_y(\theta_{K_{TA}})$, $R_y(\theta_{K_{TB}})$, the Pavičić attack method does not work with our QDS.

Table 1 For possible α_u, measurement outcomes and errors (caused by an attacker)

α_u	$A(u), TA(u)$	x, y	Errors	
			$A(u), TA(u)$	x, y
I	$\|\Phi^+\rangle$	$\|\mathrm{vac}\rangle_x\|0\rangle_y$	$\|\Psi^-\rangle$	$\|0\rangle_x\|\mathrm{vac}\rangle_y$
σ_x	$\|\Psi^+\rangle$	$\|0\rangle_x\|\mathrm{vac}\rangle_y$	$\|\Phi^-\rangle$	$\|\mathrm{vac}\rangle_x\|0\rangle_y$
$I\sigma_y$	$\|\Psi^-\rangle$	$\|0\rangle_x\|\mathrm{vac}\rangle_y$	$\|\Phi^+\rangle$	$\|\mathrm{vac}\rangle_x\|0\rangle_y$
σ_z	$\|\Phi^-\rangle$	$\|\mathrm{vac}\rangle_x\|0\rangle_y$	$\|\Psi^+\rangle$	$\|0\rangle_x\|\mathrm{vac}\rangle_y$

Here, $\theta_{K_{TA(u)}} = \frac{\pi}{4}$ is fixed

As we have seen, the QDS is secure against forgery attack, Eve's impersonation attack, the Wójcik's method, and the Pavičić attack. Ideally, Eve's presence is revealed to legitimate users by a 50% probability per a decoy photon. Therefore, the secure communication is possible if the legitimate communicators using a sufficient number of decoy photons in step ST. If the loss rate of a channel increases, the use of decoy photon should increase [35–40]. Of course, it is a drawback. But it is inevitable for the secure communication.

3.4 Discussion of the security in noisy quantum channel

The protocol proposed here is in the theoretical stage, like most QDS protocols [7–20]. What we have discussed so far is the safety of the digital signatures [41] and the security about known attacks [28, 29]. In QDS field, there is an insufficiency of research on security parameter that needs to be discussed at the experimental (or implementation) stage. In fact, the study of QDS's security parameter estimation is a big research field that is discussed alone [42, 43]. Here, we examine the security of our QDS against collective attacks when the noisy channel is taken into account. Due to the loss of the quantum channel, the certain amount of quantum states sent by the sender will be lost. We express the lost state as $|\text{vac}\rangle$.

For a start, let us consider communication between TC and Alice. The discussion in this channel applies equally to the channel between TC and Bob. In step I-1, an attacker's general collective attack on the quantum channel from TC to Alice (TC–Alice channel) can be expressed in the form

$$\begin{aligned} E_i|0\rangle_{Ai}|e\rangle_i &= \sqrt{p_{i(0v)}}|\text{vac}\rangle_{Ai}|e_i\rangle_{0v} + \sqrt{p_{i(00)}}|0\rangle_{Ai}|e_i\rangle_{00}\sqrt{p_{i(01)}}|1\rangle_{Ai}|e_i\rangle_{01} \\ E_i|1\rangle_{Ai}|e\rangle_i &= \sqrt{p_{i(1v)}}|\text{vac}\rangle_{Ai}|e_i\rangle_{1v} + \sqrt{p_{i(10)}}|0\rangle_{Ai}|e_i\rangle_{10}\sqrt{p_{i(11)}}|1\rangle_{Ai}|e_i\rangle_{11} \end{aligned} \tag{31}$$

where $p_{i(1v)}$ is the probability that Alice receives a vacuum state (because of noisy quantum channel) but TC sent the state $|1\rangle_{Ai}$. $|e_i\rangle$ and $|e_i\rangle_{jk}$ are Eve's initial ancilla state and possible quantum states of Eve's ancilla after evolution, respectively. Then, the joint density matrix of the A sequence and Eve's ancilla states is

$$\begin{aligned} \rho^{T-A}_{(AE)i} &= E_i tr_{TC} P\Big[|\Phi^+\rangle^i_{A,T_A}|e\rangle_i\Big]E_i^+ \\ &= \frac{1}{2}O\Big[\sqrt{p_{i(00)}}|0\rangle_{Ai}|e_i\rangle_{00} + \sqrt{p_{i(01)}}|1\rangle_{Ai}|e_i\rangle_{01} + \sqrt{p_{i(0v)}}|\text{vac}\rangle_{Ai}|e_i\rangle_{0v}\Big] \\ &\quad + \frac{1}{2}O\Big[\sqrt{p_{i(10)}}|0\rangle_{Ai}|e_i\rangle_{10} + \sqrt{p_{i(11)}}|1\rangle_{Ai}|e_i\rangle_{11} + \sqrt{p_{i(1v)}}|\text{vac}\rangle_{Ai}|e_i\rangle_{1v}\Big], \end{aligned} \tag{32}$$

where $O\big[|a\rangle\big] \equiv |a\rangle\langle a|$. In step S-4, Alice encode her signature information onto the elements of the A sequence by the operator α. Let us consider the case in which Alice encrypts with $\alpha_i = I$ after Eve's intervention caused $|A_i\rangle$ to $|0\rangle_{Ai}$. When the error and the loss are applied, the joint state of Alice and Eve is

$$\begin{aligned}\rho^{T-A}_{I(AE)i} &= \frac{1}{2}\,O\Big[\sqrt{p_{i(00)}}|0\rangle_{Ai}|e_i\rangle_{00} + \sqrt{p_{i(01)}}|1\rangle_{Ai}|e_i\rangle_{01} + \sqrt{p_{i(0v)}}|\mathrm{vac}\rangle_{Ai}|e_i\rangle_{0v}\Big] \\ &\quad + \frac{1}{2}\,O\Big[-\Big(\sqrt{p_{i(00)}}|0\rangle_{Ai}|e_i\rangle_{00} + \sqrt{p_{i(01)}}|1\rangle_{Ai}|e_i\rangle_{01}\Big) + \sqrt{p_{i(0v)}}|\mathrm{vac}\rangle_{Ai}|e_i\rangle_{0v}\Big] \\ &= O\Big[\sqrt{p_{i(00)}}|0\rangle_{Ai}|e_i\rangle_{00} + \sqrt{p_{i(01)}}|1\rangle_{Ai}|e_i\rangle_{01}\Big] + p_{i(0v)}O\big[|\mathrm{vac}\rangle_{Ai}|e_i\rangle_{0v}\big]\end{aligned} \tag{33}$$

In the same way, in accordance with $\alpha_i = \sigma_x, \quad i\sigma_y$, or σ_z, the following results can be obtained:

$$\rho^{T-A}_{\sigma x(AE)i} = O\Big[\sqrt{p_{i(00)}}|1\rangle_{Ai}|e_i\rangle_{00} + \sqrt{p_{i(01)}}|0\rangle_{Ai}|e_i\rangle_{01}\Big] + p_{i(0v)}O\big[|\mathrm{vac}\rangle_{Ai}|e_i\rangle_{0v}\big] \tag{34}$$

$$\rho^{T-A}_{\sigma y(AE)i} = O\Big[\sqrt{p_{i(00)}}|1\rangle_{Ai}|e_i\rangle_{00} - \sqrt{p_{i(01)}}|0\rangle_{Ai}|e_i\rangle_{01}\Big] + p_{i(0v)}O\big[|\mathrm{vac}\rangle_{Ai}|e_i\rangle_{0v}\big] \tag{35}$$

$$\rho^{T-A}_{\sigma z(AE)i} = O\Big[\sqrt{p_{i(00)}}|0\rangle_{Ai}|e_i\rangle_{00} - \sqrt{p_{i(01)}}|1\rangle_{Ai}|e_i\rangle_{01}\Big] + p_{i(0v)}O\big[|\mathrm{vac}\rangle_{Ai}|e_i\rangle_{0v}\big] \tag{36}$$

Since an middle attacker cannot get any information from the $|\mathrm{vac}\rangle_{Ai}$, we can except the vacuum state from the joint state of Alice and Eve. Then, the state of Alice in the basis $\big\{|0\rangle_{Ai}|e_i\rangle_{00}, \quad |1\rangle_{Ai}|e_i\rangle_{01}\big\}$ becomes

$$\begin{aligned}\rho_{AE} &= \frac{1}{4}\Big\{\rho^{T-A}_{I(AE)i} + \rho^{T-A}_{\sigma x(AE)i} + \rho^{T-A}_{\sigma y(AE)i} + \rho^{T-A}_{\sigma z(AE)i}\Big\} \\ &= \begin{pmatrix} \frac{p_{i(00)}}{p_{i(00)}+p_{i(01)}} & 0 \\ 0 & \frac{p_{i(01)}}{p_{i(00)}+p_{i(01)}} \end{pmatrix}\end{aligned} \tag{37}$$

where $p_{i(00)} + p_{i(01)}$ is the efficiency of the TC–Alice channel. It can be estimated in experiment. We define $\eta_{tr} \equiv p_{i(00)} + p_{i(01)}$. An attacker, Eve's von Neumann entropies on Alice's encoding bit α_i (in step S-2), is

$$\begin{aligned}S\big(\alpha_i|AE\big) &= S\big(\rho_{\alpha i(AE)}\big) - S\big(\rho_{AE}\big) \\ &= 1 - H\bigg(\frac{p_{i(01)}}{\eta_{tr}}\bigg)\end{aligned} \tag{38}$$

where H is the Shannon's binary entropy.

The total system of Alice and Eve, ρ_{AE} on quantum channel from Alice to TC (Alice–TC channel) can be considered in two parts: TC gets the elements of the A sequence from Alice and not. We expressed these two events as $\rho^{(re)}_{AE}$ and $\rho^{(ure)}_{AE}$. The purpose of this section is to get the lower bound of $H(A|E)^{re}$ which means the conditional entropy of Alice on Eve in the case TC receives the elements of the A sequence back. Then, we have

$$S\big(\alpha_i|AE\big)^{re} = S\Big(\rho^{(re)}_{\alpha i(AE)}\Big) - S\Big(\rho^{(re)}_{AE}\Big) \tag{39}$$

$$S\left(\alpha_i|AE\right)^{ure}=S\left(\rho^{(ure)}_{\alpha i(AE)}\right)-S\left(\rho^{(ure)}_{AE}\right) \tag{40}$$

Note that two conditions which TC receives the qubit or not are orthogonal. We obtain

$$S\left(\rho_{\alpha i(AE)}\right)=\eta_{re}\,S\left(\rho^{(re)}_{\alpha i(AE)}\right)\;+\;\left(1-\eta_{re}\right)S\left(\rho^{(ure)}_{\alpha i(AE)}\right)\;+\;H\left(\eta_{re}\right) \tag{41}$$

$$S\left(\rho_{AE}\right)=\eta_{re}\,S\left(\rho^{(re)}_{AE}\right)\;+\;\left(1-\eta_{re}\right)S\left(\rho^{(ure)}_{AE}\right)\;+\;H\left(\eta_{re}\right) \tag{42}$$

where η_{re} is the efficiency of the Alice–TC channel. By above expressions,

$$S\left(\alpha_i|AE\right)=\eta_{re}S\left(\alpha_i|AE\right)^{re}+\;\left(1-\eta_{re}\right)S\left(\alpha_i|AE\right)^{ure} \tag{43}$$

We assume that Eve has maximal entropy of signer's secret information α_i in the case TC does not get the backward qubit from Alice. From Eq. (38), we obtain

$$S\left(\alpha_i|AE\right)^{re}\geq 1-\frac{H\left(\frac{p_{i(01)}}{\eta_{tr}}\right)}{\eta_{re}} \tag{44}$$

When combined with the case that the state sent by TC is $|1\rangle_{Ai}$, Eve's total entropy on signer is given by:

$$S\left(\alpha_i|AE\right)^{re}\geq 1-\frac{H\left(\frac{p_{i(01)}}{\eta_{tr}}\right)+H\left(\frac{p_{i(10)}}{\eta_{tr}}\right)}{2\eta_{re}} \tag{45}$$

It means that Eve's information on signature information can be bounded by the error rates in the TC–Alice channel and the efficiency of the Alice–TC channel. Therefore, the above equation shows that increasing the channel efficiency and lowering error rates enables safe QDS. The same discussion can also be developed on the channel between TC and verifiers (Bob, etc.).

TC and Alice (Bob) can estimate the error rate e. According to Ref. [44], the secure communication rate is given by:

$$R\geq S\left(\alpha_i|AE\right)^{re}\;-\;S\left(\alpha_i|TC\right)\;\geq 1-\frac{H\left(\frac{p_{i(01)}}{\eta_{tr}}\right)+H\left(\frac{p_{i(10)}}{\eta_{tr}}\right)}{2\eta_{re}}-H(e) \tag{46}$$

where $S\left(\alpha_i|TC\right)$ is the conditional entropy for signer's signature information to TC's information. According to Eqs. (45) and (46), the signature operator causes a phase randomization to Eve's accessed system, AE. It will limit the information that can be gained by attacker.

4 Conclusion

We proposed a secure and efficient QDS network, which allows a signer (Alice) to sign a message such that the signature can be validated by a number of different users. Multi-party verification is possible because all users are connected to the communication center with individual Bell states. The trusted center, TC, duly receives the signature from Alice and sends it to Bob(s) using secure quantum channel(s). Finally, the TC confirms that Bob's signature is correct. In our protocol, the TC provides non-repudiation by confirming the signature's transmission in real time. Our QDS scheme dramatically reduces the number of quantum channels. We used hash function to achieve security and efficiency; this function maps all inputs to messages of fixed length $2n$. In our QDS scheme, the message m that is to be signed is of arbitrary length.

Most protocols require more than four transmissions per each qubit [9–19], that is, from Alice to TC, from TC to Bob, from Bob to TC, and from TC to Alice. On the other hand, in our protocol, there are only two transmissions: from Alice to TC, and from TC to Bob. The signature and verification are completed by using the information on a public board. The public board information is shared by all legitimate users, including the publisher. Thus, the public board information is not likely to be altered by an (inner) attacker. We used QKD and a one-time pad (the random numbers) to guarantee unconditional security

Acknowledgements This work was supported by the R&D Convergence Program of NST (National Research Council of Science and Technology) of Republic of Korea (Grant No. CAP-18-08-KRISS) and by Basis Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (No. 2019R1I1A1A01042699).

References

1. Pfitzmann, B.: Sorting out signature schemes. In: CCS '93 Proceedings of the 1st ACM Conference on Computer and Communications Security, pp. 74–85 (1993)
2. Rivest, R.: Cryptography, pp. 717–775. Elsevier, Amsterdam (1990)
3. Rivest, R.L., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**, 120 (1978)
4. Shor, P.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Rev. **41**, 303 (1999)
5. Shor, P.W.: Algorithms for Quantum Computation: Discrete Logarithms and Factoring, pp. 20–22. IEEE Computer Society Press, Los Alamitos (1994)
6. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. **5**, 1484 (1997)
7. Gottesman, D., Chuang, I.L.: Quantum digital signatures. e-print arXiv:quant-ph/0105032 (2001)
8. Buhrman, H., Crepeaum C., Gottesmanm D., Smith, A., Tapp, A.: Authentication of quantum messages. In: Proceedings of 43rd Annual IEEE Symposium on the Foundations of Computer Science (FOCS '02), pp. 449–458 (2002)
9. Zeng, G.H., Keitel, C.H.: Arbitrated quantum-signature scheme. Phys. Rev. A **65**, 042312 (2002)
10. Curty, M., Lutkenhaus, N.: Comment on "Arbitrated quantum-signature scheme". Phys. Rev. A **77**, 046301 (2008)

11. Zeng, G.H.: Reply to “Comment on ‘Arbitrated quantum-signature scheme’”. Phys. Rev. A **78**, 016301 (2008)
12. Lee, H., Hong, C.H., Kim, H., Lim, J., Yang, H.J.: Arbitrated quantum signature scheme with message recovery. Phys. Lett. A **321**, 295 (2004)
13. Wang, J., Zhang, Q., Liang, L.M., Tang, C.J.: Comment on: “Arbitrated quantum signature scheme with message recovery”. Phys. Lett. A **347**, 262 (2005)
14. Li, Q., Chan, W.H., Long, D.Y.: Arbitrated quantum signature scheme using Bell states. Phys. Rev. A **79**, 054307 (2009)
15. Zou, X., Qiu, D.: Unextendible product bases and extremal density matrices with positive partial transpose. Phys. Rev. A **84**, 042325 (2010)
16. Yoon, C.S., Kang, M.S., Lim, J.I., Yang, H.J.: Quantum signature scheme based on a quantum search algorithm. Phys. Scr. **90**, 15103 (2015)
17. Zhang, P., Zhou, X.Q., Li, Z.W.: Identification scheme based on quantum teleportation for wireless communication networks. Acta Phys. Sin. **63**, 130301 (2014)
18. Clarke, P.J., Collins, R.J.: Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light. Nat. Commun. **3**, 1174 (2012)
19. Maurer, P.C., et al.: Room-temperature quantum bit memory exceeding one second. Science **336**, 1283 (2012)
20. Robert, J.C., Ross, J.D., Vedran, D., Petros, W., Patrick, J.C., Erika, A., John, J., Gerald, S.B.: Realization of quantum digital signatures without the requirement of quantum memory. Phys. Rev. Lett. **113**, 040502 (2014)
21. Ekert, A.: Quantum cryptography based on Bell’s theorem. Phys. Rev. Lett. **67**, 661 (1991)
22. Yang, Y.G., Zhou, Z., Teng, Y.W., Wen, Q.Y.: Arbitrated quantum signature with an untrusted arbitrator. Eur. Phys. J. D **61**, 773–778 (2011)
23. Liu, F., Zhang, K., Cao, T.: Security weaknesses in arbitrated quantum signature protocols. Int. J. Theor. Phys. **53**, 277 (2014)
24. Kang, M.S., Hong, C., Heo, J., Lim, J.I., Yang, H.J.: Quantum signature scheme using a single qubit rotation operator. Int. J. Theor. Phys. **54**, 614–629 (2015)
25. Luo, M.X., Chen, X.B., Yun, D., Yang, Y.X.: Quantum signature scheme with weak arbitrator. Int. J. Theor. Phys. **51**, 2135 (2012)
26. Kang, M.S., Choi, H.W., Pramanik, T., Han, S.W., Moon, S.: Universal quantum encryption for quantum signature using the swap test. Quantum Inf. Process. **17**, 254 (2018)
27. Boström, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. **89**, 187902 (2002)
28. Wójcik, A.: Eavesdropping on the “Ping-Pong” quantum communication protocol. Phys. Rev. Lett. **90**, 157901 (2003)
29. Pavičić, M.: In quantum direct communication an undetectable eavesdropper can always tell Ψ from Φ Bell states in the message mode. Phys. Rev. A **87**, 042326 (2013)
30. Menezes, A.J., van Oorschot, P.C., Vantone, S.A.: Handbook of Applied Cryptography. CRC Press, Boca Raton (1996)
31. Forouzan, B.A.: Cryptography and Network Security. Mcgraw Hill International Edition, New York (2007)
32. Kashefi, E., Kerenidis, I.: Statistical zero knowledge and quantum one-way functions. Theor. Comput. Sci. **378**(1), 101–116 (2007)
33. Luo, M.X., Chen, X.B., Yun, D., Yang, Y.X.: Quantum public-key cryptosystem. Int. J. Theor. Phys. **51**, 912–924 (2012)
34. Hwang, W.Y.: Quantum key distribution with high loss: toward global secure communication. Phys. Rev. Lett. **91**, 057901 (2003)
35. Deng, F.G., Long, G.L.: Controlled order rearrangement encryption for quantum key distribution. Phys. Rev. A **68**, 042315 (2003)
36. Branciard, C., Gisin, N., Kraus, B., Scarani, V.: Security of two quantum cryptography protocols using the same four qubit states. Phys. Rev. A **72**, 032301 (2005)
37. Li, C.Y., Li, X.H., Deng, F.G., Zhou, H.Y.: Efficient quantum secure communication with a publicly known key. Chin. Phys. B **17**, 2352 (2008)
38. Shen, D., Ma, W., Wang, L.: Two-party quantum key agreement with four-qubit cluster states. Quantum Inf. Process. **13**, 2313–2324 (2014)
39. Curty, M., Xu, F., Cui, W., Lim, C.C.W., Tamaki, K., Lo, H.: Finite-key analysis for measurement-device-independent quantum key distribution. Nat. Commun. **5**, 3732 (2014)

40. Zhang, M.H., Fi, H.F., Xia, Z.Q., Feng, X.Y.: Semiquantum secure direct communication using EPR pairs. Quantum Inf. Process. **16**, 117 (2017)
41. Stinson D.R.: Cyrptography: theory and practice, 3rd edn, pp. 281–316. Chapman and Hall/CRC (2005)
42. Lim, C.C.W., Curty, M., Walenta, N., Xu, F., Zbinden, H.: Concise security bounds for practical decoy-state quantum key distribution. Phys. Rev. A **89**, 022307 (2014)
43. Amiri, R., Wallden, P., Kent, A., Andersson, E.: Secure quantum signatures using insecure quantum channel. Phys. Rev. A **93**, 032325 (2016)
44. Devetak, I., Winter, A.: Distillation of secret key and entanglement from quantum states. Proc. R. Soc. Lond. A **461**, 207 (2005)