Quantum Information Processing (2021) 20:230
https://doi.org/10.1007/s11128-021-03162-5

A practical quantum designated verifier signature scheme for E-voting applications

Mengce Zheng[1,2] · Kaiping Xue[2] · Shangbin Li[2] · Nenghai Yu[2]

Received: 23 September 2020 / Accepted: 18 June 2021

Abstract
Although most of the quantum signatures can be verified by a designated receiver, they do not match the classical designated verifier signature since an indistinguishable signature cannot be efficiently simulated. To adapt quantum signatures in specific environments like E-voting and E-bidding, several quantum designated verifier signature (QDVS) schemes have been proposed. However, it is still too complicated and infeasible to implement existing QDVS schemes in practice. In this paper, we propose a practical QDVS scheme without entanglement for E-voting applications. It only involves the quantum processing part of the underlying quantum key distribution (QKD) to generate correlated key strings, which protects the communication against potential eavesdroppers. The proposed scheme can be easily and efficiently deployed over the existing QKD network without complicated quantum operations. We further show that our QDVS scheme satisfies the required main security requirements and has the capability against several common attacks.

Keywords Quantum signature · Designated verifier · Quantum key distribution · E-voting

1 Introduction

Digital signature is always used for verifying the authenticity of digital messages. To be specific, a valid digital signature scheme has the properties that anyone (called verifier) who knows the public key of the signer can verify the validity of a signature,

This work was partially supported by the National Natural Science Foundation of China under Grant No. 62002335 and Anhui Initiative in Quantum Information Technologies under Grant AHY150400.

✉ Mengce Zheng
mengce.zheng@gmail.com

[1] Zhejiang Wanli University, Ningbo, China

[2] University of Science and Technology of China, Hefei, China

Published online: 05 July 2021

and the verifier is confirmed that the digital message did not tamper in the communications. Digital signature is a widely used cryptographic tool for software distribution, financial transactions, and other cases requiring authenticity and integrity. The security of classical digital signature schemes is commonly based on several hardness assumptions of computational complexity like integer factorization and discrete logarithm. Hence these schemes will no longer be secure in the quantum era by using Shor's algorithm [1]. On the other hand, quantum mechanisms such as non-cloning property, measurement collapse, and the uncertainty principle provide nice fundamentals for unconditional security in the sense of information theory. In 2001, quantum digital signature (QDS) was firstly investigated by Gottesman and Chuang [2], and they constructed a quantum signature scheme using quantum one-way functions.

After that, many researchers have intensively studied various kinds of quantum digital signature schemes. The arbitrated quantum signature (AQS) schemes such as [3–9] are mainly studied in the field of quantum digital signatures. The quantum blind signature (QBS) scheme is another widely studied topic, which is proposed to meet the specific requirements of various application scenarios like electronic election and e-commerce. The QBS schemes were proposed in previous works like [10–13]. The quantum proxy signature (QPS) schemes such as [14–16] are also further studied. Moreover, some other (mixed) quantum signature schemes were proposed such as quantum group signature (QGS) scheme [17], quantum group blind signature (QGBS) scheme [18], and quantum proxy blind signature (QPBS) scheme [19].

However, a generic digital signature scheme cannot be applied in several special environments over the Internet. If it is used in e-commerce, suppose each bank issues and signs its own electronic money with public verifiability, anyone in each transaction knows the identity to who the electronic money belongs. Therefore, such information may lead to the leakage of some business secrets that will be further obtained by malicious adversaries. In this sense, there exists the collision of verifiability and privacy in the cases such as electronic election, online bidding and so on. Hence, the public verifiability of a usual digital signature is not desired in some special situations such as E-voting, E-bidding, and software distribution because the signer does not wish his/her receiver to transfer the belief of the signature to anyone else.

To solve the above problem, Jakobsson et al. [20] introduced the concept of designated verifier signature (DVS) scheme. A DVS scheme is a digital signature scheme with special security goals, which makes it possible to convince a designated verifier that a message was correctly signed by the sender and meanwhile this designated verifier cannot transfer the conviction to any third party. This security requirement is achieved using an efficient simulation algorithm of the designated verifier to generate a simulated signature that is indistinguishable from the real signature of the signer.

Although a designated verifier of the above quantum digital signature schemes can verify the signature by using the shared key with the signer, these schemes do not satisfy the definition of common DVS schemes. The reason is that the designated one is not able to explicitly and efficiently generate a simulated signature. To overcome this problem, a quantum designated verifier signature (QDVS) scheme was proposed in [21] using GHZ states, quantum one-way functions, and complicated quantum operations. Later, more QDVS schemes were proposed in [22,23] by converting existing schemes. But both of them use quantum entanglement and complicated quantum operations. To overcome the security drawbacks and improve the efficiency of previous QDVS schemes [21–23], Xin et al. [24,25] proposed more secure and efficient QDVS schemes. In their schemes, the partners need not use any quantum one-way function or perform any quantum state comparison.

Recently, QDS using quantum key distribution (QKD) technology achieves rapid developments as mentioned in [26]. It has attracted plenty of interest in both theory [27–29] and experiment [30–32]. While the QDS scheme presented in [2] needs nondestructive state comparison, longtime quantum memory, and a secure quantum channel for practical application, these problems were sequentially fixed in [30–32] and QDS further extended to more variants such as [33–35]. As for experiments, a more than 100-km QDS experiment was demonstrated based on a decoyed BB84 system [36] and DPS QKD [37], both of which are secure against a PNS attack. Moreover, MDI QDS schemes were implemented in both the laboratory [38] and field [39].

In this paper, based on the recent developments presented in [33], we propose a practical and efficient QDVS scheme without entanglement. We summarize the advantages as follows.

- We present the quantum designated verifier signature scheme with its main security properties and threat assumptions. In our QDVS scheme, only a designated verifier can verify the validity of a signature, and he/she cannot prove to a third party whether the received signature was produced by the signer or by himself/herself.
- We not only provide a new approach for constructing QDVS schemes but also provides useful properties of privacy protection required in the E-voting or E-bidding scenarios.
- Compared to previous schemes like [21,24,25], our QDVS scheme based on the quantum processing part of the QKD technology is simpler and more practical. Similar to [33], we remove all trust assumptions on the quantum channels, and the noise threshold for each quantum channel is less strict than for distilling a secret key using QKD. Thus, the proposed scheme can be easily deployed and implemented over the existing QKD network.

We mainly focus on the QDVS scheme for E-voting applications in this paper. The rest of the paper is organized as follows. In Sect. 2, we give a detailed description of our QDVS scheme. The security issues are analyzed and discussed in Sect. 3. In Sect. 4, we further apply the proposed QDVS scheme to E-voting scenarios. Finally, we conclude the paper in Sect. 5.

2 The proposed QDVS scheme

2.1 Overview

Our QDVS scheme involves four entities as follows. A signer Alice wants to send the message and its signature to a designated verifier. A designated verifier Bob will verify the signature from Alice. A malicious participant Eve aims to learn some useful information about the key strings or the signed messages through eavesdropping. The trusted center Trent controls and monitors the whole signing procedure. Trent only transmits communications between Alice and Bob and would not forge a member's signature in the domain.

The proposed QDVS scheme has the following design goals. Firstly, no one except the trusted center can learn any useful information about the content of a signed message. Secondly, all the signatures are verified by a designated verifier, who can efficiently generate a simulated signature that is indistinguishable from a signer's real signature. Thirdly, if a dispute happens, the trusted center can check what happened before and then deal with the signed message using the records.

The main QDVS procedure has three sequential phases, namely distribution, signing, and verification. To meet the specific requirement of the QDVS scheme, we require a simulation phase for generating an indistinguishable signature. The communication of the distribution phase involves both quantum and classical information transmission. The remaining phases only deal with the communication of classical information.

We briefly describe the QDVS scheme for signing on one-bit message m. In the distribution phase, Trent distributes correlated key strings between Alice and Bob using the key generation protocol (KGP). In the signing phase, Alice sends a pre-signature indicating the message to Trent and then Trent sends the real signature to the designated receiver Bob. In the verification phase, Bob calculates the mismatch rate between the received signature and his kept key strings. Bob accepts the signature if the mismatch rate is less than a small threshold. In the simulation phase, Bob can generate a simulated signature on the same message by using the simulation algorithm. A detailed description and a toy example are given below.

2.2 Key generation protocol

We modify the KGP that was introduced in [33] and aimed to perform the quantum part of the QKD technology to generate raw keys without error correction or privacy amplification. The underlying QKD is the prepare-and-measure decoy-state BB84 protocol using weak coherent pulses as described in [40]. When the KGP is performed by Trent, we assume that Trent has a phase-randomized source of coherent states. The intensity of each light pulse is decided by Trent to be u_1, u_2 or u_3 for $u_1 > u_2 > u_3$. The intensities are chosen due to predetermined probabilities p_{u_1}, p_{u_2} and p_{u_3}. We also use all intensity levels for KGP as showed in [40]. To encode bitstreams, Trent will randomly select one of the following four possible polarization states:

$$\begin{aligned}&|0_Z\rangle \text{ and } |1_Z\rangle \text{ for } Z \text{ basis},\\ &\quad |0_X\rangle = 1/\sqrt{2}\,(|0_Z\rangle + |1_Z\rangle) \text{ and } |1_X\rangle = 1/\sqrt{2}\,(|0_Z\rangle - |1_Z\rangle) \text{ for } X \text{ basis}.\end{aligned}$$

The X and Z bases are randomly chosen with probabilities $p_X \geq 1/2$ and $p_Z = 1 - p_X \leq 1/2$, respectively. Such asymmetric generating probabilities will increase the efficiency. Trent independently chooses intensities and states are to avoid correlations between intensity and stream encoding. Alice/Bob will choose the X and Z measurement bases with respective probabilities p_X and p_Z. For each received state, Alice/Bob derives one of four possible results $\{0, 1, \emptyset, d\}$, where 0 and 1 are two bit values, $\emptyset$ indicates no detection, and d means a double click event. If double clicks appear, Alice/Bob randomly chooses 0 or 1. Then the basis and intensity choices will be announced over an authenticated classical channel. If states are transmitted and measured in different bases, or if there is no detection, they are discarded. The protocol is executed until a sufficient number of measurement results have been obtained.

A raw preliminary key string is obtained by choosing a random sample of length $n+n_k$ of the X basis counts. The bit string generated by Alice (for example) can be split into three parts (X_A, Z_A, K_A^m) for $m = 0$ or 1. Trent holds the corresponding string (X_T, Z_T, C_A^m). The X string has length n_k and is derived from X basis measurements, which is used to estimate the correlation between Alice's and Trent's key strings. After that, the X strings will be discarded. The Z string is generated from Z basis measurements, which is used to quantify the level of eavesdropping by Eve. The K_A^m string of length n can be further split into E_A^m and $\tilde{E}_A^m$ strings of the same length $n/2$. We will explain how to deal with E_A^m and $\tilde{E}_A^m$ afterward.

One may refer to [33] for more details and its further security analysis. We roughly show the following security conclusion.

$$c_{X,0}^L + c_{X,1}^L[1 - h(\phi_{X,1}^U)] - h(p_E) = 0.$$

Here $c_{X,i}^L$ denotes the lower bound on the count rate for X basis pulses containing i photons. $\phi_{X,1}^U$ denotes the phase error rate in X basis measurements coming from single-photon pulses. The superscripts U and L denote worst-case scenario estimates consistent with parameter estimation performed on a finite sample. p_E is defined as the minimum rate at which Eve can make errors. Suppose the error rate on X basis measurements between Alice/Bob and Trent is upper bounded as e_X^U. We always have suitable parameters and a sufficiently large string length that makes KGP secure as long as $p_E > e_X^U$. In our QDVS scheme, KGP is used as an underlying protocol for the distribution phase.

2.3 Distribution phase

Step D1 The trusted center Trent uses KGP to generate correlated key strings shared between Alice and Bob, respectively. Thus, Alice-Trent and Bob-Trent will derive several bit strings as their private keys. For each possible message m, Alice has K_A^m while Trent has C_A^m, where key strings K_A^m and C_A^m are different but correlated. To be specific, we assume K_A^m and C_A^m are as follows.

$$K_A^m = (k_{A,1}^m, k_{A,2}^m, \ldots, k_{A,n}^m), \quad C_A^m = (c_{A,1}^m, c_{A,2}^m, \ldots, c_{A,n}^m). \tag{1}$$

In the same way, Bob has K_B^m while Trent has C_B^m as follows.

$$K_B^m = (k_{B,1}^m, k_{B,2}^m, \ldots, k_{B,n}^m), \quad C_B^m = (c_{B,1}^m, c_{B,2}^m, \ldots, c_{B,n}^m). \tag{2}$$

All the key strings are distributed using QKD technology through the quantum channel that has been proven unconditionally secure. Besides, the length of the above key strings is an even number n.

Step D2 Alice and Bob should exchange half of their private keys with the corresponding bit positions through authenticated classical channels via Trent. The exchanged bit positions are chosen uniformly at random by Trent using a locating function $L(\cdot)$. To be specific, it takes the time stamp TS_{AB} when Trent conducts KGP for Alice and Bob as the input. Its output $L(\mathsf{TS}_{AB})$ induces the exchange set $E = \{e_1, e_2, \dots, e_{n/2}\}$ of cardinality $n/2$ from the set $\{1, 2, \dots, n\}$. Trent then transfer E to Alice and Bob. For simplicity, we denote the complementary set

$$\tilde{E} := \{1, 2, \dots, n\} \setminus E = \{\tilde{e}_1, \tilde{e}_2, \dots, \tilde{e}_{n/2}\},$$

which will be used for privacy protection of the message to be signed.

Step D3 After Alice and Bob receive the exchange set E from Trent, Alice/Bob sends the key strings with respect to the bit positions in E that are assumed as

$$E_A^m = (k_{A,e_1}^m, k_{A,e_2}^m, \dots, k_{A,e_{n/2}}^m), \quad E_B^m = (k_{B,e_1}^m, k_{B,e_2}^m, \dots, k_{B,e_{n/2}}^m) \tag{3}$$

to Bob/Alice via Trent using the authenticated classical channels. The key strings they do not forward are respectively denoted by

$$\tilde{E}_A^m = (k_{A,\tilde{e}_1}^m, k_{A,\tilde{e}_2}^m, \dots, k_{A,\tilde{e}_{n/2}}^m), \quad \tilde{E}_B^m = (k_{B,\tilde{e}_1}^m, k_{B,\tilde{e}_2}^m, \dots, k_{B,\tilde{e}_{n/2}}^m). \tag{4}$$

Next, $\tilde{E}_A^m$ and E_B^m will be combined together into the final key strings S_A^m while $\tilde{E}_B^m$ and E_A^m contribute to S_B^m. Concretely, Alice fills those received bits into the bit positions contained in E in order and Bob does that in the same way. Finally, the key strings kept by Alice and Bob are as follows (assuming $\tilde{e}_1 < \cdots < e_1 < \cdots < e_{n/2} < \cdots < \tilde{e}_{n/2}$).

$$S_A^m = (s_{A,1}^m, \dots, s_{A,n}^m) = (k_{A,\tilde{e}_1}^m, \dots, k_{B,e_1}^m, \dots, k_{B,e_{n/2}}^m, \dots, k_{A,\tilde{e}_{n/2}}^m), \tag{5}$$

$$S_B^m = (s_{B,1}^m, \dots, s_{B,n}^m) = (k_{B,\tilde{e}_1}^m, \dots, k_{A,e_1}^m, \dots, k_{A,e_{n/2}}^m, \dots, k_{B,\tilde{e}_{n/2}}^m). \tag{6}$$

2.4 Signing phase

Step S1 Alice wants to sign a one-bit message m and send the signature to Bob. Alice first sends the pre-signature $\tilde{E}_A^{\mathsf{m}}$ to the trusted center Trent and asks for transferring the corresponding signature to Bob.

Step S2 Once Trent receives $\tilde{E}_A^{\mathsf{m}}$ from Alice, Trent figures out the message m, on which Alice wants to generate a signature by the distinguishing algorithm. To be specific, it outputs the correct value of m by comparing $\tilde{E}_A^{\mathsf{m}}$ with C_A^0 and C_A^1 on the bit positions in $\tilde{E}$. Trent calculates the mismatch rate $r_{A,T}^0$ between $\tilde{E}_A^{\mathsf{m}}$ and C_A^0 as

$$r_{A,T}^0 = \frac{\#\{\tilde{e}_i : k_{A,\tilde{e}_i}^{\mathsf{m}} \neq c_{A,\tilde{e}_i}^0,\ i = 1, 2, \dots, n/2\}}{n/2}, \tag{7}$$

and the mismatch rate $r^{1}_{A,T}$ between $\tilde{E}^{\mathsf{m}}_{A}$ and C^{1}_{A} as

$$r^{1}_{A,T}=\frac{\#\{\tilde{e}_i : k^{\mathsf{m}}_{A,\tilde{e}_i}\neq c^{1}_{A,\tilde{e}_i},\ i=1,2,\ldots,n/2\}}{n/2}. \tag{8}$$

Trent identifies $\mathsf{m}=0$ if $r^{0}_{A,T}<t$ or $\mathsf{m}=1$ if $r^{1}_{A,T}<t$, where t is a small threshold value determined by the underlying KGP. Finally, Trent records Alice's action for future dispute or repudiation.

Step S3 Trent sends $C^{\mathsf{m}}_{S}=(c^{\mathsf{m}}_{S,1},c^{\mathsf{m}}_{S,2},\ldots,c^{\mathsf{m}}_{S,n})$ as the signature on m from Alice to Bob. In detail, C^{m}_{S} is made up of $c^{\mathsf{m}}_{A,e_i}\oplus c^{\mathsf{m}}_{B,\tilde{e}_i}$ and $c^{1-\mathsf{m}}_{B,\tilde{e}_i}$ that are defined as

$$c^{\mathsf{m}}_{S,e_i}=c^{\mathsf{m}}_{A,e_i}\oplus c^{\mathsf{m}}_{B,\tilde{e}_i},\quad c^{\mathsf{m}}_{S,\tilde{e}_i}=c^{1-\mathsf{m}}_{B,\tilde{e}_i} \tag{9}$$

for $i=1,2,\ldots,n/2$, where $\oplus$ represents the XOR operation. Note that the message m needs not to be transmitted since Bob can figure out the correct value of m. Hence, we can guarantee the confidentiality of m to protect privacy.

2.5 Verification phase

Step V1 Bob receives C^{m}_{S} and know this received signature is generated from Alice on message m. To be specific, Bob uses the distinguishing algorithm to figure out the correct value of m by comparing

$$(c^{\mathsf{m}}_{S,\tilde{e}_1},c^{\mathsf{m}}_{S,\tilde{e}_2},\ldots,c^{\mathsf{m}}_{S,\tilde{e}_{n/2}})=(c^{1-\mathsf{m}}_{B,\tilde{e}_1},c^{1-\mathsf{m}}_{B,\tilde{e}_2},\ldots,c^{1-\mathsf{m}}_{B,\tilde{e}_{n/2}})$$

with $\tilde{E}^{0}_{B}$ and $\tilde{E}^{1}_{B}$. Bob calculates the mismatch rates

$$r^{0}_{T,B}=\frac{\#\{\tilde{e}_i : c^{1-\mathsf{m}}_{B,\tilde{e}_i}\neq k^{0}_{B,\tilde{e}_i},\ i=1,2,\ldots,n/2\}}{n/2}, \tag{10}$$

$$r^{1}_{T,B}=\frac{\#\{\tilde{e}_i : c^{1-\mathsf{m}}_{B,\tilde{e}_i}\neq k^{1}_{B,\tilde{e}_i},\ i=1,2,\ldots,n/2\}}{n/2}. \tag{11}$$

Bob knows $\mathsf{m}=1$ if $r^{0}_{T,B}<t$ or $\mathsf{m}=0$ if $r^{1}_{T,B}<t$, where t is the same small threshold value determined by the underlying KGP.

Step V2 Bob uses the corresponding key strings S^{m}_{B} that consist Alice's E^{m}_{A} and his own $\tilde{E}^{\mathsf{m}}_{B}$ to verify the validity of the received signature. To do so, Bob calculates the mismatch rate

$$r^{\mathsf{m}}=\frac{\#\{e_i : c^{\mathsf{m}}_{S,e_i}\neq s^{\mathsf{m}}_{B,e_i}\oplus s^{\mathsf{m}}_{B,\tilde{e}_i},\ i=1,2,\ldots,n/2\}}{n/2}. \tag{12}$$

Step V3 If the mismatch rate r^{m} is less than a small threshold value $2t$, Bob discovers the message m and accepts the signature on m. Otherwise, Bob rejects and claims to abort the protocol this time.

2.6 Simulation phase

Step F Bob can generate a simulated signature $F_S^m = (f_{S,1}^m, f_{S,2}^m, \ldots, f_{S,n}^m)$ that is indistinguishable from the real signature $C_S^m = (c_{S,1}^m, c_{S,2}^m, \ldots, c_{S,n}^m)$ via his knowledge of K_B^m. For simulating

$$c_{S,\tilde{e}_i}^m = c_{B,\tilde{e}_i}^{1-m},\ i = 1, 2, \ldots, n/2,$$

Bob modifies the remained $\tilde{E}_B^{1-m}$ through bit flipping on a random set $G \subset \tilde{E}$ as

$$f_{S,\tilde{e}_i}^m = k_{B,\tilde{e}_i}^{1-m},\ \tilde{e}_i \in \tilde{E} \backslash G, \quad f_{S,\tilde{e}_i}^m = 1 - k_{B,\tilde{e}_i}^{1-m},\ \tilde{e}_i \in G. \tag{13}$$

The flipping set G is chosen to satisfy the following equations

$$\frac{\#\{\tilde{e}_i : f_{S,\tilde{e}_i}^m \neq k_{B,\tilde{e}_i}^{1-m},\ i = 1, 2, \ldots, n/2\}}{n/2} < t, \tag{14}$$

$$\frac{\#\{\tilde{e}_i : f_{S,\tilde{e}_i}^m \neq c_{S,\tilde{e}_i}^m,\ i = 1, 2, \ldots, n/2\}}{n/2} < t. \tag{15}$$

For simulating

$$c_{S,e_i}^m = c_{A,e_i}^m \oplus c_{B,\tilde{e}_i}^m,\ i = 1, 2, \ldots, n/2,$$

Bob directly replaces c_{A,e_i}^m by k_{A,e_i}^m and modifies the kept $k_{B,\tilde{e}_i}^m$ to approach $c_{B,\tilde{e}_i}^m$. In more detail, Bob applies bit flipping on a random set $H \subset E$ as

$$f_{B,\tilde{e}_i}^m = k_{B,\tilde{e}_i}^m,\ \tilde{e}_i \in \tilde{E} \backslash H, \quad f_{B,\tilde{e}_i}^m = 1 - k_{B,\tilde{e}_i}^m,\ \tilde{e}_i \in H. \tag{16}$$

The flipping set H is designed to satisfy the following equations

$$\frac{\#\{e_i : f_{B,e_i}^m \neq k_{B,\tilde{e}_i}^m,\ i = 1, 2, \ldots, n/2\}}{n/2} < t, \tag{17}$$

$$\frac{\#\{e_i : k_{A,e_i}^m \oplus f_{B,\tilde{e}_i}^m \neq c_{S,e_i}^m,\ i = 1, 2, \ldots, n/2\}}{n/2} < 2t. \tag{18}$$

Hence, Bob uses

$$f_{S,e_i}^m = k_{A,e_i}^m \oplus f_{B,\tilde{e}_i}^m,\ i = 1, 2, \ldots, n/2, \tag{19}$$

and derives the simulated signature F_S^m.

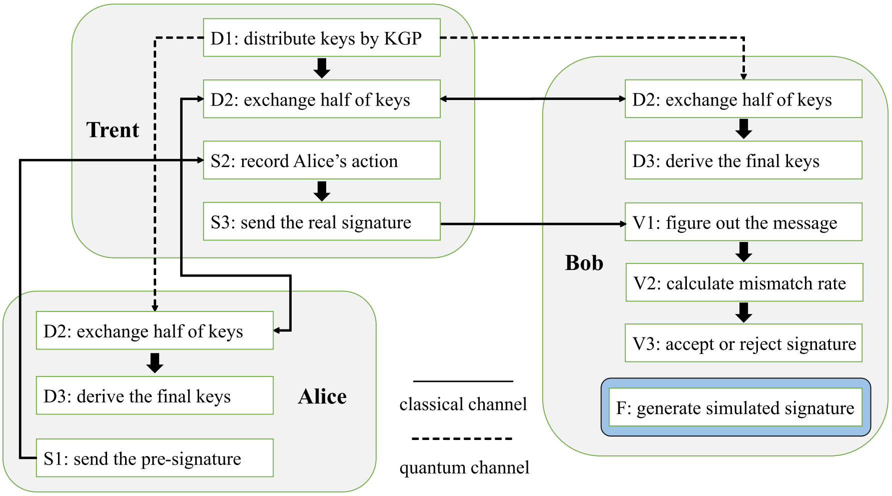
Trent
D1: distribute keys by KGP
D2: exchange half of keys
S2: record Alice's action
S3: send the real signature
Bob
D2: exchange half of keys
D3: derive the final keys
V1: figure out the message
V2: calculate mismatch rate
V3: accept or reject signature
F: generate simulated signature
Alice
D2: exchange half of keys
D3: derive the final keys
S1: send the pre-signature
classical channel
quantum channel

Fig. 1 The diagram of the proposed quantum designated verifier signature scheme

2.7 Toy example

We summarize the corresponding operations performed by each participant, namely Alice, Bob, and Trent in the QDVS process in Fig. 1.

For completeness and visualization, we provide a toy numerical example for further explanation to understand our QDVS scheme. Let public parameters be $n = 16$ and thus we have $n/2 = 8$. Let the small threshold value be $t = 15\%$. The whole QDVS procedure is stated as follows.

Step D1 The trusted center Trent uses KGP to distribute key strings. Alice and Trent hold different but correlated key strings K_A^m and C_A^m

$$K_A^0 = 0100111010110000, \quad K_A^1 = 1001011100100110,$$
$$C_A^0 = 0110111010110010, \quad C_A^1 = 1001010100101110.$$

Bob and Trent hold different but correlated key strings K_B^m and C_B^m

$$K_B^0 = 1000111001010011, \quad K_B^1 = 1100010010011110,$$
$$C_B^0 = 1000101001011011, \quad C_B^1 = 1100110010011111.$$

Step D2 Alice and Bob exchange half of their private keys through authenticated classical channels via Trent. The timestamp is $\mathsf{TS}_{AB} = 1614571200$ and the location function $L(\mathsf{TS}_{AB})$ outputs two sets

$$E = \{1, 2, 3, 4, 5, 6, 7, 8\}, \quad \tilde{E} = \{9, 10, 11, 12, 13, 14, 15, 16\}.$$

Step D3 Alice/Bob sends the private keys concerning E as

$$E_A^0 = 01001110,\ E_A^1 = 10010111, \quad E_B^0 = 10001110,\ E_B^1 = 11000100$$

to Bob/Alice. The key strings they do not forward are

$$\tilde{E}_A^0 = 10110000,\ \tilde{E}_A^1 = 00100110, \quad \tilde{E}_B^0 = 01010011,\ \tilde{E}_B^1 = 10011110.$$

The final keys kept by Alice and Bob are

$$\begin{aligned} S_A^0 &= 1000111010110000, \quad S_A^1 = 1100010000100110, \\ S_B^0 &= 0100111001010011, \quad S_B^1 = 1001011110011110. \end{aligned}$$

Step S1 Alice wants to sign a one-bit message $\mathsf{m} = 1$. Alice first sends the pre-signature $\tilde{E}_A^{\mathsf{m}} = 00100110$ to Trent.

Step S2 Once Trent receives 00100110 from Alice, Trent calculates the mismatch rates

$$\begin{aligned} r_{A,T}^0 &= \frac{\#\{00100110 \neq 10110010\}}{n/2} = \frac{3}{8} = 37.5\%, \\ r_{A,T}^1 &= \frac{\#\{00100110 \neq 00101110\}}{n/2} = \frac{1}{8} = 12.5\% \end{aligned}$$

Trent identifies $\mathsf{m} = 1$ since $r_{A,T}^1 = 12.5\% < t = 15\%$ and records Alice's action for future dispute or repudiation.

Step S3 Trent sends

$$C_S^{\mathsf{m}} = C_S^1 = (10010101 \oplus 10011111, 01011011) = 0000101001011011$$

as the signature from Alice to Bob.

Step V1 Once Bob receives 0000101001011011, he calculates the mismatch rates

$$\begin{aligned} r_{T,B}^0 &= \frac{\#\{01011011 \neq 01010011\}}{n/2} = \frac{1}{8} = 12.5\%, \\ r_{T,B}^1 &= \frac{\#\{01011011 \neq 10011110\}}{n/2} = \frac{3}{8} = 37.5\% \end{aligned}$$

Bob knows $\mathsf{m} = 1$ since $r_{T,B}^0 = 12.5\% < t = 15\%$.

Step V2 Bob finds the corresponding keys

$$S_B^{\mathsf{m}} = S_B^1 = 1001011110011110.$$

Bob checks the mismatch rate

$$r^1 = \frac{\#\{00001010 \neq 10010111 \oplus 10011110\}}{n/2}$$
$$= \frac{\#\{00001010 \neq 00001001\}}{n/2} = \frac{2}{8} = 25\%.$$

Step V3 Since the final mismatch rate $r^1 = 25\%$ is less than $2t = 30\%$, Bob finally knows $\mathsf{m} = 1$ and accepts the signature on m.

Step F Bob aims to generate the simulated signature

$$F_S^1 = (f_{S,1}^1, f_{S,2}^1, \ldots, f_{S,n}^1)$$

that is indistinguishable from the real signature $C_S^1 = 0000101001011011$. To simulate

$$c_{S,j}^1 = 0, 1, 0, 1, 1, 0, 1, 1, \;\; j = 9, 10, 11, 12, 13, 14, 15, 16.$$

Bob modifies $\tilde{E}_B^0 = 01010011$ via random bit flipping on $G = \{13\}$ and has

$$f_{S,j}^1 = 0, 1, 0, 1, 1, 0, 1, 1, \;\; j = 9, 10, 11, 12, 13, 14, 15, 16.$$

To simulate

$$c_{S,j}^1 = 0, 0, 0, 0, 1, 0, 1, 0, \;\; j = 1, 2, 3, 4, 5, 6, 7, 8.$$

Bob modifies $\tilde{E}_B^1 = 10011110$ via random bit flipping on $H = \{16\}$ and has

$$f_{B,j}^1 = 1, 0, 0, 1, 1, 1, 1, 1, \;\; j = 9, 10, 11, 12, 13, 14, 15, 16.$$

Then Bob combines $E_A^1 = 10010111$ with above 10011111 to compute

$$f_{S,j}^1 = 0, 0, 0, 0, 1, 0, 0, 0, \;\; j = 1, 2, 3, 4, 5, 6, 7, 8.$$

Finally, Bob obtains the simulated signature on message $m = 1$,

$$F_S^1 = 0000100001011011$$

that is a valid signature and can pass the verification phase.

3 Security analysis

3.1 Security properties

Before analyzing the security issues of the proposed QDVS scheme, we briefly mention the threat assumptions. We assume the malicious adversary Eve has the ability to eavesdropping over the quantum and classical channels. More precisely, Eve can eavesdrop, capture, and measure partial quantum information over the quantum channel. Eve has the chance to probabilistically catch and resend the quantum states. Eve is only assumed to eavesdrop but not to tamper classical information over the classical channel. Eve may conduct several common attacks such as forgery attack, inter-resend attack, and impersonation attack.

We refer to the security definitions in [41,42] and conclude the following security properties specified for our proposed QDVS scheme.

- *Designated verifiability* If the signer properly produces the signature under the signing procedure, then it should be correctly accepted by the designated verifier in the verification phase.
- *Unforgeability* It is infeasible for any adversary to forge a valid signature without the knowledge of the key strings of either the signer or the designated verifier.
- *Non-repudiation* After signing on the message, the signer cannot deny it. The trusted center can check the relative signing record to identify the creator of the signature.
- *Non-transferability* The designated verifier cannot transfer the conviction to any third party. In other words, the designated verifier cannot prove to any third party whether the signature was produced by the signer or by himself/herself.
- *Message-privacy* The message can only be recognized by the trusted center and the designated verifier, an adversary cannot learn any knowledge of this message.
- *Source-anonymity* Given a valid signature, it is infeasible to figure out the signature is produced by the original signer or the designated verifier even if the secret key strings are disclosed.

The security analysis is provided below to demonstrate that the proposed scheme is a designated verifier signature scheme with desired security properties. One may refer to [33] for more details and parameter constraints of the underlying KGP.

3.2 Designated verifiability

The designated verifiability is also regarded as the correctness of the proposed QDVS scheme. It means that the designated verifier Bob can simply check the validity of a signature by calculating the mismatch rate between the received signature and his kept key string.

As discussed in [33], KGP is built upon the underlying QKD protocol, which will be the prepare-and-measure decoy-state BB84 protocol [43] using weak coherent pulses as described in [40]. KGP has been proven secure with a sufficiently large n. The correctness of our proposed QDVS scheme is based on the security of KGP, which relates to the mismatch rates (10), (11), and (12) in the verifying phase.

Bob can correctly derive the value of the signed message due to calculation and comparison of the mismatch rates (10), (11). Once the signing procedure is properly executed, one of the judging conditions $r^0_{T,B} < t$ and $r^1_{T,B} < t$ must be satisfied, which implies the exact message signed by the signer. Afterwards, Bob applies the judging condition $r^{\mathsf{m}} < 2t$ and decide to accept or reject the signature. Based on the security analysis of KGP, the following inequalities hold.

$$\frac{\#\{e_i : c^{\mathsf{m}}_{A,e_i} \neq s^{\mathsf{m}}_{B,e_i},\ i = 1, 2, \ldots, n/2\}}{n/2} < t,$$
$$\frac{\#\{\tilde{e}_i : c^{\mathsf{m}}_{B,\tilde{e}_i} \neq s^{\mathsf{m}}_{B,\tilde{e}_i},\ i = 1, 2, \ldots, n/2\}}{n/2} < t.$$

As defined in (9), the XOR operation will increase the mismatch rate (12) to $2t$ at most. The judging condition $r^{\mathsf{m}} < 2t$ is suitable for checking the validity of the signature. Hence, the verifiability can be achieved when the proposed QDVS scheme runs honestly by Alice and Bob even if there exists an adversary Eve.

3.3 Unforgeability

The trusted center Trent transits all the keys between the signer Alice and the designated verifier Bob in our proposed QDVS scheme. Additionally, the keys are distributed using KGP based on QKD [43], which is proven unconditionally secure and a potential adversary cannot obtain any useful information of the private keys by eavesdropping. If an adversary attempts to catch any information from eavesdropping on the quantum channel, he/she will be detected because of the resulted disturbance.

It is infeasible for an adversary to learn some knowledge from the transited signature. As S^m_A and S^m_B are randomly created by Trent using (5) and (6) through the locating function with a private time stamp.

$$S^m_A = (k^m_{A,1}, \ldots, k^m_{B,e_1}, \ldots, k^m_{A,n/2}, \ldots, k^m_{B,e_{n/2}}, \ldots, k^m_{A,n}),$$
$$S^m_B = (k^m_{B,1}, \ldots, k^m_{A,e_1}, \ldots, k^m_{B,n/2}, \ldots, k^m_{A,e_{n/2}}, \ldots, k^m_{B,n}).$$

As defined in (9), the signature C^{m}_S consisting of $c^{\mathsf{m}}_{A,e_i} \oplus c^{\mathsf{m}}_{B,\tilde{e}_i}$ and $c^{1-\mathsf{m}}_{B,\tilde{e}_i}$ does not leak any useful information since c^{m}_{A,e_i}, $c^{\mathsf{m}}_{B,\tilde{e}_i}$ and $c^{1-\mathsf{m}}_{B,\tilde{e}_i}$ are secret. The possibility of a successful forgery is

$$\frac{1}{2^{n/2}} \times \frac{1}{2^{n/2}} = \frac{1}{2^n}$$

that will be negligible for a sufficiently large n. To guarantee strong security, the proposed QDVS scheme should be used as a one-time protocol.

The signature is unforgeable even by the signer Alice once she requested Trent to generate and transmit the signature. This is due to the action record of the trusted center Trent. It is an advantage of our proposed QDVS scheme and hence the replay attack fails.

3.4 Non-repudiation

Given a signature C_S^m as defined in (9), if this valid signature is sent from Alice, then she cannot deny it. With the help of the trusted center Trent, the signer's request will be recorded. In more detail, Alice aims to sign the message m and asks Trent for transferring its signature C_S^m to a designated verifier Bob. Since the correlated QKD keys (1)

$$K_A^m = (k_{A,1}^m, k_{A,2}^m, \ldots, k_{A,n}^m), \quad C_A^m = (c_{A,1}^m, c_{A,2}^m, \ldots, c_{A,n}^m)$$

are generated particularly for Alice, Trent confirms that the pre-signature

$$\tilde{E}_A^m = (k_{A,\tilde{e}_1}^m, k_{A,\tilde{e}_2}^m, \ldots, k_{A,\tilde{e}_{n/2}}^m)$$

defined in (4) is produced by Alice, not anyone else. Trent will check whether $m = 0$ or $m = 1$ by calculating the mismatch rates (7) and (8). Finally, Trent records Alice's request, which will be the evidence of her involvement.

3.5 Non-transferability

Bob can generate a simulated signature

$$F_S^m = (f_{S,1}^m, f_{S,2}^m, \ldots, f_{S,n}^m)$$

by using the simulation algorithm. As defined in (9), the received signature consists of

$$c_{S,e_i}^m = c_{A,e_i}^m \oplus c_{B,\tilde{e}_i}^m, \quad c_{S,\tilde{e}_i}^m = c_{B,\tilde{e}_i}^{1-m}.$$

Note that the crucial verification can be divided into two parts. The first part compares $c_{S,\tilde{e}_i}^m$ with $k_{B,\tilde{e}_i}^{1-m}$ to figure m. The second part compares c_{S,e_i}^m with $k_{A,e_i}^m \oplus k_{B,\tilde{e}_i}^m$ to verify the validity of the signature.

The following strategy is performed to derive the simulated signature F_S^m. As defined in (13), $f_{S,\tilde{e}_i}^m = k_{B,\tilde{e}_i}^{1-m}$ is directly used for simulating the first part under constraints (14) and (15), which ensure the correctness and indistinguishability. Concretely, direct replacement of $c_{S,\tilde{e}_i}^m$ by $f_{S,\tilde{e}_i}^m$ will not affect the verification of the simulated signature. At the same time, $c_{S,\tilde{e}_i}^m$ and $f_{S,\tilde{e}_i}^m$ are indistinguishable to any third party.

Similarly as defined in (16) and (19), $f_{S,e_i}^m = k_{A,e_i}^m \oplus f_{B,\tilde{e}_i}^m$ is designed for simulating the second part under constraints (17) and (18), which also ensure the correctness and indistinguishability. The mismatch rate r^m (12) of the simulated signature F_S^m for a signed message m will be less than $2t$ and F_S^m can be correctly verified. It means that the signature F_S^m simulated by Bob and the real one C_S^m generated by Alice are indistinguishable from each other. Bob cannot prove to any third party whether the signature is produced by Alice or by himself. Thus, non-transferability can be achieved via the simulation algorithm.

3.6 Message-privacy

To protect the privacy of the signed message m,

$$\tilde{E}_A^m = (k^m_{A,\tilde{e}_1}, k^m_{A,\tilde{e}_2}, \ldots, k^m_{A,\tilde{e}_{n/2}}), \quad \tilde{C}_B^{1-m} = (c^{1-m}_{B,\tilde{e}_1}, c^{1-m}_{B,\tilde{e}_2}, \ldots, c^{1-m}_{B,\tilde{e}_{n/2}})$$

are used in the pre-signature and signature, respectively. Thanks to the security guarantee of the underlying KGP, key strings K_A^m and C_B^{1-m} are secure and secret. Hence, $\tilde{E}_A^m$ (derived from K_A^m) and $\tilde{C}_B^{1-m}$ (derived from C_B^{1-m}) are also secure and secret before they are used.

Assuming the message to be signed is m, then $\tilde{E}_A^m$ will be transmitted from Alice to notice Trent which message needs to be signed. On the one hand, $\tilde{E}_A^m$ would not leak any information of C_A^m and C_B^m, which are later partially transmitted to Bob as the signature (9) by Trent. On the other hand, running the distinguishing algorithm (7), (8) on $\tilde{E}_A^m$ with respective C_A^0 and C_A^1 gives the correct value of m.

Similarly, $\tilde{C}_B^{1-m}$ is used to protect the privacy of the message m when the real signature is transmitted from Trent to Bob. On the one hand, $\tilde{C}_B^{1-m}$ would not leak any information of m. On the other hand, running the distinguishing algorithm (10), (11) on $\tilde{C}_B^{1-m}$ with respective $\tilde{E}_B^0$ and $\tilde{E}_B^1$ gives the correct value of m. Thus, the property of message-privacy can be achieved.

3.7 Source-anonymity

This property relates to non-transferability since both of them depend on the infeasibility of figuring out whether the signature is produced by the original signer Alice or the designated verifier Bob. By applying the simulation algorithm, Bob can generate a valid simulated signature F_S^m intended for himself, so even if any third party knows the shared keys of both Alice and Bob, it is still infeasible to identify whether the signature C_S^m is generated by Alice or Bob. The infeasibility is guaranteed by the constraints (15) and (18), (19).

$$\frac{\#\{\tilde{e}_i : f^m_{S,\tilde{e}_i} \neq c^m_{S,\tilde{e}_i},\ i = 1, 2, \ldots, n/2\}}{n/2} < t,$$
$$\frac{\#\{e_i : f^m_{S,e_i} \neq c^m_{S,e_i},\ i = 1, 2, \ldots, n/2\}}{n/2} < 2t.$$

Meanwhile, the correctness is guaranteed by the constraints (14) and (17).

$$\frac{\#\{\tilde{e}_i : f^m_{S,\tilde{e}_i} \neq k^{1-m}_{B,\tilde{e}_i},\ i = 1, 2, \ldots, n/2\}}{n/2} < t,$$
$$\frac{\#\{e_i : f^m_{B,e_i} \neq k^m_{B,\tilde{e}_i},\ i = 1, 2, \ldots, n/2\}}{n/2} < t.$$

Thus, we achieve the property of source-anonymity.

3.8 Attack resistance

In our proposed scheme, the quantum states are only transmitted in the distribution phase. Eve has the chance to catch the above quantum states when they are transmitted from Trent to Alice and Bob. However, Eve can never replicate those quantum bits and the decoy states ensure the security of the quantum states. Consequently, any effective attack will be discovered by the legal members. From the above analysis, it can be seen that Eve cannot elicit any helpful information from the transmitted strings if Eve does not want to bring any disturbance to the decoy states. In this condition, Eve can obtain nothing about K^m_A, C^m_A (1) and K^m_B, C^m_B (2). Though E is transmitted over the classical channel and E^m_A (3) may leak to Eve, $\tilde{E}^m_A$ (4) is kept secret and secure, which ensures the security of the transmitted pre-signature. On the other hand, C^m_A and C^m_B kept by Trent are secret, which ensures the security of the transmitted signature C^m_S (9).

Furthermore, we demonstrate that the proposed QDVS scheme is secure against several common attacks such as forgery attack, inter-resend attack, and impersonation attack as follows.

3.8.1 Security against forgery attack

Similar to the discussion of the unforgeability property above, C^m_A and C^m_B are used to sign a message m according to the signing phase. However, it is impossible for an adversary to obtain C^m_A, C^m_B and K^m_A, K^m_B from the quantum communication according to the above security analysis. Furthermore, to generate a forged signature, the adversary may apply a similar simulation algorithm. In this case, the private key strings K^m_B have to be used as defined in (13) and (16). More precisely, the simulated signature F^m_S consists of f^m_{S,e_i} and $f^m_{S,\tilde{e}_i}$ defined in (13) and (19). f^m_{S,e_i} and $f^m_{S,\tilde{e}_i}$ are generated using $\tilde{E}^m_B$ and $\tilde{E}^{1-m}_B$ that does not leak any useful information since they are kept secret. Thus, the adversary needs to guess each bit of a n-bit string to carry out a successful forgery attack. This possibility is $1/2^n$ that is negligible for a sufficiently large n.

To guarantee security against forgery attack, the proposed QDVS scheme should be used as a one-time protocol. Therefore, it is infeasible for the adversary to forge a valid signature without knowledge of C^m_A, C^m_B and K^m_B.

3.8.2 Security against inter-resend attack

In our proposed scheme, Trent sends the quantum sequences using KGP to Alice and Bob, respectively. An adversary Eve may intercept and replace some of the particles with other states and then resend them to Alice and Bob. However, notice KGP inserts decoy particles into the quantum sequences for checking eavesdropping actions. The adversary's eavesdropping actions or tampering with the transmitted quantum bits will inevitably disturb part of the decoy particles. Therefore, the eavesdropping actions or tampering on the quantum channels must be discovered by Alice and Bob. It is infeasible for Eve to eavesdrop and tamper with the quantum bits transmitted in the quantum channels. Hence, the adversary's inter-resend attack on the quantum sequences must be discovered by Alice and Bob.

Since it is infeasible to eavesdrop or tamper with the quantum channels, an adversary tries to intercept and resend the classical messages transmitted in the classical channel under our QDVS scheme. However, Bob can discover the adversary's resending action since the same signature has been received before. Hence, the adversary's inter-resend attack would not affect the security.

3.8.3 Security against impersonation attack

An adversary Eve may impersonate the signer Alice, the designated verifier Bob or even the trusted center Trent during the whole signature procedure. Firstly, Eve can't impersonate Trent to forge the valid key strings K_A^m, K_B^m during the distribution phase. The reason is that only the trusted center Trent has sufficient resources to launch quantum communication for all other participants. Thus, without knowing the private key strings, it is infeasible for Eve to do the following steps. Even if Eve successfully know K_A^m, C_A^m (5) and K_B^m, C_B^m (6), it is infeasible for Eve to compute the exchange set E without using Trent's secret time stamp TS_{AB}. Therefore, this kind of impersonation attack is infeasible for the adversary.

Secondly, if Eve wants to impersonate Alice to forge effective authentication information, as the same as the above analysis of the forgery attack, the proposed QDVS scheme can withstand the impersonation sender attack. The reason is that Eve cannot forge the valid $\tilde{E}_A^m$ without knowing Alice's secret K_A^m.

Thirdly, if Eve wants to impersonate the intended designated receiver Bob in order to verify the signature generated by Alice, the proposed QDVS scheme can withstand the impersonation receiver attack because a valid signature can only be verified by Bob using his key strings S_B^m and K_B^m. Furthermore, only Bob can figure out the message m that is signed by Alice using his secret K_B^m. As a result, the adversary's impersonation attack would not affect the security of the proposed QDVS scheme.

4 The application to E-voting

We concentrate on the application scenario of binary (Yes/No) E-voting, where a ballot of the one-bit message, namely bit 0 or 1, will be signed and verified. Quantum voting protocol is extensively studied in the field of quantum information and its application. Hillery et al. [44] presented the traveling ballot and distributed ballot schemes for quantum voting. Later, quantum voting protocols based on quantum teleportation, quantum entanglement and other techniques were proposed in [45–55]. Recently, Joy et al. [56] showed the implementation of a new quantum binary voting protocol in the IBM quantum computer. One may refer to [57] for a different but comprehensive theoretical analysis of quantum E-voting protocols. Most of the above voting protocols make use of quantum entanglement, which is difficult to maintain due to decoherence effects. Therefore, getting rid of the entanglement requirement is a significant step toward the practical realization of the quantum voting protocols.

We start with the quantum E-voting system and then describe the corresponding binary E-voting protocol equipped with our proposed QDVS scheme. Hence, this new binary E-voting protocol is more efficient, which can be deployed over the existing QKD network.

4.1 Quantum E-voting system

Consider using the proposed QDVS scheme for E-voting, where each participant is connected with a trusted center equipped with a noisy untrusted quantum channel and an authenticated classical channel. Several specific properties of the quantum E-voting system are described as follows.

- The trusted center has sufficient quantum resource and computation capability while all the participators in the same domain have limited resources.
- All the participants share distributed and correlated key strings with each other by performing the quantum part of QKD through the trusted center.
- A predetermined participant serves as the initiator and the ballot collector to launch electronic voting. The trusted center broadcasts the voting content as a judgment question to other participants.
- Other potential participants create their pre-signatures of a one-bit answer, where bit 1 (Yes) stands for approval or bit 0 (No) for disapproval as their ballots.
- The participants send their pre-signatures to the trusted center and ask for sending the real signatures to the ballot collector.
- The ballot collector gathers all the signatures and finally counts the number of issued ballots, which completes the voting procedure.

4.2 Quantum binary E-voting protocol

We assume the quantum E-voting system consists of the following entities: N voter A_i for $i = 1, 2, \ldots, N$, a tally clerk Bob and the trusted voting center Trent. Here ID_{A_i} are strings of length u, where $u := \lceil \log_2 N \rceil$ is determined by the number of potential participants N.

Each voter can choose his/her preferred answer for the broadcast question ID_e of length ℓ. The voting results of all the votes are counted by the tally clerk Bob, who counts the received answers and check the validity of their signatures. Then based on the number of votes, Bob selects the final winning judgment option and announces the result. The specific steps of the quantum binary E-voting protocol are as follows.

4.2.1 Initialization phase

Step I1 The trusted voting center Trent sets up a bulletin board for all the participants and announces N, ID_{A_i} and ID_e on it.

Step I2 A voter A_i sends an application for registration to Trent, who verifies A_i's identity and voting qualifications. After that, Trent stores A_i's relative information.

Step I3 Trent chooses a sufficiently large security parameter n to conduct our proposed QDVS scheme. For each A_i and tally clerk Bob, Trent generates respective key strings using KGP. According to the process in the distribution phase of the QDVS scheme, A_i and Bob hold correlated secret key strings, respectively.

Step I4 Trent begins to ask for a ballot from the voter A_i. The form of a ballot is a one-bit message $\mathsf{0}$ or $\mathsf{1}$. Moreover, Trent just asks for a signature of the ballot since its privacy is protected in our QDVS scheme. The generation of the signature is described in Sect. 2.

4.2.2 Voting phase

Step V1 After receiving Trent's voting notification, A_i makes his/her answer m and generates its pre-signature $\mathsf{pSig}_i^{\mathsf{m}}$ following the process in the signing phase of the QDVS scheme.

Step V2 Once Trent receives $\mathsf{pSig}_i^{\mathsf{m}}$ from A_i, Trent figures out the message m and records $(\mathsf{ID}_{A_i}, \mathsf{ID}_B, \mathsf{ID}_e, \mathsf{m})$ for future dispute or repudiation.

Step V3 Trent sends the real signature $\mathsf{Sig}_i^{\mathsf{m}} = C_S^{\mathsf{m}}$ along with identification information $\mathsf{ID}_{A_i}, \mathsf{ID}_e$ to Bob. If Trent detects eavesdropping from an adversary over the communication channel or finds malicious attacks, the vote procedure will be aborted.

4.2.3 Counting phase

Step C1 Bob receives $(C_S^{\mathsf{m}}, \mathsf{ID}_{A_i}, \mathsf{ID}_e)$ from Trent, then Bob know this received signature is actually generated from A_i on message m.

Step C2 Bob searches the private keys and finds the corresponding keys. Bob then check the validity of the signature C_S^{m}. After confirming the correctness, Bob records A_i's answer to event ID_e.

Step C3 After N participants A_i for $i = 1, 2, \ldots, N$ have finished voting, Bob publishes the final voting results and the corresponding ID_{A_i} on the bulletin board for further checking the availability. Finally, Bob counts all the voting results and announces the winning judgment option on the bulletin board.

5 Conclusion

In this paper, we propose a practical quantum designated verifier signature scheme without entanglement based on quantum key distribution technology. Compared to previous QDVS schemes [21–25], our proposed scheme is also unconditional secure (based on underlying QKD) and has the property that only a verifier designated can verify the validity of a signature. The designated verifier has the capability of efficiently simulating a signature that is indistinguishable from that of the signer.

Additionally, our proposed QDVS scheme has the following advantage. It depends on much simpler operations that only consist of the quantum part of the quantum key distribution procedure and other classical bit operations. As a result, our QDVS scheme requires less computation and resource consumption and thus is more efficient and concise than previous QDVS ones. Moreover, as mentioned in [33], all trust assumptions on the quantum channels can be removed, and the noise threshold for each quantum channel is less strict than for distilling a secret key using QKD. Thus, our QDVS scheme can be easily deployed over the existing QKD network for E-voting applications. In contrast, the disadvantage of our scheme is the heavy reliance on the trusted center.

The proposed QDVS scheme meets the desired security demands, namely verifiability, unforgeability, non-repudiation, non-transferability, and source-anonymity. We give detailed security analysis and show that the proposed QDVS scheme can resist major attacks such as forgery attack, inter-resend attack, and impersonation attack.

As an application of our QDVS scheme, we show how to embed it in specific environments like E-voting. We describe the quantum E-voting system and present a simple quantum binary E-voting protocol.

References

1. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Rev. **41**(2), 303 (1999)
2. Gottesman, D., Chuang, I.: Quantum Digital Signatures. arXiv preprint arXiv:quant-ph/0105032 (2001)
3. Zeng, G., Keitel, C.H.: Arbitrated quantum-signature scheme. Phys. Rev. A **65**(4), 042312 (2002)
4. Li, Q., Chan, W.H., Long, D.Y.: Arbitrated quantum signature scheme using Bell states. Phys. Rev. A **79**(5), 054307 (2009)
5. Li, Q., Li, C., Long, D., Chan, W.H., Wang, C.: Efficient arbitrated quantum signature and its proof of security. Quantum Inf. Process. **12**(7), 2427 (2013)
6. Liu, F., Qin, S.J., Su, Q.: An arbitrated quantum signature scheme with fast signing and verifying. Quantum Inf. Process. **13**(2), 491 (2014)
7. Li, F.G., Shi, J.H.: An arbitrated quantum signature protocol based on the chained CNOT operations encryption. Quantum Inf. Process. **14**(6), 2171 (2015)
8. Yang, Y.G., Lei, H., Liu, Z.C., Zhou, Y.H., Shi, W.M.: Arbitrated quantum signature scheme based on cluster states. Quantum Inf. Process. **15**(6), 2487 (2016)
9. Feng, Y., Shi, R., Shi, J., Zhou, J., Guo, Y.: Arbitrated quantum signature scheme with quantum walk-based teleportation. Quantum Inf. Process. **18**(5), 154 (2019)
10. Wang, M., Chen, X., Yang, Y.: A blind quantum signature protocol using the GHZ state. Sci.China Phys. Mech. Astron. **56**(9), 1636 (2013)
11. Khodambashi, S., Zakerolhosseini, A.: A sessional blind signature based on quantum cryptography. Quantum Inf. Process. **13**(1), 121 (2014)
12. Shi, W.M., Zhang, J.B., Zhou, Y.H., Yang, Y.G.: A new quantum blind signature with unlinkability. Quantum Inf. Process. **14**(8), 3019 (2015)
13. Lai, H., Luo, M., Pieprzyk, J., Qu, Z., Li, S., Orgun, M.A.: An efficient quantum blind digital signature scheme. Sci. China Inf. Sci. **60**(8), 082501 (2017)
14. Zhou, J., Zhou, Y., Niu, X., Yang, Y.: Quantum proxy signature scheme with public verifiability. Sci. China Phys. Mech. Astron. **54**(10), 1828 (2011)

15. Wang, T.Y., Wei, Z.L.: One-time proxy signature based on quantum cryptography. Quantum Inf. Process. **11**(2), 455 (2012)
16. Qin, H., Tang, W.K., Tso, R.: Efficient quantum multi-proxy signature. Quantum Inf. Process. **18**(2), 53 (2019)
17. Xu, G.B., Zhang, K.J.: A novel quantum group signature scheme without using entangled states. Quantum Inf. Process. **14**(7), 2577 (2015)
18. Xu, R., Huang, L., Yang, W., He, L.: Quantum group blind signature scheme without entanglement. Opt. Commun. **284**(14), 3654 (2011)
19. Guo, W., Xie, S.C., Zhang, J.Z.: A novel quantum proxy blind signature scheme. Int. J. Theor. Phys. **56**(5), 1708 (2017)
20. Jakobsson, M., Sako, K., Impagliazzo, R.: Designated Verifier Proofs and Their Applications. in Advances. In: Maurer, U. (ed.) Cryptology – EUROCRYPT'96, pp. 143–154. Springer, Berlin, (1996)
21. Shi, W.M., Zhou, Y.H., Yang, Y.G.: A real quantum designated verifier signature scheme. Int. J. Theor. Phys. **54**(9), 3115 (2015)
22. Shi, W.M., Wang, Y.M., Zhou, Y.H., Yang, Y.G., Zhang, J.B.: A scheme on converting quantum signature with public verifiability into quantum designated verifier signature. Optik **164**, 753 (2018)
23. Shi, S., Wei-Min Wang, Y.M., Wang, Y.H., Zhou, Y.G.Yang: A scheme on converting quantum deniable authentication into universal quantum designated verifier signature. Optik **190**, 10 (2019)
24. Xin, X., Wang, Z., Yang, Q., Li, F.: Identity-based quantum designated verifier signature. Int. J. Theor. Phys. **59**, 1–12 (2020)
25. Xin, X., Wang, Z., Yang, Q., Li, F.: Quantum designated verifier signature based on Bell states. Quantum Inf. Process. **19**(3), 1 (2020)
26. Xu, F., Ma, X., Zhang, Q., Lo, H.K., Pan, J.W.: Secure quantum key distribution with realistic devices. Rev. Mod. Phys. **92**(2), 025002 (2020)
27. Andersson, E., Curty, M., Jex, I.: Experimentally realizable quantum comparison of coherent states and its applications. Phys. Rev. A **74**, 022304 (2006). https://doi.org/10.1103/PhysRevA.74.022304
28. Dunjko, V., Wallden, P., Andersson, E.: Quantum digital signatures without quantum memory. Phys. Rev. Lett. **112**(4), 040502 (2014)
29. Wallden, P., Dunjko, V., Kent, A., Andersson, E.: Quantum digital signatures with quantum-key-distribution components. Phys. Rev. A **91**(4), 042304 (2015)
30. Clarke, P.J., Collins, R.J., Dunjko, V., Andersson, E., Jeffers, J., Buller, G.S.: Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light. Nat. Commun. **3**(1), 1 (2012)
31. Collins, R.J., Donaldson, R.J., Dunjko, V., Wallden, P., Clarke, P.J., Andersson, E., Jeffers, J., Buller, G.S.: Realization of quantum digital signatures without the requirement of quantum memory. Phys. Rev. Lett. **113**(4), 040502 (2014)
32. Donaldson, R.J., Collins, R.J., Kleczkowska, K., Amiri, R., Wallden, P., Dunjko, V., Jeffers, J., Andersson, E., Buller, G.S.: Experimental demonstration of kilometer-range quantum digital signatures. Phys. Rev. A **93**, 012309 (2016). https://doi.org/10.1103/PhysRevA.93.012329
33. Amiri, R., Wallden, P., Kent, A., Andersson, E.: Secure quantum signatures using insecure quantum channels. Phys. Rev. A **93**(3), 032325 (2016)
34. Yin, H.L., Fu, Y., Chen, Z.B.: Practical quantum digital signature. Phys. Rev. A **93**(3), 032316 (2016)
35. Zhang, H., An, X.B., Zhang, C.H., Zhang, C.M., Wang, Q.: High-efficiency quantum digital signature scheme for signing long messages. Quantum Inf. Process. **18**(1), 3 (2019)
36. Yin, H.L., Fu, Y., Liu, H., Tang, Q.J., Wang, J., You, L.X., Zhang, W.J., Chen, S.J., Wang, Z., Zhang, Q., et al.: Experimental quantum digital signature over 102 km. Phys. Rev. A **95**(3), 032334 (2017)
37. Collins, R.J., Amiri, R., Fujiwara, M., Honjo, T., Shimizu, K., Tamaki, K., Takeoka, M., Andersson, E., Buller, G.S., Sasaki, M.: Experimental transmission of quantum digital signatures over 90 km of installed optical fiber using a differential phase shift quantum key distribution system. Opt. Lett. **41**(21), 4883 (2016)
38. Roberts, G.L., Lucamarini, M., Yuan, Z.L., Dynes, J.F., Comandar, L.C., Sharpe, A.W., Shields, A.J., Curty, M., Puthoor, I.V., Andersson, E.: Experimental measurement-device-independent quantum digital signatures. Nat. Commun. **8**(1), 1 (2017)
39. Yin, H.L., Wang, W.L., Tang, Y.L., Zhao, Q., Liu, H., Sun, X.X., Zhang, W.J., Li, H., Puthoor, I.V., You, L.X., Andersson, E., Wang, Z., Liu, Y., Jiang, X., Ma, X., Zhang, Q., Curty, M., Chen, T.Y., Pan, J.W.: Experimental measurement-device-independent quantum digital signatures over a metropolitan network. Phys. Rev. A **95**, 042338 (2017). https://doi.org/10.1103/PhysRevA.95.042338

40. 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**(2), 022307 (2014)
41. Kang, B., Boyd, C., Dawson, E.: A novel identity-based strong designated verifier signature scheme. J. Syst. Software **82**(2), 270 (2009)
42. Lee, J.S., Chang, J.H., Lee, D.H.: Arbitrated quantum signature scheme using Bell states. Comput. Electr. Eng. **36**(5), 948 (2010)
43. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. Theor. Comput. Sci. **560**(12), 7 (2014)
44. Hillery, M., Ziman, M., Bužek, V., Bieliková, M.: Towards quantum-based privacy and voting. Phys. Lett. A **349**(1–4), 75 (2006)
45. Tian, J.H., Zhang, J.Z., Li, Y.P.: A voting protocol based on the controlled quantum operation teleportation. Int. J. Theor. Phys. **55**(5), 2303 (2016)
46. Thapliyal, K., Sharma, R.D., Pathak, A.: Protocols for quantum binary voting. Int. J. Quantum Inf. **15**(01), 1750007 (2017)
47. Xue, P., Zhang, X.: A simple quantum voting scheme with multi-qubit entanglement. Sci. Rep. **7**(1), 1 (2017)
48. Zhang, J.L., Xie, S.C., Zhang, J.Z.: An elaborate secure quantum voting scheme. Int. J. Theor. Phys. **56**(10), 3019 (2017)
49. Cao, H.J., Ding, L.Y., Jiang, X.L., Li, P.F.: A new proxy electronic voting scheme achieved by six-particle entangled states. Int. J. Theor. Phys. **57**(3), 674 (2018)
50. Niu, X.F., Zhang, J.Z., Xie, S.C., Chen, B.Q.: An improved quantum voting scheme. Int. J. Theor. Phys. **57**(10), 3200 (2018)
51. Wang, S.L., Zhang, S., Wang, Q., Shi, R.H.: Fault-tolerant quantum anonymous voting protocol. Int. J. Theor. Phys. **58**(3), 1008 (2019)
52. Jiang, D.H., Wang, J., Liang, X.Q., Xu, G.B., Qi, H.F.: Quantum voting scheme based on locally indistinguishable orthogonal product states. Int. J. Theor. Phys. **59**(2), 436 (2020)
53. Zhang, X., Zhang, J.Z., Xie, S.C.: A secure quantum voting scheme based on quantum group blind signature. Int. J. Theor. Phys. **59**(3), 719 (2020)
54. Zhou, B.M., Zhang, K.J., Zhang, X., Wang, Q.L.: The cryptanalysis and improvement of a particular quantum voting model. Int. J. Theor. Phys. **2020**, 1–12 (2020)
55. Li, Y.R., Jiang, D.H., Zhang, Y.H., Liang, X.Q.: A quantum voting protocol using single-particle states. Quantum Inf. Process. **20**(3), 1 (2021)
56. Joy, D., Sabir, M., Behera, B.K., Panigrahi, P.K.: Implementation of quantum secret sharing and quantum binary voting protocol in the IBM quantum computer. Quantum Inf. Process. **19**(1), 1 (2020)
57. Arapinis, M., Kashefi, E., Lamprou, N., Pappa, A.: Definitions and Analysis of Quantum E-voting Protocols. arXiv preprint arXiv:1810.05083 (2018)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.