INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE
A. Aktaş et al., Vol.12, No.3, pp.14-28.
https://doi.org/10.55859/ijiss.1294840

High Dimensional Quantum Digital Signature Depending on Entanglement Swapping

Arzu Aktaş [1], İhsan Yılmaz [2]

[1] School of Graduate Studies, Çanakkale Onsekiz Mart University, Çanakkale, Turkiye
[2] Department of Computer Engineering, Çanakkale Onsekiz Mart University, Çanakkale, Turkiye
Corresponding Author: aktas_arzu@hotmail.com

Research Paper Received: 21.05.2023 Revised: 24.07.2023 Accepted: 06.09.2023

Abstract—While a single qubit information can be carried with a single photon in $2-$dimensional quantum technology, it is possible to carry more than one qubit information with a single photon in high-dimensional quantum technologies. The amount of qubit to be transported depends on the size of the system obtained in the high dimension. In other words, the more high-dimensional quantum structure it creates, the more qubit-carrying system is obtained. In this study, a high dimensional quantum digital signature(QDS) scheme is proposed for multi-partied by using entanglement swapping and super-dense coding. QDS, which is proposed as high-dimensional, allows more data and high-rate keys to be transferred. Security analysis of propesed QDS in high-dimensional show that the propablity of anyone obtaining information is much lower than in qubit states. Since all data(quantum and classic) in this protocol is instantly sent by using entanglement channels it is more resilient eavesdropping attacks. Today, developments in high-dimensional experimental studies show that the high-dimensional QDS proposed in this study can be implemented practically.

Keywords—Quantum digital signature, high dimension, entanglement swapping, superdence coding

1. Introduction

Quantum digital signature is essential for both quantum cryptography and secure quantum communication. QDS was first defined by Gottesman and Chuang [1]. There are many studies on QDS in the literature. This is the quantum version of the classical digital signatures[2] by using quantum effects. In 2018, Zhao et al. [3] have proposed a new multiparty quantum key agreement protocol with the entanglement swapping. In 2019, Li et al. [4] have created an efficient quantum custom comparison protocol with entanglement change. Cai et al. [5] have studied cryptanalysis of a multi-part quantum digital signature scheme and then a new attack strategy. In 2015, a blind signature with quantum entanglement was put forward by Zhang and Li [6]. In 2019, Qu et al. [7] have researched a multiparty public QDS scheme that could effectively deal with the problem of unnecessary quantum connections. Huawang et al. [8] in 2020 have suggested a quantum (t, n) threshold group signature. Weng et al. [9] have suggested an effective multipart QDS framework to overcome

these challenges based on a six-state non-orthogonal coding protocol. The number of quantum channels in their protocol depends only on the number of users linearly.

In addition to these studies, quantum digital signatures have been started experimentally due to the development of quantum technologies. Clarke et al. [10] have demonstrated an experiment that quantum digital signatures allow sending messages from one sender to two receivers, guaranteed against forgery and rejection. For classical messages, Wang et al. [11] show that the security of quantum digital signatures. Yin et al. [12] have presented a quantum digital signature protocol that removes the assumption of authenticated quantum channels and is secure against attacks. In 2017, Yin et al. [13] have experimentally demonstrated a quantum digital signature protocol without any secure channel assumptions. Yin et al. [14] have demonstrated the quantum digital signatures independent of the experimental measuring device over a metropolitan network. Lu et al. [15] have proposed an efficient quantum digital signature scheme without using a symmetrical step. An experimental quantum secure network with digital signatures and encryption is demonstrated by Yin et al. [16]. An experimental demonstration of an unconditionally secure digital signature protocol implemented in a fully connected quantum network without trusted nodes is presented by Pelet et al. [17]. Mooney et al. [18] have demonstrated the generation and verification of 27 qubit GHZ states using a superconducting quantum computer.

Quantum digital signatures in the above studies have been developed in 2 dimensions. There are security, noise and low-level key generation problems in 2-state quantum networks. The biggest problem of today's practical qubit-based 2-dimensional technologies can be expressed as information loss, noise and the need for more memory. Due to the above problems, great difficulties are encountered in practical applications. High dimensional quantum processes find solutions to the problems of information loss, noise problem and more memory needs [19].

In this context, technologies are being developed in the literature for practical high dimensional quantum operations. There are many experimental high dimensional studies in the literature and they can be summarized as follows. Imany et al. [20] have demonstrated the installation of integrated optical micro-resonators as a source for high dimensional frequency box-encoded quantum computing and dense quantum key distribution. Paesani et al. [21] have present the universal high dimensional quantum computing algorithm for GHZ states with linear optics. Shen et al. [22] have demonstrated how to create and control multi-partite classically entangled light in eight dimensions. Srivastav et al. [23] have experimentally demonstrated quantum steering up to 53 dimensions, showing improvements over qubit-based systems and high dimension overcoming loss and noise. Hu and Kais [24] show that quantum wave gates exist and the wave-particle duality of qudit quantum space.

High dimensional QDS studies have not been found in the literature. Also, existence of high dimensional experimental studies allows the practical application of high dimensional QDS. Since high-dimensional quantum computing allows to overcome the noise problem, transfer more data and generate a high rate of key, in this study, a secure quantum digital signature protocol is developed depending on high dimensional entanglement swapping for multi participants.

Cozzolino et al. [25] showed that high-dimensional quantum computing has advantages such as increasing information and communication capacity, higher noise resistance, improved

robustness for quantum cloning, greater violations of local theories, and communication complexity problems.

In this respect, the paper can be outlined as follows; in Section 2, necessary preliminaries and notations used in this article are given. In Section 3, multi-partied quantum digital signature scheme is proposed in high dimension using entanglement swapping and super dense coding. In Section 4, the four-participant case of the proposed high-dimensional quantum digital signature scheme is given as an example. In Section 5, the security of the proposed quantum digital signature schema is investigated. Finally, in the Conclusion section, some results of the proposed multi-partied quantum digital signature scheme for the high dimensional are presented.

2. Preliminaries and Notations

All operations except measurement used in quantum information processing are performed with unitary transformations. Unitary transformation is expressed mathematically as follows.

$$(U^*)^t = U^{-1} \Rightarrow U \text{ is unitary.} \tag{1}$$

The $n-$particle cat state in quantum is defined as follows [26].

$$|\psi(x_1,\ldots,x_n)\rangle = \frac{1}{\sqrt{N}} \times \sum_{j=0}^{N-1} w^{jx_1} |j, j+x_2, \ldots, j+x_n\rangle \tag{2}$$

here $x_1,\ldots,x_n$ run from 0 to $N-1$. The cat states given by Equation (2) are complete and orthonormal. If the unitary transformation U in Equation (1) is Hadamard(H), X, Y, Z, these transformations are called H, X, Y, Z gates in quantum information, respectively. Similarly, 2-qubit and 3-qubit quantum gates can be obtained using the unitary transform U. The superposition property, which is one of the superior properties of the quantum, is obtained by applying the Hadamard gate to the qubits. By applying Hadamard gate and controlled NOT gate to qubits, entanglement, one of the superior properties of quantum, is obtained.

When two particles are strongly related, these particles lose their individual quantum states and share a single, unified state no matter how far apart they are. This combined state was called quantum entanglement.

The generalization of $N-$dimensional entangled Bell states for qudits is as follows [26], [27].

$$|\psi(x,y)\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} w^{jx} |j\rangle \otimes |j+y \mod N\rangle \tag{3}$$

here, x and y run from 0 to $N-1$, and $w = e^{\frac{2\pi i}{N}}$.

For $x = y = 0$, we get [26]

$$|\psi(0,0)\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |j\rangle \otimes |j\rangle \tag{4}$$

The $\left|U_{(x,y)}\right\rangle$ transformation is a uniatry transformation that converts our Bell-basis to computational bases. Unitary gates, which are frequently used in high dimensions, can be expressed as follows [26], [28].

$$\left|U_{(x,y)}\right\rangle = \sum_j w^{xj} |j+y \mod N\rangle\langle j| \tag{5}$$

Any $|\psi(x,y)\rangle$ Bell state is produced by the effect of $\left|U_{(x,y)}\right\rangle$ given by Equation (5) on $|\psi(0,0)\rangle$ [26].

$$\left(I \otimes \left|U_{(x,y)}\right\rangle\right) |\psi(0,0)\rangle = |\psi(x,y)\rangle \tag{6}$$

Entanglement transfer, another outstanding feature of quantum, is a protocol for mixing quantum systems that have never interacted in the past. The formula for the entanglement swapping between the

$|\psi(x,y)\rangle_{s,s'}$ Bell state and the $\left|\psi_(x_1,\ldots,x_n)\right\rangle_{1,\ldots,n}$ cat state is expressed as follows [26]..

$$|\psi(x_1,\ldots,x_n)\rangle_{1,\ldots,n} \otimes |\psi(x,y)\rangle_{s,s'} = \frac{1}{N}\sum_{k,l=0}^{N-1} w^{lk} \times$$
$$|\psi(x_1+k, x_2, \ldots, y+l, \ldots, x_n)\rangle_{1,2,\ldots,s',\ldots,n}$$
$$\otimes |\psi(x-k\, x_m - l)\rangle_{s,m} \qquad (7)$$

By using entanglement, super-dense coding (transfer of classical binary information from one place to another at the speed of light) and teleportation (transfer of quantum information from one place to another at the speed of light), which are superior properties of quantum, can be obtained.

The abbreviations and notations used in the article are given in the following Table (1).

Table 1.
Abbreviations Table

Abbreviations	**Definition**
QDS	Quantum Digital Signature
BSM	Bell State Measurement
$\otimes$	Tensor product
$\oplus$	Binary sum
U, $U^\dagger$	Unitary transform, hermitian of U
H_N	Generalized Hadamard gate
$\left\|U_{(x,y)}\right\rangle$	High dimensional unitary gate
$\|\psi(x,y)\rangle$	High dimensional entanglement Bell state
$\|\psi(x_1,\ldots,x_n)\rangle$	High dimensional $n-$particle cat state
$\left\|\psi_{P_1}^m\right\rangle = m_i^1$	$n-$length message that participant P_1 wants to send
$\left\|m_i^1\right\rangle$	Quantum state of m_i^1
$\bar{m}_i^1$	fake m_i^1 message
P_i	$i-$th participant
p_i	private key of $i-$th participant
p_i^g	global key of $i-$th participant
$\bar{p}_i^g$	fake global key of $i-$th participant
$\|\delta_i\rangle$	New basis
$Sig_{P_i}^G$	Global QDS of $i-$th participant
$\overline{Sig}_{P_i}^G$	Fake global QDS of $i-$th participant
$Sig_{P_i}^{P_j}$	QDS of the $i-$th participant calculated by the $j-$th participant

3. Proposed Multi-Partied Quantum Digital Signature Scheme In High Dimension

Let $P_1,\ldots,P_M$ be participants. P_1 participant wants to send message

$$m_i^1 = m_1^1 m_2^1 \ldots m_n^1 \qquad (i=1,\ldots,n)$$

to P_M participant. All participants sequentially share the $|\psi(0,0)_{i,i+1}\rangle^{\otimes n}$ Bell pair to create the entanglement channel between them. This operation takes place by Equation (3). This situation is shown in Figure (1).

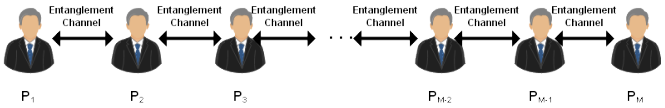

Figure 1. Establishment of the entanglement channel among the participants.

Generally, QDS protocols exist steps such that key sharing step, messaging and validation step. The proposed quantum digital signature protocol can be defined as follows:

3.1. Key Sharing Steps

Let us define key sharing steps as follows,

1. The P_1 participant converts the

$$m_i^1 = m_1^1 m_2^1 \ldots m_n^1 \qquad (i=1,\ldots,n)$$

message which wants to send to the P_M participant into the quantum state in Equation (8).

$$\left|\psi_{P_1}^m\right\rangle = \otimes_{i=1}^n \left|m_i^1\right\rangle \qquad (8)$$

To increase the security of the protocol, the message to be sent is converted into new basis $(\{|\delta_0\rangle, |\delta_1\rangle, \ldots, |\delta_{N-1}\rangle\})$.

$$U = \left|U_{(1,0)}\right\rangle H_N \qquad (9)$$

By applying the unitary operator U given by Equation (9) to Equation (8), participant P_1 expresses its message in new basis. Generalized Hadamard gate s as follows [29].

$$H_N = \frac{1}{\sqrt{N}} \sum_{j,l=0}^{N-1} w^{jl} |j\rangle\langle l| \tag{10}$$

The state of the message in new basis is given as

$$|\psi_{P_1}\rangle = \otimes_{i=1}^{n} U \left|m_i^1\right\rangle = \otimes_{i=1}^{n} \left|\delta_{m_i^1}\right\rangle \tag{11}$$

2. P_{M-1} participant swaps an entanglement channel with P_{M-2} participant to P_M participant via entanglement swapping [30]. He/She makes Bell state measurement on his/her own qubits to achieve that swapping and gets one of the

$$val_{M-1}^1 val_{M-1}^2 = \{00, 01, \ldots, (N-1)(N-1)\} \tag{12}$$

values. Then he/she calculates following values.

$$p_{M-1} = \otimes_{i=1}^{n} \left((val_{M-1}^1)_i (val_{M-1}^2)_i\right) \tag{13}$$

p_{M-1} represents the $2n-$length private key of the P_{M-1} participant. Also, $(val_{M-1}^1)_i (val_{M-1}^2)_i$ shows the measurement result of the P_{M-1} participant. These results are any element of the set in Equation (12).

$$p_{M-1}^g = \otimes_{i=1}^{n} \left((val_{M-1}^1)_i \oplus (val_{M-1}^2)_i\right) \tag{14}$$

p_{M-1}^g represents the $n-$length global key of the P_{M-1} participant.
P_{M-1} sends securely p_{M-1}^g key to all P_j $(j = 2, \ldots, M$ and $j \neq M-1)$ participants by using Equation (15) and super-dense coding through entanglement channel [31]. Since p^g has classical bits here, it can do this sharing in the classical way. But since this will not be a secure channel, it performs key sharing with super-dense encoding [31].

$$p_{M-1}^{gg} = \otimes_{i=1}^{n} \left((p_{M-1}^g)_i (p_{M-1}^g)_i\right) \tag{15}$$

Therefore, in Equation (15) p^{gg} data is obtained by copying each bit value in the p^g data.
The entanglement channel formed between $P_{M-2}$and P_M participants as a result of the measurement of the P_{M-1} participant is given in the Figure (2). The figure also shows the sharing of the global key obtained by the measurement made by the P_{M-1} participant with other participants (except for the P_1 participant).

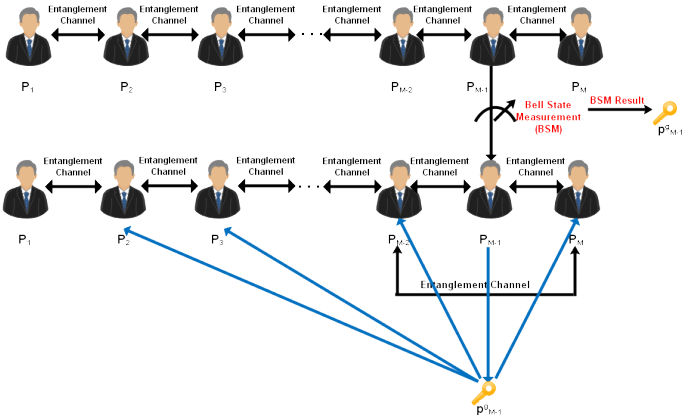

Figure 2. First entanglement swapping and key sharing step

3. All of the above operations must be performed one after the other and in the same way for all P_j $(j = (M-2), \ldots, 2)$ participants. After all the entanglement swapping processes, entanglement channel occurs between sender P_1 participant and receiver P_M participant. All val_i^1, val_i^2 measurement results of the other P_j participants are effective in channel occurrence. This step can be seen in Figure 3.

INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE
A. Aktaş et al., Vol.12, No.3, pp.14-28.
https://doi.org/10.55859/ijiss.1294840

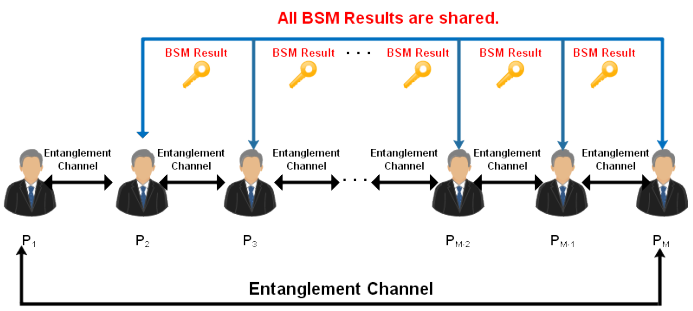

Figure 3. Last entanglement swapping and key sharing step

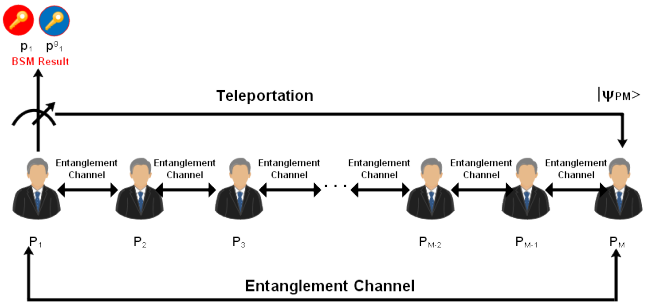

Figure 4. Teleportation of quantum state

4. P_1 participant obtains one of the

$$val_1^1 val_1^2 = \{00, \ldots, 0(N-1), \ldots, (N-1)(N-1)\}$$

values by measuring the Bell in its own qubits in the entanglement channel formed between the P_M participant and the P_1 participant. Then P_1 participant uses $val_1^1 val_1^2$ to calculate the following values and obtain the pair $\{p_1, p_1^g\}$. The P_1 participant saves the p_1 key as its private key and the p_1^g key as the global key, which it will share only with the P_M participant.

$$p_1 = \otimes_{i=1}^{n} \left((val_1^1)_i (val_1^2)_i \right) \tag{16}$$

$$p_1^g = \otimes_{i=1}^{n} \left((val_1^1)_i \oplus (val_1^2)_i \right) \tag{17}$$

After these measurements, P_M participant has the following quantum state.

$$|\psi_{P_M}\rangle = \otimes_{i=1}^{n} U_{j_i k_i}^{\dagger} |\psi_{P_1}\rangle \tag{18}$$

here, $U^{\dagger}$ is the hermitian of the U,

$$j_i = \oplus_{r=1}^{M-1} (p_r^1)_i = (val_1^1)_i \oplus \cdots \oplus (val_{M-1}^1)_i$$

and

$$k_i = \oplus_{r=1}^{M-1} (p_r^2)_i = (val_1^2)_i \oplus \cdots \oplus (val_{M-1}^2)_i$$

This step can be seen in Figure 4.

Participant P_1 measures on the basis of $\{|\delta_0\rangle, |\delta_1\rangle, \ldots, |\delta_{N-1}\rangle\}$ as given in Equation (19). Then P_1 participant calculates and publishes $Sig_{P_1}^G$ global signature. It is given in Figure (5).

$$\left|\psi_{P_1}^G\right\rangle = \otimes_{i=1}^{n} U_{(val_1^1)_i (val_1^2)_i}^{\dagger} \left|\delta_{m_i^1}\right\rangle \tag{19}$$

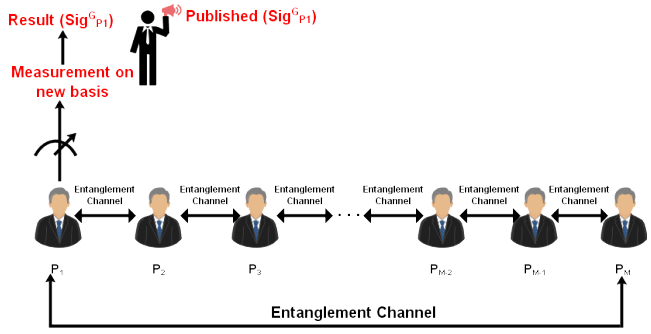

Figure 5. The formation and sharing step of global signature of P_1 participant

5. P_M participant performs measurements on Equation (18) with $\{|\delta_0\rangle, |\delta_1\rangle, \ldots, |\delta_{N-1}\rangle\}$ basis and calculates his/her own signature of P_1 as $Sig_{P_M}^{P_1}$. Here, overscript and underscript demonstrate real owner and receiver, respectively.

3.2. *Messaging and Validation Step*

1. P_1 participant wants to send message m_i^1 to P_M participant. Then P_1 participant sends $\{m_i^1, p_1^g\}$ pair to P_M participant.

2. P_M participant checks $\{\bar{m}_i^1, \bar{p}_1^g\}$ which has been received from P_1 participant to determine any repudiation. Therefore, P_M participant performs the following validations. Here,$\{\bar{m}_i^1, \bar{p}_1^g\}$ denotes the fake $\{m_i^1, p_1^g\}$ sent by the P_1 participant during the sending phase, respectively. P_1 participant sends $\{m_i^1, p_1^g\}$ if it is a trusted participant, and $\{\bar{m}_i^1, \bar{p}_1^g\}$ if it is not. These steps can be seen in Figure 6.

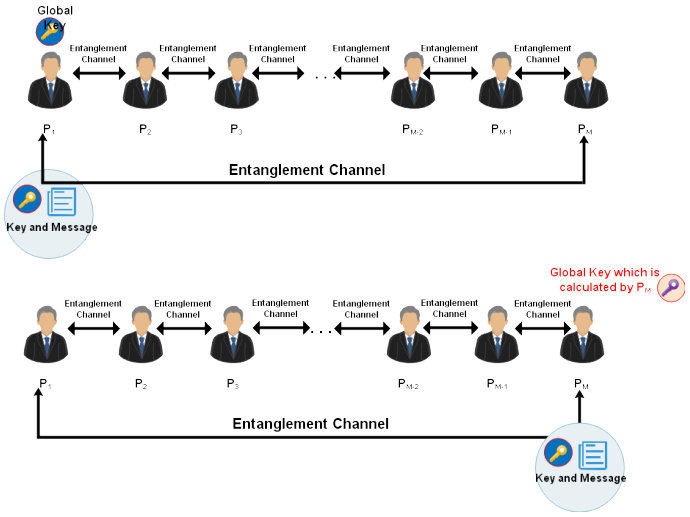

Figure 6. Messaging step for multi participant

a) Validation-1: P_M participant calculates $\overline{Sig}_{P_1}^G$ by using Equation (19) and $\{\bar{m}_i^1, \bar{p}_1^g\}$ pair, then P_M participant checks the equality of the calculated $\overline{Sig}_{P_1}^G$ and $Sig_{P_1}^G$ global signature of P_1 as follows.

$$(\overline{Sig}_{P_1}^G)_i = (Sig_{P_1}^G)_i, \;\; i = 1, \ldots, n \tag{20}$$

b) Validation-2: P_M participant checks the equality of $Sig_{P_1}^G$ and the calculated $Sig_{P_M}^{P_1}$ by using keys which have been sent by the other participants.

i run from 1 to n,

$$\begin{cases} (Sig_{P_1}^G)_i = (Sig_{P_M}^{P_1})_i, & \text{if } \oplus_{r=2}^{M-1} (p_r^g)_i = 0 \\ (Sig_{P_1}^G)_i \neq (Sig_{P_M}^{P_1})_i, & \text{if } \oplus_{r=2}^{M-1} (p_r^g)_i \neq 0 \end{cases} \tag{21}$$

3. Firstly, P_M participant accepts that the message from P_1 is correct and valid, and then sends $\{\bar{m}_i^1, \bar{p}_1^g, \overline{Sig}_{P_M}^{P_1}\}$ triple to the other $(1 < T < M)$ P_T participant. P_T participant performs the following validations to determine the correctness of the message and whether it is a forgery or repudiation.

a) Validation-3: Signature calculation is carried out by using the global signature of P_1. So any value which have been sent by P_M is not used.

i) He/She prepares the following state by utilizing the global signature of P_1.

$$\begin{aligned} &\otimes_{i=1}^n U_{j_i k_i}^\dagger (|\psi_{P_1}\rangle)_i = \\ &\qquad \otimes_{i=1}^n U_{(p_T^1)_i (p_T^2)_i}^\dagger \left(|\psi_{P_1}^G\rangle\right)_i \end{aligned} \tag{22}$$

here

$$j_i = \oplus_{r=2, r\neq T}^{M-1} (p_r^1)_i$$

and

$$k_i = \oplus_{r=2, r\neq T}^{M-1} (p_r^2)_i$$

ii) P_T participant makes measurement on that state with $\{|\delta_0\rangle, |\delta_1\rangle, \ldots, |\delta_{N-1}\rangle\}$ basis and gets $Sig_{P_T}^{P_M}$ signature. Then P_T participant checks the equality of the signature with the one which has been sent by P_M participant as follows.

i run from 1 to n,

$$\begin{cases} (Sig_{P_T}^{P_M})_i = & (\overline{Sig}_{P_M}^{P_1})_i, \\ & \text{if } \oplus_{r=2, r\neq T}^{M-1} (p_r^g)_i = 0 \\ (Sig_{P_T}^{P_M})_i \neq & (\overline{Sig}_{P_M}^{P_1})_i, \\ & \text{if } \oplus_{r=2, r\neq T}^{M-1} (p_r^g)_i \neq 0 \end{cases} \tag{23}$$

By this way, P_T participant checks whether there is a forgery by P_M participant.

b) P_T participant also takes Validation-1 and Validation-2 steps like P_M participant, so P_T

participant determines whether there is any repudiation by P_1 participant.

4. As a second case, if P_M participant accepts that the message is correct and valid, then P_M participant may send $\{\bar{m}_i^1, \bar{p}_1^g, \overline{Sig}_{P_M}^{P_1}\}$ to the participant P_{M-1}. P_{M-1} participant takes the same validation steps like P_T participant. Besides if P_{M-1} participant accepts the message, then he may send the calculated $\overline{Sig}_{P_{M-1}}^{P_1}$ value to P_{M-2} with $\{\bar{m}_i^1, \bar{p}_1^g, \overline{Sig}_{P_M}^{P_1}\}$ triple. By this way,the validation steps can be taken by $P_{M-1} \dots P_2$ subsequently. So every participant can use fewer validation keys to examine correctness and validity of the message, and to detect whether there is any forgery by the previous participant.

4. Example

If we exemplify the proposed quantum digital signature protocol for four participants, it is assumed that Alice is the sender and Bob the receiver. Also, Charlie and David are other participants in the protocol. Alice wants to send message

$$m_i^a = m_1^a m_2^a \dots m_n^a \qquad (i = 1, \dots, n)$$

to Bob. Here Alice is the first, Charlie is the second, David is the third and Bob is the fourth participant.

For this,

- Alice and Charlie share n Bell pair $|\psi(0,0)_{AC}\rangle^{\otimes n}$.

$$Alice \xleftrightarrow{\text{Entanglement Channel}} Charlie$$

- Charlie and David share n Bell pair $|\psi(0,0)_{CD}\rangle^{\otimes n}$. ,

$$Charlie \xleftrightarrow{\text{Entanglement Channel}} David$$

- David and Bob share n Bell pair $|\psi(0,0)_{DB}\rangle^{\otimes n}$. ,

$$David \xleftrightarrow{\text{Entanglement Channel}} Bob$$

Bell pair is obtained from Equation (3). The entanglement channel formed between the participants as a result of the sharing of entangled couples is given in Figure (7).

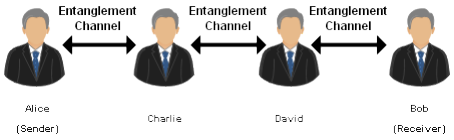

Figure 7. Establishment of the entanglement channel among the participants.

Signature protocol can be shown as follows:.

4.1. Key Sharing Stage

1. Alice converts the m_i^a message which wants to send to the Bob into the quantum state in Equation (24).

$$|\psi_{Alice}^m\rangle = \otimes_{i=1}^n |m_i^a\rangle \tag{24}$$

Then, she transforms these qubits into the new basis $\{|\delta_0\rangle, |\delta_1\rangle, \dots, |\delta_{N-1}\rangle\}$ by using Equation (5).

The new state of Alice with new the basis can be seen as follows:

$$|\psi_{Alice}\rangle = \otimes_{i=1}^n U|m_i^a\rangle = \otimes_{i=1}^n |\delta_{m_i^a}\rangle \tag{25}$$

2. David swaps entanglement channel with Charlie to Bob by doing Bell measurement on his own qubits of entanglement channel with Bob [30]. So that a new entanglement channel occurs between Charlie and Bob. The results of David's Bell measurement are one of the

$$d^1 d^2 = \{00, 01, \dots, 0(N-1), \dots, (N-1)(N-1)\}$$

values. Then, David calculates the following values.

$$d = \otimes_{i=1}^n \left(d_i^1 d_i^2\right) \tag{26}$$

$$d^g = \otimes_{i=1}^{n} \left(d_i^1 \oplus d_i^2\right) \tag{27}$$

David sends value d^g to Bob and Charlie via authenticated classical channel and saves the value d as a private key. The super-dense coding [31] can be used to send any classical data to the participants to increase the security of the protocol. Therefore all bit values of $d^g = \otimes_{i=1}^{n} \left(d_i^1 \oplus d_i^2\right)$ are copying.

$$d^{gg} = \otimes_{i=1}^{n} \left((d^g)_i (d^g)_i\right) \tag{28}$$

Then the bit values of d^{gg} are sent to Bob and Charlie by using super-dense coding.

As a result of David's measurement, the entanglement channel formed between Charlie and Bob is given in Figure (8). The figure also shows the sharing of the global key David obtained as a result of his measurement with Charlie and Bob.

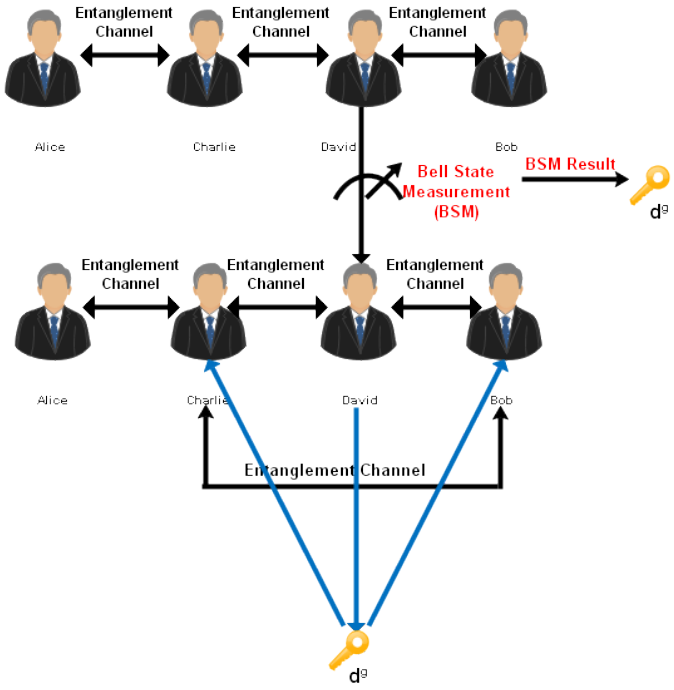

Figure 8. Sharing d^g key and establishment of the entanglement channel between Charlie and Bob.

3. As seen in the first step, Charlie makes Bell measurement on qubits of entanglement channel with Bob, so he swaps entanglement channel with Alice to the Bob. Charlie gets one of the results

$$c^1 c^2 = \{00, 01, \ldots, 0(N-1), \ldots, (N-1)(N-1)\}$$

and then calculates the following values.

$$c = \otimes_{i=1}^{n} \left(c_i^1 c_i^2\right) \tag{29}$$

$$c^g = \otimes_{i=1}^{n} \left(c_i^1 \oplus c_i^2\right) \tag{30}$$

$$c^{gg} = \otimes_{i=1}^{n} \left((c^g)_i (c^g)_i\right) \tag{31}$$

Charlie sends value c^{gg} to the David and Bob via super-dense coding. Then he saves value c as private key.

As a result of Charlie's measurement, the entanglement channel formed between Alice and Bob is given in Figure (9). The figure also shows the sharing of the global key Charlie obtained as a result of his measurement with David and Bob.

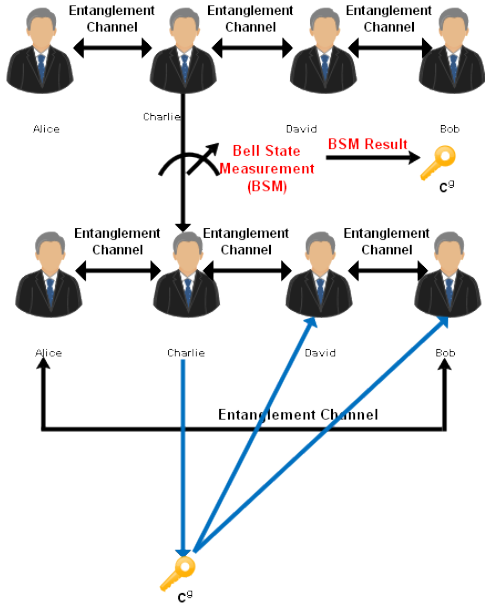

Figure 9. Sharing c^g key and establishment of the entanglement channel between Alice and Bob.

The distribution of the keys formed as a result of the Bell measurement is shown in Figure (10).

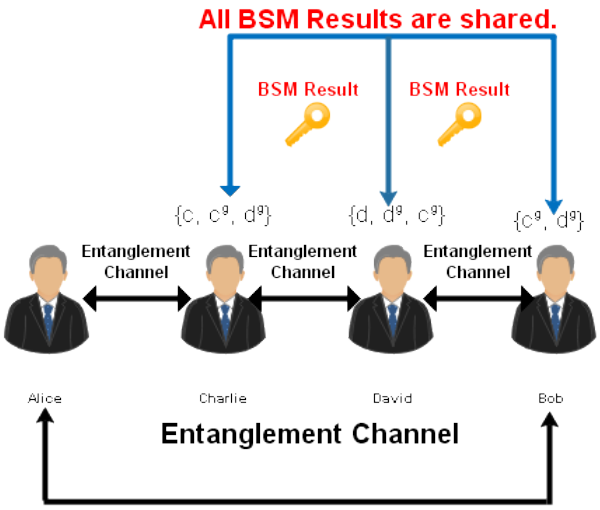

Figure 10. Key sharing step

4. Alice teleports $|\psi_{Alice}\rangle$ to Bob by making Bell state measurement on qubits of entanglement channel with Bob. Alice gets one of the

$$a^1a^2 = \{00, 01, \ldots, 0(N-1), \ldots, (N-1)(N-1)\}$$

values and calculates the following values.

$$a = \otimes_{i=1}^{n} \left(a_i^1 a_i^2\right) \tag{32}$$

$$a^g = \otimes_{i=1}^{n} \left(a_i^1 \oplus a_i^2\right) \tag{33}$$

Alice saves stores the a key as her private key and the a^g key as the global key, which it will share only with Bob.

As a result of Bell measurements performed by Alice in her own qubits, the quantum state given by Equation (34) occurs in Bob.

$$|\psi_{Bob}\rangle = \otimes_{i=1}^{n} U_{j_i k_i}^{\dagger}(|\psi_{Alice}\rangle)_i \tag{34}$$

here, $j_i = a_i^1 \oplus c_i^1 \oplus d_i^1$ and $k_i = a_i^2 \oplus c_i^2 \oplus d_i^2$. Teleportation step and key formation as a result of Bell measurement performed by Alice in her own qubit are given in Figure (11).

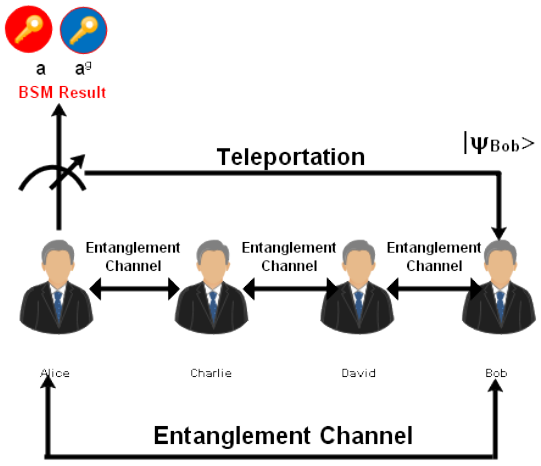

Figure 11. Teleportation of quantum state

5. Bob caries out measurements on $|\psi_{Bob}\rangle$ state with $\{|\delta_0\rangle, |\delta_1\rangle, \ldots, |\delta_{N-1}\rangle\}$ basis. Then he saves the result as Sig_{Bob}^{Alice}.

6. Alice calculates her global signature by using the following equation.

$$\left|\psi_{Alice}^{G}\right\rangle = \otimes_{i=1}^{n} U_{a_i^1 a_i^2}^{\dagger}(|\psi_{Alice}\rangle)_i \tag{35}$$

Then she makes measurement on that state with $\{|\delta_0\rangle, |\delta_1\rangle, \ldots, |\delta_{N-1}\rangle\}$ basis and saves and publishes the result Sig_{Alice}^{G} as her global signature. This step is given in Figure (12).

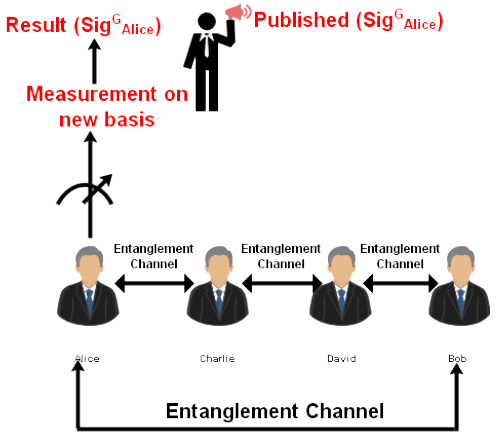

Figure 12. The formation and sharing step of Alice's global signature

4.2. Messaging and Validation Step

In notation, $\bar{a}$ symbolizes that real a is changed by the sender or for any reason.

1. Alice sends $\{\bar{m}_i^a, \bar{a}^g\}$ pair to Bob. Alice may change values of m_i^a and a^g represented as $\{\bar{m}_i^a, \bar{a}^g\}$.
The step of sharing the $\{\bar{m}_i^a, \bar{a}^g\}$ pair of Alice is given in Figure (13).

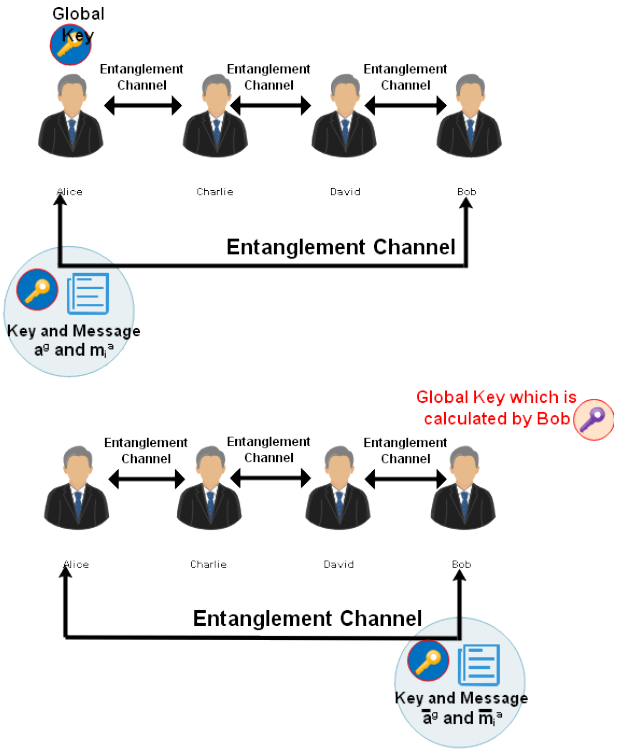

Figure 13. Messaging step for four participant

Bob takes the following validation steps.

a) Validation-1: Bob calculates $\overline{Sig}^G_{Alice}$ by using Equation (35) and $\{\bar{m}_i^a, \bar{a}^g\}$ pair, then Bob checks the equality of the calculated $\overline{Sig}^G_{Alice}$ and Alice's global signature Sig^G_{Alice} as follows.

$$(\overline{Sig}^G_{Alice})_i = (Sig^G_{Alice})_i, \quad i = 1, \ldots, n \tag{36}$$

b) Validation-2: Then he checks the Equation (37) by using values d^g, c^g, which have been sent by David and Charlie.

i run from 1 to n,

$$\begin{cases} (Sig^G_{Alice})_i = (Sig^{Alice}_{Bob})_i, & \text{if } c^{g_i} \oplus d^{g_i} = 0 \\ (Sig^G_{Alice})_i \neq (Sig^{Alice}_{Bob})_i, & \text{if } c^{g_i} \oplus d^{g_i} \neq 0 \end{cases} \tag{37}$$

2. Notice that Bob caries out the first validation based on the values which have been sent by Alice. Then the second one is realized with the global signature of Alice and d^g, c^g values, which have been sent by the other participants. The second validation does not depend on the measurement results $a^1 a^2$ of Alice. Though Alice passes the first validation by sending the changed $\{m_i^a, a^g\}$ values to Bob, she will fail in the second validation step.
If Bob is sure about the correctness of the message, then he sends $\{\bar{m}_i^a, \bar{a}^g, \overline{Sig}^{Alice}_{Bob}\}$ to David. Thus the transferability of the message will be tested.

3. Validation-3: David calculates signature $\{Sig^{Alice}_{Bob}\}$ by using the global signature of Alice as follows.

$$\otimes_{i=1}^n \left(U^\dagger_{c_i^1 c_i^2}(|\psi_{Bob}\rangle)_i = U^\dagger_{d_i^1 d_i^2}(|\psi^G_{Alice}\rangle)_i \right) \tag{38}$$

Then, as given in Equation (38), he makes the measurements by using $\{|\delta_0\rangle, |\delta_1\rangle, \ldots, |\delta_{N-1}\rangle\}$ basis and gets value Sig^{Bob}_{David}. Then he checks the following equalities.

i run from 1 to n,

$$\begin{cases} (\overline{Sig}^{Alice}_{Bob})_i = (Sig^{Bob}_{David})_i, & \text{if } c^{g_i} = 0 \\ (\overline{Sig}^{Alice}_{Bob})_i \neq (Sig^{Bob}_{David})_i, & \text{if } c^{g_i} \neq 0 \end{cases} \tag{39}$$

4. David takes the same validation steps of Bob and checks whether Alice makes repudiation or not. If all validations are correct then we can decide that the message is transferable. Then David sends $\{\bar{m}_i^a, \bar{a}^g, \overline{Sig}^{Alice}_{Bob}\}$ triple to Charlie.

5. Charlie uses value d^g to perform validations.

$$\otimes_{i=1}^{n}\left(U^{\dagger}_{d_i^1 d_i^2}(|\psi_{Bob}\rangle)_i = U^{\dagger}_{c_i^1 c_i^2}(|\psi^G_{Alice}\rangle)_i\right) \quad (40)$$

Then, as given in Equation (40), he makes measurement on that state with $\{|\delta_0\rangle, |\delta_1\rangle, \ldots, |\delta_{N-1}\rangle\}$ basis and gets $Sig^{Bob}_{Charlie}$ value and checks the following equality.

i run from 1 to n,

$$\begin{cases} (\overline{Sig}^{Alice}_{Bob})_i = (Sig^{Bob}_{Charlie})_i, & \text{if } d^{g_i} = 0 \\ (\overline{Sig}^{Alice}_{Bob})_i \neq (Sig^{Bob}_{Charlie})_i, & \text{if } d^{g_i} \neq 0 \end{cases} \quad (41)$$

6. If David sends $\{\bar{m}_i^a, \bar{a}^g, \overline{Sig}^{Bob}_{David}\}$ triple to Charlie, then Charlie can easily validate values as follows.

$$\otimes_{i=1}^{n}\left((|\psi_{Bob}\rangle)_i = U^{\dagger}_{c_i^1 c_i^2}(|\psi^G_{Alice}\rangle)_i\right) \quad (42)$$

Then, as given in Equation (42), he makes measurements on that state by using $\{|\delta_0\rangle, |\delta_1\rangle, \ldots, |\delta_{N-1}\rangle\}$ basis and gets $Sig^{David}_{Charlie}$ value and checks the following.

$$\left((Sig^{David}_{Charlie})_i = (\overline{Sig}^{Bob}_{David})_i\right), \quad i = 1, \ldots, n \quad (43)$$

5. Security Analysis

Since the proposed protocol is high-dimensional, the probability of anyone obtaining information is much lower than in qubit states. Security analysis of proposed QDS based on super-dense coding and entanglement for multi participants in $N-$ dimension is as follows.

1. Non-repudiation: If the sender P_1 participant does not know any of the p_i^g of $P_2, P_3, \ldots, P_{M-1}$ participants, then he/she cannot change m^1 and p_1^g, so does not pass Validation-1 and Validation-2. Validation-2 depends on the p_i^g $(i = 2, \ldots, M-1)$ private keys of $P_2, \ldots, P_{M-1}$ participants.

2. Transferability: If P_M participant accepts that the message from P_1 participant is authenticated, then P_M participant sends it to P_T participant. If P_T participant does not accept that the message is valid and authenticated, then the message is not transferable. Moreover, P_T participant calculates the message from P_1 participant by using the global key of P_1 participant, then P_T participant performs the Validation-1 and Validation-2 of P_M participant. If P_M participant does not commit forgery then P_T participant will accept that the message is valid and authenticated.

3. Forgery: If P_M participant sends invalid $\{\bar{m}_i^1, \bar{p}_1^g, \overline{Sig}^{P_1}_{P_m}\}$ triple to P_T, then P_T accepts that the message is authenticated and valid; P_M has successfully committed forgery. P_M participant knows $\{m_i^1, p_1^g\}$ and $Sig^G_{P_1}$, $Sig^{P_1}_{P_m}$ values. However, P_T uses only the global key of P_1 in Validation-3 instead of the values which have been sent by P_M, thus P_M cannot commit any forgery.

4. Message creation by the receiver: This is not feasible because the global signature of the sender is publicly available, and every participant uses this global signature in validation process.

5. Change of the message by the receiver: The global signature and the sent message include information from the other participants, so this is not feasible.

6. Internal Attack: As it can be seen from the validation steps(see sections 3.2 and 4.2) in the proposed QDS, since each participant checks each other, every participant can use fewer validation keys to examine correctness and validity of the message, and to detect whether there is any forgery by the previous participant.

7. External Attack: Let's imagine that the external attacker, called Eve, was trying to get information

from the P_M participants. Since the message to be sent is converted to different $N-$dimensional bases and there is entanglement between the participants, it is difficult for Eve to intervene and retrieve the message and key. As seen above, the proposed QDS is resistant to external attacks.

6. Conclusion

In this study, we attempted to develop a multi-partied N-dimensional quantum digital signature protocol based on entanglement, entanglement swapping and super-dense coding. In some of the quantum signature protocols, quantum data must be saved in a quantum memory. This is not feasible by modern quantum technology due to the short quantum decoherence time. In this protocol, all data(quantum and classic) is instantly sent by using entanglement channels. Furthermore measurement results are sent by super-dense coding to increase the security of the protocol.

Also, information sharing in N-dimensional provides a more secure information sharing since high-dimensional quantum computing allows to overcome the noise problem, to transfer more data, and to generate a high rate of keys [25].

We can briefly illustrate this situation below. In N dimensions, $\log_2 N$ gives the number of qubits (or classical bits) needed to encode the same amount of information [25]. For example,

For $N = 4$, since $\log_2 4 = 2$, 2 bits of information can be encoded.

$$|0\rangle = 00, |1\rangle = 01, |2\rangle = 10, |3\rangle = 11$$

For $N = 8$, since $\log_2 8 = 3$, 3 bits of information can be encoded.

$$|0\rangle = 000, |1\rangle = 001, |2\rangle = 010, |3\rangle = 100,$$
$$|4\rangle = 011, |5\rangle = 101, |6\rangle = 011, |7\rangle = 111$$

Another advantage of high dimension for quantum communication is that it is more resilient to noise from environmental factors or eavesdropping attacks.

Let P_m be any participant. Let one of the P_m participant Bell measurement results be any of the elements of the set below.

$$p_m^1 p_m^2 = \{00, 01, \ldots, 0(N-1), \ldots, (N-1)(N-1)\} \tag{44}$$

Therefore, the probability that participant P_m obtains one of these measurement results is $\frac{1}{2^N}$. Therefore, the probability of an outside listener receiving the measurement result of participant P_m is also $\frac{1}{2^N}$. Since in N dimensions, $N \to \infty$ will be $\frac{1}{2^N} \to 0$, as the size increases, the probability of an outside listener intercepting the measurement result will approach zero, meaning it is impossible.

Let the private(p) and public(p_m^g) keys generated by the P_m participant be as follows.

$$p = \otimes_{i=1}^{n} \left(p_i^1 p_i^2\right) = \underbrace{p_1^1 p_1^2 p_2^2 p_2^2 \ldots p_n^2 p_n^2}_{\text{2n length}}$$

$$\begin{aligned} p_m^g &= \otimes_{i=1}^{n} (p_i^1 \oplus p_i^2) \\ &= \underbrace{(p_1^1 \oplus p_1^2)(p_2^2 \oplus p_2^2) \ldots (p_n^2 \oplus p_n^2)}_{\text{n length}} \\ &= \underbrace{p_1^{12} p_2^{12} \ldots p_n^{12}}_{\text{n length}} \end{aligned}$$

P_m Participant does the following to transmit p_m^g with the help of super-dense encoding.

$$p_m^{gg} = \otimes_{i=1}^{n} (p_i^g \wedge p_i^g) = \underbrace{(p_1^g p_1^g)(p_2^g p_2^g) \ldots (p_n^g p_n^g)}_{\text{2n length}}$$

Participant P_m shares the obtained p_m^{gg} global key with other participants with the help of super-dense coding. The probability of an outside listener

correctly obtaining the global key shared by the P_m participant is $\frac{1}{2^{2n}} = \frac{1}{4^n}$. In Ndimension, $\log_2 N$ classical bits (or qubits) are needed to encode a data. That is, as the size increases, the information capacity also increases. When $N \to \infty$, the length of the information string will also increase. Therefore, it approaches $n \to \infty$. For $n \to \infty$, it approaches $\frac{1}{4^n} \to 0$. Therefore, the probability of the listener obtaining the global key shared by the participant P_m approaches zero. So it is impossible.

Because entanglement swapping allows us to entanglement two quantum systems without direct interaction, information can be easily transmitted over long distances without any change. Super-dense coding was used in any classical data transmission requirement to increase the security of the protocol. This protocol is experimentally realized by using experimental methods such as [32], [33], [34], [35], [36], [37].

Acknowledgment

This study is a part of Arzu AKTAŞ's doctoral thesis. We are grateful to the referees for their valuable suggestion.

References

[1] D. Gottesman and I. Chuang, "Quantum digital signatures," *eprint arXiv:quant-ph/0105032*, 2001. [Online]. Available: https://arxiv.org/pdf/quant-ph/0105032.pdf

[2] L. Lamport, "Constructing digital signatures from a one-way function," Tech. Rep., 1979.

[3] X. Zhao, N. Zhou, H. Chen, and L. Gong, "Multiparty quantum key agreement protocol with entanglement swapping," *International Journal of Theoretical Physics*, vol. 58, no. 2, pp. 436–450, 2019.

[4] C. Li, X. Chen, H. Li, Y. Yang, and J. Li, "Efficient quantum private comparison protocol based on the entanglement swapping between four-qubit cluster state and extended bell state," *Quantum Information Processing*, vol. 18, no. 5, pp. 1–12, 2019.

[5] X. Cai, T. Wang, C. Wei, and F. Gao, "Cryptanalysis of multiparty quantum digital signatures," *Quantum Information Processing*, vol. 18, no. 8, pp. 1–12, 2019.

[6] M. Zhang and H. Li, "Weak blind quantum signature protocol based on entanglement swapping," *Photon. Res.*, vol. 3, no. 6, pp. 324–328, 2015.

[7] W. Qu, Y. Zhang, H. Liu, T. Dou, J. Wang, Z. Li, S. Yang, and H. Ma, "Multi-party ring quantum digital signatures," *Journal of the Optical Society of America B Optical Physics*, vol. 36, no. 5, pp. 1335–1341, 2019.

[8] H. Qin, W. K. S. Tang, and R. Tso, "Quantum (t, n) threshold group signature based on bell state," *Quantum Information Processing*, vol. 19, no. 2, pp. 1–10, 2020.

[9] C. Weng, Y. Lu, R. Gao, Y. Xie, J. Gu, C. Li, B. Li, H. Yin, and Z. Chen, "Secure and practical multiparty quantum digital signatures," *Opt. Express*, vol. 29, no. 17, pp. 27 661–27 673, 2021.

[10] P. J. Clarke, R. J. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G. S. Buller, "Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light," *Nature Communications*, vol. 3, pp. 1–8, 2012.

[11] T. Wang, X. Cai, Y. Ren, and R. Zhang, "Security of quantum digital signatures for classical messages," *Scientific Reports*, vol. 5, pp. 1–4, 2015.

[12] H. Yin, Y. Fu, and Z. Chen, "Practical quantum digital signature," *Physical Review A*, vol. 93, no. 3, pp. 1–13, 2016.

[13] H. Yin, Y. Fu, H. Liu, Q. Tang, J. Wang, L. You, W. Zhang, S. Chen, Z. Wang, Q. Zhang, T. Chen, Z. Chen, and J. Pan, "Experimental quantum digital signature over 102 km," *Physical Review A*, vol. 95, no. 3, pp. 1–10, 2017.

[14] H. Yin, W. Wang, Y. Tang, Q. Zhao, H. Liu, X. Sun, W. Zhang, H. Li, I. V. Puthoor, L. You, E. Andersson, Z. Wang, Y. Liu, X. Jiang, X. Ma, Q. Zhang, M. Curty, T. Chen, and J. Pan, "Experimental measurement-device-independent quantum digital signatures over a metropolitan network," *Physical Review A*, vol. 95, no. 4, pp. 1–5, 2017.

[15] Y. Lu, X. Cao, C. Weng, J. Gu, Y. Xie, M. Zhou, H. Yin, and Z. Chen, "Efficient quantum digital signatures without symmetrization step," *Opt. Express*, vol. 29, no. 7, pp. 10 162–10 171, 2021.

[16] H. Yin, Y. Fu, C. Li, C. Weng, B. Li, J. Gu, Y. Lu, S. Huang, and Z. Chen, "Experimental quantum secure network with digital signatures and encryption," *National Science Review*, vol. 10, no. 4, pp. 1–11, 2022.

[17] Y. Pelet, I. V. Puthoor, N. Venkatachalam, S. Wengerowsky, M. Lončarić, S. P. Neumann, B. Liu, Ž. Samec, M. Stipčević, R. Ursin, E. Andersson, J. G. Rarity, D. Aktas, and S. K. Joshi, "Unconditionally secure digital signatures implemented in an eight-user quantum network," *New Journal of Physics*, vol. 24, no. 9, pp. 1–11, 2022.

[18] G. J. Mooney, G. A. L. White, C. D. Hill, and L. C. L. Hollenberg, "Generation and verification of 27-qubit greenberger-horne-zeilinger states in a superconducting quantum computer," *Journal of Physics Communications*, vol. 5, no. 9, pp. 1–18, 2021.

[19] I. Vagniluca, B. Da Lio, D. Rusca, D. Cozzolino, Y. Ding,

H. Zbinden, A. Zavatta, L. K. Oxenløwe, and D. Bacco, "Efficient time-bin encoding for practical high-dimensional quantum key distribution," *Phys. Rev. Applied*, vol. 14, pp. 1–8, 2020.

[20] P. Imany, J. A. Jaramillo, O. D. Odele, K. Han, D. E. Leaird, J. M. Lukens, P. Lougovski, M. Qi, and A. M. Weiner, "50-ghz-spaced comb of high-dimensional frequency-bin entangled photons from an on-chip silicon nitride microresonator," *Opt. Express*, vol. 26, no. 2, pp. 1825–1840, 2018.

[21] S. Paesani, J. F. F. Bulmer, A. E. Jones, R. Santagati, and A. Laing, "Scheme for universal high-dimensional quantum computation with linear optics," *Physical Review Letters*, vol. 126, no. 23, pp. 1–6, 2021.

[22] Y. Shen, I. Nape, X. Yang, X. Fu, M. Gong, D. Naidoo, and A. Forbes, "Creation and control of high-dimensional multi-partite classically entangled light," *Light: Science & Applications*, vol. 10, no. 1, pp. 1–10, 2021.

[23] V. Srivastav, N. H. Valencia, W. McCutcheon, S. Leedumrongwatthanakun, S. Designolle, R. Uola, N. Brunner, and M. Malik, "Quick quantum steering: Overcoming loss and noise with qudits," *Physical Review X*, vol. 12, no. 4, pp. 1–13, 2022.

[24] Z. Hu and S. Kais, "The wave-particle duality of the qudit quantum space and the quantum wave gates," *arXiv e-prints*, p. arXiv:2207.05213, 2022. [Online]. Available: https://arxiv.org/ftp/arxiv/papers/2207/2207.05213.pdf

[25] D. Cozzolino, B. Da Lio, D. Bacco, and L. Katsuo Oxenlowe, "High-dimensional quantum communication: benefits, progress, and future challenges," *arXiv e-prints*, p. arXiv:1910.07220, 2019. [Online]. Available: https://arxiv.org/pdf/1910.07220.pdf

[26] J. Zhao and Y. Tian, "Multi-party quantum private comparison based on the entanglement swapping of d-level cat states and d-level bell states," *Quantum Information Processing*, vol. 16, no. 7, pp. 1–20, 2017.

[27] S. Lin, Y. Sun, X.-F. Liu, and Z.-Q. Yao, "Quantum private comparison protocol with d-dimensional bell states," *Quantum Information Processing*, vol. 12, no. 1, pp. 559–568, 2013.

[28] Y. Wang, Z. Hu, B. C. Sanders, and S. Kais, "Qudits and high-dimensional quantum computing," *Frontiers in Physics*, vol. 8, pp. 1–24, 2020.

[29] E. Acar, S. Gündüz, G. Akpınar, and I. Yılmaz, "High-dimensional grover multi-target search algorithm on cirq," *European Physical Journal Plus*, vol. 137, no. 2, pp. 1–9, 2022.

[30] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, "Event-ready-detectors bell experiment via entanglement swapping," *Phys. Rev. Lett.*, vol. 71, pp. 4287–4290, 1993.

[31] F. Wang, M. Erhard, A. Babazadeh, M. Malik, M. Krenn, and A. Zeilinger, "Generation of the complete four-dimensional bell basis," *Optica*, vol. 4, no. 12, pp. 1–6, 2017.

[32] V. Srivastav, N. H. Valencia, W. McCutcheon, S. Leedumrongwatthanakun, S. Designolle, R. Uola, N. Brunner, and M. Malik, "Quick quantum steering: Overcoming loss and noise with qudits," *Physical Review X*, vol. 12, no. 4, pp. 1–13, 2022.

[33] Y. Zhou, M. Mirhosseini, S. Oliver, J. Zhao, S. M. H. Rafsanjani, M. P. J. Lavery, A. E. Willner, and R. W. Boyd, "Using all transverse degrees of freedom in quantum communications based on a generic mode sorter," *Optics Express*, vol. 27, no. 7, pp. 10 383–10 394, 2019.

[34] B. Da Lio, D. Cozzolino, N. Biagi, Y. Ding, K. Rottwitt, A. Zavatta, D. Bacco, and L. K. Oxenlowe, "Path-encoded high-dimensional quantum communication over a 2-km multicore fiber," *npj Quantum Information*, vol. 7, pp. 1–6, 2021.

[35] T. Feng, Q. Xu, L. Zhou, M. Luo, W. Zhang, and X. Zhou, "Quantum information transfer between a two-level and a four-level quantum systems," *Photon. Res.*, vol. 10, no. 12, pp. 2854–2865, 2022.

[36] H. Iqbal and W. O. Krawec, "New security proof of a restricted high-dimensional qkd protocol," *arXiv e-prints*, p. arXiv:2307.09560, 2023. [Online]. Available: https://arxiv.org/pdf/2307.09560.pdf

[37] Y. Chi, J. Huang, Z. Zhang, J. Mao, Z. Zhou, X. Chen, C. Zhai, J. Bao, T. Dai, H. Yuan, M. Zhang, D. Dai, B. Tang, Y. Yang, Z. Li, Y. Ding, L. K. Oxenlowe, M. G. Thompson, J. L. O'Brien, Y. Li, Q. Gong, and J. Wang, "A programmable qudit-based quantum processor," *Nature Communications*, vol. 13, pp. 1–10, 2022.