# Measurement-Device-Independent Quantum Secure Direct Communication with User Authentication

Nayana Das\*

Applied Statistics Unit, Indian Statistical Institute, Kolkata, India.

Goutam Paul<sup>†</sup>

Cryptology and Security Research Unit, R. C. Bose Centre for Cryptology and Security, Indian Statistical Institute, Kolkata, India.

### Abstract

Quantum secure direct communication (QSDC) and deterministic secure quantum communication (DSQC) are two important branches of quantum cryptography, where one can transmit a secret message securely without encrypting it by a prior key. In the practical scenario, an adversary can apply detector-side-channel attacks to get some non-negligible amount of information about the secret message. Measurement-device-independent (MDI) quantum protocols can remove this kind of detector-side-channel attacks, by introducing an untrusted third party (UTP), who performs all the measurements during the protocol with imperfect measurement devices. In this paper, we put forward the first MDI-QSDC protocol with user identity authentication, where both the sender and the receiver first check the authenticity of the other party and then exchange the secret message. Then we extend this to an MDI quantum dialogue (QD) protocol, where both the parties can send their respective secret messages after verifying the identity of the other party. Along with this, we also report the first MDI-DSQC protocol with user identity authentication. Theoretical analyses prove the security of our proposed protocols against common attacks.

*Keywords*- Collective attacks Deterministic secure quantum communication Identity authentication Measurement-device-independent Quantum cryptography Quantum dialogue

# 1 Introduction

Quantum cryptography is an application of quantum mechanical properties into the field of cryptography, where the security does not depend on some mathematical hard problems. Here the fundamental principles of quantum mechanics are used to guarantee the unconditional communication security of the quantum cryptographic protocols. In 1984, Bennett and Brassard proposed the first quantum key distribution (QKD) protocol [1], based on Wiesner's theory of quantum conjugate coding [2], and this is the first protocol of quantum cryptography. Since then, QKD has received extensive attention both theoretically [3, 4, 5, 6] and experimentally [7, 8, 9, 10, 11].

<sup>\*</sup>Email address: dasnayana920gmail.com

<sup>&</sup>lt;sup>†</sup>Email address: goutam.paul@isical.ac.in

**QSDC and DSQC:** Besides QKD, quantum secure direct communication (QSDC) [5, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29] and deterministic secure quantum communication (DSQC) [30, 31, 32, 33, 34, 35, 36, 37] are also two important primitives of quantum cryptography. The basic difference between QKD and QSDC or DSQC is that, QKD is designed for generating the random keys between communication parties, while QSDC or DSQC is used for direct transmission of secret information. Both QSDC and DSQC are used to securely transmit a secret message directly over a quantum channel, without using any pre-shared secret key for encryption and decryption. In QSDC, no other classical information is needed other than the security checking process, whereas, in DSQC, at least one bit of additional classical information is required to decode one qubit.

**Quantum dialogue (QD):** It is a natural generalization of QSDC, i.e., a bidirectional QSDC, where both the parties can exchange their secret messages simultaneously through a quantum channel. In 2004 Nguyen proposed the first QD protocol [38] by generalizing the ping-pong-protocol [39]. Over the past two decades, QD has gone through rapid developments [40, 41, 42, 43, 44, 45, 46, 47]. QSDC protocols for more than two parties are discussed in [48, 49, 50, 51, 52, 53, 54, 55, 56].

**MDI-QSDC:** However in practice, due to lack of perfect measurement devices, an adversary (Eve) can take advantage of this loophole of an imperfect measurement device and tries to steal information without being detected. In order to solve this problem, Lo et al. first proposed the concept of measurement-device-independent (MDI) QKD protocol [57]. In MDI protocols, a UTP performs all the measurements during the protocol using imperfect devices, and thus it removes all the detector side-channel attacks introduced by Eve [58, 59, 60, 61]. Using the same technique as MDI-QKD, Zhou et al. proposed the first MDI-QSDC protocol [62], and some other MDI-QSDC and MDI-QD protocols also proposed recently [63, 64, 65, 66, 67, 68, 46, 23, 47]. Similar to MDI-QKD, in 2021 Yang et al. proposed the first MDI-DSQC protocol [69] based on the polarization-spatial-mode hyperencoded qudits.

**QSDC** with authentication: For any secure communication, identity authentication of each user is very necessary to defeat an impersonation attack. The first-ever quantum user identification scheme was proposed by Crépeau et al. [70] in 1995. After that, Lee et al. proposed the first QSDC protocol with user authentication [71]. Later on, a number of new QSDC protocols with authentication are presented [72, 73, 74, 75, 24, 25].

**Our contribution:** Here in this paper, we compose both the above concepts of MDI-QSDC and user identity authentication and present the first protocol of MDI-QSDC with user authentication. We extend our MDI-QSDC protocol to an MDI-QD protocol, which also provides user authentication. Then we also propose an MDI-DSQC protocol with user authentication and prove the security of all the above three protocols.

**Comparison with existing works:** We compare the efficiency of our proposed MDI-QSDC protocol with the existing works (see Table 1). In [62], authors proposed an MDI-QSDC protocol based on the idea of quantum teleportation, where the sender prepares a Bell state and the receiver prepares a single qubit state. First, they do a Bell measurement, by UTP, to teleport the receiver's qubit to the sender, and then the sender encodes its secret message. To decode the secret message they do a single qubit measurement on Z basis by UTP. Therefore the protocol [62] requires three qubits and two measurements to communicate a single-bit message. In [63], the authors proposed an MDI-QSDC protocol using entanglement swapping. To share a two-bit secret message, both the sender and the receiver prepare Bell states and perform entanglement swapping with the help of a third party. After that, the sender encodes the secret message. This protocol requires two Bell states and two Bell measurements for sending a two-bit message.

In [68], authors found a security loophole in [63] and proposed a modification over that. The modified version also requires the same resource as before. In [67], the authors proposed a long-distance MDI-QSDC protocol by using ancillary entangled photon-pair sources and relay nodes. To transmit a single-bit message, they use two Bell states and a single qubit state. The protocol also requires two Bell measurements and a Z-basis measurement. Here in our present protocol, to send a two-bit message, we only use a Bell state and a Bell measurement. Therefore, on average it requires a qubit and half measurement to transfer a single-bit message. Also, none of the above existing works provide the user authentication feature before transferring the secret information.

Daman	No. of qubits	No. of Bell Meas.	No. of S.B. Meas.	User
Paper	per message bit	per message bit	per message bit	authentication
Zhou et al. $[62]$	3	1	1	No
Neu et al. [63]	2	1	0	No
Gao et al. [67]	5	2	1	No
Das et al. [68]	2	1	0	No
Present protocol	1	1/2	0	Yes

 Table 1: Comparison between existing MDI-QSDC and our work

\*Bell Meas.: Bell basis measurement, S.B. Meas.: Single basis measurement.

The rest of this paper is organized as follows: in Section 2, we briefly describe our proposed MDI-QSDC with user authentication protocol and its security analysis. Then in the next section, we generalize MDI-QSDC protocol into an MDI-QD with user authentication protocol. Then Section 4 presents our MDI-DSQC protocol and finally Section 5 concludes our results.

# Notations

Throughout the paper, we use some notations and we describe those common notations here.

- Z basis =  $\{|0\rangle, |1\rangle\}$  basis.
- $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \ |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle |1\rangle).$
- X basis =  $\{|+\rangle, |-\rangle\}$  basis.
- $I = |0\rangle \langle 0| + |1\rangle \langle 1|.$
- $\sigma_x = |1\rangle \langle 0| + |0\rangle \langle 1|.$
- $i\sigma_y = |0\rangle \langle 1| |1\rangle \langle 0|.$
- $\sigma_z = |0\rangle \langle 0| |1\rangle \langle 1|.$
- $H = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z)$  is the Hadamard operator.
- $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle).$
- $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle |11\rangle) = \frac{1}{\sqrt{2}}(|+-\rangle + |-+\rangle).$
- $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = \frac{1}{\sqrt{2}}(|++\rangle |--\rangle).$

- $|\Psi^{-}\rangle = \frac{1}{\sqrt{2}}(|01\rangle |10\rangle) = \frac{1}{\sqrt{2}}(|+-\rangle |-+\rangle).$
- Bell basis =  $\{ |\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle \}$  basis.
- $S_i = i$ -th element of finite sequence S.
- $S_{A,i} = i$ -th element of finite sequence  $S_A$ .
- Pr(A) = Probability of occurrence of an event A.
- Pr(A|B) = Probability of occurrence of an event A given that the event B has already occurred.

# 2 Proposed MDI-QSDC protocol with user authentication

In this section, we propose our new MDI-QSDC protocol with user identity authentication process.

Suppose Alice has an *n*-bit secret message m, which she wants to send Bob through a quantum channel with the help of some untrusted third-party (UTP), who performs all the measurements during the protocol. Alice and Bob have their secret user identities  $Id_A$  and  $Id_B$  (each of 2k bits) respectively, which they have shared previously by using some secured QKD. The protocol is as follows:

1. Alice chooses c check bits and inserts those bits in random positions of m. Let the new bit string be m' of length n + c. We assume this length to be even, i.e., n + c = 2N for some integer N.

# 2. Bob:

- (a) Prepares (N + k) EPR pairs randomly in  $|\Phi^+\rangle$ ,  $|\Phi^-\rangle$ ,  $|\Psi^+\rangle$  and  $|\Psi^-\rangle$  states. He separates the entangled qubit pairs into two particle sequences  $S_A$  and  $S_B$  each of length (N + k), where  $S_A$  is formed by taking out one qubit from each pair, and the remaining partner qubits form  $S_B$ .
- (b) He also prepares k EPR pairs according to his identity  $Id_B$ . For  $1 \leq i \leq k$ , the *i*-th qubit pair  $I_i$  is prepared as one of  $|\Phi^+\rangle$ ,  $|\Phi^-\rangle$ ,  $|\Psi^+\rangle$  and  $|\Psi^-\rangle$ , if the value of  $Id_{B,(2i-1)}Id_{B,2i}$  is one of 00, 01, 10 and 11 respectively. He creates two sequences  $I_A$  and  $I_B$  of single photons, such that for  $1 \leq i \leq k$ , the *i*-th qubits of  $I_A$  and  $I_B$  are partners of each other in the *i*-th EPR pair  $I_i$ .
- (c) Bob chooses two sets  $D_A$  and  $D_B$ , each of d many decoy photons randomly prepared in Z-basis or X-basis. Then he randomly interleaves the qubits of  $I_A(I_B)$  and  $D_A(D_B)$  and  $S_A(S_B)$  (maintaining the relative ordering of each set) to get a new sequence of single qubits  $Q_A(Q_B)$  (i.e.,  $Q_P = S_P \cup I_P \cup D_P$ , P = A, B).
- (d) Bob retains the  $Q_B$ -sequence and sends the  $Q_A$ -sequence to Alice through a quantum channel.
- (e) After Alice receives  $Q_A$ -sequence, Bob announces the positions of the qubits of  $I_A$  and  $D_A$ .
- 3. Alice:

- (a) She separates the qubits of  $S_A$ ,  $I_A$  and  $D_A$  from  $Q_A$ . Then from the sequence  $S_A$ , she randomly chooses N qubits to encode the secret message and the remaining k qubits (say, the set  $C_A$ ) are used to encode her secret identity  $Id_A$ . The encoding processes for m' and  $Id_A$  are the same. Alice encodes two bits of classical information into one qubit by applying an unitary operator. To encode 00,01,10 and 11, she applies the Pauli operators [76] I,  $\sigma_x$ ,  $i\sigma_y$  and  $\sigma_z$  respectively. After encoding the classical information, let  $S_A$  become  $S'_A$ .
- (b) Alice randomly applies I,  $\sigma_x$ ,  $i\sigma_y$  and  $\sigma_z$  on the qubits of  $I_A$  and resulting in a new sequence  $I'_A$ . She randomly inserts the qubits of  $I'_A$  into random positions of  $S'_A$  and the new sequence be  $Q'_A$ .
- (c) She randomly applies cover operations from  $\{I, i\sigma_y, H, i\sigma_y H\}$  on the qubits of  $D_A$ , resulting in a new new sequence  $D_A^1$ .
- (d) Alice sends  $D_A^1$  sequence to UTP to check the security of the channel from Bob to Alice.
- 4. After the UTP receives the sequence  $D_A^1$ , Bob announces the preparation bases of the qubits of  $D_A$  and Alice announces the corresponding cover operations which she applies on those qubits.
- 5. UTP measures the qubits of  $D_A^1$  in proper bases and announces the measurement result. Note that if the cover operation belongs to the set  $\{H, i\sigma_y H\}$ , then UTP changes the basis to measure the corresponding qubit. For example, let the *i*-th qubit of  $D_A$  be prepared in Z-basis and the *i*-th cover operation be  $i\sigma_y H$ , then UTP measures the *i*th qubit of  $D_A^1$  in X-basis. From the measurement results, Alice and Bob calculate the error in the channel from Bob to Alice, and decide to continue or abort the protocol.
- 6. Alice inserts a new set of d' decoy photons  $D'_A$  into random positions of  $Q'_A$ , resulting in a new sequence  $Q''_A$ . Alice sends  $Q''_A$ -sequence to UTP.
- 7. Alice announces the positions and the preparation bases of the decoy qubits of  $D'_A$ . UTP measures the decoy qubits and publishes the measurement results, and from that Alice calculates the error in the quantum channel between Alice and UTP. If the estimated error is greater than some threshold value, then they terminate the protocol and otherwise go to the next step.
- 8. Bob sends the sequence  $Q_B$  to UTP and when all the qubits of  $Q_B$  are reached to UTP, Bob announces the positions and the preparation bases of the decoy qubits of  $D_B$ . UTP measures those qubits in proper bases and discloses the measurement results, and Bob calculates the error in the quantum channel between Bob and UTP. If the estimated error is greater than some threshold value, then they terminate the protocol and otherwise go to the next step.

#### 9. Authentication process:

(a) Alice announces the positions of the qubits of  $I'_A$  and Bob announces the positions of the qubits of  $I_B$ . For  $1 \le i \le k$ , UTP measures the *i*-th qubit pair  $(I'_{A,i}, I_{b,i})$  in Bell basis and announces the result. As Alice knows  $Id_B$ , she knows the exact state of each  $I_i$ , which is the joint state  $I_{A,i}I_{B,i}$ . Since she randomly applies Pauli operators on  $I_{A,i}$ , the joint state changes to  $I'_{A,i}I_{B,i}$ . Alice compares the measurement result with

 $I'_{A,i}I_{B,i}$  to confirm Bob's identity. If she finds a non-negligible error then she aborts the protocol.

- (b) Alice announces the positions of the qubits of  $C_A$  corresponding to her identity  $Id_A$  and UTP measures those qubits with their partner qubits from  $S_B$  (say, the set  $C_B$ ) in Bell bases and announces the measurement result. Since Bob knows  $Id_A$ , he compares the measurement results with  $Id_A$  and checks if Alice is a legitimate party or not. If he finds a non-negligible error, he aborts the protocol.
- 10. The UTP measures each qubit pair from  $(S'_A, S_B)$  in Bell basis and announces the measurement result. From the knowledge of  $(S_A, S_B)$  and  $(S'_A, S_B)$ , Bob decodes the classical bit string m' using Table (2).
- 11. Alice and Bob publicly compare the random check bits to check the integrity of the messages. If they find an acceptable error rate then Bob gets the secret message m and the communication process is completed.

Bob prepares	Secret message	Alice's unitary	Final joint	Decoded
$(S_A,S_B)$	bits of Alice	$S_A$ to $S_A'$	state $(S'_A, S_B)$	message bits
	00	Ι	$ \Phi^+ angle$	00
$ \Phi^+ angle$	01	$\sigma_x$	$ \Psi^+ angle$	01
	10	$i\sigma_y$	$ \Psi^{-} angle$	10
	11	$\sigma_z$	$ \Phi^{-} angle$	11
	00	Ι	$ \Phi^{-} angle$	00
$ \Phi^{-} angle$	01	$\sigma_x$	$ \Psi^{-} angle$	01
	10	$i\sigma_y$	$ \Psi^+ angle$	10
	11	$\sigma_z$	$ \Phi^+ angle$	11
	00	Ι	$ \Psi^+ angle$	00
$ \Psi^+\rangle$	01	$\sigma_x$	$ \Phi^+ angle$	01
¥ /	10	$i\sigma_y$	$ \Phi^{-} angle$	10
	11	$\sigma_z$	$ \Psi^{-} angle$	11
$ \Psi^{-} angle$	00	Ι	$ \Psi^{-} angle$	00
	01	$\sigma_x$	$ \Phi^{-} angle$	01
	10	$i\sigma_y$	$ \Phi^+ angle$	10
	11	$\sigma_z$	$ \Psi^+ angle$	11

Table 2: Encoding and decoding rules of our proposed MDI-QSDC.

Figure 1 represents the block diagram of the proposed MDI-QSDC with user authentication protocol. We also present it in the form of an algorithm in figure 2, where we use the following notations.

- $X \to Y$ : X changes to Y.
- $\mathcal{P}(Q)$ : Positions of the qubits of Q.
- $\mathcal{C}(Q)$ : Cover operations on the qubits of Q.

- $\mathcal{B}(Q)$ : Bases of the qubits of Q.
- $\mathcal{M}(Q)$  &  $\mathcal{A}$ : Measures the qubits of Q in proper bases and announces the results.
- $\mathcal{BM}(Q_1, Q_2)$  &  $\mathcal{A}$ : Measures the qubit pairs of  $(Q_1, Q_2)$  in Bell bases and announces the results.
- Sec.chk (A, B): Checks the security of the channel from A to B.
- Cov. op.: Cover operation.
- Ins.: Inserts.

### Figure 1: Block diagram of the proposed MDI-QSDC with user authentication protocol



Alice (Identity $Id_A$ )		UTP		$\operatorname{\mathbf{Bob}}(\operatorname{Identity} Id_B)$
1. Ins. $c$ check bits into the				
secret message $m$ and $m \to m'$ .				
	<b>*</b>	$2(d). Q_A$		<b>2(a)-(c).</b> Prepares $Q_A = S_A \cup I_A \cup D_A$
				and $Q_B = S_B \cup I_B \cup D_B$ , where qubits
	<i>(</i>	$\mathbf{2(e).} \ \mathcal{P}(I_A), \ \mathcal{P}(D_A)$		pair of $(S_A, S_B)$ , $(I_A, I_B)$ are entangled,
				and qubits of $D_A$ , $D_B$ are decoy states.
<b>3(a).</b> Separates $S_A, I_A, D_A$ from $Q_A$ .				
Encodes $m'$ , $Id_A$ on $S_A$ , $S_A \to S'_A$ .				
$C_A$ : qubits corresponding to $Id_A$ .				$C_B$ : partner qubits of $C_A$
<b>3(b).</b> Random unitaries on $I_A$ , $I_A \rightarrow I'_A$ .				
Ins. $I'_A$ into $S'_A$ and $Q'_A = S'_A \cup I'_A$ .				
<b>3(c).</b> Cov. op. on $D_A$ and $D_A \to D_A^1$ .	$\mathbf{3(d)}$ . $D_A^1$			
	$\xrightarrow{ \mathbf{4'} . \ \mathcal{C}(D_A)  }  \qquad \qquad$	5. $\mathcal{M}(D^1_A)$ & $\mathcal{A}$	$ \underbrace{ \mathbf{4'}.\ \mathcal{B}(D_A) }_{ \underbrace{ \mathbf{4'}.\ \mathcal{B}(D_$	5'. Sec.chk (Bob, Alice)
<b>6.</b> Ins. $D'_A$ into $Q'_A, Q'_A \to Q''_A$ .				
$D'_A$ : set of new decoy states.	$\mathbf{6'} \cdot Q''_A \longrightarrow$			
7". Sec.chk (Alice,UTP)	$\xrightarrow{\textbf{7. }\mathcal{P}(D_A'),\ \mathcal{B}(D_A')}$	7'. $\mathcal{M}(D'_A)$ & $\mathcal{A}$		
			<b>8</b> . <i>Q</i> <sub>B</sub>	
		8". $\mathcal{M}(D_B)$ & $\mathcal{A}$		$\boldsymbol{8'''}\textbf{.} \text{ Sec.chk (Bob, UTP)}$
$9(\mathbf{a})^{\prime\prime\prime}.$ Verifies Bob's identity.	$\xrightarrow{\mathbf{9(a).} \ \mathcal{P}(I'_A)} \rightarrow$	$\mathbf{9(a)''}$ . $\mathcal{BM}(I'_A, I_B)$ & $\mathcal{A}$	$(\mathbf{g}(\mathbf{a})'. \mathcal{P}(I_B),$	
	$\xrightarrow{\mathbf{9(b).} \ \mathcal{P}(C_A)}$	9(b)'. $\mathcal{BM}(C_A, C_B)$ & $\mathcal{A}$		9(b)". Verifies Alice's identity.
		<b>10.</b> $\mathcal{BM}(S_A - C_A, S_B - C_B)$ & $\mathcal{A}$		<b>10'.</b> Decodes $m'$ .
	<	11. Compare the check bits		<b>11'.</b> Extract $m$ from $m'$ .
$ \rightarrow$ denotes quantum channel,				
$\longrightarrow$ denotes classical channel.				
Step (i)' happens just after Step (i).				

Figure 2: Proposed MDI-QSDC with user authentication protocol

# 2.1 Example of our MDI-QSDC protocol

Let us now take an example of the above discussed MDI-QSDC with user authentication protocol, where we assume all channels are noiseless.

Suppose Alice has a 6-bit secret message m = 011010 and the secret identities of Alice and Bob are  $Id_A = 1011$  and  $Id_B = 0111$  respectively, i.e., n = 6 and k = 2. Then the protocol is as follows.

1. Alice chooses c = 4 check bits 1001 and inserts those bits in random positions of m. Let the new bit string be m' = 0101100110 (bold numbers are check bits, i.e., the 2nd, 3rd, 7th and 9th bits) of length n + c = 10 = 2N, i.e., N = 5.

#### 2. Bob:

(a) Randomly prepares N + k = 7 EPR pairs

$$\Psi^{+}\rangle_{a_{1}b_{1}}, \left|\Phi^{+}\rangle_{a_{2}b_{2}}, \left|\Phi^{+}\rangle_{a_{3}b_{3}}, \left|\Psi^{-}\rangle_{a_{4}b_{4}}\right|\Phi^{-}\rangle_{a_{5}b_{5}}, \left|\Psi^{-}\rangle_{a_{6}b_{6}}, \text{ and } \left|\Psi^{+}\rangle_{a_{7}b_{7}}.$$

He separates the entangled qubit pairs into two particle sequences

$$S_A = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7\}$$
 and  $S_B = \{b_1, b_2, b_3, b_4, b_5, b_6, b_7\},\$ 

each of length 7.

- (b) He also prepares 2 EPR pairs  $I_1 = |\Phi^-\rangle_{a'_1b'_1}$  and  $I_2 = |\Psi^-\rangle_{a_2b'_2}$  corresponding to his identity  $Id_B = 0111$ , and creates two single-qubit sequences  $I_A = \{a'_1, a'_2\}$  and  $I_B = \{b'_1, b'_2\}$  by separating the EPR pairs.
- (c) Bob chooses two sets  $D_A = \{|+\rangle, |1\rangle, |0\rangle, |+\rangle\}$  and  $D_B = \{|-\rangle, |0\rangle, |1\rangle, |0\rangle\}$ , each of d = 4 many decoy photons randomly prepared in Z-basis or X-basis. Then he randomly interleaves the qubits of  $I_A(I_B)$  and  $D_A(D_B)$  and  $S_A(S_B)$  (maintaining the relative ordering of each set) to get a new sequences of single qubits  $Q_A(Q_B)$ . Let

$$Q_{A} = \{a_{1}, a_{2}, a_{1}', |+\rangle, a_{3}, |1\rangle, a_{2}', a_{4}, a_{5}, |0\rangle, a_{6}, a_{7}, |+\rangle\}$$
  
and  $Q_{B} = \{b_{1}, b_{1}', b_{2}, b_{3}, b_{4}, |-\rangle, |0\rangle, b_{2}', b_{5}, |1\rangle, b_{6}, b_{7}, |0\rangle\}.$ 

- (d) Bob retains the  $Q_B$ -sequence and sends the  $Q_A$ -sequence to Alice through a quantum channel.
- (e) After Alice receives  $Q_A$ -sequence, Bob announces the positions of the qubits of  $I_A$  (3rd and 7th) and  $D_A$  (4th, 6th, 10th and 13th).

### 3. Alice:

(a) She separates the qubits of  $S_A$ ,  $I_A$  and  $D_A$  from  $Q_A$ , i.e., she has

$$S_A = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7\}, I_A = \{a'_1, a'_2\} \text{ and } D_A = \{|+\rangle, |1\rangle, |0\rangle, |+\rangle\}.$$

She randomly chooses 5 qubits  $a_1, a_3, a_4, a_6$  and  $a_7$  from  $S_A$  to encode m' = 0101100110and the remaining 2 qubits  $a_2$  and  $a_5$  (say, the set  $C_A = \{a_2, a_5\}$ ) are used to encode  $Id_A = 1011$ . After encoding the classical information, let  $S_A$  become  $S'_A$ , then

$$S'_{A} = \{\sigma_x(a_1), i\sigma_y(a_2), \sigma_x(a_3), i\sigma_y(a_4), \sigma_z(a_5), \sigma_x(a_6), i\sigma_y(a_7)\}$$

(b) Alice randomly applies  $\sigma_z$  and I on the qubits of  $I_A$  and the resulting new sequence is  $I'_A = \{\sigma_z(a'_1), I(a'_2)\}$ . She randomly inserts the qubits of  $I'_A$  into random positions of  $S'_A$  and the new sequence is

$$Q'_A = \{\sigma_x(a_1), \sigma_z(a'_1), i\sigma_y(a_2), \sigma_x(a_3), I(a'_2), i\sigma_y(a_4), \sigma_z(a_5), \sigma_x(a_6), i\sigma_y(a_7)\}.$$

(c) She randomly applies cover operations from  $\{I, i\sigma_y, H, i\sigma_y H\}$  on the qubits of  $D_A$  and the resulting new sequence is

$$D_A^1 = \{H(|+\rangle), i\sigma_y H(|1\rangle), i\sigma_y (|0\rangle), I(|+\rangle)\} = \{|0\rangle, |+\rangle, |1\rangle, |+\rangle\}.$$

- (d) Alice sends  $D_A^1$  to UTP to check the security of the channel from Bob to Alice.
- 4. After the UTP receives the sequence  $D_A^1$ , Bob announces the preparation bases (X, Z, Z) and X of the qubits of  $D_A$  and Alice announces the corresponding cover operations  $(H, i\sigma_y H, i\sigma_y \text{ and } I)$ .
- 5. UTP measures the qubits of  $D_A^1$  in proper bases (Z, X, Z and X) and announces the measurement results  $|0\rangle, |+\rangle, |1\rangle, |+\rangle$ . Since there is no error, Alice and Bob continue the protocol.
- 6. Alice prepares a new set of d' = 4 decoy photons  $D'_A = \{|0\rangle, |+\rangle, |-\rangle, |1\rangle\}$ . She inserts the decoy qubits into random positions of  $Q'_A$  and sends the resulting new sequence  $Q''_A$  to UTP, where

$$Q_A'' = \{\sigma_x(a_1), \sigma_z(a_1'), i\sigma_y(a_2), |0\rangle, \sigma_x(a_3), I(a_2'), |+\rangle, i\sigma_y(a_4), |-\rangle, \sigma_z(a_5), \sigma_x(a_6), |1\rangle, i\sigma_y(a_7)\}.$$

- 7. Alice announces the positions (4th, 7th, 9th and 12th) and the preparation bases (Z, X, X) and Z) of the decoy qubits of  $D'_A$ . UTP measures the decoy qubits and publishes the measurement results  $|0\rangle, |+\rangle, |-\rangle, |1\rangle$ . Since there is no error, Alice and Bob continue the protocol.
- 8. Bob sends the sequence  $Q_B$  to UTP and when all the qubits of  $Q_B$  are reached to UTP, Bob announces the positions (6th, 7th, 10th and 13th) and the preparation bases (X, Z, Z)and Z) of the decoy qubits of  $D_B$ . UTP measures those qubits in proper bases and discloses the measurement results  $|-\rangle$ ,  $|0\rangle$ ,  $|1\rangle$ ,  $|0\rangle$ . Then Bob calculates the error rate (which is zero for this example) in the quantum channel between Bob and UTP and goes to the next step.

#### 9. Authentication process:

(a) Alice announces the positions (2nd and 6th) of the qubits of  $I'_A$  in the sequence  $Q''_A$ and Bob announces the positions (2nd and 8th) of the qubits of  $I_B$  in the sequence  $Q_B$ . UTP measures the *i*-th qubit pairs  $(\sigma_z(a'_1), b'_1)$  and  $(I(a'_2), b'_2)$  in Bell basis and announces the results  $|\Phi^+\rangle$  and  $|\Psi^-\rangle$ . As Alice knows  $Id_B = 0111$ , she knows the exact states of  $I_1 = |\Phi^-\rangle$  and  $I_2 = |\Psi^-\rangle$ . Since she randomly applied Pauli operators  $\sigma_z, I$  on  $a'_1, a'_2$  respectively, the joint state changes to  $|\Phi^+\rangle, |\Psi^-\rangle$ . Alice confirms Bob's identity and continues the protocol.

- (b) Alice announces the positions (2nd and 5th) of the qubits of  $C_A$  in the sequence  $S'_A$  and UTP measures those qubits with their partner qubits from  $S_B$  (say, the set  $C_B = (b_2, b_5)$ ) in Bell bases and announces the measurement results  $|\Psi^-\rangle$ ,  $|\Phi^+\rangle$ . Since the initial states of the EPR pairs are  $|\Phi^+\rangle$ ,  $|\Phi^-\rangle$ , Bob decodes the identity of Alice as  $Id_A = 1011$  and confirms Alice as a legitimate party and continues the protocol.
- 10. The UTP measures each qubit pair from  $(S'_A, S_B)$  in Bell basis and announces the measurement result  $|\Phi^+\rangle$ ,  $|\Psi^+\rangle$ ,  $|\Phi^+\rangle$ ,  $|\Phi^-\rangle$ ,  $|\Phi^-\rangle$ . From these results, Bob decodes the classical bit string m' = 0101100110.
- 11. Alice and Bob publicly compare the random check bits (2nd, 3rd, 7th and 9th bits of m') to check the integrity of the messages. Bob discards those bits to obtain the secret message m = 011010 and the communication process is completed.

# 2.2 Security analysis of our MDI-QSDC protocol

In our proposed MDI-QSDC with user authentication, the secret message is transmitted between two legitimate parties, and the potential adversary is kept ignorant of the content. There are also broadcast channels between Alice, Bob and UTP, for the necessary classical information, to execute the protocol. First, we show the security of our proposed MDI-QSDC protocol for user authentication by establishing the security against impersonation attack. Then we prove the security of the message transmission part.

### 2.2.1 Security for user authentication

Let us now discuss the security of our proposed MDI-QSDC protocol against impersonation attacks. An eavesdropper, Eve, may try to impersonate Alice in order to send a fake message to Bob. But since Eve does not know the pre-shared key  $Id_A$ , Bob can easily detect Eve with a very high probability. In the proposed MDI-QSDC protocol, suppose Eve may intercept the sequence  $Q_A$  sent from Bob to Alice in Step 2d. However, without knowing the pre-shared key  $Id_A$ , Eve applies Pauli operators randomly on k qubits of  $C_A$ , instead of performing the correct unitary to encode  $Id_A$ . She sends it to UTP, who measures these qubits with their partner qubits from  $C_B$ on the Bell basis and announces the results. Since Bob knows the initial state of those k EPR pairs  $(C_A, C_B)$  and the value of  $Id_A$ , he compares the measurement results with the expected EPR pairs and detects Eve. Since Eve applies Pauli operators randomly on each qubit, she applies correct unitary with probability  $\frac{1}{4}$  and hence the detection probability of Bob is  $1 - (\frac{1}{4})^k$ .

On the other hand, Eve may try to impersonate Bob to get the secret message from Alice. In the proposed MDI-QSDC protocol, suppose Eve initiates the protocol and generates the sequences of qubits  $Q_A$  and  $Q_B$ , which contain the sequences  $I_A$  and  $I_B$  respectively, by following the process described in Step 2. Now, since Eve does not know the value of  $Id_B$ , she prepares each  $I_i$   $(1 \le i \le k)$  as one of the EPR pairs randomly with probability  $\frac{1}{4}$ . After Alice applies cover operations on the qubits of  $I_A$ , the set becomes  $I'_A$ . In the authentication process (Step 9a), UTP measures the joint states of  $(I'_A, I_B)$  in proper bases and announces the results. As Alice knows the value of  $Id_B$ , she compares the measurement results with the expected results and detects Eve with probability  $1 - (\frac{1}{4})^k$ .

### 2.2.2 Security for message transmission

In our MDI-QSDC protocol, we are ignorant of the measurement process and strategy that an adversary may exploit, hence we focus on the system after Bob sends the sequence  $Q_A$  to Alice, where a joint state  $\rho_{AB}^{jnt}$ , consisting of maximally entangled photon pairs shared between Alice and Bob. We consider a situation where an adversary Eve attacks the system with an auxiliary system and performs a coherent attack. Here, in our protocol, Alice and Bob use decoy states to obtain the gain and quantum bit error rate (QBER) after each transmission of qubits sequences where both of them send single qubits to the UTP. Now we use the concept of virtual qubits [77, 57] and the proof technique of [65] to establish the security of our protocol against this type of attack. The idea of virtual qubit is that, instead of preparing a single qubit decoy state from  $\{|0\rangle, |1\rangle, |+\rangle |-\rangle\}$ , Alice (Bob) prepares EPR pair, which is a combined system of her (his) virtual qubit and the qubit she (he) is sending to the UTP. Subsequently, they measure their virtual qubits to decide to continue or abort the protocol. For simplicity, let us assume that initially Bob prepares all the EPR pairs in  $|\Phi^+\rangle$  and he applies the cover operations  $I, \sigma_z, \sigma_x, i\sigma_y$ on the qubits of  $S_B$  while sending this sequence  $Q_B$  to the UTP. Note that this step is equivalent to the fact that Bob prepares EPR pairs randomly from the set of all Bell states.

Let the system of Alice, Bob and Eve be A, B and E respectively. Then from Csiszár–Körner theory [78], the secrecy capacity between Alice and Bob is  $C_S$ ,

$$C_S = \max[I(A:B) - I(A:E)],\tag{1}$$

where I(X : Y) stands for mutual information of two random variables X and Y. Now if  $C_S > 0$ , then there is a forward encoding scheme with a capacity less than  $C_S$ , which can be used to transmit the message reliably and securely from Alice to Bob.

According to quantum De Finetti representation theorem [79], the joint state  $\rho_{AB}^{jnt}$  can be asymptotically approximated as a direct product of independent and identically distributed (i.i.d.) subsystems  $\rho_{AB}^{\otimes N}$ , if a randomized permutation is applied to the system. Thus Eve attacks each qubit separately by using a separate probe  $|E\rangle$  and then the coherent attack model can be considered as the collective attack by Eve.

According to [80],  $\rho_{AB}$  can be written as a linear combination of the Bell states as follows,

$$\rho_{AB} = \delta_1 \left| \Phi^+ \right\rangle \left\langle \Phi^+ \right| + \delta_2 \left| \Phi^- \right\rangle \left\langle \Phi^- \right| + \delta_3 \left| \Psi^+ \right\rangle \left\langle \Psi^+ \right| + \delta_4 \left| \Psi^- \right\rangle \left\langle \Psi^- \right|, \tag{2}$$

where  $\sum_{i=1}^{4} \delta_i = 1$ . Let  $|\Phi_{ABE}\rangle$  be a purification of the mixed state  $\rho_{AB}$ . Then it can be written as

$$\left|\Phi_{ABE}\right\rangle = \sum_{i=1}^{4} \sqrt{\delta_i} \left|\Psi_i\right\rangle \left|E_i\right\rangle,\tag{3}$$

where  $|\Psi_1\rangle = |\Phi^+\rangle$ ,  $|\Psi_2\rangle = |\Phi^-\rangle$ ,  $|\Psi_3\rangle = |\Psi^+\rangle$ ,  $|\Psi_4\rangle = |\Psi^-\rangle$  are the entangled pairs shared by Alice and Bob, and  $|E_i\rangle$ ,  $1 \le i \le 4$ , are the orthonormal states of the system  $|E\rangle$ .

After Bob sends the sequence  $Q_A$  to Alice, they calculate the bit error rate  $\epsilon_z$  and phase error rate  $\epsilon_x$  by measuring the virtual qubits by Bob and their partner qubits by Alice. They choose the same bases, either (Z, Z) or (X, X) with probability  $\frac{1}{2}$ , and measure their respective qubits. If no error occurs, then they should get the same outcomes as  $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) =$  $\frac{1}{\sqrt{2}}(|++\rangle + |--\rangle)$ . If they get different outcomes while measuring in Z-basis, i.e., the shared entangled state is either  $|\Psi^+\rangle$  or  $|\Psi^-\rangle$ , then bit flip error occurs and thus  $\epsilon_z = \delta_3 + \delta_4$ . Similarly, when they measure in X-basis and get different outcomes, phase error occurs and thus  $\epsilon_x = \delta_2 + \delta_4$ . If both the error rates are less than some predefined threshold value, then they continue the process and Alice encodes her message by applying proper unitary operators  $U_{\zeta}$ 's on the qubits of  $S_A$  and Bob applies random cover operations from the set of all Pauli operators on the qubits of  $S_B$ , and send their respective sequences to the UTP. Then the shared state becomes

$$\rho_{ABE}^{\zeta} = \frac{1}{4} U_{\zeta} (|\Phi_{ABE}\rangle \langle \Phi_{ABE}| + \sigma_{z}^{B} |\Phi_{ABE}\rangle \langle \Phi_{ABE}| \sigma_{z}^{B} 
+ \sigma_{x}^{B} |\Phi_{ABE}\rangle \langle \Phi_{ABE}| \sigma_{x}^{B} - \sigma_{y}^{B} |\Phi_{ABE}\rangle \langle \Phi_{ABE}| \sigma_{y}^{B} ) U_{\zeta}^{\dagger} 
= U_{\zeta} \rho_{ABE}^{c} U_{\zeta}^{\dagger},$$
(4)

where  $\zeta \in \{00, 01, 10, 11\}$  and  $U_{00} = I$ ,  $U_{01} = \sigma_x$ ,  $U_{10} = i\sigma_y$ ,  $U_{11} = \sigma_z$  are the message encoding operations of Alice, and  $\rho_{ABE}^c = \frac{1}{4} (|\Phi_{ABE}\rangle \langle \Phi_{ABE}| + \sigma_z^B |\Phi_{ABE}\rangle \langle \Phi_{ABE}| \sigma_z^B + \sigma_x^B |\Phi_{ABE}\rangle \langle \Phi_{ABE}| \sigma_x^B - \sigma_y^B |\Phi_{ABE}\rangle \langle \Phi_{ABE}| \sigma_y^B \rangle$ .

Let the 2N-bit message of Alice be  $m' = \zeta_1 \zeta_2 \dots \zeta_N$ , where for  $1 \leq i \leq N$ ,  $\zeta_i$  is a two-bit binary number randomly chosen from  $\mathcal{B} = \{00, 01, 10, 11\}$  and the probability distribution of each  $\zeta_i$  is  $\frac{1}{4}$ . For  $1 \leq i \leq N$ , Alice encodes  $\zeta_i$  by applying  $U_{\zeta_i}$  on  $\rho_{ABE}^c$  and the state becomes  $\rho_{ABE}^{\zeta_i}$ . We now calculate the maximum amount of accessible information of Eve about  $\zeta_i$ . Then from Holevo theorem [81], we see the mutual information I(A:E) is bounded above as,

$$I(A:E) \le S\left(\sum_{\zeta \in \mathcal{B}} p_{\zeta} \rho_{ABE}^{\zeta}\right) - \sum_{\zeta \in \mathcal{B}} p_{\zeta} S(\rho_{ABE}^{\zeta})$$
(5)

where  $p_{\zeta} = \frac{1}{4}$ , the probability of randomly selecting one element from  $\mathcal{B}$ , and  $S(\cdot)$  is the Von Neumann entropy.

One can see that Alice's encoding and Bob's cover operations make a maximal mixture of the subsystems A and B. Thus we have  $S(\rho_{ABE}^{\zeta}) = 2$  for  $\zeta \in \mathcal{B}$ , and

$$I(A:E) \le S\left(\sum_{\zeta} p_{\zeta} \rho_{ABE}^{\zeta}\right) - 2,\tag{6}$$

and

$$\sum_{\zeta} p_{\zeta} \rho_{ABE}^{\zeta} = \rho_{AB}^{mix} \otimes Tr_{AB}(|\Phi_{ABE}\rangle \langle \Phi_{ABE}|)$$

$$= \rho_{AB}^{mix} \otimes \sum_{j=1}^{4} \delta_{j} |E_{j}\rangle \langle E_{j}|, \qquad (7)$$

where  $\rho_{AB}^{mix} = \frac{I}{4}$  is the maximally mixed state of the system AB. Now we have from Equation (7),

$$S\left(\sum_{\zeta} p_{\zeta} \rho_{ABE}^{\zeta}\right) = S\left(\rho_{AB}^{mix} \otimes \sum_{j=1}^{4} \delta_{j} |E_{j}\rangle \langle E_{j}|\right)$$
$$= S(\rho_{AB}^{mix}) + S\left(\sum_{j=1}^{4} \delta_{j} |E_{j}\rangle \langle E_{j}|\right)$$
$$= S\left(\frac{I}{4}\right) + \sum_{j=1}^{4} \delta_{j} \log \frac{1}{\delta_{j}}$$
$$= 2 + H(\delta_{j}),$$
(8)

where  $H(\cdot)$  represents the Shannon entropy function.

**Lemma 1:** For a probability distribution  $\{\delta_i, 1 \leq i \leq 4\}, -\sum_{i=1}^4 \delta_i \log \delta_i \leq h(\delta_2 + \delta_4) + h(\delta_3 + \delta_4)$ , where  $h(\cdot)$  represents the binary entropy function. (See appendix for proof.)

Then from Equation (6) and Equation (8),

$$I(A:E) \le H(\delta_j) = \sum_{j=1}^4 \delta_j \log \frac{1}{\delta_j}$$

$$\le h(\delta_3 + \delta_4) + h(\delta_2 + \delta_4) \text{ (by Lemma 1)}$$

$$= h(\epsilon_z) + h(\epsilon_x),$$
(9)

Let  $\epsilon_e$  be the error rate calculated after message decoding step, and if there is a discrete symmetric channel between Alice and Bob, then the secrecy capacity is

$$C_S \ge I(A:B) - I(A:E)$$
  

$$\ge H(A) - H(A|B) - h(\epsilon_z) - h(\epsilon_x)$$
  

$$= 2 - h(\epsilon_e) - h(\epsilon_z) - h(\epsilon_x).$$

For our protocol to be secure, we need  $C_S > 0$ , i.e.,  $2 - h(\epsilon_e) > h(\epsilon_z) + h(\epsilon_x)$ .

In the next two sections, we propose MDI-QD and MDI-DSQC protocols with mutual identity authentication respectively.

# 3 Proposed MDI-QD protocol with user authentication

In this section, we generalize the MDI-QSDC protocol into an MDI-QD protocol, which also provides mutual user authentication. Here, both Alice and Bob send their *n*-bit secret message to each other simultaneously after confirming the authenticity of the other user. They use one EPR pair to exchange one-bit messages from each other. Bob randomly prepares (n + c) EPR pairs  $|\Phi^+\rangle$  or  $|\Psi^+\rangle$   $(|\Phi^-\rangle$  or  $|\Psi^-\rangle$ ) corresponding to his secret message bit 0 (1), where *c* is the number of check bits. He also randomly prepares *k* EPR pairs from  $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$  for encoding the secret identity of Alice and inserts these into the previously prepared EPR sequence. After Alice receives the qubit sequence, he announces the positions of randomly prepared EPR pairs. Alice randomly applies Pauli operator *I* or  $\sigma_z$  ( $\sigma_x$  or  $i\sigma_y$ ) to encode her message bit 0 (1) (see Table (3)). The rest of the procedure is the same as the above MDI-QSDC protocol described in Section 2. The security of this protocol directly follows from the above MDI-QSDC protocol.

Message bit		Bob prepares	Alice's unitary	Final joint state
Alice	Bob	$(S_A, S_B)$	$S_A$ to $S'_A$	$(S'_A, S_B)$
0	0	$ \Phi^+ angle$	Ι	$ \Phi^+ angle$
			$\sigma_z$	$ \Phi^{-} angle$
		$ \Psi^+ angle$	Ι	$ \Psi^+ angle$
			$\sigma_z$	$ \Psi^{-} angle$
0		$ \Phi^{-} angle$	Ι	$ \Phi^{-} angle$
	1		$\sigma_z$	$ \Phi^+ angle$
	1	$ \Psi^{-} angle$	Ι	$ \Psi^{-} angle$
			$\sigma_z$	$ \Psi^+ angle$
1		$ \Phi^+ angle$	$\sigma_x$	$ \Psi^+ angle$
	0		$i\sigma_y$	$ \Psi^{-} angle$
	0	$ \Psi^+ angle$	$\sigma_x$	$ \Phi^+ angle$
			$i\sigma_y$	$ \Phi^{-} angle$
1	1	$ \Phi^{-} angle$	$\sigma_x$	$ \Psi^{-} angle$
			$i\sigma_y$	$ \Psi^+ angle$
		)T(-)	$\sigma_x$	$ \Phi^{-} angle$
		¥ /	$i\sigma_y$	$ \Phi^+ angle$

Table 3: Encoding rules of our proposed MDI-QD.

### 3.1 Example of our MDI-QD protocol

Let us now take an example of the above discussed MDI-QD with user authentication protocol, where we assume all channels are noiseless.

Suppose Alice (Bob) has the 3-bit secret message  $m_a = 011$  ( $m_b = 100$ ) and 4-bit secret identity  $Id_A = 1011$  ( $Id_B = 0111$ ), i.e., n = 3 and k = 2. Then the protocol is as follows.

1. Alice (Bob) chooses c = 2 check bits 10 (01) and inserts those bits in random positions of  $m_a \ (m_b)$ . Let the new bit string be  $m'_a = \mathbf{10101} \ (m'_b = \mathbf{10010})$  of length 5, where the bold numbers represent the check bits.

### 2. Bob:

(a) Prepares 5 EPR pairs corresponding to  $m'_b$  and those are

$$\left|\Psi^{-}\right\rangle_{a_{1}b_{1}}, \left|\Phi^{+}\right\rangle_{a_{3}b_{3}}, \left|\Psi^{+}\right\rangle_{a_{4}b_{4}}, \left|\Phi^{-}\right\rangle_{a_{6}b_{6}}, \text{ and } \left|\Phi^{+}\right\rangle_{a_{7}b_{7}}.$$

He separates the entangled qubit pairs into two particle sequences

 $S_A = \{a_1, a_3, a_4, a_6, a_7\}$  and  $S_B = \{b_1, b_3, b_4, b_6, b_7\},\$ 

each of length 5.

(b) He also randomly prepares 2 EPR pairs  $|\Phi^+\rangle_{a_2b_2}$  and  $|\Phi^-\rangle_{a_5b_5}$  and separates into two particle sequences  $C_A = \{a_2, a_5\}$  and  $C_B = \{b_2, b_5\}$ . He inserts the qubits of  $C_A$  and  $C_B$  into the sequences  $S_A$  and  $S_B$  to form two new sequences

 $S_A' = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7\} \text{ and } S_B' = \{b_1, b_2, b_3, b_4, b_5, b_6, b_7\}$ 

respectively.

- (c) Then he prepares 2 EPR pairs  $I_1 = |\Phi^-\rangle_{a'_1b'_1}$  and  $I_2 = |\Psi^-\rangle_{a_2b'_2}$  corresponding to his identity  $Id_B = 0111$ , and creates two single-qubit sequences  $I_A = \{a'_1, a'_2\}$  and  $I_B = \{b'_1, b'_2\}$  by separating the EPR pairs.
- (d) Bob chooses two sets  $D_A = \{ |+\rangle, |1\rangle, |0\rangle, |+\rangle \}$  and  $D_B = \{ |-\rangle, |0\rangle, |1\rangle, |0\rangle \}$ , each of d = 4 many decoy photons randomly prepared in Z-basis or X-basis. Then he randomly interleaves the qubits of  $I_A(I_B)$  and  $D_A(D_B)$  and  $S'_A(S'_B)$  (maintaining the relative ordering of each set) to get a new sequences of single qubits  $Q_A(Q_B)$ . Let

$$Q_A = \{a_1, a_2, a'_1, |+\rangle, a_3, |1\rangle, a'_2, a_4, a_5, |0\rangle, a_6, a_7, |+\rangle\}$$
  
and  $Q_B = \{b_1, b'_1, b_2, b_3, b_4, |-\rangle, |0\rangle, b'_2, b_5, |1\rangle, b_6, b_7, |0\rangle\}.$ 

- (e) Bob retains the  $Q_B$ -sequence and sends the  $Q_A$ -sequence to Alice through a quantum channel.
- (f) After Alice receives  $Q_A$ -sequence, Bob announces the positions of the qubits of  $C_A$  (2nd and 9th),  $I_A$  (3rd and 7th) and  $D_A$  (4th, 6th, 10th and 13th).

### 3. Alice:

(a) She separates the qubits of  $S_A$ ,  $C_A$ ,  $I_A$  and  $D_A$  from  $Q_A$ , i.e., she has

$$S_{A} = \{a_{1}, a_{3}, a_{4}, a_{6}, a_{7}\}, C_{A} = \{a_{2}, a_{5}\}, I_{A} = \{a_{1}', a_{2}'\} \text{ and } D_{A} = \{|+\rangle, |1\rangle, |0\rangle, |+\rangle\}.$$

She encodes  $m'_a = 10101$  and  $Id_A = 1011$  on the qubits of  $S_A$  and  $C_A$  respectively. After encoding the classical information, let  $S_A$  and  $C_A$  become  $S_A^1$  and  $C_A^1$  respectively. Then

$$S_A^1 = \{\sigma_x(a_1), \sigma_z(a_3), i\sigma_y(a_4), I(a_6), i\sigma_y(a_7)\}$$

and

$$C_A^1 = \{i\sigma_y(a_2), \sigma_z(a_5)\}$$

Then she randomly inserts the qubits of  $C_A^1$  into the  $S_A^1$  and let the new sequence be

$$S''_{A} = \{\sigma_x(a_1), i\sigma_y(a_2), \sigma_z(a_3), i\sigma_y(a_4), \sigma_z(a_5), I(a_6), i\sigma_y(a_7)\}.$$

(b) Alice randomly applies  $\sigma_z$  and I on the qubits of  $I_A$  and the resulting new sequence is  $I'_A = \{\sigma_z(a'_1), I(a'_2)\}$ . She randomly inserts the qubits of  $I'_A$  into random positions of  $S''_A$  and the new sequence is

$$Q'_A = \{\sigma_x(a_1), \sigma_z(a'_1), i\sigma_y(a_2), \sigma_z(a_3), I(a'_2), i\sigma_y(a_4), \sigma_z(a_5), I(a_6), i\sigma_y(a_7)\}.$$

(c) She randomly applies cover operations from  $\{I, i\sigma_y, H, i\sigma_y H\}$  on the qubits of  $D_A$  and the resulting new sequence is

$$D_A^1 = \{H(|+\rangle), i\sigma_y H(|1\rangle), i\sigma_y (|0\rangle), I(|+\rangle)\} = \{|0\rangle, |+\rangle, |1\rangle, |+\rangle\}.$$

- (d) Alice sends  $D_A^1$  to UTP to check the security of the channel from Bob to Alice.
- 4. After the UTP receives the sequence  $D_A^1$ , Bob announces the preparation bases (X, Z, Z) and X of the qubits of  $D_A$  and Alice announces the corresponding cover operations  $(H, i\sigma_y H, i\sigma_y \text{ and } I)$ .
- 5. UTP measures the qubits of  $D_A^1$  in proper bases (Z, X, Z and X) and announces the measurement results  $|0\rangle, |+\rangle, |1\rangle, |+\rangle$ . Since there is no error, Alice and Bob continue the protocol.
- 6. Alice prepares a new set of d' = 4 decoy photons  $D'_A = \{|0\rangle, |+\rangle, |-\rangle, |1\rangle\}$ . She inserts the decoy qubits into random positions of  $Q'_A$  and sends the resulting new sequence  $Q''_A$  to UTP, where

 $Q_A'' = \{\sigma_x(a_1), \sigma_z(a_1'), i\sigma_y(a_2), |0\rangle, \sigma_z(a_3), I(a_2'), |+\rangle, i\sigma_y(a_4), |-\rangle, \sigma_z(a_5), I(a_6), |1\rangle, i\sigma_y(a_7)\}.$ 

- 7. Alice announces the positions (4th, 7th, 9th and 12th) and the preparation bases (Z, X, X and Z) of the decoy qubits of  $D'_A$ . UTP measures the decoy qubits and publishes the measurement results  $|0\rangle$ ,  $|+\rangle$ ,  $|-\rangle$ ,  $|1\rangle$ . Since there is no error, Alice and Bob continue the protocol.
- 8. Bob sends the sequence  $Q_B$  to UTP and when all the qubits of  $Q_B$  are reached to UTP, Bob announces the positions (6th, 7th, 10th and 13th) and the preparation bases (X, Z, Z)and Z) of the decoy qubits of  $D_B$ . UTP measures those qubits in proper bases and discloses the measurement results  $|-\rangle$ ,  $|0\rangle$ ,  $|1\rangle$ ,  $|0\rangle$ . Then Bob calculates the error rate (which is zero for this example) in the quantum channel between Bob and UTP and goes to the next step.

#### 9. Authentication process:

- (a) Alice announces the positions (2nd and 6th) of the qubits of  $I'_A$  in the sequence  $Q''_A$ and Bob announces the positions (2nd and 8th) of the qubits of  $I_B$  in the sequence  $Q_B$ . UTP measures the *i*-th qubit pairs  $(\sigma_z(a'_1), b'_1)$  and  $(I(a'_2), b'_2)$  in Bell basis and announces the results  $|\Phi^+\rangle$  and  $|\Psi^-\rangle$ . As Alice knows  $Id_B = 0111$ , she knows the exact states of  $I_1 = |\Phi^-\rangle$  and  $I_2 = |\Psi^-\rangle$ . Since she randomly applied Pauli operators  $\sigma_z, I$  on  $a'_1, a'_2$  respectively, the joint state changes to  $|\Phi^+\rangle, |\Psi^-\rangle$ . Alice confirms Bob's identity and continues the protocol.
- (b) Alice announces the positions (2nd and 5th) of the qubits of  $C'_A$  in the sequence  $S''_A$ and UTP measures those qubits with their partner qubits from  $C_B = (b_2, b_5)$  in Bell bases and announces the measurement results  $|\Psi^-\rangle$ ,  $|\Phi^+\rangle$ . Since the initial states of the EPR pairs are  $|\Phi^+\rangle$ ,  $|\Phi^-\rangle$ , Bob decodes the identity of Alice as  $Id_A = 1011$  and confirms Alice as a legitimate party and continues the protocol.

- 10. The UTP measures each qubit pair from  $(S'_A, S_B)$  in Bell basis and announces the measurement result  $|\Phi^-\rangle$ ,  $|\Phi^-\rangle$ ,  $|\Phi^-\rangle$ ,  $|\Psi^-\rangle$ . From these results, Alice (Bob) decodes the classical bit string  $m'_b = 10010$  ( $m'_a = 10101$ ).
- 11. Alice and Bob publicly compare the random check bits to check the integrity of the messages. They discard those bits to obtain the secret message  $m_a = 011$  and  $m_b = 100$ . This completes the communication process.

# 4 Proposed MDI-DSQC Protocol with user authentication

In this section, we propose our new MDI-DSQC protocol with user identity authentication process.

Let Alice has an *n*-bit secret message m, which she wants to send Bob through a quantum channel with the help of some UTP, who performs all the measurements during the protocol. Alice and Bob have their 2k-bit secret user identities  $Id_A$  and  $Id_B$  respectively which they have shared previously by using some secured QKD. The protocol is as follows:

Steps 1, 2, 3(a) are the same as before in the MDI-DSQC protocol of Section 2.

3. Alice:

- (a) She separates the qubits of  $S_A$ ,  $I_A$  and  $D_A$  from  $Q_A$ . Then from the sequence  $S_A$  she randomly chooses N qubits to encode the secret message and the remaining k qubits are used to encode her secret identity  $Id_A$ . The encoding processes for m' and  $Id_A$  are the same. Alice encodes two bits of classical information into one qubit by applying an unitary operator. To encode 00,01,10 and 11 she applies the Pauli operators [76] I,  $\sigma_x$ ,  $i\sigma_y$  and  $\sigma_z$  respectively. After encoding the classical information, suppose  $S_A$  becomes  $S'_A$ .
- (b) Alice randomly applies I,  $\sigma_x$ ,  $i\sigma_y$  and  $\sigma_z$  on the qubits of  $I_A$  to get, say,  $I'_A$ . She randomly inserts the qubits of  $I'_A$  and  $D_A$  into random positions of  $S'_A$  and let the new sequence be  $Q'_A$ .
- (c) She randomly applies cover operations from  $\{I, i\sigma_y, H, i\sigma_yH\}$  on the qubits of  $Q'_A$  and inserts a new set of d' decoy photons  $D'_A$  into random positions of  $Q'_A$ , to obtain, say,  $Q''_A$ , which Alice sends to UTP.
- 4. After UTP receives the sequence  $Q''_A$ , Alice announces the positions and the preparation bases of the decoy qubits of  $D'_A$ . UTP measures the decoy qubits and publishes the measurement results, and Alice calculates the error in the quantum channel between Alice and UTP. If the estimated error is greater than some threshold value, then they terminate the protocol and otherwise go to the next step.
- 5. Bob sends the sequence  $Q_B$  to UTP and when all the qubits of  $Q_B$  are reached to UTP, Bob announces the positions and the preparation bases of the decoy qubits of  $D_B$ . UTP measures those qubits in proper bases and discloses the measurement results, and Bob calculates the error in the quantum channel between Bob and UTP. If the estimated error is greater than some threshold value, then they terminate the protocol and otherwise go to the next step.

- 6. To check the security of the quantum channel from Bob to Alice, Bob announces the preparation bases of the qubits of  $D_A$  and Alice announces the corresponding positions and the cover operations which she applies on those qubits. UTP measures those qubits, from the announced measurement results Alice and Bob calculate the error in the channel and decide to continue or stop the protocol.
- 7. UTP discards all the measured qubits and Alice announces all cover operations for the remaining qubits.
- 8. Authentication process: Same as before in the MDI-DSQC protocol of Section 2.
- 9. UTP measures each qubit pair from  $(S'_A, S_B)$  in Bell basis and announces the measurement result. From the knowledge of  $(S_A, S_B)$  and  $(S'_A, S_B)$ , Bob decodes the classical bit string m'.
- 10. Alice and Bob publicly compare the random check bits to check the integrity of the messages. If they find an acceptable error rate then Bob gets the secret message m and the communication process is completed.

Using similar arguments as in Section 2.2, we can prove the security of our proposed MDI-DSQC Protocol with user authentication.

### 4.1 Example of our MDI-DSQC protocol

Let us now take an example of the above discussed MDI-DSQC with user authentication protocol, where we assume all channels are noiseless.

Suppose Alice has a 6-bit secret message m = 011010 and the secret identities of Alice and Bob are  $Id_A = 1011$  and  $Id_B = 0111$  respectively, i.e., n = 6 and k = 2. Then the protocol is as follows.

1. Alice chooses c = 4 check bits 1001 and inserts those bits in random positions of m. Let the new bit string be m' = 0101100110 (bold numbers are check bits, i.e., the 2nd, 3rd, 7th and 9th bits) of length n + c = 10 = 2N, i.e., N = 5.

### 2. Bob:

(a) Randomly prepares N + k = 7 EPR pairs

$$\left|\Psi^{+}\right\rangle_{a_{1}b_{1}},\left|\Phi^{+}\right\rangle_{a_{2}b_{2}},\left|\Phi^{+}\right\rangle_{a_{3}b_{3}},\left|\Psi^{-}\right\rangle_{a_{4}b_{4}}\left|\Phi^{-}\right\rangle_{a_{5}b_{5}},\left|\Psi^{-}\right\rangle_{a_{6}b_{6}},\text{ and }\left|\Psi^{+}\right\rangle_{a_{7}b_{7}}$$

He separates the entangled qubit pairs into two particle sequences

$$S_A = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7\}$$
 and  $S_B = \{b_1, b_2, b_3, b_4, b_5, b_6, b_7\},\$ 

each of length 7.

(b) He also prepares 2 EPR pairs  $I_1 = |\Phi^-\rangle_{a'_1b'_1}$  and  $I_2 = |\Psi^-\rangle_{a_2b'_2}$  corresponding to his identity  $Id_B = 0111$ , and creates two single-qubit sequences  $I_A = \{a'_1, a'_2\}$  and  $I_B = \{b'_1, b'_2\}$  by separating the EPR pairs. (c) Bob chooses two sets  $D_A = \{ |+\rangle, |1\rangle, |0\rangle, |+\rangle \}$  and  $D_B = \{ |-\rangle, |0\rangle, |1\rangle, |0\rangle \}$ , each of d = 4 many decoy photons randomly prepared in Z-basis or X-basis. Then he randomly interleaves the qubits of  $I_A(I_B)$  and  $D_A(D_B)$  and  $S_A(S_B)$  (maintaining the relative ordering of each set) to get a new sequences of single qubits  $Q_A(Q_B)$ . Let

$$Q_{A} = \{a_{1}, a_{2}, a_{1}', |+\rangle, a_{3}, |1\rangle, a_{2}', a_{4}, a_{5}, |0\rangle, a_{6}, a_{7}, |+\rangle\}$$
  
and  $Q_{B} = \{b_{1}, b_{1}', b_{2}, b_{3}, b_{4}, |-\rangle, |0\rangle, b_{2}', b_{5}, |1\rangle, b_{6}, b_{7}, |0\rangle\}$ 

- (d) Bob retains the  $Q_B$ -sequence and sends the  $Q_A$ -sequence to Alice through a quantum channel.
- (e) After Alice receives  $Q_A$ -sequence, Bob announces the positions of the qubits of  $I_A$  (3rd and 7th) and  $D_A$  (4th, 6th, 10th and 13th).

# 3. Alice:

(a) She separates the qubits of  $S_A$ ,  $I_A$  and  $D_A$  from  $Q_A$ , i.e., she has

$$S_A = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7\}, I_A = \{a'_1, a'_2\} \text{ and } D_A = \{|+\rangle, |1\rangle, |0\rangle, |+\rangle\}.$$

She randomly chooses 5 qubits  $a_1, a_3, a_4, a_6$  and  $a_7$  from  $S_A$  to encode m' = 0101100110and the remaining 2 qubits  $a_2$  and  $a_5$  (say, the set  $C_A = \{a_2, a_5\}$ ) are used to encode  $Id_A = 1011$ . After encoding the classical information, let  $S_A$  become  $S'_A$ , then

$$S'_{A} = \{\sigma_x(a_1), i\sigma_y(a_2), \sigma_x(a_3), i\sigma_y(a_4), \sigma_z(a_5), \sigma_x(a_6), i\sigma_y(a_7)\}.$$

(b) Alice randomly applies  $\sigma_z$  and I on the qubits of  $I_A$  and the resulting new sequence is  $I'_A = \{\sigma_z(a'_1), I(a'_2)\}$ . She randomly inserts the qubits of  $I'_A$  and  $D_A$  into random positions of  $S'_A$  and the new sequence is

$$Q'_{A} = \{\sigma_{x}(a_{1}), \left|+\right\rangle, \sigma_{z}(a'_{1}), i\sigma_{y}(a_{2}), \left|1\right\rangle, \left|0\right\rangle, \sigma_{x}(a_{3}), I(a'_{2}), i\sigma_{y}(a_{4}), \left|+\right\rangle, \sigma_{z}(a_{5}), \sigma_{x}(a_{6}), i\sigma_{y}(a_{7})\}$$

(c) She randomly applies cover operations from  $\{I, i\sigma_y, H, i\sigma_y H\}$  on the qubits of  $Q'_A$  and the resulting new sequence is

$$\begin{aligned} Q'_{A}{}^{1} &= \{ i\sigma_{y}H\sigma_{x}(a_{1}), H(|+\rangle), I\sigma_{z}(a'_{1}), Hi\sigma_{y}(a_{2}), I(|1\rangle), i\sigma_{y}(|0\rangle), H\sigma_{x}(a_{3}), \\ HI(a'_{2}), i\sigma_{y}Hi\sigma_{y}(a_{4}), I(|+\rangle), i\sigma_{y}\sigma_{z}(a_{5}), i\sigma_{y}H\sigma_{x}(a_{6}), Hi\sigma_{y}(a_{7}) \}. \end{aligned}$$

Alice choses a set  $D'_A = \{ |-\rangle, |1\rangle, |0\rangle \}$  of d' = 3 decoy qubits randomly prepared in Z-basis or X-basis. Then she inserts those decoy qubits into some random positions of  $Q'_A$  and the resulting new sequence is

$$Q_A'' = \{ |-\rangle, i\sigma_y H \sigma_x(a_1), H(|+\rangle), I\sigma_z(a_1'), H i\sigma_y(a_2), I(|1\rangle), |1\rangle, i\sigma_y(|0\rangle), H\sigma_x(a_3), HI(a_2'), i\sigma_y H i\sigma_y(a_4), I(|+\rangle), i\sigma_y \sigma_z(a_5), i\sigma_y H \sigma_x(a_6), |0\rangle, H i\sigma_y(a_7) \}.$$

Alice sends  $Q''_A$  to UTP.

- 4. After the UTP receives the sequence  $Q''_A$ , Alice announces the positions (1st, 7th and 15th) and the preparation bases (X, Z and Z) of the decoy qubits of  $D'_A$ . UTP measures the decoy qubits and publishes the measurement results  $|-\rangle, |1\rangle, |0\rangle$ . Since there is no error, the quantum channel between Alice and UTP is secure and they continue the protocol.
- 5. Bob sends the sequence  $Q_B$  to UTP and when all the qubits of  $Q_B$  are reached to UTP, Bob announces the positions (6th, 7th, 10th and 13th) and the preparation bases (X, Z, Z)and Z) of the decoy qubits of  $D_B$ . UTP measures those qubits in proper bases and discloses the measurement results  $|-\rangle$ ,  $|0\rangle$ ,  $|1\rangle$ ,  $|0\rangle$ . Then Bob calculates the error rate (which is zero for this example) in the quantum channel between Bob and UTP and goes to the next step.
- 6. Bob announces the preparation bases (X, Z, Z and X) of the qubits of  $D_A$  and Alice announces the corresponding positions (3rd, 6th, 8th and 12th) in the sequence  $Q''_A$  and the cover operations  $(H, I, i\sigma_y \text{ and } I)$  which she applies on those qubits. UTP measures those qubits and from the announced measurement results, Alice and Bob find the channel is secure. They decide to continue the protocol.
- 7. UTP discards all the measured qubits from  $Q''_A$  and  $Q_B$ , then UTP has the following sequences

$$\begin{aligned} Q_A^1 &= \{ i\sigma_y H\sigma_x(a_1), I\sigma_z(a_1'), Hi\sigma_y(a_2), H\sigma_x(a_3), HI(a_2'), i\sigma_y Hi\sigma_y(a_4), \\ &i\sigma_y\sigma_z(a_5), i\sigma_y H\sigma_x(a_6), Hi\sigma_y(a_7) \} \end{aligned}$$

and

$$Q_B^1 = \{b_1, b_1', b_2, b_3, b_4, b_2', b_5, b_6, b_7\}.$$

Alice announces all cover operations  $(i\sigma_y H, I, H, H, H, i\sigma_y H, i\sigma_y, i\sigma_y H$  and H) for the qubits of  $Q_A^1$ . Then UTP applies the inverse of the cover operation on the corresponding qubits and gets back

$$Q_A^2 = \{\sigma_x(a_1), \sigma_z(a_1'), i\sigma_y(a_2), \sigma_x(a_3), I(a_2'), i\sigma_y(a_4), \sigma_z(a_5), \sigma_x(a_6), i\sigma_y(a_7)\}.$$

#### 8. Authentication process:

- (a) Alice announces the positions (2nd and 5th) of the qubits of  $I'_A$  in the sequence  $Q^2_A$ and Bob announces the positions (2nd and 6th) of the qubits of  $I_B$  in the sequence  $Q^1_B$ . UTP measures the qubit pairs  $(\sigma_z(a'_1), b'_1)$  and  $(I(a'_2), b'_2)$  in Bell basis and announces the results  $|\Phi^+\rangle$  and  $|\Psi^-\rangle$ . As Alice knows  $Id_B = 0111$ , she knows the exact states of  $I_1 = |\Phi^-\rangle$  and  $I_2 = |\Psi^-\rangle$ . Since she randomly applied Pauli operators  $\sigma_z$ , I on  $a'_1, a'_2$ respectively, the joint state changes to  $|\Phi^+\rangle$ ,  $|\Psi^-\rangle$ . Alice confirms Bob's identity and continues the protocol.
- (b) Alice announces the positions (2nd and 5th) of the qubits of  $C_A$  in the sequence  $S'_A$  and UTP measures those qubits with their partner qubits from  $S_B$  (say, the set  $C_B = (b_2, b_5)$ ) in Bell bases and announces the measurement results  $|\Psi^-\rangle$ ,  $|\Phi^+\rangle$ . Since the initial states of the EPR pairs are  $|\Phi^+\rangle$ ,  $|\Phi^-\rangle$ , Bob decodes the identity of Alice as  $Id_A = 1011$  and confirms Alice as a legitimate party and continues the protocol.

- 9. The UTP discards the measured qubits and measures the remaining qubit pairs from  $(S'_A, S_B)$  in Bell basis and announces the measurement result  $|\Phi^+\rangle$ ,  $|\Psi^+\rangle$ ,  $|\Phi^+\rangle$ ,  $|\Phi^-\rangle$ ,  $|\Phi^-\rangle$ . From these results, Bob decodes the classical bit string m' = 0101100110.
- 10. Alice and Bob publicly compare the random check bits (2nd, 3rd, 7th and 9th bits of m') to check the integrity of the messages. Bob discards those bits to obtain the secret message m = 011010 and the communication process is completed.

# 5 Conclusion

In this paper, we report the first-ever protocol for MDI-QSDC which provides mutual identity authentication of the users. Here, both the parties have their previously shared secret identity keys, and the sender first verifies the authenticity of the receiver and then sends the secret message with the help of a UTP, who performs all the measurements. Similarly, the receiver also verifies the sender's identity before receiving the message. Then we extend it to an MDI-QD protocol, where both the parties check the authenticity of the other party before exchanging their secret messages. Next, we also present an MDI-DSQC protocol with user authentication and analyses the security of these protocols.

# Appendix: Proof of Lemma 1

**Lemma 1:** For a probability distribution  $\{\delta_i, 1 \leq i \leq 4\}, -\sum_{i=1}^4 \delta_i \log \delta_i \leq h(\delta_2 + \delta_4) + h(\delta_3 + \delta_4),$ where  $h(\cdot)$  represents the binary entropy function.

**Proof:** Let X be a random variable such that

$$X = \begin{cases} 00 & \text{with probability } \delta_1, \\ 01 & \text{with probability } \delta_2, \\ 10 & \text{with probability } \delta_3, \\ 11 & \text{with probability } \delta_4. \end{cases}$$

Let Y and Z be the following events,

$$Y = \begin{cases} 1, & \text{if the least significant bit of } X = 1 \\ 0, & \text{otherwise.} \end{cases}$$
$$Z = \begin{cases} 1, & \text{if the most significant bit of } X = 1 \\ 0, & \text{otherwise.} \end{cases}$$

In other words,

$$Y = \begin{cases} 1 & \text{with probability } \delta_2 + \delta_4 \\ 0 & \text{with probability } \delta_1 + \delta_3. \end{cases}$$

and

$$Z = \begin{cases} 1 & \text{with probability } \delta_3 + \delta_4 , \\ 0 & \text{with probability } \delta_1 + \delta_2. \end{cases}$$
(10)

Then the entropy of the events Y and Z are as follows

$$H(Y) = -\sum_{y \in \{0,1\}} \Pr(Y = y) \log[\Pr(Y = y)] = h(\delta_2 + \delta_4).$$
$$H(Z) = -\sum_{z \in \{0,1\}} \Pr(Z = z) \log[\Pr(Z = z)] = h(\delta_3 + \delta_4).$$

The joint entropy H(Y, Z) of the events Y and Z is

$$\begin{split} H(Y,Z) &= -\sum_{y \in \{0,1\}} \sum_{z \in \{0,1\}} \Pr(Y = y, Z = z) log[\Pr(Y = y, Z = z)] \\ &= -\sum_{x \in \{00,01,10,11\}} \Pr(X = x) log[\Pr(X = x)] \\ &= -\sum_{i=1}^{4} \delta_i log \delta_i. \end{split}$$

Now using sub-additivity property of entropy, i.e., the fact that the joint entropy of a set of variables is less than or equal to the sum of the individual entropies of the variables in the set. Therefore,

$$H(Y, Z) \le H(Y) + H(Z)$$
  
or,  $-\sum_{i=1}^{4} \delta_i \log \delta_i \le h(\delta_2 + \delta_4) + h(\delta_3 + \delta_4).$ 

# References

- [1] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. arXiv preprint arXiv:2003.06557, 2020.
- [2] Stephen Wiesner. Conjugate coding. ACM Sigact News, 15(1):78-88, 1983.
- [3] Artur K Ekert. Quantum cryptography based on Bell's theorem. *Physical review letters*, 67(6):661, 1991.
- [4] Charles H Bennett. Quantum cryptography using any two nonorthogonal states. *Physical review letters*, 68(21):3121, 1992.
- [5] Gui-Lu Long and Xiao-Shu Liu. Theoretically efficient high-capacity quantum-keydistribution scheme. *Physical Review A*, 65(3):032302, 2002.
- [6] Jian Li, Na Li, Lei-Lei Li, and Tao Wang. One step quantum key distribution based on EPR entanglement. Scientific reports, 6:28767, 2016.
- [7] Charles H Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *Journal of cryptology*, 5(1):3–28, 1992.

- [8] Yi Zhao, Bing Qi, Xiongfeng Ma, Hoi-Kwong Lo, and Li Qian. Experimental quantum key distribution with decoy states. *Physical review letters*, 96(7):070502, 2006.
- [9] Zhiyuan Tang, Zhongfa Liao, Feihu Xu, Bing Qi, Li Qian, and Hoi-Kwong Lo. Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. *Physical review letters*, 112(19):190503, 2014.
- [10] Robert Bedington, Xueliang Bai, Edward Truong-Cao, Yue Chuan Tan, Kadir Durak, Aitor Villar Zafra, James A Grieve, Daniel KL Oi, and Alexander Ling. Nanosatellite experiments to enable future space-based QKD missions. *EPJ Quantum Technology*, 3(1):12, 2016.
- [11] Xiaoqing Zhong, Jianyong Hu, Marcos Curty, Li Qian, and Hoi-Kwong Lo. Proof-of-principle experimental demonstration of twin-field type quantum key distribution. *Physical Review Letters*, 123(10):100506, 2019.
- [12] Fu-Guo Deng, Gui Lu Long, and Xiao-Shu Liu. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. *Physical Review A*, 68(4):042317, 2003.
- [13] Fu-Guo Deng and Gui Lu Long. Secure direct communication with a quantum one-time pad. Physical Review A, 69(5):052319, 2004.
- [14] Chuan Wang, Fu-Guo Deng, Yan-Song Li, Xiao-Shu Liu, and Gui Lu Long. Quantum secure direct communication with high-dimension quantum superdense coding. *Physical Review A*, 71(4):044305, 2005.
- [15] Jian-Yong Hu, Bo Yu, Ming-Yong Jing, Lian-Tuan Xiao, Suo-Tang Jia, Guo-Qing Qin, and Gui-Lu Long. Experimental quantum secure direct communication with single photons. *Light: Science & Applications*, 5(9):e16144, 2016.
- [16] Wei Zhang, Dong-Sheng Ding, Yu-Bo Sheng, Lan Zhou, Bao-Sen Shi, and Guang-Can Guo. Quantum secure direct communication with quantum memory. *Physical review letters*, 118(22):220501, 2017.
- [17] Chen Xie, Lvzhou Li, Haozhen Situ, and Jianhao He. Semi-quantum secure direct communication scheme based on bell states. *International Journal of Theoretical Physics*, 57(6):1881– 1887, 2018.
- [18] Shan-Shan Chen, Lan Zhou, Wei Zhong, and Yu-Bo Sheng. Three-step three-party quantum secure direct communication. *Science China Physics, Mechanics & Astronomy*, 61(9):1–5, 2018.
- [19] Zheng Tao, Yan Chang, Shibin Zhang, Jinqiao Dai, and Xueyang Li. Two semi-quantum direct communication protocols with mutual authentication based on bell states. *International Journal of Theoretical Physics*, 58(9):2986–2993, 2019.
- [20] Jiawei Wu, Zaisheng Lin, Liuguo Yin, and Gui-Lu Long. Security of quantum secure direct communication based on wyner's wiretap channel theory. *Quantum Engineering*, 1(4):e26, 2019.

- [21] Georgi Bebrov and Rozalina Dimova. Efficient quantum secure direct communication protocol based on quantum channel compression. *International Journal of Theoretical Physics*, 59(2):426–435, 2020.
- [22] Lan Zhou, Yu-Bo Sheng, and Gui-Lu Long. Device-independent quantum secure direct communication against collective attacks. *Science Bulletin*, 65(1):12–20, 2020.
- [23] Lu Liu, Jia-Lei Niu, Chen-Rui Fan, Xue-Ting Feng, and Chuan Wang. High-dimensional measurement-device-independent quantum secure direct communication. *Quantum Information Processing*, 19(11):404, 2020.
- [24] Nayana Das and Goutam Paul. Cryptanalysis of quantum secure direct communication protocol with mutual authentication based on single photons and bell states. *Europhysics Letters, arXiv preprint arXiv:2007.03710*, 2020.
- [25] Nayana Das, Goutam Paul, and Ritajit Majumdar. Quantum secure direct communication with mutual authentication using a single basis. International Journal of Theoretical Physics, arXiv preprint arXiv:2101.03577, 2021.
- [26] Chuan Wang. Quantum secure direct communication: Intersection of communication and cryptography. Fundamental Research, 1(1):91–92, 2021.
- [27] Zhang-Dong Ye, Dong Pan, Zhen Sun, Chun-Guang Du, Liu-Guo Yin, and Gui-Lu Long. Generic security analysis framework for quantum secure direct communication. Frontiers of Physics, 16(2):1–9, 2021.
- [28] Gui-Lu Long and Haoran Zhang. Drastic increase of channel capacity in quantum secure direct communication using masking. *Science Bulletin*, 2021.
- [29] Lu Yin-Ju. A novel practical quantum secure direct communication protocol. International Journal of Theoretical Physics, pages 1–5, 2021.
- [30] Almut Beige, Berthold-Georg Englert, Christian Kurtsiefer, and Harald Weinfurter. Secure communication with single-photon two-qubit states. *Journal of Physics A: Mathematical and General*, 35(28):L407, 2002.
- [31] Cai Qing-Yu and Li Bai-Wen. Deterministic secure communication without using entanglement. Chinese Physics Letters, 21(4):601, 2004.
- [32] Marco Lucamarini and Stefano Mancini. Secure deterministic communication without entanglement. *Physical review letters*, 94(14):140501, 2005.
- [33] Gui-lu Long, Fu-guo Deng, Chuan Wang, Xi-han Li, Kai Wen, and Wan-ying Wang. Quantum secure direct communication and deterministic secure quantum communication. Frontiers of Physics in China, 2(3):251–272, 2007.
- [34] Xiao-Ming Xiu, Hai-Kuan Dong, Li Dong, Ya-Jun Gao, and Feng Chi. Deterministic secure quantum communication using four-particle genuine entangled state and entanglement swapping. Optics communications, 282(12):2457–2459, 2009.
- [35] Yong-Gang Hu. Deterministic secure quantum communication with four-qubit ghz states. International Journal of Theoretical Physics, 57(9):2831–2842, 2018.

- [36] Hao Yuan, Jun Song, Xiang-Yuan Liu, and Xiao-Feng Yin. Deterministic secure four-qubit ghz states three-step protocol for quantum communication. *International Journal of Theoretical Physics*, 58(11):3658–3666, 2019.
- [37] Tarek A Elsayed. Deterministic secure quantum communication with and without entanglement. Physica Scripta, 96(2):025101, 2020.
- [38] Ba An Nguyen. Quantum dialogue. Physics Letters A, 328(1):6–10, 2004.
- [39] Kim Boström and Timo Felbinger. Deterministic secure direct communication using entanglement. *Physical Review Letters*, 89(18):187902, 2002.
- [40] Man Zhong-Xiao, Zhang Zhan-Jun, and Li Yong. Quantum dialogue revisited. Chinese Physics Letters, 22(1):22, 2005.
- [41] Yan Xia, Chang-Bao Fu, Shou Zhang, Suc-Kyoung Hong, Kyu-Hwang Yeon, and Chung-In Um. Quantum dialogue by using the GHZ state. arXiv preprint quant-ph/0601127, 2006.
- [42] Ji Xin and Zhang Shou. Secure quantum dialogue based on single-photon. Chinese Physics, 15(7):1418, 2006.
- [43] Xia Yan, Song Jie, Nie Jing, and Song He-Shan. Controlled secure quantum dialogue using a pure entangled GHZ states. *Communications in Theoretical Physics*, 48(5):841, 2007.
- [44] Yong-gang Tan and Qing-Yu Cai. Classical correlation in quantum dialogue. International Journal of Quantum Information, 6(02):325–329, 2008.
- [45] Gan Gao. Two quantum dialogue protocols without information leakage. Optics communications, 283(10):2288–2293, 2010.
- [46] Arpita Maitra. Measurement device-independent quantum dialogue. Quantum Information Processing, 16(12):305, 2017.
- [47] Nayana Das and Goutam Paul. Two efficient measurement device independent quantum dialogue protocols. International Journal of Quantum Information, page 2050038, 2020.
- [48] Ting Gao, Feng-Li Yan, and Zhi-Xi Wang. Deterministic secure direct communication using GHZ states and swapping quantum entanglement. *Journal of Physics A: Mathematical and General*, 38(25):5761, 2005.
- [49] Xing-Ri Jin, Xin Ji, Ying-Qiao Zhang, Shou Zhang, Suc-Kyoung Hong, Kyu-Hwang Yeon, and Chung-In Um. Three-party quantum secure direct communication based on ghz states. *Physics Letters A*, 354(1-2):67–70, 2006.
- [50] Gao Ting, Yan Feng-Li, and Wang Zhi-Xi. A simultaneous quantum secure direct communication scheme between the central party and other m parties. *Chinese Physics Letters*, 22(10):2473, 2005.
- [51] Jian Wang, Quan Zhang, and Chao-jing Tang. Multiparty controlled quantum secure direct communication using greenberger-horne-zeilinger state. Optics Communications, 266(2):732-737, 2006.

- [52] Fei Gao, Su-Juan Qin, Qiao-Yan Wen, and Fu-Chen Zhu. Cryptanalysis of multiparty controlled quantum secure direct communication using greenberger-horne-zeilinger state. *Optics Communications*, 283(1):192–195, 2010.
- [53] Xiaoqing Tan, Xiaoqian Zhang, and Cui Liang. Multi-party quantum secure direct communication. 2014 Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing, pages 251–255, 2014.
- [54] Anindita Banerjee, Kishore Thapliyal, Chitra Shukla, and Anirban Pathak. Quantum conference. Quantum Information Processing, 17(7):1–22, 2018.
- [55] Ye-Feng He and Wen-Ping Ma. Multiparty quantum secure direct communication immune to collective noise. Quantum Information Processing, 18(1):1–11, 2019.
- [56] Nayana Das and Goutam Paul. Secure multi-party quantum conference and xor computation. Quantum Information and Computation, 21(3 & 4):0203-0232, 2021.
- [57] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Physical review letters*, 108(13):130503, 2012.
- [58] Vadim Makarov\* and Dag R Hjelme. Faked states attack on quantum cryptosystems. Journal of Modern Optics, 52(5):691–705, 2005.
- [59] Vadim Makarov, Andrey Anisimov, and Johannes Skaar. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Physical Review A*, 74(2):022313, 2006.
- [60] Bing Qi, Chi-Hang Fred Fung, Hoi-Kwong Lo, and Xiongfeng Ma. Time-shift attack in practical quantum cryptosystems. arXiv preprint quant-ph/0512080, 2005.
- [61] Vadim Makarov. Controlling passively quenched single photon detectors by bright light. New Journal of Physics, 11(6):065003, 2009.
- [62] Zeng Rong Zhou, Yu Bo Sheng, Peng-Hao Niu, Liu Guo Yin, GuiLu Long, and Lajos Hanzo. Measurement-device-independent quantum secure direct communication. *Science China Physics, Mechanics & Astronomy*, 63(3):1–6, 2020.
- [63] Peng-Hao Niu, Zeng-Rong Zhou, Zai-Sheng Lin, Yu-Bo Sheng, Liu-Guo Yin, and Gui-Lu Long. Measurement-device-independent quantum communication without encryption. *Sci*ence Bulletin, 63(20):1345–1350, 2018.
- [64] Xu-Dong Wu, Lan Zhou, Wei Zhong, and Yu-Bo Sheng. High-capacity measurementdevice-independent quantum secure direct communication. *Quantum Information Process*ing, 19(10):1–14, 2020.
- [65] Peng-Hao Niu, Jia-Wei Wu, Liu-Guo Yin, and Gui-Lu Long. Security analysis of measurement-device-independent quantum secure direct communication. *Quantum Information Processing*, 19(10):1–14, 2020.
- [66] Zi-Kang Zou, Lan Zhou, Wei Zhong, and Yu-Bo Sheng. Measurement-device-independent quantum secure direct communication of multiple degrees of freedom of a single photon. *EPL (Europhysics Letters)*, 131(4):40005, 2020.

- [67] Zikai Gao, Tao Li, and Zhenhua Li. Long-distance measurement-device-independent quantum secure direct communication. EPL (Europhysics Letters), 125(4):40004, 2019.
- [68] Nayana Das and Goutam Paul. Improving the security of "Measurement-device-independent quantum communication without encryption". *Science Bulletin*, 65(24):2048–2049, 2020.
- [69] Yu-Guang Yang, Jing-Ru Dong, Yong-Li Yang, Jian Li, Yi-Hua Zhou, and Wei-Min Shi. High-capacity measurement-device-independent deterministic secure quantum communication. *Quantum Information Processing*, 20(6):1–19, 2021.
- [70] Claude Crépeau and Louis Salvail. Quantum oblivious mutual identification. In International Conference on the Theory and Applications of Cryptographic Techniques, pages 133–146. Springer, 1995.
- [71] Hwayean Lee, Jongin Lim, and HyungJin Yang. Quantum direct communication with authentication. *Physical Review A*, 73(4):042305, 2006.
- [72] Zhan-jun Zhang, Jun Liu, Dong Wang, and Shou-hua Shi. Comment on "quantum direct communication with authentication". *Physical Review A*, 75(2):026301, 2007.
- [73] Liu Dan, Pei Chang-Xing, Quan Dong-Xiao, and Zhao Nan. A new quantum secure direct communication scheme with authentication. *Chinese Physics Letters*, 27(5):050306, 2010.
- [74] Yan Chang, Chunxiang Xu, Shibin Zhang, and Lili Yan. Controlled quantum secure direct communication and authentication protocol based on five-particle cluster state and quantum one-time pad. *Chinese science bulletin*, 59(21):2541–2546, 2014.
- [75] Tzonelih Hwang, Yi-Ping Luo, Chun-Wei Yang, and Tzu-Han Lin. Quantum authencryption: one-step authenticated quantum secure direct communications for off-line communicants. *Quantum information processing*, 13(4):925–933, 2014.
- [76] Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information. Cambridge University Press, 10th Anniversary edition, page 65, 2010.
- [77] Daniel Gottesman, H-K Lo, Norbert Lutkenhaus, and John Preskill. Security of quantum key distribution with imperfect devices. In *International Symposium onInformation Theory*, 2004. ISIT 2004. Proceedings., page 136. IEEE, 2004.
- [78] Imre Csiszár and Janos Korner. Broadcast channels with confidential messages. IEEE transactions on information theory, 24(3):339–348, 1978.
- [79] Renato Renner. Symmetry of large physical systems implies independence of subsystems. *Nature Physics*, 3(9):645–649, 2007.
- [80] Barbara Kraus, Nicolas Gisin, and Renato Renner. Lower and upper bounds on the secretkey rate for quantum key distribution protocols using one-way classical communication. *Physical review letters*, 95(8):080501, 2005.
- [81] Alexander Semenovich Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii*, 9(3):3–11, 1973.