J. Math. Math. Sci., 2022 (**1**), 87–102

INFORMATION-LEAKAGE-FREE QUANTUM DIALOGUE VIA GREENBERGER-HORNE-ZEILINGER STATES

Nguyen Ba An

(Received 1 January 2022; accepted 10 May 2022)

Abstract. Secure communication in general and secure dialogue in particular are highly demanded, especially in the current information exploding era. Here we are concerned with secure dialogue. Because any dialogue conducted merely by classical means is fully eavesdropped without traces left behind, quantum version of dialogue, the so-called quantum dialogue, offers a promising solution to the security problem. The security desired does not simply focus on the exchanged information but also on their classical correlations, i.e., a quantum dialogue protocol should be protected from both information theft and information leakage. Such a secure quantum dialogue protocol is proposed in this paper employing Greenberger–Horne–Zeilinger states as the quantum channel. The above-mentioned requirement for security is achieved in message rounds by using extra random bits for the encoding/decoding processes combined with two kinds of control rounds which are designed to detect eavesdropping, if any.

1. Introduction

Quantum mechanics (QM) was invented to make sense of physical phenomena occurring in the microscopic world. Theoretically, it is a set of postulates built to explore the invisible quantum universe. It is highly counter-intuitive exhibiting bizarre traits such as uncertainty relation, wave-particle duality, no-cloning theorem, impossibility to gain information without measurement, measurement yields probabilistic outcomes and collapses the measured object, etc. which are not encountered in the everyday macroscopic life.

Key words and phrases: Quantum dialogue, GHZ states, information leakage.

At the very heart of QM are the state superposition and quantum entanglement. If a quantum system can exist in either one of a number of different quantum states, then it can also exist in a state that is linearly superposed of those states. More surprisingly, if two quantum subsystems are entangled with each other, then they behave as a whole entity losing their individuality and from a probabilistic outcome of measurement on one subsystem the state of the other untouched subsystem can be deterministically predicted, regardless of the distance between the two subsystems. This constitutes what was commonly referred to as Einstein-Podolsky-Rosen (ERP) paradox, which, in Einstein's words, implies "*spooky action at a distance*" [1]. Based on the state superposition and quantum entanglement many intriguing protocols are possible such as quantum teleportation [2], quantum superdense coding [3], quantum secret sharing [4], remote state preparation [5], joint remote state preparation [6] and so on, all of which find no counterparts in the classical world.

Of importance is the topic of secure communication. Because classical communication is totally insecure, informative messages should not be directly transferred via public media means. Instead, encrypted messages are sent which will be decrypted upon receipt. Absolute security was proved in the private key system using an encryption technique that cannot be cracked (see, e.g., [7]): the communicating partners share in advance a secret key to encode/decode the real message. However, there is a big inconvenience because the partners must meet in person for key sharing and each key must be used only one time (so the name "one-time-pad" encryption). At present, widely used is the public key system [8] in which each partner has two keys, one is put in the public key directory accessible to everyone and the other kept secret. Either key can be used to encrypt the message but decryption requires both the keys. The two keys are created using a mathematical recipe in such a way that it is extremely hard to obtain the secret key from the known public key. Thus, any sender is able to use the public key of a wanted receiver to encrypt a message but only the relevant receiver could decrypt it. The public key system is very convenient because there is no need of a prior secret key sharing as in the private key system. Nevertheless, its security is not unconditional: whenever quantum computer (a future device that can, by performing a proper quantum algorithm, easily calculate the secret key given the public one) comes to birth the public key system will be entirely broken.

Because genuine quantum computer will sooner or later be produced, one may bypass the public key system and try to more creatively exploit the proved absolute security of the "one-time-pad" encryption. It would be nice if the secret key sharing process could be done remotely under the nose of an outsider who attempts to gain content of the key. In this connection, QM enters the game showing its power through quantum key distribution (QKD) protocols which rely on superposition principle [9] or quantum entanglement [10]. The

unconditional security of QKD protocols is guaranteed by the foundations of QM, in contrast to the public key system, which relies on the computational difficulty of reversing a certain one-way mathematical function. Although QKD can be made remotely, the real message cannot be read before QKD. Hence, a reasonable problem arises as for how can ones communicate securely in urgent situations when there is no time to perform any QKD protocol? To cope with such an issue, schemes of quantum secure direct communication (QSDC) [11, 12, 13, 14, 15] have been developed allowing sending secret messages from one partner to another without a prior QKD. Yet, QSDC is just a unidirectional protocol by which the partners cannot at the same time exchange their messages. In 2004 a new kind of protocol was, for the first time, devised which is bidirectional favoring two partners to communicate with each other without doing QKD in advance, i.e., in a fashion much like in a dialogue, so the terminology "quantum dialogue" (QD) [16] (see also [17]). Since then a great deal of QD protocols (see, e.g., [18, 19, 20, 21, 22, 23, 24, 25, 26, 27]) has been put forward under different angles and via various quantum resources.

Let Alice and Bob be two remote partners enjoying a QD protocol. In all the above-cited QD protocols, although Alice and Bob safely obtain each other's information, there exists a security loophole that any third party is able to obtain some classical correlation between the partners' information simply by listening to their public announcements [28, 29]. In information theory this kind of security loophole bears the name "information leakage". To get rid of the information leakage problem, a number of interesting protocols have been devised. Those protocols utilize different quantum resources/technologies such as EPR pairs [30], two-qutrit entangled states [31], W states [32], single quantum entangled states [33], single-photon states [34], auxiliary quantum operations [35], hyperentanglement [36], entanglement swapping [37], quantum authentication [38], single photons in both polarization and spatial-mode degrees of freedom [39] and reference frame independence combined with measurement device independence [40] and so on. However, the above proposals employ ordered batches of quantum states, so the full message can be read only at the end of a protocol, losing the taste of a dialogue.

In this paper we suggest an information-leakage-free quantum dialogue protocol using three-qubit Greenberger–Horne–Zeilinger (GHZ) states [41] of which two qubits travel forth and back between Alice and Bob. The desired security is ensured by random checking possible eavesdropping in both directions from Alice to Bob and vice versa. Classical correlations between Alice's and Bob's information are not leaked out to any unauthorized outsider thanks to a judicious fashion of encryption/decryption. In Section 2 we outline the GHZ states. Section 3 describes the encoding and decoding processes. Section 4 presents typical kinds of eavesdropping. Section 5 introduces methods to detect eavesdropping attacks. Section 6 is the quantum dialogue protocol.

Finally, Section 7 is the conclusion.

2. GHZ states

There are two non-equivalent classes of genuine tripartite entangled states, the GHZ class and the W one [42]. Here we are concerned with the GHZ class. In terms of the single-qubit Pauli operators

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{2.1}$$

and

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{2.2}$$

the complete set of the GHZ class consists of 8 orthonormal states $\{|G_{ijk}\rangle_{ABC}; i,j,k \in \{0,1\}\}$ that exhibit entanglement among three qubits A, B and C in the following form

$$|G_{i,j,k}\rangle_{ABC} = Z_A^i X_A^j \otimes X_B^k |G_{0,0,0}\rangle_{ABC}, \tag{2.3}$$

where $Z_A^i X_A^j$ act on qubit A, X_B^k on qubit B and

$$|G_{0,0,0}\rangle_{ABC} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ABC}, \tag{2.4}$$

with $|mnl\rangle_{ABC} \equiv |m\rangle_A \otimes |n\rangle_B \otimes |l\rangle_C \equiv |m\rangle_A |n\rangle_B |l\rangle_C$ for any $m,n,l \in \{0,1\}$. The entangled state$|G_{0,0,0}\rangle_{ABC}$ can be generated from the product state $|000\rangle_{ABC}$ by application of the unitary operators $CNOT_{AC}CNOT_{BC}H_C$, with H_C the single-qubit Hadarmard gate,

$$H_A |m\rangle_A = \frac{1}{\sqrt{2}}[(-1)^m |m\rangle_A + |m \oplus 1\rangle_A], \tag{2.5}$$

and $CNOT_{TC}$ the two-qubit controlled-NOT ($CNOT$) gate with C the control qubit and T the target one,

$$CNOT_{TC} |m\rangle_T |n\rangle_C = |m \oplus n\rangle_T |n\rangle_C, \tag{2.6}$$

where $\oplus$ represents the XOR operation. Indeed,

$$\begin{aligned} & CNOT_{AC}CNOT_{BC}H_C\left|000\right\rangle_{ABC} \\ = \; & CNOT_{AC}CNOT_{BC}\left|0\right\rangle_A\left|0\right\rangle_B\frac{(\left|0\right\rangle+\left|1\right\rangle)_C}{\sqrt{2}} \\ = \; & \frac{1}{\sqrt{2}}CNOT_{AC}\left|0\right\rangle_A(\left|00\right\rangle+\left|11\right\rangle)_{BC} \\ = \; & \frac{1}{\sqrt{2}}\left|000\right\rangle+\left|111\right\rangle)_{ABC}\equiv\left|G_{0,0,0}\right\rangle_{ABC}. \end{aligned} \tag{2.7}$$

Putting (2.4) into (2.3) and resorting to the action rule of the Pauli operators,

$$X^p\left|m\right\rangle=\left|m\oplus p\right\rangle, \tag{2.8}$$

$$Z^q\left|m\right\rangle=(-1)^{qm}\left|m\right\rangle, \tag{2.9}$$

where $\left|m\right\rangle$ is a Fock state with $m\in\{0,1\}$ and p,q are any nonnegative integers, we have another more explicit expression of $\left|G_{i,j,k}\right\rangle_{ABC}$:

$$\left|G_{i,j,k}\right\rangle_{ABC}=\frac{1}{\sqrt{2}}[\left|j\right\rangle_A\left|k\right\rangle_B\left|0\right\rangle_C+(-1)^i\left|j\oplus 1\right\rangle_A\left|k\oplus 1\right\rangle_B\left|1\right\rangle_C]. \tag{2.10}$$

Furthermore, in terms of two-qubit maximally entangled states (the Bell-states),

$$\left|\mathcal{B}_{mn}\right\rangle_{AB}=\frac{1}{\sqrt{2}}\sum_{s=0}^{1}(-1)^{ms}\left|s\right\rangle_A\left|s\oplus n\right\rangle_B \tag{2.11}$$

and the Hadamard-states

$$\left|\pm\right\rangle_C=\frac{1}{\sqrt{2}}(\left|0\right\rangle_C\pm\left|1\right\rangle_C), \tag{2.12}$$

$\left|G_{i,j,k}\right\rangle_{ABC}$ can also be re-expressed as

$$\left|G_{i,j,k}\right\rangle_{ABC}=\frac{1}{\sqrt{2}}[\left|\mathcal{B}_{i,j\oplus k}\right\rangle_{AB}\left|+\right\rangle_C+(-1)^j\left|\mathcal{B}_{i\oplus 1,j\oplus k}\right\rangle_{AB}\left|-\right\rangle_C]. \tag{2.13}$$

The expressions (2.3), (2.10) and (2.13) for $\left|G_{i,j,k}\right\rangle_{ABC}$ are helpful for later consideration.

3. Exchanging secret bits

Suppose that Alice has two secret bits a_1, a_2 while Bob has one secret bit b_1. How can they securely exchange their secret bits? As a reminder, the

security here is meant in the sense that no third party is able to learn *any* information about Alice's and Bob's bits, i.e., not only a_1, a_2, b_1 themselves but also their classical correlations (i.e., their XOR values) $a_1 \oplus a_2$, $a_1 \oplus b_1$, $a_2 \oplus b_1$, $a_1 \oplus a_2 \oplus b_1$ must be kept confidential from the outsider. To achieve such level of security Bob prepares a GHZ state $|G_{i,j,k}\rangle_{ABC}$ with certain $i, j, k \in \{0, 1\}$ which are picked up at his own choice (that is, except Bob noone knows the values of i, j, k). Bob keeps qubit C with himself but sends qubits A, B to Alice. Alice applies $Z_A^{a_1} X_A^{a_2}$ on qubit A and X_B^r on qubit B, with r a random bit, transforming $|G_{i,j,k}\rangle_{ABC}$ to $Z_A^{a_1} X_A^{a_2} \otimes X_B^r |G_{i,j,k}\rangle_{ABC}$. On one hand, using the relationships

$$X^a X^b = X^{a \oplus b}, \tag{3.1}$$

$$Z^a Z^b = Z^{a \oplus b}, \tag{3.2}$$

$$Z^a X^b = (-1)^{ab} X^b Z^a \tag{3.3}$$

and (2.3) we have (up to a common sign)

$$\begin{aligned} Z_A^{a_1} X_A^{a_2} \otimes X_B^r |G_{i,j,k}\rangle_{ABC} &= Z_A^{i \oplus a_1} X_A^{j \oplus a_2} \otimes X_B^{k \oplus r} |G_{0,0,0}\rangle_{ABC} \\ &= |G_{i \oplus a_1, j \oplus a_2, k \oplus r}\rangle_{ABC}. \end{aligned} \tag{3.4}$$

On the other hand, using (2.10) with the action rules (2.8) and (2.9) yields

$$\begin{aligned} & Z_A^{a_1} X_A^{a_2} \otimes X_B^r |G_{i,j,k}\rangle_{ABC} \\ = \; & \frac{1}{\sqrt{2}} Z_A^{a_1} X_A^{a_2} \otimes X_B^r [|j\rangle_A |k\rangle_B |0\rangle_C \\ & + (-1)^i |j \oplus 1\rangle_A |k \oplus 1\rangle_B |1\rangle_C] \\ = \; & \frac{1}{\sqrt{2}} [|j \oplus a_2\rangle_A |k \oplus r\rangle_B |0\rangle_C \\ & + (-1)^{i + a_1} |j \oplus a_2 \oplus 1\rangle_A |k \oplus r \oplus 1\rangle_B |1\rangle_C]. \end{aligned} \tag{3.5}$$

After application of $Z_A^{a_1} X_A^{a_2} \otimes X_B^r$ on $|G_{i,j,k}\rangle_{ABC}$, Alice sends qubits A, B back to Bob, who is able to extract Alice's bits a_1, a_2, r by performing a suitable joint measurement on the three qubits A, B, C. Namely, Bob's measurement proceeds as follows. First, he applies $H_C CNOT_{BC} CNOT_{AC}$ on $Z_A^{a_1} X_A^{a_2} \otimes$

$X_B^r \left|G_{i,j,k}\right\rangle_{ABC}$. By virtue of (2.5), (2.6) and (3.5) Bob gets

$$\begin{aligned}
& H_C CNOT_{BC} CNOT_{AC} Z_A^{a_1} X_A^{a_2} \otimes X_B^r \left|G_{i,j,k}\right\rangle_{ABC} \\
= \; & \frac{1}{\sqrt{2}} H_C CNOT_{BC} CNOT_{AC} [\left|j \oplus a_2\right\rangle_A \left|k \oplus r\right\rangle_B \left|0\right\rangle_C \\
& + (-1)^{(i \oplus a_1)} \left|j \oplus a_2 \oplus 1\right\rangle_A \left|k \oplus r \oplus 1\right\rangle_B \left|1\right\rangle_C] \\
= \; & \frac{1}{\sqrt{2}} \left|j \oplus a_2\right\rangle_A H_C CNOT_{BC} [\left|k \oplus r\right\rangle_B \left|0\right\rangle_C \\
& + (-1)^{(i \oplus a1)} \left|k \oplus r \oplus 1\right\rangle_B \left|1\right\rangle_C] \\
= \; & \frac{1}{\sqrt{2}} \left|j \oplus a_2\right\rangle_A \left|k \oplus r\right\rangle_B H_C [\left|0\right\rangle_C + (-1)^{(i \oplus a_1)} \left|1\right\rangle_C] \\
= \; & \left|j \oplus a_2\right\rangle_A \left|k \oplus r\right\rangle_B \left|i \oplus a_1\right\rangle_C . \qquad (3.6)
\end{aligned}$$

Next, since the qubits A, B, C have become disentangled, Bob independently measures each of them in their computational bases. If the outcomes of measurement on qubits A, B and C are respectively a, b and c, then, as seen from (3.6), $a = j \oplus a_2$, $b = k \oplus r$ and $c = i \oplus a_1$. Because Bob knew i, j and k, it is straightforward for him and only him to decode Alice's bits as $a_1 = c \oplus i$, $a_2 = a \oplus j$ and $r = b \oplus k$. Because the bit r is random, Bob can exploit it to hide his secret bit b_1 in $d = b_1 \oplus r$ and publicly announces d via a reliable (classical) channel to enable Alice to decode Bob's secret bit b_1 as $d \oplus r$. Only Alice is able to do the correct decoding because r was set by herself. Of course, a third party can hear d from Bob's public announcement but he/she can by no means infer b_1 from d because d itself is random thanks to the randomness of r.Note that d does not express any classical correlations between a_1, a_2 and b_1 so no information leakage occurs, in contrast to Refs. [18, 19, 20, 21, 22, 23, 24, 25, 26, 27]. All the above-described actions constitute a round called message round. In the message round the secret bits are exchanged securely between Alice and Bob without any information leakage, if there are no attacks from the outsider.

4. Outsider's attacks

In practice there is often an outside enemy intending to eavesdrop others' communication. Name such eavesdropper Eve who is supposed to be capable of doing anything allowed by the laws of QM. As qubit C remains always with Bob, Eve can physically attack only qubits A and B when they travel forth and back between Alice and Bob. Eve is aware that these qubits are members of a GHZ state, which is maximally entangled, so their reduced density matrix

is $I/2$ (I is the 2×2 identity matrix) and no information can be extracted from them. Hence, one of Eve's strategies is to disturb the secret bits' exchanging.

Eve can undertake the so-called measure-resend attack: when qubits A, B are traveling Eve measures them and then let them go on along their route. Eve may utilize either the computational basis $\{|0\rangle_A, |1\rangle_A\}$ to measure one qubit (say, qubit A) or the Bell basis $\{|\mathcal{B}_{mn}\rangle_{AB}; m, n \in \{0,1\}\}$ to measure two qubits A and B jointly. In case of the computational basis $|G_{i,j,k}\rangle_{ABC}$ collapses to $|j\rangle_A |k\rangle_B |0\rangle_C$ or $|j\oplus 1\rangle_A |k\oplus 1\rangle_B |1\rangle_C$],while in case of the Bell basis $|G_{i,j,k}\rangle_{ABC} \to |\mathcal{B}_{i,j\oplus k}\rangle_{AB} |+\rangle_C$ or $|\mathcal{B}_{i\oplus 1,j\oplus k}\rangle_{AB} |-\rangle_C$. In both cases the genuine tripartite entanglement is demolished and Bob's joint measurement on the three qubits A, B, C would generally yields the outcomes $a \neq j \oplus a_2$, $b \neq k \oplus r$ and $c \neq i \oplus a_1$. As a consequence, Bob's decoding is wrong and so is Alice's.

An easier way for Eve to disturb is application of the Pauli X operator on either qubit A or B. This does not destroy the tripartite entanglement but changes $|G_{i,j,k}\rangle_{ABC}$ to another GHZ state, i.e., modifies the quantum correlation on which Alice and Bob rely for securely exchanging their secret bits. Such type of disturbance is sometimes referred to as denial-of-service attack.

Also, Eve can implement another kind of attack in which she captures qubits A, B while they travel from Bob to Alice and replace them by two ancillary qubits A', B' which are of course not entangled with qubit C. By Eve's doing so, the bits that Alice and Bob decrypt would differ from those they expect to obtain. Because of the manner this kind of attack is implemented, it gets its own name too: the capture-replace attack. A disadvantage of the capture-replace attack is the cost to pay for ancillary qubits A', B'.

Interestingly, there is a delicate kind of attack under the name intercept-replace attack. This kind of attack allows Eve to gain full information at a cost of consuming additional quantum entanglement resource together with quantum memory. It is pretty wise and proceeds as follows. Eve prepares ahead a GHZ state $|G_{i'j'k'}\rangle_{A'B'C'}$ of her three qubits A', B', C' with certain i', j', k' chosen at her will and ambushes *en route* between Bob and Alice. When Bob sends qubits A, B of the state $|G_{ijk}\rangle_{ABC}$ to Alice, Eve intercepts them and stores them in her quantum memory. After that she keeps qubit C' with herself and sends qubits A', B' to Alice. Alice (being unaware of the qubits' substitution: $A, B \to A', B'$) encodes her secret bits a_1, a_2 on $A'$and a random bit r on B' then sends A', B' back to Bob. This time Eve intercepts the qubits A', B' and performs a suitable joint measurement on A', B', C' to learn the values of a_1, a_2 and r. Having known a_1, a_2, r Eve takes out the qubits A, B which she has previously stored in the quantum memory and encodes a_1, a_2 on qubit A while r on qubit B, followed by sending A, B back to Bob. Bob, with all the three qubits A, B, C at hand, is in the position to carry out a suitable joint measurement on the trio to readily infer the bits a_1, a_2, r. Finally, Bob

publicly discloses the bit $d = b_1 \oplus r$ from which not only Alice but also Eve can deduce Bob's secret bit $b_1 = d \oplus r$. In other words, by the intercept-replace attack Eve is able to eavesdrop all the secret bits that Alice and Bob have exchanged.

5. Unmasking eavesdropper

To detect presence of the eavesdropper Eve, Alice and Bob must deploy appropriate checking methods. One of the checking methods is like this. Alice and Bob switch the mode of actions from exchanging secret bits to detecting Eve's possible interference. Then, instead of the encoding procedure as in the message round mentioned in Section 3, Alice measures qubits A and B, while Bob measures qubit C, with their measurement outcomes to be compared. They have two options for their measurement bases. In the first option both Alice and Bob use the computational bases $\{|0\rangle_{A(B,C)}, |1\rangle_{A(B,C)}\}$. In the second option Alice uses the Bell basis $\{|\mathcal{B}_{mn}\rangle_{AB}; m, n \in \{0,1\}\}$ but Bob the Hadamard basis $\{|\pm\rangle_C\}$. If it is the first option and the measurement outcomes are $x, y, z \in \{0,1\}$ (corresponding to the event when Alice finds states $|x\rangle_A |y\rangle_B$ and Bob finds state $|z\rangle_C$) then, from (2.10), the outcomes must satisfy the following constraint: either $\{x = j, y = k, z = 0\}$ or $\{x = j \oplus 1, y = k \oplus 1, z = 1\}$. If it is the second option, then, from (2.13), the measurement outcomes must satisfy the constraint that Alice finds $|\mathcal{B}_{i,j\oplus k}\rangle_{AB}$ and Bob finds $|+\rangle_C$ or Alice finds $|\mathcal{B}_{i\oplus 1,j\oplus k}\rangle_{AB}$ and Bob finds $|-\rangle_C$. It can be verified that the above-specified constraints are generally violated by the denial-of-service, capture-replace and intercept-replace attacks. For the measure-resend attack, if Eve uses the computational basis when Alice and Bob choose the first option or if Eve uses the Bell basis when Alice and Bob choose the second option, then Eve safely passes the test. This feature helps to correctly design the checking method. In detail, Bob should decide to switch to the checking mode after Alice's confirmation of her receipt of qubits and only then Alice and Bob discuss with each other on the choice of measurement option. Because Eve undertakes the measure-resend attack earlier she does not know the option chosen by Alice and Bob. It is this fact that could unmask presence of Eve in the Bob-to-Alice route. However, Eve can attack on the Alice-to-Bob route as well. So, that route must also be 'guarded'. This time Alice is the person who decides to switch to the checking mode in which Alice encodes three random bits r_1, r_2, r_3 and sends the encoded qubits back to Bob. Upon Bob's receipt of the qubits Alice requests Bob to cooperate as follows. First, Bob performs the joint measurement on the three qubits A, B, C as described in Section 3 to obtain the outcomes a, b, c. After

that Alice tells Bob the values of r_1, r_2, r_3. Since Bob knows i, j, k he is able to check whether all the equalities $a = j \oplus r_2$, $b = k \oplus r_3$, $c = i \oplus r_1$ hold or not. Transparently, if Eve attacks along the Alice-to-Bob route then the above equalities will not be always held. Therefore, if both routes from Bob to Alice and from Alice to Bob are often put under checking processes the probability for Eve to survive is vanishing after a large enough number of checking process. To not confuse between the two kinds of checking processes, the round of checking in the Bob-to-Alice route is called forward checking round, while the round of checking in the Alice-to-Bob route is called backward checking round.

6. Quantum dialogue protocol

So far three kinds of rounds of action have been designed, which are message round, forward checking round and backward checking round. The message round allows Alice and Bob to exchange their bits, the forward checking round tests Eve's interference during the time when Bob sends his two qubits to Alice and the backward checking round controls the time when Alice returns the two qubits back to Bob.

Quantum dialogue protocol consists of a number of consecutive rounds of actions each of which takes place impromptu with a probability p_m, p_f and p_b ($p_m + p_f + p_b = 1$) for message round, forward checking round and backward checking round, respectively. If in a checking (either forward or backward) round Eve is unmasked, Alice and Bob abort the protocol. Otherwise, in each message round Alice "asks" by two bits and Bob "answers" by one bit. Therefore, message round by message round, it resembles that Alice and Bob "talk" one to another akin in a dialogue which is here quantum. Similarly to the calculations in Refs. [16, 26], for the present protocol the probability that Eve survives (i.e., remains masked) can also be evaluated which approaches zero for a long enough dialogue, i.e., the protocol is asymptotically secure against Eve's attacks.

A primitive version of the present quantum dialogue protocol that seems to boost capacity of the quantum channel can be thought of. Namely, in a message round, instead of encoding a_1, a_2, r, Alice may encode three secret bits a_1, a_2, a_3. Then, after decoding Alice's bits, Bob can also hide his three secret bits b_1, b_2, b_3 respectively into the encrypted bits $d_1 = a_1 \oplus b_1$, $d_2 = a_2 \oplus b_2$, $d_3 = a_3 \oplus b_3$, which are to be revealed openly. Since Alice knows a_1, a_2, a_3 she is able to easily decrypt Bob's bits as $b_1 = a_1 \oplus d_1$, $b_2 = a_2 \oplus d_2$, $b_3 = a_3 \oplus d_3$. In this way each partner can exchange three secret bits per GHZ state, a considerable increase in the quantum channel capacity. Unfortunately,

although Eve is unable to exploit the publicly announced bits d_1, d_2, d_3 to deduce Alice's and Bob's secret bits $a_1, a_2, a_3, b_1, b_2, b_3$ with certainty [27], she knows classical correlations between Alice's and Bob's bits through d_1, d_2, d_3. From the cryptography perspective, a protocol is secure if Eve cannot have any information about the secret communicated bits both before and after classical announcement. The just outlined primitive quantum dialogue protocol thus suffers a weakness under the name "information leakage". That is why in the present quantum dialogue protocol among the bits Alice encodes there is one random bit r. This random bit guarantees security of Bob's secret bit b_1 because from the published bit $d = b_1 \oplus r$ nobody except Alice is able to deduce b_1. It is this random bit that serves to prevent the present quantum dialogue protocol from information leakage.

Variations of the present protocol are possible. In the present protocol in a message round Alice can "ask" two bits a_1, a_2 but Bob can "answer" just one bit b_1. In case Alice needs to "ask" just one bit a_1 but Bob wishes to "answer" two bits b_1, b_2, they let each other know their intention. Upon their agreement, Alice now encodes a_1, r_1, r_2 with r_1, r_2 two random bits. Later, after deducing Alice's bits, Bob broadcasts two encrypted bits $d_1 = r_1 \oplus b_1$, $d_2 = r_2 \oplus b_2$. Obviously, only Alice is able to decode Bob's two secret bits b_1, b_2 from d_1, d_2 thanks to her knowledge of the random bits r_1, r_2. Such a modified quantum dialogue protocol is also free of information leakage.

Furthermore, the present protocol can be extended to be symmetric with respect to Alice and Bob in the sense that in each message round each of the two can communicate two secret bits with the other. Such a symmetric quantum dialogue protocol requires Bob to prepare fourpartite GHZ states of the form $|G_{ijkl}\rangle_{ABCD} = [|j\rangle_A |k\rangle_B |l\rangle_C |0\rangle_D + (-1)^i |j \oplus 1\rangle_A |k \oplus 1\rangle_B |l \oplus 1\rangle_C |1\rangle_D]/\sqrt{2}$ of which qubit D is kept at home but qubits A, B, C are sent to Alice. In this extended version of quantum dialogue Alice encodes on the qubits A, B, C four bits a_1, a_2, r_1, r_2 with a_1, a_2 being the two secret bits and r_1, r_2 two random ones. This provides room for Bob to encrypt his two secret bits b_1, b_2 into $d_1 = r_1 \oplus b_1$, $d_2 = r_2 \oplus b_2$ which will be safely decrypted only by Alice. The mathematical formulation of such a symmetric quantum dialogue protocol is cumbersome but straightforward, so we will not represent it in detail here.

7. Conclusion

In summary, we have proposed a quantum dialogue protocol which uses GHZ states as the working quantum channel. Two of the three qubits in the GHZ state travel like a shuttle between two remote partners carrying secret

and random bits: the secret bits can be exchanged safely while the random bits are to protect the quantum dialogue from information leakage. As in most bidirectional communication protocols, three kinds of rounds of actions, named message round, forward checking round and backward checking round, are designed in the present protocol. The message round serves as an exchanger of meaningful information between the communicators. The forward and backward checking rounds are to detect the eavesdropper's attacks in both routes between the communicators. The figure of merit in the present quantum dialogue protocol is its high level of security featured by keeping confidential not only the communicators' informative bits themselves but also any their classical correlations. In other words, the proposed quantum dialogue protocol is both safe and free of information leakage. In a message round of the present protocol Alice can communicate two bits with Bob, while Bob can communicate only one bit with Alice. Yet, we also outline possible variations of the present quantum dialogue protocol towards those in which Bob can communicate two bits with Alice and Alice communicates only one bit with Bob or Alice can communicate two bits with Bob and Bob can also communicate two bits with Alice. In theory, constructions of information-leakage-free quantum dialogue protocols for Alice and Bob to exchange any numbers of bits are possible, but the bigger number of exchangeable bits the higher scale of multipartite entanglement and the more complicated the manipulation of qubits.

References

[1] **Einstein A., Podolsky B. and Rosen N.**, *Can Quantum-Mechanical Description of Physical Reality be Considered Complete?*, Physical Review, **47** (1935), 777.

[2] **Bennett C. H., Brassard G., Crépeau C., Jozsa R., Peres A. and Wootters W. K.**, Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels, Physical Review Letters, **70** (1993), 1895.

[3] **Bennett C. H. and Wiesner S.**, *Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states*, Physical Review Letters, **69** (1992), 2881.

[4] **Hillery M., Buzek V. and Berthiaume A.**, *Quantum secret sharing*, Physical Review A, **59** (1999), 1829.

[5] **Bennett C. H., DiVincenzo D. P., Shor P. W., Smolin 0J. A., Terhal B. M. and Wootters W. K.**, *Remote state preparation*, Physical Review Letters, **87** (2001), 077902.

[6] **Nguyen B. A. and Kim J.**, *Joint remote state preparation*, Journal of Physics B, **41** (2008), 095501.

[7] **Shannon C.**, *Communication Theory of Secrecy Systems*, Bell System Technical Journal, **28** (1949), 656.

[8] **Rivest R., Shamir A. and Adleman L.**, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM, **21** (1978), 120.

[9] **Bennett C. H. and Brassard G.**, *Quantum cryptography: Public key distribution and coin tossing*, Proceedings of IEEE International Conference on Computers, Syst ems and Signal Processing, **175** (1984), 8.

[10] **Ekert A.**, *Quantum cryptography based on Bell's theorem*, Physical Review Letters, **67** (1991), 661.

[11] **Long G. L. and Liu X. S.**, *Theoretically efficient high-capacity quantum-key-distribution scheme*, Physical Review A, **65** (2002), 032302.

[12] **Bostrom K. and Felbinger T.**, *Deterministic secure direct communication using entanglement*, Physical Review Letters, **89** (2002), 187902.

[13] **Li X. H., Li C. Y., Deng F. G., Zhou P., Liang Y. J. and Zhou H. Y.**, *Quantum secure direct communication with quantum encryption based on pure entangled states*, Chinese Physics, **16** (2007), 2149.

[14] **Sun Z. W., Du R. G. and Long D. Y.**, *Quantum secure direct communication with two-photon fourqubit cluster states*, International Journal of Theoretical Physics, **51** (2012), 1946.

[15] **Liu D., Chen J. L. and Jiang W.**, *High-capacity quantum secure direct communication with single photons in both polarization and spatial- mode degrees of freedom*, International Journal of Theoretical Physics, **51** (2012), 2923.

[16] **Nguyen B. A.,** *Quantum dialogue,* Physics Letters A, **328** (2004), 6.

[17] **Nguyen B. A.**, *Secure Dialogue Without a Prior Key Distribution*, Journal of Korean Physical Society, **47** (2005), 562.

[18] **Jina X. R., Jia X., Zhang Y. Q., Zhang S., Hong S. K., Yeon K. H. and Um C. I.**, *Three-party quantum secure direct communicationbased on GHZ states*, Physics Letters A, **354** (2006), 67.

[19] **Ji X. and Zhang S.**, , Chinese Physics, 15 (2006), 1418.

[20] **Man Z. X., Xia Y. J. and Nguyen B. A.**, *Quantum secure direct communication by using GHZ states and entanglement swapping*, Journal of Physics B, **39** (2006), 3855.

[21] **Yang Y. G. and Wen Q. Y.**, *Quasi-secure quantum dialogue using single photons*, Science in China Series G: Physics, Mechanics and Astronomy, **50** (2007), 558.

[22] **Xia Y., Song J.and Song H. S.**, *Quantum dialogue using non-maximally entangled states based on entanglement swapping*, Physica Scripta, **76** (2007), 363.

[23] **Shan C. J., Liu J. B., Cheng W. W., Liu T. K., Huang Y. X. and Li H.**, *Bidirectional quantum secure direct communication in driven cavity QED*, Modern Physics Letters B, **23** (2009), 3225.

[24] **Dong L., Xiu X. M., Gao Y. J. and Chi F.**, *Quantum dialogue protocol using a class of three-photon W states*, Communications in Theoretical Physics, **52** (2009), 853.

[25] **Yin A. H.and Tang Z. H.**, *Two-step efficient quantum dialogue with three-particle entangled W state*, International Journal of Theoretical Physics, **53** (2014), 2760.

[26] **Nguyen B. A.**, *Quantum dialogue by nonselective measurements*, Advances in Natural Sciences: Nanoscience and Nanotechnology, **9** (2018), 025001.

[27] **Nguyen B. A.**, *Quantum dialogue mediated by EPR-type entangled coherent states*, Quantum Information Processing, **20** (2021), 100.

[28] **Gao F., Guo F. Z., Wen Q. Y. and Zhu F. C.**, *Revisiting the security of quantum dialogue and bidirectional quantum secure direct communication*, Science in China Series G: Physics, Mechanics and Astronomy, **51** (2008), 559.

[29] **Tan Y. G. and Cai Q. Y.**, *Classical correlation in quantum dialogue*, International Journal of Quantum Information, **6** (2008), 325.

[30] **Gao G.**, *Two quantum dialogue protocols without information leakage,* Optics Communications, **283** (2010), 2288.

[31] **Wang H., Zhang Y. Q. and Hu Y. P.**, *Efficient quantum dialogue by using the two-qutrit entangled states without information leakage*, International Journal of Theoretical Physics, **52** (2013), 1745.

[32] **Zhou N. R., Wu G. T., Gong L. H. and Liu S. Q.**, *Secure quantum dialogue protocol based on W states without information Leakage*, International Journal of Theoretical Physics, **52** (2013), 3204.

[33] **Ye T. Y.**, *Quantum Dialogue Without Information Leakage Using a Single Quantum Entangled State,* International Journal of Theoretical Physics, **53** (2014), 3719.

[34] **Zhou N. R., Hua T. X., Wu G. T., He C. S. and Zhang Y.**, *Single-Photon Secure Quantum Dialogue Protocol Without Information Leakage*, International Journal of Theoretical Physics, **53** (2014), 3829.

[35] **Huang L. Y. and Ye T. Y.,** *A Kind of Quantum Dialogue Protocols Without Information Leakage Assisted by Auxiliary Quantum Operation*, International Journal of Theoretical Physics, **54** (2015), 2494.

[36] **Liu Z. H., Chen H. W. and Liu W. J.**, *Information Leakage Problem in Efficient Bidirectional Quantum Secure Direct Communication with Single Photons in Both Polarization and Spatial-Mode Degrees of Freedom*, International Journal of Theoretical Physics, **55** (2016), 4681.

[37] **Liu Z. H. and Chen H. W.**, *Cryptanalysis and improvement of efficient quantum dialogue using entangled states and entanglement swapping without information leakage*, Quantum Information Processing, **16** (2017), 229.

[38] **Wang H., Zhang Y. Q.., Wu G. F. and Ma H.**, *Authenticated Quantum Dialogue Without Information Leakage*, Chinese Journal of Electronics, **27** (2018), 270.

[39] **Ye T. Y., Li H. K. and Hu J. L.**, *Information leakage resistant quantum dialogue with single photons in both polarization and spatial-mode degrees of freedom*, Quantum Information Processing, **20** (2021), 209.

[40] **Basak J., Maitra A. and Maitra S.**, *Improved and practical proposal for measurement device independent quantum dialogue*, Quantum Information Processing, **20** (2021), 361.

[41] **Greenberger D.M., HorneM. A., Zeilinger A.**, in M. Kafatos (ed.): *Bell's Theorem, Quantum Theory, and Conceptions of the Universe* (Kluwer, Dordrecht 1989, 73–76).

[42] **Dür W. Vidal G. and Cirac I. I.**, *Three qubits can be entangled in two inequivalent ways*, Physical Review A, **62** (2000), 062314.

Nguyen Ba An
Thang Long Institute of Mathematics and Applied Sciences
Thang Long University, Nghiem Xuan Yem, Hoang Mai
Hanoi
Vietnam
annb@thanglong.edu.vn