A generalized architecture of quantum secure direct communication for $N$ disjointed users with authentication

Ahmed Farouk$^{1,2}$, Magdy Zakaria$^2$, Adel Megahed$^3$ & Fatma A. Omara$^4$

In this paper, we generalize a secured direct communication process between $N$ users with partial and full cooperation of quantum server. So, $N-1$ disjointed users $u_1, u_2, \ldots, u_{N-1}$ can transmit a secret message of classical bits to a remote user $u_N$ by utilizing the property of dense coding and Pauli unitary transformations. The authentication process between the quantum server and the users are validated by EPR entangled pair and CNOT gate. Afterwards, the remained EPR will generate shared GHZ states which are used for directly transmitting the secret message. The partial cooperation process indicates that $N-1$ users can transmit a secret message directly to a remote user $u_N$ through a quantum channel. Furthermore, $N-1$ users and a remote user $u_N$ can communicate without an established quantum channel among them by a full cooperation process. The security analysis of authentication and communication processes against many types of attacks proved that the attacker cannot gain any information during intercepting either authentication or communication processes. Hence, the security of transmitted message among $N$ users is ensured as the attacker introduces an error probability irrespective of the sequence of measurement.

The pioneering work of Bennett and Brassard$^1$ has been developed for the purpose of understanding quantum cryptography which is one of the most significant aspects of the laws of the quantum mechanics. This cryptography guarantees unconditional security$^{2-5}$ that is proven through the no-cloning theorem$^6$ as the transmitted quantum bit cannot be replicated or copied but its state can be teleported. Quantum teleportation and dense coding are the most often used quantum principles. In the former, the quantum information can be transmitted based on both classical communication and the maximally shared quantum entanglement among the distant parties$^{7-10}$. In the latter, the classical information can be encoded and transmitted based on one quantum bit and on the maximally shared quantum entanglement among the distant parties as each quantum bit can transmit two classical bits$^{11,12}$. A number of approaches and prototypes can be used to exploit quantum principles in order to secure communication between two parties and multiple parties$^{13-17}$. While these approaches use different techniques to ensure private communication among authorized users, most of them still depend on the generation of secret random keys$^{18,19}$.

A quantum secret communication concept has recently been introduced; it is a kind of quantum communication in which secret messages can be transmitted through a quantum channel with or without additional classical communications$^{20-58}$. A quantum secure direct communication (QSDC) transmits the secret messages directly between the communicating parties, from sender to receiver, without additional classical communication protocols, except for those used for the necessary eavesdropping.

$^1$Information Technology Department, Al-Zahra College for Women, Oman. $^2$Faculty of Computer and Information Sciences, Mansoura University, Egypt. $^3$Faculty of Engineering, Cairo University, Egypt. $^4$Faculty of Computers and Information Sciences, Cairo University, Egypt. Correspondence and requests for materials should be addressed to A.F. (email: dr.ahmedfarouk85@yahoo.com)
check. In other words, the quantum key distribution (QKD) process and the classical communication of ciphertext are reduced into one single quantum communication procedure in QSDC. In QSDC, the concept of direct transmission of secret messages involves two kinds of meaning: On one hand, secret messages rather than raw keys are transmitted; on the other hand, the receiver does not require any separate classical communication from the sender to decode out secret messages\(^{6,31,32,39-52,57,59}\). In 2002, Long and Liu\(^2\) put forward the first QSDC protocol, in which the secret message is transmitted directly. In the same year, by taking advantage of Einstein-Podolsky-Rosen (EPR) pairs as quantum information carriers, Bostrom and Felbinger\(^2\) put forward the famous QSDC protocol referred to as the ping-pong protocol later. In\(^4\), the authors enhanced the capability of the ping-pong protocol by adding two more unitary operations. In\(^2\), a two-step quantum secure direct communication protocol was proposed for transferring quantum information by utilizing Einstein-Podolsky-Rosen (EPR) pair blocks to secure the transmission. In\(^5\), the authentication and communication process was performed using Greenberg–Horne–Zeilinger (GHZ) states. First, the GHZ states were used for authentication purposes; the remaining GHZ states were used to transmit the secret message directly. In\(^1\), the architecture for a centralized multicast scheme was proposed basing on a hybrid model of quantum key distribution and classical symmetric encryption. The proposed scheme solved the key generation and the management problem using a single entity called centralized Quantum Multicast Key Distribution Centre. In\(^6\), a novel multiparty concurrent quantum secure direct communication protocol based on GHZ states and dense coding is introduced. In\(^6\), a managed quantum secure direct communication protocol based on quantum encoding and incompletely entangled states is presented. In\(^7\), a scheme for quantum secure direct dialogue protocols, which is adapted to both collective-dephasing noise and collective-rotation noise, is proposed by using the logical Bell states as the traveling states to resist collective noise. Different from QSDC, there is another kind of quantum secret communication named deterministic secure quantum communication (DSQC), where the receiver needs a separate classical communication from the sender to help decode out secret messages. In the framework of DSQC, the receiver can read out the secret message only after the transmission of at least one bit of additional classical information for each quantum bit, different from QSDC in which the secret message can be read out directly without exchanging any classical information\(^20,23,24,26,29,36,38,53,55,56,58\). In\(^3\), a novel scheme for deterministic secure quantum communication (DSQC) over collective-rotation noisy channel is proposed as a four special two-qubit states are found can constitute a noise-free subspaces, and so are utilized as quantum information carriers. In 2002, Beige et al.\(^4\) first proposed a DSQC scheme based on single-photon two-quantum bit states. Then in 2004, Yan and Zhang\(^4\) proposed a DSQC scheme based on EPR pairs and quantum teleportation. In 2005, Gao et al.\(^5\) and Man et al.\(^6\) proposed two DSQC protocols also based on entanglement swapping. In 2006, with EPR pairs based on the secret transmitting order of particles, Zhu et al.\(^20\) proposed two DSQC schemes, one is a round trip scheme, and the other is a one way trip scheme. Lee et al.\(^23\) proposed a protocol for controlled DSQC with Greenberger–Horne–Zeilinger (GHZ) states. In 2009, Xiu et al.\(^26\) proposed a controlled DSQC scheme using five qubit entangled states and two-step security test. In\(^6\), a hyper entangled Bell state is used to design faithful deterministic secure quantum communication and authentication protocol over collective-rotation and collective-dephasing noisy channel, which doubles the channel capacity compared with using an ordinary Bell state as a carrier; a logical hyper entangled Bell state immune to collective-rotation and collective-dephasing noise is constructed. Different quantum authentication approaches have been developed for preventing various types of attacks and especially man-in-the-middle attack\(^62–66\).

However, these quantum secure direct communication approaches are still prone to provide a low degree of effectiveness and an inadequate level of security. Here, we propose a convenient and efficient scheme for transmitting a series of classical messages among two, three, or more users (generalized to \(N\) users). Therefore, \(N – 1\) disjointed users \(u_1, u_2, \ldots, u_{N-1}\) can transmit a secret message consisting of classical bits to a remote user \(u_N\). The transmission process is accomplished by utilizing the property of dense coding and Pauli unitary transformations. First, the quantum server authenticates and verifies the identities of the communicated disjointed users through the generated entangled shared key and the Controlled-\(\neg\)NOT gate. After the authentication is completed successfully, the remaining generated entangled shared key is used to generate shared GHZ states, which are intended for directly transmitting the secret message. If there is a quantum channel among the users, they can communicate using our partial cooperation process. In that case, \(N – 1\) disjointed users generate a random sequence of bit strings of the transmitted plain message. Next, each user applies an appropriate unitary transformation according to his plain message bit string value and transmits the transformed message to \(u_N\). Then, \(u_N\) retrieves the original sent secret message by applying the \(N – \text{GHZ}\) measurement to his/her particle and \(u_1, u_2, \ldots, u_{N-1}\) particles. Afterwards, the quantum server calculates the status of his or her particle according to \(x\) basis and announces his or her measurement results. Then, \(u_N\) uses those measurements and the quantum server publication to retrieve the original sent secret bits by \(u_1, u_2, \ldots, u_{N-1}\). If there is no quantum channel among the users, they can use our full cooperation process, but in this case the transformed message will be sent to the quantum server instead of \(u_N\).

The efficiency and effectiveness of our protocol can be summarized into five points. First, the GHZ state is the maximally entangled state, so that the correlation can be more easily destroyed once any single \(N\) particle is attacking. Second, using the \(N – \text{GHZ}\) particle makes eavesdropping detection more
effective and secure in comparison to some of the other QSDC protocols. For example\textsuperscript{22}, proposed a two-step quantum secure direct communication where an EPR pair block is used to transfer the secret message. Furthermore\textsuperscript{24}, proposed a multi-step quantum secure direct communication protocol where blocks of a multi-particle maximally entangled states are used to transmit secret messages. These protocols fail because the eavesdropper can capture some of the particles in the sequence and transmit what is left to the receiver through the quantum channel. If the eavesdropper intercepts the message sequence and conducts a GHZ measurement, he/she can retrieve some of the secret message. Therefore, the probability of information leakage exists. Third, our protocol increases the transmitted information capacity by using $N - GHZ$ states as these provide a large Hilbert space. Fourth, $N - 1$ users can transmit a particular message to the receiver, $u_{N}$, so the protocol is more effective as no quantum bits have to be discarded. Furthermore, the protocol is instantaneous as the receiver, $u_{N}$, is able to decode the message while receiving it and there is no additional classical exchange between $N - 1$ (sender) users and $u_{N}$ (receiver). Finally, the security analysis of the authentication and communication processes of our protocol against many types of attacks proves that our protocol is unconditionally secured and the attacker will not reveal any information about the key or the transmitted message in the case of directly calculating the transferred particles over the communicated channel from the quantum server to the disjoint user, and vice versa, as the attacker introduces an error probability irrespective of the sequence of measurement.

**Methods**

**Bell States and Controlled – NOT.** The Bell states are one of the main theories of quantum information processing that denote entanglement\textsuperscript{65,68}. Bell states are specific, highly entangled quantum states of two particles denoted by EPR. There are many research groups that proposed different approaches for realizing and experimentally generating EPR states. In\textsuperscript{69} a high-intensity source of polarization-entangled photon pairs can be realized with high momentum definition. The proposed scheme allowed ready preparation of all four of EPR-Bell states with two-photon fringe visibilities in excess of 97%. In\textsuperscript{70} EPR can be experimentally setup by utilizing light pulse from a mode-locked Ti-sapphire laser through a frequency doubler. The ultraviolet pulse from the doubler is split into two beams by a balanced beam-splitter and is focused on four pairs of BBO crystals to provide four EPR photon pairs. In our scheme, EPR pair can be realized by utilizing the same concept introduced in\textsuperscript{70}.

These entangled particles have interrelated physical characteristics despite being spatially separated. When the quantum state is a multi-qubit, transformation can be achieved by applying the controlled quantum gates CNOT (Controlled – NOT), FREDKIN (Controlled – SWAP), and TOFFOLI (Controlled – Controlled – NOT). CNOT has an input of two qubits. It transforms the computational basis states by flipping the state of the second qubit only when the first qubit has a measurement of 1; otherwise, the quantum state remains unchanged\textsuperscript{2,3,5,7,11}. The four Bell states (EPR pairs) used in both the authentication and communication processes in our scheme are defined by (Eq. (1)). Authentication between the quantum server and users is achieved by the generated entangled shared key $|\Phi_{qu}^{+}\rangle$ and the Controlled – NOT gate. At the time of registration, the quantum server and disjoint user share a binary authentication key, $A_{K}$. Each sends one entangled particle to form an EPR pair, $|\Phi_{qu}^{+}\rangle$, in which the $q$ and $u$ particles correspond with the quantum server and disjoint user, respectively. The quantum server preserves $q$ at its location and transmits the $u$ particle to the intended disjoint user, as shown in (Eq. (2)). Once the disjoint user obtains its particle, it prepares a new state particle, $n$ (See Eq. (3)), by encoding the shared authentication information according to the specified operation. When the quantum CNOT gate $\mathcal{C}_{op}$ is performed on the transmitted particle and $n$, the resulted particle $r$ is a state of three entanglement particles (See Eq. 4). After applying the requested operation, the disjoint user keeps particle $u$ at its side and sends the resulted particle $|\Phi_{r}\rangle$ to the quantum server. Once the quantum server receives the resulted particle, $|\Phi_{r}\rangle$, it decodes it by applying a quantum CNOT gate $\mathcal{C}_{op}$ on both the local particle $q$ and $n$ (See Eq. 6, 7). The quantum server verifies the identity of the disjoint user by measuring $|\psi_{u}\rangle$ on the basis of $Z$. The resulted state must measure at either 0 or 1. If the measurement is equal to $|A_{2i - 1}\rangle$, the disjoint user is authenticated. However, if the resulted measurement is erroneous—meaning it is greater than the agreed threshold—then the authentication process will be terminated. Afterwards, the key is increased to authenticate the next disjoint user, sending the quantum server recursively back to step one until all disjoint users are authenticated.

$$\begin{align*}
|\Phi^{\pm}\rangle &= \frac{1}{\sqrt{2}} (|00\rangle \pm |11\rangle),
|\psi^{\pm}\rangle &= \frac{1}{\sqrt{2}} (|01\rangle \pm |10\rangle) \\
|\Phi_{qu}^{+}\rangle &= \frac{1}{\sqrt{2}} (|0_{q}0_{u}\rangle + |1_{q}1_{u}\rangle) \\
|\psi_{u}\rangle &= |A_{2i - 1} \otimes A_{2i}\rangle
\end{align*}$$

(1)
where \( 1 \leq i \leq N \) and \( \otimes \) denotes the specified user operation.

\[
|\Phi_i\rangle = \mathcal{C}_{OP}(|\phi_i\rangle \otimes |\Phi_i^+\rangle)
\]

(4)

where \( \mathcal{C}_{OP} = \mathcal{C}_0 \) at \( A_{2i-1} = 0 \) and \( \mathcal{C}_{OP} = \mathcal{C}_1 \) at \( A_{2i-1} = 1 \). \( \mathcal{C}_0 \) and \( \mathcal{C}_1 \) are described by (Eq. (5))

\[
\mathcal{C}_0 = |0\rangle \langle 0| \otimes I + |1\rangle \langle 1| \otimes X,
\]

\[
\mathcal{C}_1 = |+\rangle \langle +| \otimes I + |\rangle \langle \rangle \otimes X
\]

(5)

where \( |+\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \), \( |-\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \)

\[
|\Phi_i\rangle = \mathcal{C}_{OP}(|\Phi_i\rangle)
\]

(6)

\[
|\Phi_i^+\rangle = \mathcal{C}_{OP}(x |\phi_i\rangle \otimes |\Phi_i^\perp\rangle)
\]

(7)

Quantum Bit Transformation. Quantum computers can manipulate quantum information to transform a pure or mixed quantum state into another corresponding pure or mixed state2,3,5,7,11. In our scheme, the unitary transformation operations are defined by (Eq. (8)). For simplicity, we use \( X, Y, Z \) instead of \( \sigma_x, i\sigma_y, \sigma_z \), respectively. These are used to transform the GHZ state at the side of the sender(s) into an unreadable form that corresponds to the generated original classical message before transmitting it to the receiver.

\[
I = |0\rangle \langle 0| + |1\rangle \langle 1|
\]

\[
X = |0\rangle \langle 1| + |1\rangle \langle 0|
\]

\[
Y = |0\rangle \langle 1| - |1\rangle \langle 0|
\]

\[
Z = |0\rangle \langle 0| - |1\rangle \langle 1|
\]

(8)

Tables 1–4 describe the correlation between the received classical value and its corresponding unitary and GHZ transformations. Tables 1 and 2 illustrate the correlation that occurs during the communication process between two disjoint users (\( u_i, u_j \)) with partial and full cooperation of the quantum server, respectively. The \( u_i \) generates a sequence of random bit strings of transmitted, plain message. According to each two transmitted bits, (00, 01, 10, 11), the disjoint user, \( u_j \), applies one of the unitary transformation operations, \( \hat{U} = \{ \hat{U}_1, \hat{U}_2, \hat{U}_3, \hat{U}_4 \} \), which correspond to the four Pauli operations, \( \{ I, X, Y, Z \} \), respectively. Afterwards, the GHZ states convert according to the transmitted bits and the \( u_j \) transformation.

| Value | First Bit | Second Bit | \( u_i \) Transformation | GHZ Transformation |
|-------|-----------|------------|-------------------------|-------------------|
| 0     | 0         | 0          | \( I_u \)               | \( \frac{1}{2}(|\Phi_i^0\rangle + |\Phi_i^1\rangle + \langle \Phi_i^0| - \langle \Phi_i^1|) \) |
| 1     | 0         | 1          | \( X_u \)               | \( \frac{1}{2}(|\Phi_i^0\rangle + |\Phi_i^1\rangle - \langle \Phi_i^0| + \langle \Phi_i^1|) \) |
| 2     | 1         | 0          | \( Y_u \)               | \( \frac{1}{2}(|\Phi_i^0\rangle + |\Phi_i^1\rangle + \langle \Phi_i^0| - \langle \Phi_i^1|) \) |
| 3     | 1         | 1          | \( Z_u \)               | \( \frac{1}{2}(|\Phi_i^0\rangle + |\Phi_i^1\rangle + \langle \Phi_i^0| + \langle \Phi_i^1|) \) |

Table 1. Correlation between Received Classical Value and its Corresponding Unitary, GHZ Transformations and Quantum Bit Transformation Correlation during the Communication Process between Two Disjoint Users with Partial Cooperation of Quantum Server.

| Value | First Bit | Second Bit | \( u_i \) Transformation | GHZ Transformation |
|-------|-----------|------------|-------------------------|-------------------|
| 0     | 0         | 0          | \( I_u \)               | \( \frac{1}{2}(|\Phi_i^0\rangle + |\Phi_i^1\rangle + \langle \Phi_i^0| - \langle \Phi_i^1|) \) |
| 1     | 0         | 1          | \( X_u \)               | \( \frac{1}{2}(|\Phi_i^0\rangle + |\Phi_i^1\rangle - \langle \Phi_i^0| + \langle \Phi_i^1|) \) |
| 2     | 1         | 0          | \( Y_u \)               | \( \frac{1}{2}(|\Phi_i^0\rangle + |\Phi_i^1\rangle + \langle \Phi_i^0| - \langle \Phi_i^1|) \) |
| 3     | 1         | 1          | \( Z_u \)               | \( \frac{1}{2}(|\Phi_i^0\rangle + |\Phi_i^1\rangle + \langle \Phi_i^0| + \langle \Phi_i^1|) \) |

Table 2. Correlation between Received Classical Value and its Corresponding Unitary, GHZ Transformations and Quantum Bit Transformation Correlation during the Communication Process between Two Disjoint Users with Full Cooperation of Quantum Server.
(See Supplementary Information 1) for the communication process between two disjointed users with partial and full cooperation of the quantum server).

Tables 3 and 4 describe the same correlation but among three disjointed users (ui, uj and uk) with partial and full cooperation of quantum server respectively. The difference is new user uk among Three Disjoint Users with Full Cooperation of Quantum Server.

GHZ States, Measurement and Source. A GHZ state is a certain type of maximally entangled quantum state that includes at least three qubits (particles). This kind of state was first examined by Greenberger, Horne, and Zeilinger in 1989. The standard GHZ state is defined as a qubits = 3; when qubits > 3, the GHZ state is defined by Eq. (9) seen below:

$$|\text{GHZ}\rangle = \frac{|0\rangle^{\otimes \text{qubits}} + |1\rangle^{\otimes \text{qubits}}}{\sqrt{2}}$$

In our scheme, when the quantum server receives a user’s request for communication with another user, the quantum server distributes GHZ entanglement states among the involved participants’ users in the communication process. Distribution is established after successful completion of the authentication process prior to the commencement of the communication process. The quantum server distributes all generated particles but holds one for itself. As a consequence, the quantum server and the participated users become entangled due to the presence of only one particle per distributed GHZ state. In addition, GHZ measurement is used by the receiver or quantum server, depending on the type of cooperation used during inter-user communication. Consistent with the GHZ measurement result, the receiver determines

| Value | ui Bits | uj Bit | uk Bit | ui and uj Transformations | GHZ Transformations |
|-------|---------|--------|--------|--------------------------|-------------------|
| 0     | 0       | 0      | 0      | (I_u \otimes I_u)        | \frac{1}{\sqrt{2}} (|\Psi\rangle_{ul} + |\phi\rangle_{ul}) |
| 1     | 0       | 0      | 1      | (I_u \otimes X_u)        | \frac{1}{\sqrt{2}} (|\Psi\rangle_{ul} + |\phi\rangle_{ul}) |
| 2     | 0       | 1      | 0      | (X_u \otimes I_u)        | \frac{1}{\sqrt{2}} (|\Psi\rangle_{ul} + |\phi\rangle_{ul}) |
| 3     | 0       | 1      | 1      | (X_u \otimes X_u)        | \frac{1}{\sqrt{2}} (|\Psi\rangle_{ul} + |\phi\rangle_{ul}) |
| 4     | 1       | 0      | 0      | (Y_u \otimes I_u)        | \frac{1}{\sqrt{2}} (|\Psi\rangle_{ul} + |\phi\rangle_{ul}) |
| 5     | 1       | 0      | 1      | (Y_u \otimes X_u)        | \frac{1}{\sqrt{2}} (|\Psi\rangle_{ul} + |\phi\rangle_{ul}) |
| 6     | 1       | 1      | 0      | (Z_u \otimes I_u)        | \frac{1}{\sqrt{2}} (|\Psi\rangle_{ul} + |\phi\rangle_{ul}) |
| 7     | 1       | 1      | 1      | (Z_u \otimes X_u)        | \frac{1}{\sqrt{2}} (|\Psi\rangle_{ul} + |\phi\rangle_{ul}) |

Table 3. Correlation between Received Classical Value and its Corresponding Unitary, GHZ Transformations and Quantum Bit Transformation Correlation during the Communication Process among Three Disjoint Users with Partial Cooperation of Quantum Server.

| Value | ui Bits | uj Bit | uk Bit | ui and uj Transformations | GHZ Transformations |
|-------|---------|--------|--------|--------------------------|-------------------|
| 0     | 0       | 0      | 0      | (I_u \otimes I_u)        | \frac{1}{\sqrt{2}} (|\Psi\rangle_{ul} + |\phi\rangle_{ul}) |
| 1     | 0       | 0      | 1      | (I_u \otimes X_u)        | \frac{1}{\sqrt{2}} (|\Psi\rangle_{ul} + |\phi\rangle_{ul}) |
| 2     | 0       | 1      | 0      | (X_u \otimes I_u)        | \frac{1}{\sqrt{2}} (|\Psi\rangle_{ul} + |\phi\rangle_{ul}) |
| 3     | 0       | 1      | 1      | (X_u \otimes X_u)        | \frac{1}{\sqrt{2}} (|\Psi\rangle_{ul} + |\phi\rangle_{ul}) |
| 4     | 1       | 0      | 0      | (Y_u \otimes I_u)        | \frac{1}{\sqrt{2}} (|\Psi\rangle_{ul} + |\phi\rangle_{ul}) |
| 5     | 1       | 0      | 1      | (Y_u \otimes X_u)        | \frac{1}{\sqrt{2}} (|\Psi\rangle_{ul} + |\phi\rangle_{ul}) |
| 6     | 1       | 1      | 0      | (Z_u \otimes I_u)        | \frac{1}{\sqrt{2}} (|\Psi\rangle_{ul} + |\phi\rangle_{ul}) |
| 7     | 1       | 1      | 1      | (Z_u \otimes X_u)        | \frac{1}{\sqrt{2}} (|\Psi\rangle_{ul} + |\phi\rangle_{ul}) |

Table 4. Correlation between Received Classical Value and its Corresponding Unitary, GHZ Transformations and Quantum Bit Transformation Correlation during the Communication Process among Three Disjoint Users with Full Cooperation of Quantum Server.
which unitary operations are used by the senders to transform the GHZ state according to the original generated classical message before it is transmitted to the receiver. By obtaining the applied unitary operations, the receiver can retrieve the original sent message. The Eight GHZ States are defined by (Eq. (10)).

\[ |\Psi^+\rangle = \frac{1}{\sqrt{2}} (|000\rangle \pm |111\rangle), \quad |\Psi^-\rangle = \frac{1}{\sqrt{2}} (|011\rangle \pm |100\rangle) \]

\[ |\phi^+\rangle = \frac{1}{\sqrt{2}} (|010\rangle \pm |101\rangle), \quad |\phi^-\rangle = \frac{1}{\sqrt{2}} (|001\rangle \pm |110\rangle) \]

(10)

There are many research groups proposed different approaches for realizing and experimentally generating multi-photon GHZ states. In 73, an experimental entanglement of six-photon GHZ states, cluster states, and graph states is proposed. The generating of six-photon GHZ states and cluster states is achieved by EPR-entangled photon pairs. In 73 an effective protocol for preparation of \( N \) - photon GHZ states with conventional photon detectors and can be realized through a simpler optical setup with a high success probabilities. In 74 a proposed a linear optical protocol to generate GHZ states of \( N \) distant photons with certain success probabilities. The proposed set up involved simple linear optical elements \( N \) pairs of the two-photon polarization entangled states, and the conventional photon detectors. In 75 an Experimental demonstration of five-photon entanglement and open-destination teleportation is proposed by utilizing two entangled photon pairs to generate a four-photon entangled state, which is then combined with a single-photon state. In 76 \( N \)- particle GHZ states can be generated easily using the \( N \) encoders preparation with cross-Kerr nonlinearities and can be realized simply through linear optical elements and homodyne detectors. In 77 Experimental generation of an eight-photon GHZ state is proposed. An eight-photon GHZ state with a measured fidelity of 0.59 \( \pm \) 0.02 proved the presence of genuine eight-partite entanglement. This is achieved by improving the photon detection efficiency to 25\% with a 300-mW laser pump. In our scheme, we use the same concept introduced in 70,72 to generate shared GHZ states. In order to develop the realization of \( N \) – particle GHZ states, the photon detection efficiency has to be improved basing on laser pump. Furthermore, a large capacity of memory for all parties to store and retrieve the required information has to take into consideration.

After a successful completion of the authentication process between the quantum server and a specified user, the remaining EPR is used to generate shared GHZ states to transmit the secret message among communicated users directly. Figure 1 demonstrates how the GHZ states among \( u_i \), the quantum server, and \( u_j \) are generated according to the remaining EPR. Suppose, for example, the generated EPR for the authentication process between the quantum server and \( u_i \) is given by (Eq. (11)). The quantum server particle is a part of another generated EPR for the purpose of authenticating \( u_j \) (See Eq. 12). The result will then be a shared GHZ state among \( u_i \), the quantum server, and \( u_j \) (See Eq. 13).

\[ |\Phi_{ij}^+\rangle = \frac{1}{\sqrt{2}} (|0_i 0_j\rangle + |1_i 1_j\rangle) \]

(11)

\[ |\Phi_{ij}^-\rangle (|0_i\rangle + |1_i\rangle) = \frac{1}{\sqrt{2}} (|0_i 0_j\rangle + |1_i 1_j\rangle) (|0_i\rangle + |1_i\rangle) \]

(12)

\[ |\Psi_{ij}^+\rangle = \frac{1}{\sqrt{2}} (|0_i 0_j\rangle + |1_i 1_j\rangle) \]

(13)

Tables 5–8 show the correlation between the quantum server publication, receiver measurement, sender operation(s), and sent bits. (Table 5) describes the correlation between the quantum server
publication, $u_j$ measurement, $u_i$ operation, and sent bits during a partial cooperation process between two disjoint users. The $u_j$ performs a Bell measurement on its particle and the $u_i$ particle; the quantum server then calculates the status of its particle according to the $x$ basis $\{+, -\}$ and announces the measurement results. The $u_i$ uses its measurements and the quantum server publications to retrieve the original secret bits sent by $u_i$. For example, when the $u_i$ measurement is equivalent to $|\psi^-\rangle$ and the quantum server publication is $|\phi^-\rangle$, $u_i$ concludes that the $u_j$ applied an $X$ operation and the sent bits were 01 (See Supplementary Table S1) for correlation during a full cooperation process between two disjoint users. Table 6 describes the same correlation of a partial process, but among three disjoint users. Here, $u_l$ performs a GHZ measurement on its particle, $u_i$ particles, and $u_j$ particles. The quantum server calculates the status of its particle according to the $x$ basis $\{+, -\}$ and announces the measurement results. Then, $u_l$ uses its measurement and the quantum server publications to retrieve the original secret bits sent by both $u_i$ and $u_j$. For example, when the $u_l$ measurement is equivalent to $|\phi^+\rangle$ and the quantum server publication is $|\phi^-\rangle$, $u_l$ can conclude that $u_i$ and $u_j$ applied $Y$ and $X$ operations, respectively, and the sent bits were 101 (See Supplementary Table S4) for correlation during a full cooperation process between.

| Quantum Server Publication | u_j Measurement | u_i Operation | Sent Bits |
|----------------------------|-----------------|--------------|-----------|
| $|\Phi^\perp\rangle_q$     |                  | $I$          | 00        |
| $|\Phi^\parallel\rangle_q$  |                  | $I$          | 00        |
| $|\Phi^\parallel\rangle_q$  |                  | $X$          | 01        |
| $|\Phi^\perp\rangle_q$     |                  | $X$          | 10        |
| $|\Phi^\perp\rangle_q$     |                  | $Z$          | 11        |

Table 5. Correlation between Quantum Server Publication, Receiver Measurement, Sender (s) Operation(s) and Sent Bits during partial cooperation process between Two Disjoint Users. (C, D) shows an illustrative example for transmitting a message 100111 from $u_i$ to $u_j$ with partial and full support of quantum server respectively.

| Quantum Server Publication | u_l Measurement | u_i Operation | Sent Bits | u_i Operation | Sent Bits | Message Sent |
|----------------------------|-----------------|--------------|-----------|--------------|-----------|--------------|
| $|\Phi^\perp\rangle_q$     |                  | $I$          | 00        | $I$          | 000       |
| $|\Phi^\parallel\rangle_q$  |                  | $I$          | 00        | $X$          | 1001      |
| $|\Phi^\parallel\rangle_q$  |                  | $X$          | 01        | $I$          | 0010      |
| $|\Phi^\perp\rangle_q$     |                  | $X$          | 01        | $X$          | 1111      |
| $|\Phi^\perp\rangle_q$     |                  | $Z$          | 11        | $I$          | 1110      |
| $|\Phi^\parallel\rangle_q$  |                  | $I$          | 00        | $X$          | 0001      |
| $|\Phi^\parallel\rangle_q$  |                  | $X$          | 01        | $I$          | 0101      |
| $|\Phi^\perp\rangle_q$     |                  | $X$          | 01        | $X$          | 1111      |
| $|\Phi^\perp\rangle_q$     |                  | $Y$          | 10        | $I$          | 0100      |
| $|\Phi^\parallel\rangle_q$  |                  | $Y$          | 10        | $X$          | 1111      |
| $|\Phi^\perp\rangle_q$     |                  | $Z$          | 11        | $I$          | 1110      |

Table 6. Correlation between Quantum Server Publication, Receiver Measurement, Sender (s) Operation(s) and Sent Bits during partial cooperation process among Three Disjoint Users.
three disjoint users). Tables 7 and 8 illustrate the transmission of messages 100111 from \( u_i \) to \( u_j \) with partial and full support of the quantum server, respectively.

### Results and Discussion

**Masquerade as Dishonest Disjoint User Security Analysis.** If an attacker would like to masquerade as dishonest disjoint user, then the attacker will work on the transmitting particle \( u \) (disjoint user particle) from the quantum server to the disjoint user. With the assumption that the attacker applying a universal operation \( \mathcal{R} \) on \( u \) see (Eq. (14, 15)).

\[
\begin{align*}
|0_u, \mathcal{R}\rangle &\rightarrow \alpha_0|0_u0_a\rangle + \beta_0|0_u1_a\rangle + \gamma_0|1_u0_a\rangle + \delta_0|1_u1_a\rangle \quad (14) \\
|1_u, \mathcal{R}\rangle &\rightarrow \alpha_1|0_u0_a\rangle + \beta_1|0_u1_a\rangle + \gamma_1|1_u0_a\rangle + \delta_1|1_u1_a\rangle \quad (15)
\end{align*}
\]

where \( \mathcal{R} \) represents an additional state which is created by the attacker, \( a \) represents the attacker particle and,

\[
|\alpha_0^2| + |\beta_0^2| + |\gamma_0^2| + |\delta_0^2| = |\alpha_1^2| + |\beta_1^2| + |\gamma_1^2| + |\delta_1^2| = 1
\]

When the attacker applying its operation, a new shared key state will be created see (Eq. (17, 18)).

\[
|\Phi^{+'}_{qu}\rangle \rightarrow |\Phi^{+'}_{qu}\rangle
\]

\[
|\Phi^{+'}_{qu}\rangle = \frac{1}{\sqrt{2}} (\alpha_0|0_q0_u0_a\rangle + \beta_0|0_q0_u1_a\rangle + \gamma_0|0_q1_u0_a\rangle + \delta_0|0_q1_u1_a\rangle + \\
\alpha_1|1_q0_u0_a\rangle + \beta_1|1_q0_u1_a\rangle + \gamma_1|1_q1_u0_a\rangle + \delta_1|1_q1_u1_a\rangle)
\]

The attacker transmits the new formulated state \( |\Phi^{+'}_{qu}\rangle \) to the quantum server. Afterwards, the quantum server performs \( \mathcal{C}_q \) on the received state as a result one of four states \( |\Phi^{0'}_{qu}\rangle, |\Phi^{01'}_{qu}\rangle, |\Phi^{10'}_{qu}\rangle, |\Phi^{11'}_{qu}\rangle \) which equivalent to the dual bits 00, 01, 10 and 11. With the assumption that the dual bits are equivalent to 00 then the quantum server operation is equivalent see (Eq. (19)).

\[
|\Phi^{00}_{qu}\rangle = \mathcal{C}_q|\Phi^{+'}_{qu}\rangle
\]

Through performing \( \mathcal{C}_q \) the result is obtained by (Eq. (20)).

---

Table 7. An illustrative example for transmitting a message 100111 from \( u_i \) to \( u_j \) with partial support of quantum server.

| \( u_i \) Plain Message | 10 | 01 | 11 |
|------------------------|----|----|----|
| \( u_i \) Operation    | Y  | X  | Z  |
| GHZ Transformation     | \( \frac{1}{\sqrt{2}}(|\psi^-\rangle_u + |\psi^+\rangle_u - |\psi^-\rangle_u - |\psi^+\rangle_u \) | \( \frac{1}{\sqrt{2}}(|\psi^-\rangle_u + |\psi^+\rangle_u - |\psi^-\rangle_u - |\psi^+\rangle_u \) | \( \frac{1}{\sqrt{2}}(|\Phi^-\rangle_u + |\Phi^+\rangle_u - |\Phi^-\rangle_u - |\Phi^+\rangle_u \) |
| \( u_i \) Bell Measurement | \( \psi^- \) | \( \psi^+ \) | \( \Phi^+ \) |
| Quantum Server Publication | +  | +  | −  |
| \( u_i \) Retrieved Message | 10 | 01 | 11 |

Table 8. An illustrative example for transmitting a message 100111 from \( u_i \) to \( u_j \) with full support of quantum server.

| \( u_i \) Plain Message | 10 | 01 | 11 |
|------------------------|----|----|----|
| \( u_i \) Operation    | Y  | X  | Z  |
| GHZ Transformation     | \( \frac{1}{\sqrt{2}}(|\psi^-\rangle_u + |\psi^+\rangle_u - |\psi^-\rangle_u - |\psi^+\rangle_u \) | \( \frac{1}{\sqrt{2}}(|\psi^-\rangle_u + |\psi^+\rangle_u - |\psi^-\rangle_u - |\psi^+\rangle_u \) | \( \frac{1}{\sqrt{2}}(|\Phi^-\rangle_u + |\Phi^+\rangle_u - |\Phi^-\rangle_u - |\Phi^+\rangle_u \) |
| Quantum Server Bell Measurement | \( \psi^- \) | \( \psi^+ \) | \( \Phi^+ \) |
| \( u_i \) Publication | +  | +  | −  |
| \( u_i \) Retrieved Message | 10 | 01 | 11 |
\[
|\Phi^0\rangle = \frac{1}{\sqrt{2}} \left( (\alpha_0|0_u0_u0_u\rangle + \beta_0|0_u0_u1_u\rangle + \gamma_0|0_u1_u0_u\rangle + \delta_0|0_u1_u1_u\rangle + \alpha_1|1_u0_u0_u\rangle + \beta_1|1_u0_u1_u\rangle + \gamma_1|1_u1_u0_u\rangle + \delta_1|1_u1_u1_u\rangle \right)
\] (20)

So the chance for discovering the attacker for \(|\Phi^0\rangle\) is \(\hat{P}_{00}\) can be computed using (Eq. (20)) as by (Eq. (21))

\[
\hat{P}_{00} = \frac{1}{2} (|\alpha_1|^2 + |\gamma_1|^2 + |\beta_0|^2 + |\delta_0|^2)
\] (21)

As well when the dual bits are equivalent to 01, so the chance for discovering the attacker for \(|\psi^{01}\rangle\) is \(\hat{P}_{01}\) can be computed using Eq. (18) as shown in (Eq. (22))

\[
\hat{P}_{01} = \frac{1}{2} (|\alpha_1|^2 + |\gamma_0|^2 + |\beta_1|^2 + |\delta_1|^2)
\] (22)

When the dual bits are equivalent to 10, so the chance for discovering the attacker of \(|\psi^{10}\rangle\) is \(\hat{P}_{10}\) and equivalent to \(\hat{P}_{01}\). Furthermore the chance for discovering the attacker of \(|\psi^{11}\rangle\) is \(\hat{P}_{11}\) and equivalent to \(\hat{P}_{00}\). Accordingly, the total discovering probability of the attacker \(P_{Total}\) of each disjoint user is equivalent \(\frac{1}{2}\) see (Eq. (23, 24))

\[
\hat{P}_{Total} = \frac{1}{4} (\hat{P}_{00} + \hat{P}_{01} + \hat{P}_{10} + \hat{P}_{11})
\] (23)

\[
\hat{P}_{Total} = \frac{1}{2}
\] (24)

As stated by Simmons theory\(^77,78\), the result of the previous equation proved that the proposed scheme is unconditionally secured under this type of attack.

One-way Channel Substitution Fraudulent Attack Security Analysis. As the transmitted particle from the quantum server to the disjoint user doesn’t contain any fact about the authentication key, so in this type of attack only the restored \(n\) (new state particle) from the disjoint user to the quantum server have to be measured. The maximum reachable information which an attacker may obtain over the communicated channel between a quantum server and a disjoint user can be computed by Holevo theory\(^79\) see (Eq. (25))

\[
\chi (p) = \sum_i \mathbb{P}_i \chi (\mathbb{P}_i)
\] (25)

As \(\chi (p)\) is equivalent to Von Neumann entropy \(-Tr (p \log_2 p)\), \(\mathbb{P}_i\) is a component in the hybrid status and \(\mathbb{P}_i\) is the possibility of \(p_i\) in the universe \(p\). So the eavesdropper just has information about the authentication key by directly calculating the \(n\) (new state particle), so the resulted \(\chi (p)\) relies on the reduced density matrix of \(n\), by substitution of (Eq. (25)) as shown in (Eq. (26))

\[
\chi (\mathbb{P}_n) = \sum_i \mathbb{P}_i \chi (\mathbb{P}_{n_i})
\] (26)

As both \(\mathbb{P}_n\) and \(\mathbb{P}_{n_i}\) required reduced density matrix for \(p\) and \(p_i\), respectively. For any authentication key, the reduced density matrix of \(n\) can be represented in (Eq. (27))

\[
\mathbb{P}_n = Tr_{q_u} (|\Phi_i\rangle \langle \Phi_i|) = \frac{1}{2} I
\] (27)

In addition to, \(\mathbb{P}_{n_i}\) is equivalent to the subsequent equations from ((28) to (32))

\[
|\Phi^{00}_i\rangle = \frac{1}{\sqrt{2}} \left( (|0_u0_u0_u\rangle + |1_u1_u1_u\rangle) \right)
\] (28)

\[
|\Phi^{01}_i\rangle = \frac{1}{\sqrt{2}} \left( (|0_u0_u1_u\rangle + |1_u1_u0_u\rangle) \right)
\] (29)
\[ |\Phi^{10}\rangle = \frac{1}{\sqrt{2}} (|+u +_n\rangle + |-_u -_n\rangle) \]  

\[ |\Phi^{11}\rangle = \frac{1}{\sqrt{2}} (|+u +_n\rangle + |-_u -_n\rangle) \]

Therefore,

\[ \wp_{ni} = Tr_{q\eta}(\Phi\Phi^\dagger) = \frac{1}{2} I \]

By replacing values for both \( p_n \) and \( p_m \) in Eq. (26), \( \chi(p_n) = 0 \). So, the eavesdropper will not reveal any information about the key in case of directly calculating the transferred particles over the communicated channel from the quantum server to the disjoint user.

**Two-Way Channel Substitution Fraudulent Attack Security Analysis.** The attacker applies an operation \( \Theta_1 \) at his/her side on the transmitted particle \( u \) and supportive particle \( \varepsilon \). Afterwards, the attacker transmits the resulted particle to the disjoint user. When the disjoint user receives the transmitted particle, he/she does not realize that there is an attacker and he did an operation. The disjoint user applies his normal operation and transmits the resulted particle to the quantum server. The attacker intercepts the information particle sent by the disjoint user. The attacker applies an operation \( \Theta_2 \) at his side to the information particle and supportive particle \( \eta \). Afterwards, the attacker transmits the resulted particle to the quantum server. The attacker attempts to retrieve certain amount of information about the key by employing two supportive particles \( \varepsilon \) and \( \eta \) (See Supplementary Information 3 for Full Calculations of Two-Way Channel Substitution Fraudulent Attack along with equations).

When the two-bit key \( A_1 A_{1+1} = 00 \), so the resulting decoding state by the quantum server is given in (Eq. (33, 34))

\[ |\Phi^{00}_{q\eta}\rangle = \varepsilon_0 \Theta_2 (\varepsilon_0 (|\Phi^{10}_\varepsilon\rangle |\eta\rangle) ) |\phi^+\rangle |\eta\rangle \]

\[ |\Phi^{00}_{q\eta}\rangle = \frac{1}{\sqrt{2}} (\alpha \varepsilon_{\alpha|}\varepsilon_0 |0_q|0_n|\varepsilon_{00}|\eta_{01}) + \alpha \varepsilon_{\beta|}\varepsilon_0 |0_q|0_n|\varepsilon_{00}|\eta_{01}) \]

\[ + \beta \varepsilon_{\beta|}\varepsilon_0 |0_q|0_n|\varepsilon_{10}|\eta_{10}) + \beta \varepsilon_{\beta|}\varepsilon_0 |0_q|0_n|\varepsilon_{10}|\eta_{10}) \]

\[ + \alpha \varepsilon_{\alpha|}\varepsilon_0 |0_q|0_n|\varepsilon_{11}|\eta_{11}) + \alpha \varepsilon_{\alpha|}\varepsilon_0 |0_q|0_n|\varepsilon_{11}|\eta_{11}) \]

We can calculate the total possibility for discovering the attacker (\( \wp_{Total} \)) in the authentication process is given by (Eq. (35))

\[ \wp_{Total} = 1/2 [\wp_{Total}(A_1 = 0) + \wp_{Total}(A_1 = 1)] \]

If the attacker would like to minimize his/her detection probability, he/she has to adjust \( \wp_{Total} \) as a minimum discovering probability (See Eq. 36) which is calculated under the condition of \( \alpha_\varepsilon = \alpha_\eta = 1 \)

\[ Total = Min (\wp_{Total}) = \frac{1}{4} (1 - \cos \theta_\varepsilon) \]

So, the attacker’s total information amount on the transmitted key bits between the quantum server and the disjoint user can be estimated in (Eq. (37)).

\[ \wp(AK, \Theta_{Total}) = \sum_{x,y} \wp(AK, \Theta_{Total}) \log_2 \frac{\wp(AK, \Theta_{Total})}{\wp(AK)} \]

values \((00, 01, 10, 11)\) with probability \( \wp(x) = \frac{1}{4} \). \( AK \) indicates the selected random values from variable \( x \), \( y = \varepsilon_\eta | \mu \) with \( i, j, \mu, \tau \in \{0, 1\} \). Consequently, the joint gained information by attacker’s total operation \( \Theta_{Total} \) is given in (Eq. (38))

\[ \wp = \frac{1}{4} [(1 + \sin \theta_\varepsilon) \log_2 (1 + \sin \theta_\varepsilon) + (1 - \sin \theta_\varepsilon) \log_2 (1 - \sin \theta_\varepsilon)] \]

Since \( \theta_\varepsilon = \sqrt{8 \times Total - 16 \times Total^2} \) (see Supplementary Information (4) for Proving Relation between sin \( \theta_\varepsilon \) and Total), by substitution in (Eq. (38))
Therefore the total estimation probability $P_e$ of $A_k$ is given in (Eq. (40))

$$
\mathcal{F} = \frac{1}{4} \left[ \log_2 \left( 1 + \sqrt{8 \times \text{Total} - 16 \times \text{Total}^2} \right) \right]
$$  \hspace{1cm} (39)

By simplification of Eq. (40) $P_e$ of $A_k$ is given in (Eq. (41)) (see Supplementary Information (5) for Proving Relation between $P_e$, $P$ and $\sin \theta_c$)

$$
P_e = \frac{1}{6} \left[ \frac{(1 + \sin \theta_c)}{2} \left( \frac{1}{2} (1 - P) \right) + \frac{(1 - \sin \theta_c)}{2} \left( \frac{1}{2} (1 - P) \right) \right]
$$  \hspace{1cm} (40)

If $P = 1$ indicates that the total estimation probability $P_e$ is maximized see (Eq. (42)) (see Supplementary Information (6) for Proving Relation between $P_e$, $P_e^m$ and Total)

$$
P_e = \frac{1}{6} \left( \sin \theta_c (3 \times P - 1) + 2 \right)
$$  \hspace{1cm} (41)

Therefore, the probability of the attacker for successfully retrieving the transmitted keys $P_e^r$ for $A_k = \{A_1, A_2, A_3, \ldots, A_{2N}\}$ see (Eq. (43))

$$
P_e^r = \frac{\sqrt{8 \times \text{Total} - 16 \times \text{Total}^2} + 1}{\text{Total}}
$$  \hspace{1cm} (42)

By substituting (Eq. (42)) in equation (Eq. (43)), so

$$
P_e^r = \left[ P_e^m (1 - \text{Total}) \right]^{\text{N/2}}
$$  \hspace{1cm} (43)

Therefore, the possibility for discovering the attacker while attempting to retrieve any information about the key bits is equal to non-zero. For example if Total = 25% means the attacker can gain maximal joint information $\mathcal{F} = 0.5\text{ \textit{bit}}$ on the transmitted keys between the quantum server and disjoint user. From Fig. 2B, we can conclude that when the total estimation probability is maximized which means reaching to one, the attacker can positively maximum retrieve 0.5 bit of the transmitted key $A_k$ while the maximum total estimation probability $P_e^m$ is equal to 25%.

Figure 2C illustrates that if the minimum discovery probability is equal to [0, 12.5, 25, 50]% and $N = 2$, so the maximum values for successfully retrieving the information of the transmitted keys $A_k$ by the attacker are [0.25, 4.08 × 10^{-1}, 4.08 × 10^{-1}, 1.25 × 10^{-1}] respectively. Also, for $N = 16$ the maximum successfully for retrieving information of the transmitted keys $A_k$ by the attacker is [1.53 × 10^{-5}, 7.7 × 10^{-4}, 3.91 × 10^{-4}, 5.96 × 10^{-8}] respectively. So while the number of the transmitted bits is increasing, the possibility for successful retrieval the transmitted information is decreased (See Supplementary Figure S6 (A–D) and Table S5 (A–D) for Full Calculations for Relation between $N$, Total, $P_e^r$).

Figure 2D shows that the maximum and minimum values for successfully retrieving the information of the transmitted keys $A_k$ by the attacker while $N = [2, 4, 8, 16]$ are [0.5, 0.25, 0.0625, 3.91 × 10^{-3}] and [0.0625, 3.91 × 10^{-3}, 1.53 × 10^{-5}, 2.32 × 10^{-10}] respectively. We can conclude that all maximum values are corresponding when $P_e^m$ and Total is equal to [50, 0]%). So, the attacker can gain maximum information about the transmitted keys $A_k$ at this situation. Furthermore, the minimum value for the attacker to gain information about the transmitted keys $A_k$ is [2.32 × 10^{-10}] corresponding when the value of $P_e^m$ and Total is equal to [12.5, 50]%). (See Supplementary Figure S7 (A–D) and Table S6 (A–D) for Full Calculations for Relation between $P_e^r$ and $N$ while $P_e^m$ = [12.5, 25, 37.5, 50]% and Total = [0, 12.5, 25, 50 %]).

Figure 2E demonstrates the maximum and minimum values for successfully retrieving the information of the transmitted keys $A_k$ by the attacker while $N = [2, 4, 8, 16]$ is [1.87 × 10^{-1}, 3.51 × 10^{-2}, 1.23 × 10^{-3}, 1.53 × 10^{-6}] and [1.56 × 10^{-2}, 2.5 × 10^{-4}, 5.96 × 10^{-8}, 3.55 × 10^{-15}] respectively. From Fig. 2E, we can conclude that all maximum and minimum values are corresponding when $P_e^m$ and Total is equal to [50, 62.5]% and [12.5, 87.5]% respectively. So, the attacker can gain maximum information about the transmitted keys $A_k$ when $P_e^m$ and Total equal to [50, 62.5]% and minimum when $P_e^m$ and Total is equal to [12.5, 87.5]%). (See Supplementary Figure S8 (A–D) and Table S7 (A–D) for Full Calculations for Relation between $P_e^r$ and $N$ while $P_e^m$ = [12.5, 25, 37.5, 50]% and Total = [62.5, 75, 87.5]%).
Figure 2. Two-Way Channel Substitution Fraudulent Attack Security Analysis. (A) The correlation between the joint information $\Sigma$ and the minimum discovering probability $Total$. (B) Correlation between Maximized Total Estimation Probability $P_e^m$ and the minimum discovering probability $Total$. (C) Relation between $P_e^T$, $N= [2, 4, 8, 16]$ and $Total = [0, 12.5, 25, 50]\%$. (D) Relation between $P_e^T$ and $N$ while $P_e^m = [12.5, 25, 37.5, 50]\%$ and $Total = [0, 12.5, 25, 50]\%$. (E) As Fig. 2D while $Total = [62.5, 75, 87.5]\%$. (F) Combined Fig. 2C,D while $P_e^m = [62.5, 75, 87.5]\%$. “drawn by A.F”.

Figures 2F and 3 illustrate while the number of transmitted key bits $N$ becomes larger, the possibility of successfully retrieving $A_k$ becomes smaller and reach zero. So, the attacker will not reveal an enormous amount of information which can be ignored and avoided by updating key between the disjoint user and the quantum server periodically. In this case, the information of the attacker on the old key will be useless.
Generalization of Communication Process between N Disjoint Users with Partial Cooperation of Quantum Server. Here, we generalize our approach for Communication Process between N Disjoint Users with Partial Cooperation of Quantum Server as shown in Fig. 4A. So, N − 1 disjointed users \( u_1, u_2, \ldots, u_{N−1} \) can transmit a secret message of classical bits to a remote user \( u_N \) with partial cooperation of the quantum server. Firstly the quantum server distributes \( N \) particles of \( N + 1 \) states \( \text{GHZ} \) defined as \( \text{GHZ}_{N+1}^{y} = \frac{1}{2} \left( |00\ldots0\rangle + |11\ldots1\rangle \right) \). Next, each user applies appropriate unitary transformation according to his plain message. The bit string value \( \text{GHZ}_{N+1}^{y} \) and \( \text{GHZ}_{N+1}^{x} \) will be transformed according to \( u_1, u_2, \ldots, u_{N−1} \) and \( u_N \) to prepare classical bit string. After each user sends his plain message and his measurement results to the quantum server, the quantum server performs an N−GHZ measurement on the particles of his particle and \( u_1, u_2, \ldots, u_{N−1} \) disjointed users. Afterwards, the quantum server performs his N−GHZ measurement according to a random subset of \( \text{GHZ}_{N+1}^{y} \) and \( \text{GHZ}_{N+1}^{x} \) and announces his measurement results. \( u_N \) uses his measurements and the quantum server performs his N−GHZ measurement on the particles of his particle according to \( x \) and \( y \) bases. The quantum server verifies the measurements of \( u_N \) and announces his measurement results. After this, \( u_N \) transmits the secret bit which is expressed by \( u_N \) to \( u_1, u_2, \ldots, u_{N−1} \). (See Supplementary Figures S1 for Communication Process between Two and Three Disjoint Users with Partial Support of Quantum Server respectively).

Generalization of Communication Process between N Disjoint Users with Full Cooperation of Quantum Server. Here, we generalize our approach for Communication Process between N Disjoint Users with full Cooperation of Quantum Server as shown in Fig. 4B. The sequence of the steps is similar to a partial one except that the selected particles \( \text{GHZ}_{N+1}^{y} \) and \( \text{GHZ}_{N+1}^{x} \) will be transformed according to \( u_1, u_2, \ldots, u_{N−1} \) and \( u_N \) to prepare classical bit strings. After each user sends his plain message and his measurement results to the quantum server, the quantum server performs an N−GHZ measurement on the particles of his particle and \( u_1, u_2, \ldots, u_{N−1} \) disjointed users. Afterwards, \( u_N \) calculates the status of his particle according to \( x \) and \( y \) bases. The quantum server verifies the measurements of \( u_N \) and announces his measurement results. \( u_N \) uses his publication and the quantum server publication for retrieving the original secret sent bits by \( u_1, u_2, \ldots, u_{N−1} \). (See Supplementary Figures S2 and S4 for Communication Process between Two and Three Disjoint Users with Full Support of Quantum Server respectively).

Communication Process Security Analysis. After \( u_j \) retrieves the original secret sent bits which were transmitted by \( u_i \), \( u_j \) informs \( u_i \) about the positions of the transmitted particles and the selected unitary transformation applied to them. Afterwards, \( u_i \) verifies the selected particles by \( u_i \) and obtains an approximation of error percentage in the communication process. If the error percentage is under the specified threshold both \( u_i \) and \( u_j \) can continue the transmission of the secret messages, otherwise the communi-
cation process will be terminated. If an attacker tries to spy on the transmitted GHZ particles, the attacker at most can obtain one particle. So, the attacker couldn't decide which operation is applied by \( u_i \), consequently couldn't retrieve any transmitted secret bits. Suppose that the attacker apply an operation \( \Theta_{u_iA} \) on \( u_i \) and his qubit \( |A \rangle \) see (Eq. (45)).

**Figure 4.** (A) Generalization of Communication Process between N Disjoint Users with Partial Cooperation of Quantum Server (B) with Full Cooperation of Quantum Server “drawn by A.F”.
\[ |0_A\rangle u_A \rightarrow \alpha_e |0\rangle u_A |E_{00}\rangle_A + \beta_e |1\rangle u_A |E_{01}\rangle_A \]
\[ |1_A\rangle u_A \rightarrow \beta_e' |0\rangle u_A |E_{10}\rangle_A + \alpha_e' |1\rangle u_A |E_{11}\rangle_A \]  
(45)

Correspondingly, applying the unitary operation requires the following conditions $|\alpha_e|^2 + |\beta_e|^2 = 1$ and $|\alpha_e'|^2 + |\beta_e'|^2 = 1$.

So, the state of the protocol is transformed as follows. Firstly, the states after $u_i$ made a unitary operation see (Eq. (46)).

\[
|\Psi_i\rangle_{i(A)} = \Theta_i u_i |\Psi_i\rangle_{i(A)} \otimes |A\rangle_A
\]
\[
= \frac{1}{\sqrt{2}} (|001\rangle_{i(A)} + |101\rangle_{i(A)} + |111\rangle_{i(A)}) \otimes |A\rangle_A
\]
(46)

Secondly, the states after the attacker applies a unitary transformation on $u_i$ and his qubit $|A\rangle$ see (Eq. (47, 48))

\[
|\Psi_2\rangle_{i(A)} = \Theta_i u_i |\Psi_2\rangle_{i(A)}
\]
\[
= \frac{1}{\sqrt{2}} \left( |000\rangle_{i(A)} (\alpha_e |E_{00}\rangle + \beta_e |E_{01}\rangle)_A + |100\rangle_{i(A)} (\beta_e |E_{00}\rangle + \alpha_e |E_{01}\rangle)_A + |011\rangle_{i(A)} (\beta_e |E_{00}\rangle + \alpha_e |E_{01}\rangle)_A + |111\rangle_{i(A)} (\beta_e |E_{00}\rangle + \alpha_e |E_{01}\rangle)_A \right)
\]
(47)

\[
\left| \phi^+_{i(A)} \right> = \frac{1}{2 \sqrt{2}} \left( |+\rangle_{u_i} (\alpha_e |E_{00}\rangle + \beta_e |E_{01}\rangle) + |+\rangle_{u_i} (\beta_e |E_{00}\rangle + \alpha_e |E_{01}\rangle) \right)
\]
\[
\left| \phi^-_{i(A)} \right> = \frac{1}{2 \sqrt{2}} \left( |+\rangle_{u_i} (\alpha_e |E_{00}\rangle + \beta_e |E_{01}\rangle) - |+\rangle_{u_i} (\beta_e |E_{00}\rangle + \alpha_e |E_{01}\rangle) \right)
\]
\[
\left| \psi^+_{i(A)} \right> = \frac{1}{2 \sqrt{2}} \left( |+\rangle_{u_i} (\beta_e |E_{00}\rangle + \alpha_e |E_{01}\rangle) + |+\rangle_{u_i} (\alpha_e |E_{00}\rangle + \beta_e |E_{01}\rangle) \right)
\]
\[
\left| \psi^-_{i(A)} \right> = \frac{1}{2 \sqrt{2}} \left( |+\rangle_{u_i} (\beta_e |E_{00}\rangle + \alpha_e |E_{01}\rangle) - |+\rangle_{u_i} (\alpha_e |E_{00}\rangle + \beta_e |E_{01}\rangle) \right)
\]
(48)

As shown in (Eq. (47, 48)), the attacker can’t gain any information during intercepting the communication process. As well the attacker introduces an error probability of $\frac{1}{2}$ irrespective of the sequence of measurement. For example, suppose that the attacker measurement is the same as $u_i$, means the applied unitary transformation may be $X$ or $Y$. If the measurements are different then the possible applied unitary transformation may be $X$ or $Y$.

References

1. Bennett, C. H. & Brassard, G. Quantum Cryptography: Public Key Distribution And Coin Tossing. *Theoretical Computer Science* **560**, 7–11 (2014).
2. Nielsen, M. & Chuang, I. Quantum computation and quantum information. (Cambridge University Press, 2000).
3. Zeng, G. H. Quantum cryptography. (Science Press, 2006).
4. Assefa, G. Quantum Cryptography and Secret-Key Distillation. (Cambridge University Press, 2006).
5. Sharbaf, M. S. Quantum Cryptography: A New Generation of Information Technology Security System. Sixth International Conference on Information Technology. Nevada, USA, IEEE, 1644–1648 (April, 2009).
6. Wooters, W. K. & Zurek, W. H. A Single Quantum Cannot Be Cloned. *Nature* **299**, 802–803 (1982).
7. Simon, D. Cryptography Theory and Practice 3rd ed. (CRC press, 2006).
8. Bennett, C. H. et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **70**, 1895–1899, doi: 10.1103/PhysRevLett.70.1895 (1993).
9. Chakrabarty, I. Teleportation via a mixture of a two qubit subsystem of a N-qubit W and GHZ state. *Eur. Phys. J. D* **57** (2), 265–269, doi: 10.1140/epjd/e2010-00017-8 (2010).
10. Liang, H., Liu, J., Feng, S. & Chen, J. Quantum teleportation with partially entangled states via noisy channels. *Quantum Inf Process* **12**(8), 2671–2687 (2013).
11. Kaye, P. & Laflamme, R. *An Introduction to Quantum Computing*. (Oxford University Press, 2007).
12. Bennett, C. & Wiesner, S. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.* **69**, 2881–2884 (1992).
A generalized architecture of quantum secure direct communication

Farouk, A. et al.

How to cite this article

A.F. would like to thank Josep Batle, Yan-Bing Li, Mosayeb Naseri, Nanrun Zhou and Ming-Ming Wang for their fruitful discussion and helpful comments.

Acknowledgements

Additional Information

Supplementary information accompanies this paper at http://www.nature.com/srep

Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Farouk, A. et al. A generalized architecture of quantum secure direct communication for N disjointed users with authentication. Sci. Rep. 5, 16080; doi: 10.1038/srep16080 (2015).

This work is licensed under a Creative Commons Attribution 4.0 International License. The images or other third party material in this article are included in the article’s Creative Commons license, unless indicated otherwise in the credit line; if the material is not included under the Creative Commons license, users will need to obtain permission from the license holder to reproduce the material. To view a copy of this license, visit http://creativecommons.org/licenses/by/4.0/