Front. Phys. 13(2), 130306 (2018)
https://doi.org/10.1007/s11467-017-0717-3

RESEARCH ARTICLE

Robust general N user authentication scheme in a centralized quantum communication network via generalized GHZ states

Ahmed Farouk[1,†], J. Batle[3], M. Elhoseny[1], Mosayeb Naseri[4], Muzaffar Lone[5], Alex Fedorov[6], Majid Alkhambashi[7], Syed Hassan Ahmed[8], M. Abdel-Aty[2]

[1] *Faculty of Computer and Information Sciences, Mansoura University, Egypt*
[2] *Applied Science University, Bahrain & Mathematics Dept. Sohag University, Egypt*
[3] *Departament de Física, Universitat de les Illes Balears, 07122 Palma de Mallorca, Balearic Islands, Spain*
[4] *Department of Physics, Kermanshah Branch, Islamic Azad University, Kermanshah, Iran*
[5] *Department of Physics, University of Kashmir, Srinagar-190006, India*
[6] *Russian Quantum Center, 100 Novaya Street, Skolkovo, Moscow 143025, Russia*
[7] *Information Technology Department, Al-Zahra College for Women, P.O. Box 3365, Muscat, Oman*
[8] *School of Computer Science & Engineering, Kyungpook National University, Daegu, Republic of Korea*
Corresponding author. E-mail: [†] *dr.ahmedfarouk85@yahoo.com*
Received December 23, 2016; accepted June 13, 2017

Quantum communication provides an enormous advantage over its classical counterpart: security of communications based on the very principles of quantum mechanics. Researchers have proposed several approaches for user identity authentication via entanglement. Unfortunately, these protocols fail because an attacker can capture some of the particles in a transmitted sequence and send what is left to the receiver through a quantum channel. Subsequently, the attacker can restore some of the confidential messages, giving rise to the possibility of information leakage. Here we present a new robust General N user authentication protocol based on N-particle Greenberger–Horne–Zeilinger (GHZ) states, which makes eavesdropping detection more effective and secure, as compared to some current authentication protocols. The security analysis of our protocol for various kinds of attacks verifies that it is unconditionally secure, and that an attacker will not obtain any information about the transmitted key. Moreover, as the number of transferred key bits N becomes larger, while the number of users for transmitting the information is increased, the probability of effectively obtaining the transmitted authentication keys is reduced to zero.

Keywords quantum communication, quantum cryptography, quantum authentication, entanglement

PACS numbers 03.65.Ud, 03.67.Ac, 03.67.Dd, 03.67.Hk, 03.67.-a, 03.67.Lx

1 Introduction

Ever since the seminal work of Bennett and Brassard [1], the field of quantum cryptography has evolved rapidly. Quantum cryptography proves its unconditional security [2–5] by the no-cloning theorem [6]. A number of approaches and models have used quantum cryptography to secure communication processes between two and multiple parties [7–13]. Remarkably, confidential messages can be conveyed through a quantum channel with or without added classical communications [14–33]. Various quantum authentication approaches have been developed for verifying the identity of communicated parties before or during the transmission process and avoiding different kinds of attacks [34–47]. If two users want to verify their identity by utilizing the correlations in Einstein–Podolsky–Rosen (EPR) pairs as identification tokens, the corresponding authentication is achieved by a complete Bell state measurement [34]. Unfortunately, the proposed scheme is vulnerable to denial-of-service attacks by eavesdroppers. In Ref. [35], a cross-center quantum authentication approach based on teleportation and entanglement swapping was achieved by trans-

Frontiers of Physics

ferring the identity information through quantum and classical channels, but the approach did not provide a certain method to deliver the pre-shared EPR pairs, and a comparison of two unidentified quantum states was required. In Ref. [36] a server-based hybrid cryptographic protocol was proposed, exploiting both classical and quantum properties for generating and distributing authentication keys with the help of a trusted server. However, the suggested approach failed, because an eavesdropper could disturb the communication process in the eventual case where the communication channel was jammed or disconnected. In addition, authentic communicators are verified by a telephone company with a quantum channel sequence, on which they can communicate with each other directly and confidentially by employing some encoding operations [37]. Unfortunately, the proposed protocol is bound to fail because an eavesdropper can spy on the correspondents' conversation without introducing any error by using fake particles and local operations. This last protocol was improved in Ref. [38]. Furthermore, an untrusted server (telephone company) can retrieve the complete information of the conversation with zero risk by using false entangled particles, a situation improved in Ref. [39].

A quantum authentication protocol based on the nonlocality of the orthogonal product states of a two-particle system was proposed in Ref. [40]. In addition, a proposal for verifying the user identity and distributing quantum keys concurrently based on local unitary operations and Bell state measurement was introduced in Ref. [41]. However, the presented scheme was susceptible to a malicious user impersonating a legitimate participant and performing an intercept-and-resend attack, where the attacker can impersonate a legitimate participant without being detected. This situation was improved in Ref. [42]. Two continuous-variable quantum identity authentication schemes using Gaussian-modulated squeezed states to prevent the general Gaussian-cloner strategy and collective attacks were presented in Ref. [43]. In another proposed protocol [44], a theoretical quantum authenticated secure communication scheme using one-step quantum transmission achieved by EPR, exclusively requiring the server to be honest or to have added quantum bits prepared and checked without the use of classical channels. In addition, the authors of [13] introduced a scheme for a secure quantum communication network with authentication using Greenberger–Horne–Zeilinger (GHZ)-like states and cluster states with controlled teleportation. More recently, a continuous-variable quantum identity authentication protocol, based on quantum teleportation, was presented in Ref. [45] by employing a two-mode squeezed vacuum state and a coherent state. Finally, a mutual identity authentication scheme based on entanglement swapping and honest party was proposed in Ref. [46]. However, as shown in Ref. [47], the concomitant security analysis of the aforementioned protocol implies that an eavesdropper can retrieve the transmitted information between the communicating parties with zero risk of detection. By 2017, the improvement and growth of a real quantum computer was still in the early stages, but many practical and theoretical experiments had been implemented by different research groups [72–93].

In the following, and in view of the limited scope of the previous proposals, we present a new quantum authentication protocol that outperforms all protocols in the existing literature. The efficiency and effectiveness of our protocol can be summarized in four points. First, by utilizing N GHZ states, eavesdropping on any single particle will break the correlation among the communicated parties. Therefore, it will be more effective and efficient than other protocols that use an EPR pair to authenticate and transmit the confidential messages, because these protocols introduce an error and an unsuccessful transmission of the particles. When the sender transmits the sequence, an attacker can imprison some of them and perform a GHZ measurement. Subsequently, the attacker can restore some of the confidential messages, raising the possibility of information leakage. Secondly, by employing N GHZ states the number of authenticated users is increased, as they can afford a considerable Hilbert space. Thirdly, the security analysis of the authentication processes of our protocol — contrary to various kinds of attacks — verifies that it is unconditionally secure and that the attacker will not expose any information about the transmitted key in the case of directly analyzing the transmitted particles over the conveyed channel, from the quantum authentication server (QAS) to the disjoint user, and vice versa. Therefore, the attacker introduces an error probability regardless of the success of the measurements. Finally, as the number of transferred key bits N becomes larger and the number of users for transmitting the information is increased, the probability of effectively obtaining the transmitted authentication keys is reduced to zero. The proposed protocol achieves both the maximal security and efficiency of the transmission, which is apparent from two aspects: first, the N-GHZ state is the maximally entangled state, so that the correlation can be more easily destroyed once any single N particle is attacking; secondly, using the N-GHZ particle makes eavesdropping detection more effective and secure, in comparison to some of the other protocols. Our protocol increases the transmitted information capacity by using N-GHZ states because these provide a large Hilbert space.

There is a more fundamental question that regards the success of our protocol, and it is related to the na-

ture of the multipartite states used in our endeavor. It is an interesting question whether the use of different states rather than the GHZ ones or their multiqubit extension plays a role in achieving the expected advantage over other existing protocols, which is difficult to answer. From an operational point of view, GHZ states offer the right distribution of information among the parties involved in our protocol, as discussed herein. If one utilized different states capable of distributing the operations between the quantum server and all users *effectively* in the same fashion, the same outcome would be reached, as nothing exists that could prevent the existence of these states; this precise question is currently under our scrutiny. The fact of using GHZ states and the concomitant extension to N parties has more to do with the suitability of these pure states and the relatively easy way of experimentally generating them. It is true that GHZ states shall use more non-local resources in order to be generated than, for instance, states whose tensor product structure is that of the product of two states, and hence with a less multipartite non-locality/entanglement measure content; however, we shall address here only results attained by using GHZ and N GHZ states, and tackle the use of less quantum-correlated states elsewhere. In other words, it is the *outcome* of the distribution of tasks and not the *quantum correlation nature* of the states performing them what is relevant in the present work.

2 Methods

2.1 Entanglement and GHZ states

In entanglement, a cornerstone of quantum physics and quantum communication processing, two or multiple photons are generated or interrelated in a way such that the quantum state of the whole system cannot be described by the sole use its subsystems [52–61]. The description of entanglement has been carried out both in single-particle [62, 63] and composite systems [64, 65]. In recent years, there has been significant development in the experimental generation of multi-photon GHZ states. In Ref. [66], an experimental entangled state of five photons was used to perform open-destination teleportation. In Ref. [67], the creation of a six-atomic-qubit "Schrödinger's cat" state was proposed using the interion distances and the relative phases of dipole forces. Ref. [68] reported the experimental generation of six-photon GHZ states and cluster states, with verifiable six-partite entanglement obtained combining three EPR entangled photon pairs. The realization of N-photon GHZ entangled states by a simpler optical setup, with a high success probability, was shown in Ref. [69]. In Ref. [70], the generation of multi-atom GHZ states based on the method of partial stimulated Raman adiabatic passage was realized. In addition, Ref. [71] reported the experimental realization of an authentic eight-photon GHZ state based on EPR states, giving rise to a large successful probability exceeding the classical.

Our approach employs the concept introduced in Refs. [68, 70] to realize N-particle GHZ states. Once the authentication process between the QAS and u_A is successfully completed, the ensuing EPR state will be utilized for generating GHZ states for authentication among the QAS, u_A, and u_B. Assume we have an EPR state for the authentication process between the QAS and u_A, given by Eq. (1). The QAS particle is a part of another EPR pair, which is generated with the purpose of authenticating u_B [Eq. (2)]. Therefore, a GHZ state is generated, $|\Psi_{ASB}\rangle$, for the authentication process among the QAS, u_A, and u_B [Eq. (3)]. By the same token, $|\Psi_{ASBC}\rangle$, $|\Psi_{ASBCD}\rangle, \cdots$ and so forth can be generated (see Fig. S13 in the Supplementary Information for the generation of GHZ states).

$$|\Phi^+_{AS}\rangle = \frac{1}{\sqrt{2}}(|0_A 0_S\rangle + |1_A 1_S\rangle), \tag{1}$$

$$|\Phi^+_{SB}\rangle(|0\rangle_A + |1\rangle_A) = \frac{1}{\sqrt{2}}(|0_S 0_B\rangle + |1_S 1_B\rangle)(|0\rangle_A + |1\rangle_A), \tag{2}$$

$$|\Phi^+_{ASB}\rangle = \frac{1}{\sqrt{2}}(|0_A 0_S 0_B\rangle + |1_A 1_S 1_B\rangle). \tag{3}$$

2.2 Simmons' theory

Simmons' theory addresses the communication process in which the sender endeavors to convey its state to a remote receiver by transmitting messages over imperfect communication channels, especially during authentication. Simmons defined two basically dissimilar types of attacks in which the receiver can end up being misinformed. The first type is a limitation attack that considers the communication channel to be noisy, and therefore the characters in the transmitted message can be obtained mistakenly even if the attacker does not possess any knowledge about the actual encrypted message. The other type is a substitution attack that considers that the communicated channel is under the control of the attacker, who intercepts the transmitted encrypted message and tries to generate another one by either intentionally changing the authentic message or presenting fraudulent ones to cheat the receiver. Simmons states that the system will be unconditionally secured if the probability of detecting the eavesdropper satisfies the lower bound, which is greater than or equal to 1/2. This bound identifies what one would instinctively expect from the alteration between the amount of information transferred over the communicated channel, and the one required by the receiver to solve the confusion

about the sender state, and thus to authenticate correctly [48, 49]. In our approach, we utilize the concept of Simmons' theory for the masquerade dishonest (one, two and three user(s)) attack security analysis. In this type of attack, the eavesdropper would like to impersonate as a fraudulent user by controlling the transferred particle, B or C, from the QAS to u_A, u_B and u_C by performing a universal operation $\mathbb{R}$ on A, B, and C. We prove that the sum of probabilities for detecting the eavesdropper $\mathbb{P}_{Sum_{(A)}}$, $\mathbb{P}_{Sum_{(B)}}$, $\mathbb{P}_{Sum_{(C)}}$, $\mathbb{P}_{Sum_{(AB)}}$, $\mathbb{P}_{Sum_{(AC)}}$, $\mathbb{P}_{Sum_{(BC)}}$, $\mathbb{P}_{Sum_{(ABC)}}$ is equivalent to 1.2, which satisfies the lower bound imposed by Simmons. Therefore, our approach is unconditionally secured under this type of attack.

2.3 Holevo theory

Many uses are known for quantum communication channels, such as the transmission of classical information, private classical information, or only quantum information, which is the case considered here. Additionally, it can be used alone, with shared entanglement, or together with other channels, and for each of these settings there exists a capacity that measures the communication potential of that channel. The Holevo theorem proves an upper bound to the amount of accessible information that can be recognized about a quantum state. The amount of accessible information can be identified between two communicated parties as the maximum value of the mutual information $I(X:Y)$ between the random variables X and Y over all probable measurements that the receiver can perform. The upper bound given by Holevo for the amount of accessible information about the variable X with respect to the outcome Y of the measurement is shown by [50, 51]

$$I(X:Y) \leq \hat{\mathrm{s}}(\mathrm{P}) - \sum_i \mathrm{p}_i \hat{\mathrm{s}}(\mathrm{P}_i), \tag{4}$$

where P and $\sum_i \mathrm{p}_i \mathrm{P}_i$ and $\hat{\mathrm{s}}(\mathrm{P})$ is Von Neumann entropy, and the Holevo $\mathcal{X}$ quantity can be calculated using

$$\mathcal{X}(\mathrm{P}) = \hat{\mathrm{s}}(\mathrm{P}) - \sum_i \mathrm{p}_i \hat{\mathrm{s}}(\mathrm{P}_i). \tag{5}$$

In our approach, the Holevo theorem will be applied for one-way channel substitution fraudulent attack security analysis in order to find an upper bound to the total of accessible information that can be known about, or enclosed by a quantum state extracted from a particular ensemble. Thus, an eavesdropper may retrieve from the user's perspective some information throughout the transmission channel to the QAS over all possible measurements. We prove that the eavesdropper will not retrieve any knowledge about the key in the case of measuring the encrypted secret identity information from the user's perspective to QAS which fulfills the Holevo' s upper bound. Therefore, our approach is unconditionally secured under this type of attack as well.

3 Results and discussion

3.1 Generalization of an authentication scheme among N users via generalized GHZ states

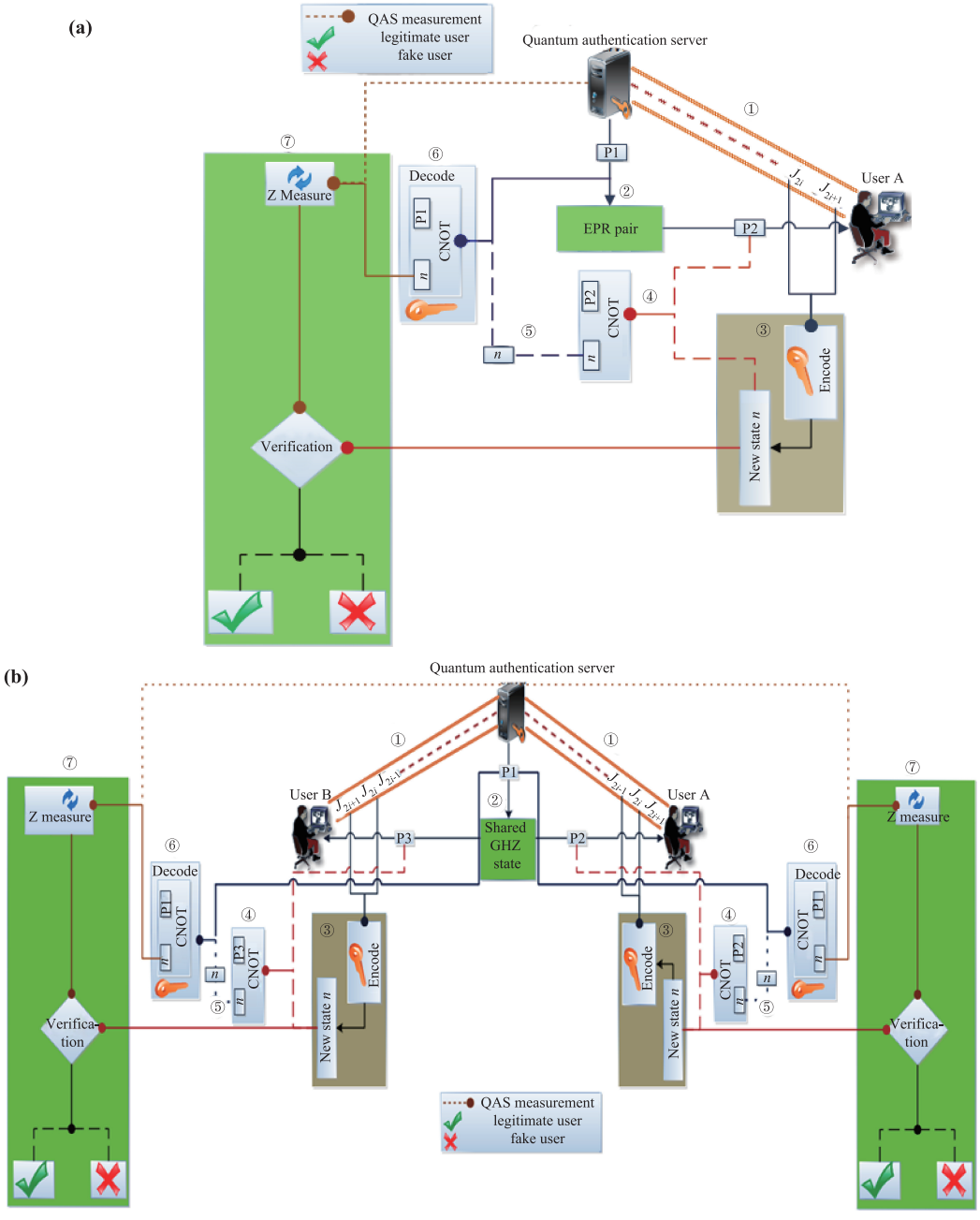
With the objective of protection against "man-in-the-middle", "masquerade as dishonest user", and "exchange fake" attacks, the QAS must verify and authenticate the identity of the communicating users, so that they can transmit quantum messages in a secure manner. Here, we propose a convenient and efficient scheme for the authentication process among the QAS and one [Fig. 1(a)], two [Fig. 1(b)], or more users [generalized to $^\circ N^\circ$ users, Fig. 1(c)]. First, the QAS and $u_1, u_2, \ldots, u_N$ have a joint binary authentication key $J_k = \{J_1, J_2, \ldots, J_N\}$ at the time of registration, which must be kept confidential between the QAS and the N users. Next, if u_1 would like to send a secret message over the network, u_1 first informs the QAS and the other $N-1$ users. When the QAS receives the request, it generates N particles of $N+1$ GHZ states $|\Psi\rangle_{1\ldots N} = \frac{1}{\sqrt{2}}(|\underbrace{0}_{1}\underbrace{0}_{S}\underbrace{0}_{2}\cdots\underbrace{0}_{N-1}\underbrace{0}_{N}\rangle + |\underbrace{1}_{1}\underbrace{1}_{S}\underbrace{1}_{2}\cdots\underbrace{1}_{N-1}\underbrace{1}_{N}\rangle$, as the QAS reserves S at its location and transfers $1, 2, \ldots, N$ particles to $u_1, u_2, \ldots, u_N$, respectively. Afterwards, once $u_1, u_2, \ldots, u_N$ obtain their $1, 2, \ldots, N$ particles, each of them prepares its own new state. The new state results from the encryption of the secret identity information for a particular user operation $|\Phi_{n_{(1)}}\rangle = |J_{2i-1} \otimes J_{2i}\rangle, |\Phi_{n_{(2)}}\rangle = |J_{2i+1} \otimes J_{2i}\rangle, \ldots, |\Phi_{n_{(N)}}\rangle = |J_{2i+(N-1)} \otimes J_{2i}\rangle$.

Then, $u_1, u_2, \ldots, u_N$ perform a $\not\Phi$ operation on both the transmitted particle and n (new state particle) together. The produced particle p will constitute an $N+1$ entangled particle state $|\phi_{p_{(1)}}\rangle = \not\Phi_{NOT}(|\Phi_{n_{(1)}}\rangle \otimes |\Psi\rangle)$, $|\phi_{p_{(2)}}\rangle = \not\Phi_{NOT}(|\Phi_{n_{(2)}}\rangle \otimes |\Psi\rangle), \ldots, |\phi_{p_{(N)}}\rangle = \not\Phi_{NOT}(|\Phi_{n_{(N)}}\rangle \otimes |\Psi\rangle)$. Next, $u_1, u_2, \ldots, u_N$ preserve their own particles, which means u_1 keeps 1 and u_N keeps N at their locations, and transmit the produced particles $|\phi_{p_{(1)}}\rangle \ldots |\phi_{p_{(N)}}\rangle$ to the QAS. When the QAS receives $|\phi_{p_{(1)}}\rangle \ldots |\phi_{p_{(N)}}\rangle$, it starts decrypting them by performing a $\not\Phi_{NOT}$ operation on both its particle S and n $|\phi_{p_{(1)}}\rangle = \not\Phi(|\phi_{p_{(1)}}\rangle), \ldots, |\phi_{p_{(N)}}\rangle = \not\Phi(|\phi_{p_{(N)}}\rangle)$. Finally, the QAS starts the identity verification for $u_1, u_2, \ldots, u_N$ by measuring $|\Phi_{n_{(1)}}\rangle, \ldots, |\Phi_{n_{(N)}}\rangle$ with respect to σ_z. The ensuing state must be either 0 or 1. If the measurement result is identical to $|J_{2i-1}, J_{2i}\rangle, \ldots, |J_{2i+(N-1)}, J_{2i}\rangle$, then $u_1, \ldots, u_N$ are authenticated and verified. Therefore, they can proceed with the communication process. On the contrary, if the result of the measurement is in-

valid, then the authentication process will be aborted and $u_1, u_2, \ldots, u_N$ are not authenticated (refer to Supplementary Information parts 1, 2, and 3 for the authentication process between the QAS and one user, two users and three users, respectively; see also Fig. S1).

3.2 Masquerade as dishonest one, two, and three user(s) security analysis

If an eavesdropper wants to impersonate as a fraudulent user, then the eavesdropper will take control of the transferring particles A, B, or C from QAS to u_A, u_B and u_C respectively. We shall suppose that the eavesdropper performs a universal operation $\mathbb{R}$ on A, B, and C, where $|\mathbb{R}\rangle$ denotes a superfluous state that is generated by the eavesdropper, and E represents the eavesdropper's particle. The eavesdropper will work only on particle A, which means that particles B and C are excluded from the transmitted state, so that the eavesdropper will perform its operations $|0_A\mathbb{R}\rangle$ and $|1_A\mathbb{R}\rangle$, and a new transmitted state will be generated and transferred to the QAS [see Eq. (6)]. The QAS applies $\not{C}_{NOT}$ to the received state, having as an outcome one of following four states: $|\Psi^{00}_{(SA)}\rangle$, $|\Psi^{01}_{(SA)}\rangle$, $|\Psi^{10}_{(SA)}\rangle$, or $|\Psi^{11}_{(SA)}\rangle$. The result of applying the same sequence of operations on the two particles A, B and the three particles A, B, and C at



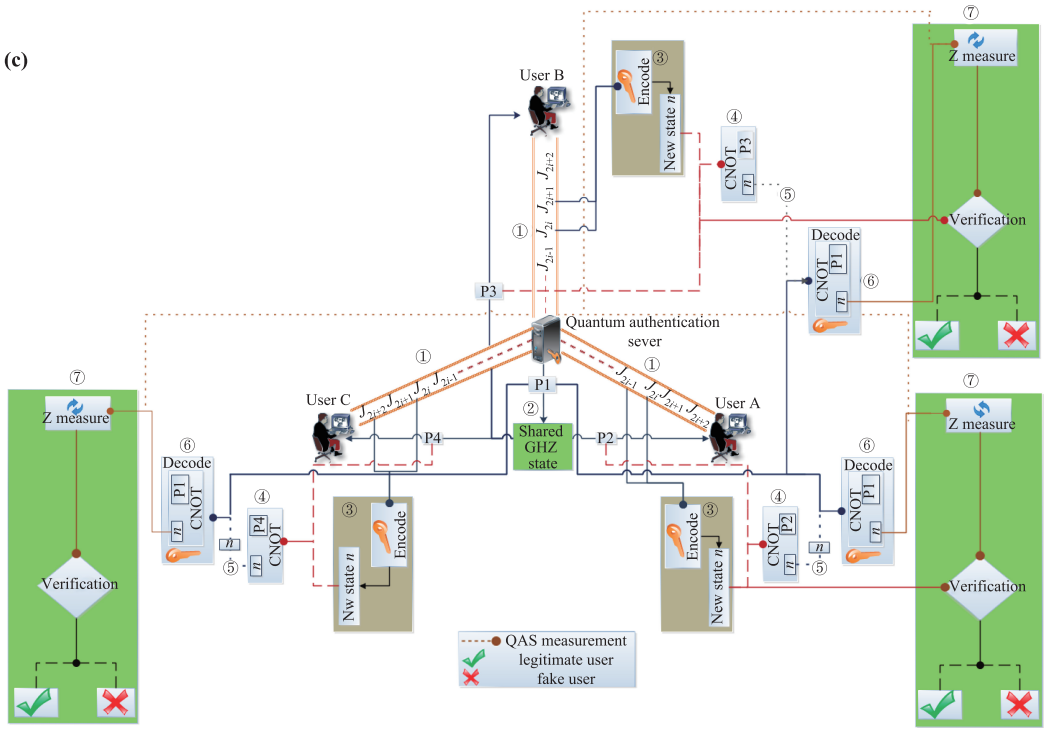


Fig. 1 Authentication process: **(a)** Between the QAS and one user. **(b)** Among QAS and two users. **(c)** Among QAS and three users. **(1)** QAS and $u_1, u_2, \ldots, u_N$ have a joint binary authentication key J_k. **(2)** EPR/GHZ states generation and distribution. **(3)** Encrypting the secret identity authentication as per the particular user operation. **(4)** $u_1, u_2, \ldots, u_N$ performs the operation on both the transmitted particle and n together. The produced particle will become an $N+1$ entangled particle state. **(5)** The remaining produced particles will be transmitted to the QAS. **(6)** The QAS decrypts the secret identity authentication by performing **(7)** Identity verification for $u_1, u_2, \ldots, u_N$ is accomplished by the QAS.

the same time is shown in Eqs. (7) and (8). Therefore, the sum of the probabilities for detecting the eavesdropper $\mathbb{P}_{Sum_{(A)}}$, $\mathbb{P}_{Sum_{(SAB)}}$ and $\mathbb{P}_{Sum_{(SABC)}}$ is equal to 1/2 as shown in Eqs. (9), (10), and (11). Thus, according to Simmons' theory [48, 49], the proposed scheme is unconditionally secured under this kind of attack (See Supplementary Information, part 4, for the "masquerade as dishonest multicast user" security analysis in detail.).

$$|\Psi'_{(SA)}\rangle = \frac{1}{\sqrt{2}}(\alpha_0|0_S0_A0_E\rangle + \beta_0|0_S0_A1_E\rangle + \gamma_0|0_S1_A0_E\rangle + \delta_0|0_S1_A1_E\rangle + \alpha_1|1_S0_A0_E\rangle + \beta_1|1_S0_A1_E\rangle + \gamma_1|1_S1_A0_E\rangle + \delta_1|1_S1_A1_E\rangle), \tag{6}$$

$$|\Psi'_{(SAB)}\rangle = \frac{1}{\sqrt{2}}(\alpha_0\alpha_2|0_S0_A0_B0_E\rangle + \beta_0\beta_2|0_S0_A0_B1_E\rangle + \alpha_0\gamma_2|0_S0_A1_B0_E\rangle + \beta_0\delta_2|0_S0_A1_B1_E\rangle + \gamma_0\alpha_2|0_S1_A0_B0_E\rangle + \delta_0\beta_2|0_S1_A0_B1_E\rangle + \gamma_0\gamma_2|0_S1_A1_B0_E\rangle + \delta_0\delta_2|0_S1_A1_B1_E\rangle + \alpha_1\alpha_3|1_S0_A0_B0_E\rangle + \beta_1\beta_3|1_S0_A0_B1_E\rangle + \alpha_1\gamma_3|1_S0_A1_B0_E\rangle + \beta_1\delta_3|1_S0_A1_B1_E\rangle + \gamma_1\alpha_3|1_S1_A0_B0_E\rangle + \delta_1\beta_3|1_S1_A0_B1_E\rangle + \gamma_1\gamma_3|1_S1_A1_B0_E\rangle + \delta_1\delta_3|1_S1_A1_B1_E\rangle), \tag{7}$$

$$|\Psi'_{(SABC)}\rangle = \frac{1}{\sqrt{2}}(\alpha_0\alpha_2\alpha_4|0_S0_A0_B0_C0_E\rangle + \beta_0\beta_2\beta_4|0_S0_A0_B0_C1_E\rangle + \alpha_0\alpha_2\gamma_4|0_S0_A0_B1_C0_E\rangle + \beta_0\beta_2\delta_4|0_S0_A0_B1_C1_E\rangle + \alpha_0\gamma_2\alpha_4|0_S0_A1_B0_C0_E\rangle + \beta_0\delta_2\beta_4|0_S0_A1_B0_C1_E\rangle + \alpha_0\gamma_2\gamma_4|0_S0_A1_B1_C0_E\rangle + \beta_0\delta_2\delta_4|0_S0_A1_B1_C1_E\rangle + \gamma_0\alpha_2\alpha_4|0_S1_A0_B0_C0_E\rangle + \delta_0\beta_2\beta_4|0_S1_A0_B0_C1_E\rangle + \gamma_0\alpha_2\gamma_4|0_S1_A0_B1_C0_E\rangle + \delta_0\beta_2\delta_4|0_S1_A0_B1_C1_E\rangle + \gamma_0\gamma_2\alpha_4|0_S1_A1_B0_C0_E\rangle + \delta_0\delta_2\beta_4|0_S1_A1_B0_C1_E\rangle + \gamma_0\gamma_2\gamma_4|0_S1_A1_B1_C0_E\rangle + \alpha_0\alpha_2\alpha_4|0_S1_A1_B1_C1_E\rangle + \alpha_1\alpha_3\alpha_5|1_S0_A0_B0_C0_E\rangle + \beta_1\beta_3\beta_5|1_S0_A0_B0_C1_E\rangle + \alpha_1\alpha_3\gamma_5|1_S0_A0_B1_C0_E\rangle + \beta_1\beta_3\delta_5|1_S0_A0_B1_C1_E\rangle + \alpha_1\gamma_3\alpha_5|1_S0_A1_B0_C0_E\rangle + \beta_1\delta_3\beta_5|1_S0_A1_B0_C1_E\rangle + \alpha_1\gamma_3\gamma_5|1_S0_A1_B1_C0_E\rangle$$

$$+\beta_1\delta_3\delta_5|1_S0_A1_B1_C1_E\rangle+\gamma_1\alpha_3\alpha_5|1_S1_A0_B0_C0_E\rangle+\delta_1\beta_3\beta_5|1_S1_A0_B0_C1_E\rangle+\gamma_1\alpha_3\gamma_5|1_S1_A0_B1_C0_E\rangle$$
$$+\delta_1\beta_3\delta_5|1_S1_A0_B1_C1_E\rangle+\gamma_1\gamma_3\alpha_5|1_S1_A1_B0_C0_E\rangle+\delta_1\delta_3\beta_5|1_S1_A1_B0_C1_E\rangle+\gamma_1\gamma_3\gamma_5|1_S1_A1_B1_C0_E\rangle$$
$$+\delta_1\delta_3\delta_5|1_S1_A1_B1_C1_E\rangle), \tag{8}$$

$$\mathbb{P}_{Sum_{(A)}}=\frac{1}{4}(\mathbb{P}_{00_{(A)}}+\mathbb{P}_{01_{(A)}}+\mathbb{P}_{10_{(A)}}+\mathbb{P}_{11_{(A)}})=\frac{1}{2}, \tag{9}$$

$$\mathbb{P}_{Sum_{(SAB)}}=\frac{1}{8}(\mathbb{P}_{000_{(SAB)}}+\mathbb{P}_{001_{(SAB)}}+\mathbb{P}_{010_{(SAB)}}+\mathbb{P}_{011_{(SAB)}}+\mathbb{P}_{100_{(SAB)}}+\mathbb{P}_{101_{(SAB)}}+\mathbb{P}_{110_{(SAB)}}+\mathbb{P}_{111_{(SAB)}}), \tag{10}$$

$$\mathbb{P}_{Sum_{(SABC)}}=\frac{1}{16}(\mathbb{P}_{0000_{(SABC)}}+\mathbb{P}_{0001_{(SABC)}}+\mathbb{P}_{0010_{(SABC)}}+\mathbb{P}_{0011_{(SABC)}}+\mathbb{P}_{0100_{(SABC)}}+\mathbb{P}_{0101_{(SABC)}}$$
$$+\mathbb{P}_{0110_{(SABC)}}+\mathbb{P}_{0111_{(SABC)}}+\mathbb{P}_{1000_{(SABC)}}+\mathbb{P}_{1001_{(SABC)}}+\mathbb{P}_{1010_{(SABC)}}+\mathbb{P}_{1011_{(SABC)}}$$
$$+\mathbb{P}_{1100_{(SABC)}}+\mathbb{P}_{1101_{(SABC)}}+\mathbb{P}_{1110_{(SABC)}}+\mathbb{P}_{1111_{(SABC)}})=\frac{1}{2}. \tag{11}$$

3.3 One-way channel substitution fraudulent attack

The transmitted particle from the QAS to the user's perspective does not contain any information about the authentication key. Therefore, if an eavesdropper would like to perform a one-way channel substitution fraudulent attack, the eavesdropper will work and measure only new state particle $\Phi_{n_{(u)}}$ from the user's perspective to the QAS. The maximum mutual information that an eavesdropper may retrieve over the transmission channel between the QAS to the perspective user can be calculated by the Holevo theory [50, 51]:

$$\chi(\mathbb{P})=\hat{s}(\mathbb{P})-\sum_i \mathbb{p}_i\hat{s}(\mathbb{P}_i). \tag{12}$$

$\hat{s}(\mathbb{P})$ is equal to Von Neumann entropy $-\mathrm{Tr}(\mathbb{P}\log_2\mathbb{P})$, $\mathbb{P}_i$ is a part in the mixture state $\mathbb{P}$, and $\mathbb{p}_i$ is the probability of $\mathbb{P}_i$ in $\mathbb{P}$. Therefore, the attacker obtains information about the authentication key only by computing the $n_{(u)}$ particle. The corresponding $\chi(\mathbb{P})$ depends on the reduced density matrix of $n_{(u)}$ as shown by

$$\chi(\mathbb{P}_{n_{(u)}})=\hat{s}(\mathbb{P}_{n_{(u)}})-\sum_i \mathbb{p}_i\hat{s}(\mathbb{P}_{n_{(u)}i}). \tag{13}$$

For every authentication key, the reduced density matrix of $n_{(u)}$ can be stated as

$$\mathbb{P}_{n_{(u)}}=Tr_{Su}(|\phi_{p_{(u)}}\rangle\langle\phi_{p_{(u)}}|)=\frac{1}{2}I. \tag{14}$$

Likewise, $\mathbb{P}_{n_{(u)}i}$ is equal to the consequent set of equations:

$$|\phi^{00}_{p_{(u)}}\rangle=\frac{1}{\sqrt{2}}(|0_s0_u0_{n_{(u)}}\rangle+|1_q1_u1_{n_{(u)}}\rangle), \tag{15}$$

$$|\phi^{01}_{p_{(u)}}\rangle=\frac{1}{\sqrt{2}}(|0_s0_u1_{n_{(u)}}\rangle+|1_q1_u0_{n_{(u)}}\rangle), \tag{16}$$

$$|\phi^{10}_{p_{(u)}}\rangle=\frac{1}{\sqrt{2}}(|+_s+_u1_{n_{(u)}}\rangle+|-_q-_u0_{n_{(u)}}\rangle), \tag{17}$$

$$|\phi^{11}_{p_{(u)}}\rangle=\frac{1}{\sqrt{2}}(|+_s+_u0_{n_{(u)}}\rangle+|-_q-_u1_{n_{(u)}}\rangle), \tag{18}$$

Therefore,

$$\mathbb{P}_{n_{(u)}i}=Tr_{Su}(|\phi^i_{p_{(u)}}\rangle\langle\phi^i_{p_{(u)}}|)=\frac{1}{2}I. \tag{19}$$

By substituting for both $\mathbb{P}_{n_{(u)}}$ and $\mathbb{P}_{n_{(u)}i}$ in Eq. (13), $\chi(\mathbb{P}_{n_{(u)}})=0$. Therefore, the eavesdropper will not retrieve any knowledge about the key in the case of measuring $\Phi_{n_{(u)}}$ from the user's perspective to QAS.

3.4 Two-way channel substitution fraudulent attack security analysis

Let us suppose that an eavesdropper wants to perform a two-way channel substitution fraudulent attack on the transmitted particle for u_A. First, the eavesdropper listens to the communication channel and intercepts the transmitted particle from QAS to u_A. The eavesdropper then applies operations Θ_1, along with supportive particles $\mathcal{E}$ on his/her side, on the transmitted particles. Subsequently, the eavesdropper transfers the produced particle to u_A. Upon obtaining the corresponding transferred particle, u_A does not know that an eavesdropper executed an operation. u_A applies its ordinary operations and transfers the ensuing particle to the QAS. The eavesdropper interrupts the new state particle sent by u_A and performs operation Θ_2, along with supportive particles μ on his/her side, on the new particles $|\Phi_{n_{(A)}}\rangle$. Successively, the eavesdropper transfers the ensuing particle to the QAS. The eavesdropper attempts to obtain a confident amount of information about the key by utilizing two supportive particles $\mathcal{E}$, μ on particle A. The whole attack operation is represented in Fig. 3(a). When the two-bit key J_iJ_{i+1} is equal to 00, then the subsequent encrypted state by the QAS is given by Eqs. (20) and (21) (See Supplementary Information part 5 for details on the two-way channel substitution fraudulent attackbetween QAS and one user.).

$$|\Psi^{00}_{(SA)}\rangle = \Phi_0\Theta_2\{\Phi_0[\Theta_1(\Psi^{00}_{(SA)}|\mathcal{E}\rangle)||\Phi_{n_{(A)}}\rangle]|\mu\rangle\}, \tag{20}$$

$$\begin{aligned}|\Psi^{00}_{(SA)}\rangle = \frac{1}{\sqrt{2}}\Big(&\alpha_\mathcal{E}\alpha_\mu|0_S0_A0_{n_{(A)}}\mathcal{E}_{00}\mu_{00}\rangle + \alpha_\mathcal{E}\beta_\mu|0_S0_A1_{n_{(A)}}\mathcal{E}_{00}\mu_{01}\rangle + \beta_\mathcal{E}\beta_\mu|0_S1_A0_{n_{(A)}}\mathcal{E}_{01}\mu_{10}\rangle\\ &+\beta_\mathcal{E}\alpha_\mu|0_S1_A1_{n_{(A)}}\mathcal{E}_{01}\mu_{11}\rangle + \beta_\mathcal{E}\alpha_\mu|1_S0_A1_{n_{(A)}}\mathcal{E}_{10}\mu_{00}\rangle + \beta_\mathcal{E}\beta_\mu|1_S0_A0_{n_{(A)}}\mathcal{E}_{01}\mu_{01}\rangle\\ &+\alpha_\mathcal{E}\beta_\mu|1_S1_A1_{n_{(A)}}\mathcal{E}_{11}\mu_{10}\rangle + \alpha_\mathcal{E}\alpha_\mu|1_S1_A0_{n_{(A)}}\mathcal{E}_{11}\mu_{11}\rangle\Big).\end{aligned} \tag{21}$$

Therefore, we can compute that the total probability of detecting the eavesdropper in the authentication process by

$$\mathbb{P}_{\text{Sum}} = \frac{1}{2}[\mathbb{P}_{\text{Sum}}(J_i = 0) + \mathbb{P}_{\text{Sum}}(J_i = 1)]. \tag{22}$$

To reduce the detection probability, the eavesdropper must adopt $\mathbb{P}_{\text{Sum}}$ as the minimum detection probability [Eq. (23)]. Notice that Eq. (23) is computed under the assumption $\alpha_\beta = \alpha_\mu = 1$:

$$Sum = Min(\mathbb{P}_{\text{Sum}}) = \frac{1}{4}(1 - \cos\theta_\mathcal{E}). \tag{23}$$

From Eq. (23) it is plain that $Min(\mathbb{P}_{\text{Sum}})$ depends on $\theta_\mathcal{E}$ but not on θ_μ. Therefore, the eavesdropper's unconditional information amount on the transferred key bits among QAS and u_A can be approximated by

$$\Im(J_K, \Theta_{Total}) = \sum_{x,y} \mathcal{P}(J_K, \Theta_{Total}) \log_2 \frac{\mathcal{P}(J_K, \Theta_{Total})}{\mathcal{P}(J_K)\mathcal{P}(\Theta_{Total})}, \tag{24}$$

where Θ_{Total} denotes the total operation Θ_1 and Θ_2 applied by the eavesdropper, x denotes the key values (00, 01, 10, 11) with probability $\mathcal{P}(x) = \frac{1}{4}$, J_K specifies the chosen random values from variable x, and $y = \mathcal{E}_i j \mu_{\upsilon\tau}$ with $i, j, \upsilon, \tau \in \{0, 1\}$, which denotes 16 probabilities of the joint measurement result for the eavesdropper at positions Θ_1 and Θ_2. The amount of unconditional information that can be retrieved by the eavesdropper is expressed in Eq. (24). $\mathcal{P}(J_K)$ and $\mathcal{P}(\Theta_{Total}|J_K)$ are given by

$$\mathcal{P}(J_K, \Theta_{Total}) = \mathcal{P}(J_K)\mathcal{P}(\Theta_{Total}|J_K). \tag{25}$$

Therefore, the mutual information obtained by the eavesdropper's total operation Θ_{Total} is given by

$$\begin{aligned}\Im = \frac{1}{4}[&(1 + \sin\theta_\mathcal{P})\log_2(1 + \sin\theta_\mathcal{P})\\ &+(1 - \sin\theta_\mathcal{P})\log_2(1 - \sin\theta_\mathcal{P})].\end{aligned} \tag{26}$$

Because $\sin\theta_\mathcal{P} = \sqrt{8 \times Sum - 16 \times Sum^2}$ (see Supplementary Information, part 7), substituting in Eq. (26) we obtain

$$\begin{aligned}\Im = \frac{1}{4}[&(1 + \sqrt{8 \times Sum - 16 \times Sum^2})\log_2(1 + \sqrt{8 \times Sum - 16 \times Sum^2})\\ &+(1 - \sqrt{8 \times Sum - 16 \times Sum^2})\log_2(1 - \sqrt{8 \times Sum - 16 \times Sum^2})].\end{aligned} \tag{27}$$

Consequently, the unconditional detection possibility $\mathcal{P}_e$ of J_K is given by

$$\mathcal{P}_e = \frac{1 + \sin\theta_\mathcal{E}}{2}\left[\frac{1}{2}\mathcal{P} + \frac{1}{4}(1 - \mathcal{P})\right] + \frac{1 - \sin\theta_\mathcal{E}}{2}\left[\frac{1}{4}(1 - \mathcal{P})\right]. \tag{28}$$

Further simplification of Eq. (28) leads to $\mathcal{P}$ of J_K, given by (see Supplementary Information part 8)

$$\mathcal{P}_e = \frac{1}{8}[\sin\theta_\mathcal{E}(3 \times \mathbb{P} - 1) + 4]. \tag{29}$$

$\mathcal{P} = 1$ implies that the detection probability $\mathcal{P}_e$ is maximized (see Supplementary Information part 9):

$$\mathcal{P}^m_e = \frac{1}{4}(\sqrt{16 \times Sum - 16 \times Sum^2 + 1}). \tag{30}$$

The previous result holds when applying the same sequence of operations to perform a two-way channel substitution fraudulent attack on transmitting two particles for u_A and u_B as the eavesdropper applies operations Θ_1 and Θ_2, along with support particles $\mathcal{E}$, γ on his/her side, on the transmitted particles A and B, respectively. Furthermore, the eavesdropper performs operations Θ_3 and Θ_4, along with supportive particles μ, η on his/her side, on the new particles $|\Phi_{n_{(A)}}\rangle$ and $|\Phi_{n_{(B)}}\rangle$ respectively. When the three-bit key $J_{i-1}J_iJ_{i+1} = 000$, then the subsequent encrypted state by the QAS is given by Eqs. (31) and (32) (See Supplementary Information part 6 for details on the two-way channel substitution fraudulent attackbetween QAS and two users.).

$$|\Psi^{000}_{(SAB)}\rangle = \Phi_0\Theta_3\Theta_4\{\Phi_0[\Theta_1(\Psi^{000}_{(SAB)}|\mathcal{E}\rangle)||\Theta_{n_{(A)}}\rangle][\Theta_2(\Psi^{000}_{i_{(SAB)}}|\gamma\rangle)||\Psi_{n_{(B)}}\rangle]|\mu\rangle|\eta\rangle\}, \tag{31}$$

$$\begin{aligned}|\Psi^{000}_{(SAB)}\rangle = \frac{1}{\sqrt{2}}[&(\alpha_\mathcal{E}\alpha_\mu|0_S0_A0_{n_{(A)}}\mathcal{E}_{00}\mu_{00}\rangle + \alpha_\mathcal{E}\beta_\mu|0_S0_A1_{n_{(A)}}\mathcal{E}_{00}\mu_{01}\rangle + \beta_\mathcal{E}\beta_\mu|0_S1_A0_{n_{(A)}}\mathcal{E}_{01}\mu_{10}\rangle\\ &+\beta_\mathcal{E}\alpha_\mu|0_S1_A1_{n_{(A)}}\mathcal{E}_{01}\mu_{11}\rangle + \beta_\mathcal{E}\alpha_\mu|1_S0_A1_{n_{(A)}}\mathcal{E}_{10}\mu_{00}\rangle + \beta_\mathcal{E}\beta_\mu|1_S0_A0_{n_{(A)}}\mathcal{E}_{01}\mu_{01}\rangle\\ &+\alpha_\mathcal{E}\beta_\mu|1_S1_A1_{n_{(A)}}\mathcal{E}_{11}\mu_{10}\rangle + \alpha_\mathcal{E}\alpha_\mu|1_S1_A0_{n_{(A)}}\mathcal{E}_{11}\mu_{11}\rangle)] + [(\alpha_\gamma\alpha_\eta|0_S0_B0_{n_{(B)}}\gamma_{00}\eta_{00}\rangle\\ &+\alpha_\gamma\beta_\eta|0_S0_B1_{n_{(B)}}\gamma_{00}\eta_{01}\rangle + \beta_\gamma\beta_\eta|0_S1_B0_{n_{(B)}}\gamma_{01}\eta_{10}\rangle + \beta_\gamma\alpha_\eta|0_S1_B1_{n_{(B)}}\gamma_{01}\eta_{11}\rangle\\ &+\beta_\gamma\alpha_\eta|1_S0_B1_{n_{(B)}}\gamma_{10}\eta_{00}\rangle + \beta_\gamma\beta_\eta|1_S0_B0_{n_{(B)}}\gamma_{01}\eta_{01}\rangle + \alpha_\gamma\beta_\eta|1_S1_B1_{n_{(B)}}\gamma_{11}\eta_{10}\rangle\\ &+\alpha_\gamma\alpha_\eta|1_S1_B0_{n_{(B)}}\gamma_{11}\eta_{11}\rangle)].\end{aligned} \tag{32}$$

We can compute the total probability of detecting the eavesdropper in the authentication process, given by

$$\mathbb{P}_{\text{Sum}} = \frac{1}{2}[\mathbb{P}_{\text{Sum}}(J_{i-1}=0) + \mathbb{P}_{\text{Sum}}(J_{i-1}=1)]. \tag{33}$$

To reduce the detection probability, the eavesdropper must adopt $\mathbb{P}_{\text{Sum}}$ as small as possible by Eq. (34). Eq. (34) is computed under the assumptions of $\alpha_\mathcal{E} = \alpha_\eta = \alpha_\mu = \alpha_\gamma = 1$:

$$Sum = Min(\mathbb{P}_{\text{Sum}}) = \frac{1}{4}(1-\cos\theta_\mathcal{E} + 1 - \cos\theta_\gamma). \tag{34}$$

From Eq. (34) it is plain that $Min(\mathbb{P}_{\text{Sum}})$ is correlated with $\theta_\mathcal{E}$ and θ_γ, but uncorrelated with θ_η and θ_μ. Therefore, the eavesdropper's unconditional information amount on the transferred key bits among QAS, u_A, and u_B can be approximated by

$$\Im(J_K,\Theta_{Total}) = \sum_{x,y,z}\mathcal{P}(J_K,\Theta_{Total})\log_2\frac{\mathcal{P}(J_K,\Theta_{Total})}{\mathcal{P}(J_K)\mathcal{P}(\Theta_{Total})}, \tag{35}$$

where Θ_{Total} denotes the total operation applied by the eavesdropper Θ_1, Θ_2, Θ_3, and Θ_4, x denotes the key values (000, 001, 010, 011, 100, 101, 110, 111) with probability $\mathcal{P}(x) = \frac{1}{8}$. J_K specifies the chosen random values from variable x, $y = \mathcal{E}_{ij}\mu_{\upsilon\tau}$ with $i,j,\upsilon,\tau \in \{0,1\}$, which denotes 16 probabilities of the joint measurement result of the eavesdropper at positions Θ_1 and Θ_3, $z = \gamma_{kl}\eta_{\varsigma\mathcal{H}}$ with $k,l,\varsigma,\mathcal{H} \in \{0,1\}$, which in turn denotes 16 probabilities of the joint measurement result of the eavesdropper at positions Θ_2 and Θ_4. To restore the value of the eavesdropper's unconditional information amount from Eq. (35), one should only compute $\mathcal{P}(J_K)$ and $\mathcal{P}(\Theta_{Total}|J_K)$, given by

$$\mathcal{P}(J_K|\Theta_{Total}) = \mathcal{P}(J_K)\mathcal{P}(\Theta_{Total}|J_K). \tag{36}$$

Therefore, the mutual obtained information by the eavesdropper's total operation Θ_{Total} is given by

$$\begin{aligned}\Im = \frac{1}{8}[&(1+\sin\theta_{Sum})\log_2(1+\sin\theta_{Sum})\\ &+(1-\sin\theta_{Sum})\log_2(1-\sin\theta_{Sum})].\end{aligned} \tag{37}$$

Because $\sin\theta_{Sum} = \sqrt{16\times Sum - 16\times Sum^2 - 3}$, we have

$$\begin{aligned}\Im = \frac{1}{8}[&(1+\sqrt{16\times Sum - 16\times Sum^2 - 3})\log_2(1+\sqrt{16\times Sum - 16\times Sum^2 - 3})\\ &+(1-\sqrt{16\times Sum - 16\times Sum^2 - 3})\log_2(1-\sqrt{16\times Sum - 16\times Sum^2 - 3})].\end{aligned} \tag{38}$$

Consequently, the unconditional detection probability $\mathcal{P}_e$ of J_K is given by

$$\begin{aligned}\mathcal{P}_e = &\frac{2+\sin\theta_{Sum}}{2}\left[\frac{1}{2}\mathcal{P} + \frac{1}{4}(1-\mathcal{P})\right]\\ &+\frac{2-\sin\theta_{Sum}}{2}\left[\frac{1}{4}(1-\mathcal{P})\right].\end{aligned} \tag{39}$$

or simply

$$\mathcal{P}_e = \frac{1}{8}[\sin\theta_{Sum}(3\times\mathcal{P}-1)+4]. \tag{40}$$

$\mathcal{P} = 1$ implies that the detection possibility $\mathcal{P}_e$ is maximized (see Supplementary Information part 12 for the relation between $\mathcal{P}_e$, $\mathcal{P}_e^m$ and Sum):

$$\mathcal{P}_e^m = \frac{1}{4}(\sqrt{16\times Sum - 16\times Sum^2 - 3}+2). \tag{41}$$

3.5 Analysis of unconditional retrieved mutual information for one and two users by the attacker

Figure 2(a) shows the probability of detecting the eavesdropper whileattempting to achieve a non-zero confident amount of information about the key. The maximum mutual information that can retrieved is equal to 0.5 and 0.75 when the minimum detection proba-

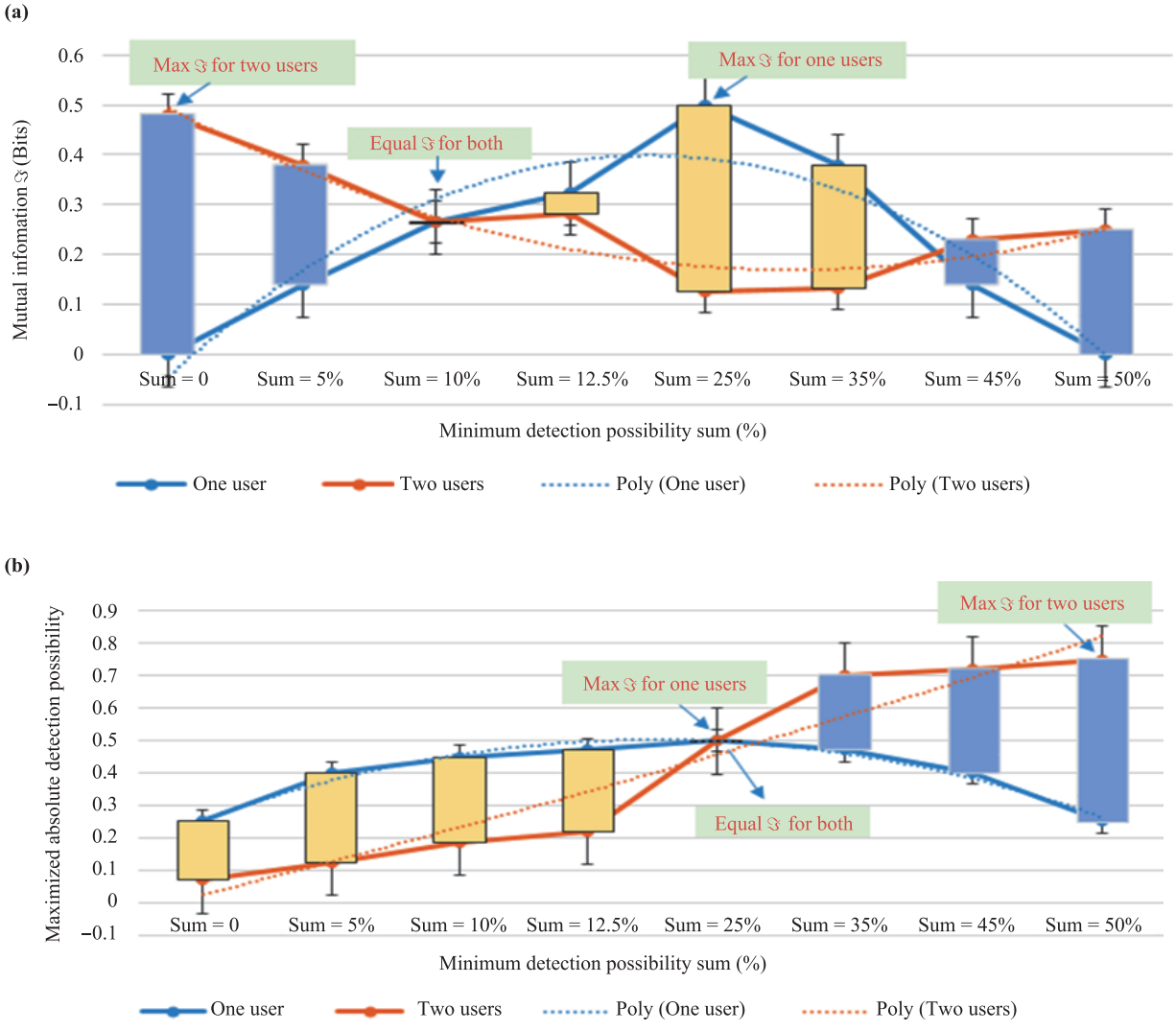


Fig. 2 Analysis of unconditional retrieved mutual information for one and two users by the eavesdropper. **(a)** Correlation between the mutual information $\Im$ and the minimum detection probability Sum for the eavesdropper calculated by $\Im = \frac{1}{4}[(1+\sqrt{8\times Sum - 16\times Sum^2})\log_2(1+\sqrt{8\times Sum - 16\times Sum^2}) + (1-\sqrt{8\times Sum - 16\times Sum^2})\log_2(1-\sqrt{8\times Sum - 16\times Sum^2})]$ for one user and $\Im = \frac{1}{8}[(1+\sqrt{16\times Sum - 16\times Sum^2})\log_2(1+\sqrt{16\times Sum - 16\times Sum^2}) + (1-\sqrt{16\times Sum - 16\times Sum^2})\log_2(1-\sqrt{16\times Sum - 16\times Sum^2})]$ for two users. **(b)** Correlation between maximized unconditional detection probability $\mathcal{P}_e^m$ and Sum calculated by $\mathcal{P}_e^m = \frac{1}{4}(\sqrt{16\times Sum - 16\times Sum^2}+1)$ for one user and $\mathcal{P}_e^m = \frac{1}{4}(\sqrt{16\times Sum - 16\times Sum^2 - 3}+2)$ for two users.

bility $Sum = 25\%, 50\%$ for one and two users, respectively. Both one and two users have equality for retrieving mutual information by the attacker 0.5, when $Sum = 25\%$ (see Table 1, Supplementary Information Tables S1 and S3, and Figs. S2 and S4). Figure 2(b) shows that when the unconditional detection probability $\mathcal{P}_e^m$ is maximized, the eavesdropper can retrieve a maximum mutual information of 0.5 and 0.75 for one and two users, respectively (see Table 2, Supplementary Information Tables S2 and S4, and Figs. S3 and S5).

Figure 3(a) shows that when $Sum = [0, 12.5, 25]\%$, the retrieved mutual information by the eavesdropper for two users is reduced by $[93, 79, 38.8]\%$, $[52, 95, 62.5]\%$, $[99.7, 98.5, 85]\%$, and $[99.9, 99.3, 98]\%$ for $N = [2, 4, 8, 16]$, respectively, for one user. On the other hand, when $Sum = [50]\%$ the retrieved mutual information by the attacker for two users is increased by $[78]$, $[64]$, $[44]$, and $[29]\%$ for $N = [2, 4, 8, 16]$, respectively, for one user. Figure 3(b) shows that when $Sum = [0, 50, 62.5, 87.5]\%$ and $\mathcal{P}_e^m = [12.5, 50]\%$ the retrieved mutual information by the attacker for two users is reduced by $[30, 75, 56.16, 87.5]$, $[50.59, 93, 81.2, 98.48]\%$, $[75, 97.32, 97.88, 98.87]\%$, and $[93.76, 98.12, 99.2, 99.9]\%$ for $N = [2], [4], [8]$, and $[16]$, respectively, as compared

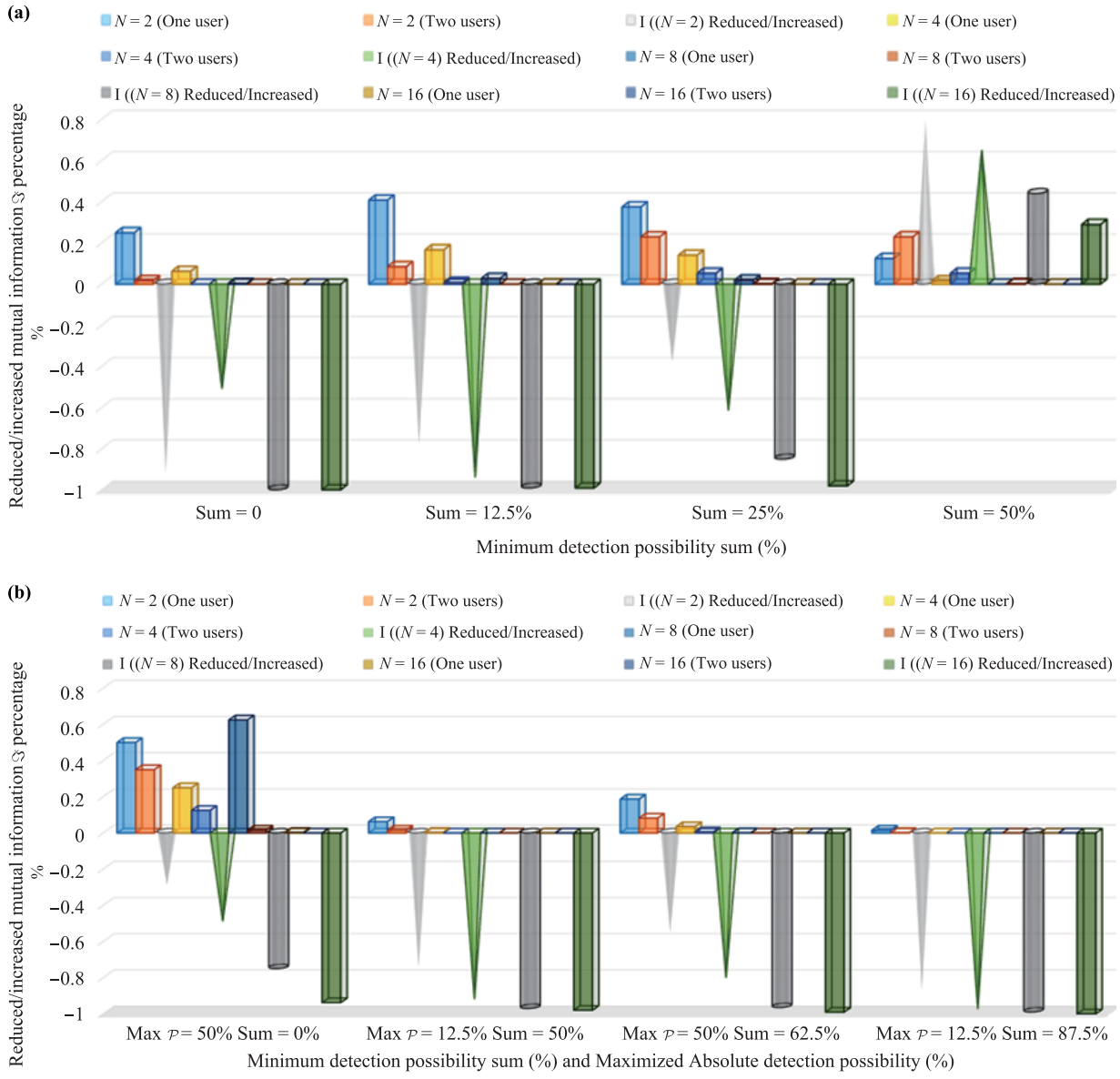


Fig. 3 Relation between reduced/increased mutual information $\Im$ percentage and minimum detection possibility for **(a)** Sum $= [0, 12.5, 25, 50]\%$, **(b)** Sum $= [0, 50, 62.5, 87.5]\%$ and maximized absolute detection possibility $\mathcal{P}_e^m = [12.5, 50]\%$.

Table 1 Correlation between mutual information $\Im$ and minimum detecting possibility sum for one and two users.

Sum	5%	10%	15%	20%	25%	35%	45%	50%
$\Im$(Bits) one user	0.139	0.2655	0.378795	0.459653	0.5	0.47	0.4	0.25
$\Im$(Bits) two users	0.07	0.125	0.187	0.22	0.5	0.7	0.72	0.75

to the case of one user. Therefore, we can conclude that as the number of transferred key bits N becomes larger and the number of users for transmitting the information is increased, the probability of effectively obtaining J_k is reduced and eventually zero (see Supplementary Information part 19).

Figures 4(b) and (a) show that if the minimum detection possibility is equal to $[0, 12.5, 25, 50]\%$ and $= 2$, then the highest values for achieving the information of the transferred keys J_k by the eavesdropper are $[0.25, 4.08 \times 10^{-1}, 3.75 \times 10^{-1}, 1.25 \times 10^{-1}]$ and $[1.73 \times 10^{-2}, 8.5 \times 10^{-2}, 0.2296, 2.3 \times 10^{-1}]$ for one and two users, respectively. Additionally, for $N = 16$ the highest obtained information of the transferred keys J_k by the eavesdrop-

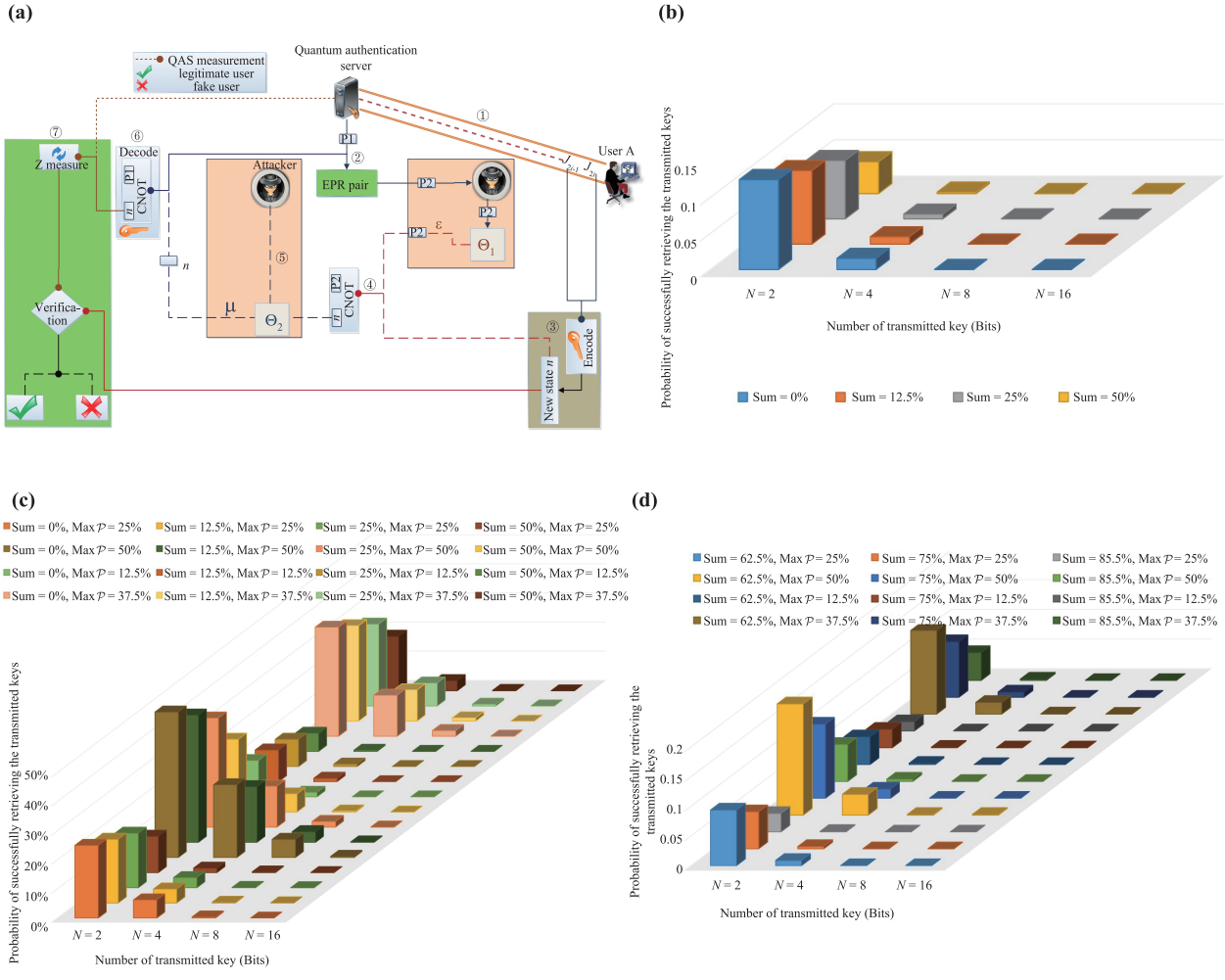
Table 2 Correlation between maximized unconditional detection possibility $\mathcal{P}_e^m$ and sum for one and two users.

Sum	0%	5%	10%	12.5%	25%	35%	45%	50%
$\mathcal{P}_e^m$ one user	0.25	0.40	0.45	0.47	0.50	0.47	0.4	0.25
$\mathcal{P}_e^m$ two users	0.07	0.125	0.187	0.22	0.50	0.72	0.74	0.75

per are $[1.53\times10^{-5}, 7.7\times10^{-4}, 3.91\times10^{-4}, 5.96\times10^{-8}]$ and $[7.73\times10^{-6}, 2.66\times10^{-9}, 8.15\times10^{-15}, 7.73\times10^{-6}]$ for one and two users, respectively. Therefore, we can conclude that as the number of transferred bits increases, the probability for effectively achieving the transferred information is reduced (see Supplementary Information parts 13 and 16).

Figures 4(d) and (c) show that the highest and lowest values for effectively obtaining the information of the transferred keys J_k by the eavesdropper with $N = [2, 4, 8, 16]$ are $[1.87\times10^{-1}, 3.51\times10^{-2}, 1.23\times10^{-3}, 1.53\times10^{-6}]$ and $[1.56\times10^{-2}, 2.5\times10^{-4}, 5.96\times10^{-8}, 3.55\times10^{-15}]$ for one user, and $[8.2\times10^{-2}, 6.6\times10^{-3}, 4.35\times10^{-5}, 1.9\times10^{-9}]$ and $[1.95\times10^{-3}, 3.8\times10^{-6}, 1.5\times10^{-11}, 2.12\times10^{-22}]$ for two users. We can conclude that the corresponding highest values are attained when $\mathcal{P}_e^m$ and Sum are equal to $[50, 62.5]\%$ and $[12.5, 87.5]\%$, respectively. The attacker can retrieve maximum information about the transferred keys J_k when $\mathcal{P}_e^m$ and Sum are equal to $[50, 62.5]\%$ and minimum information when $\mathcal{P}_e^m$ and Sum are equal to $[12.5, 87.5]\%$ (See Supplementary Information parts 15 and 18 for detailed computations of the relation between $\mathcal{P}_e^r$ and N when $\mathcal{P}_e^m = [12.5, 25, 37.5, 50]\%$ and $Sum = [62.5, 75, 87.5]\%$ for one and two users, respectively.).

Figures 4(c) and (b) show that the highest and lowest values for effectively obtaining the information of the transferred keys J_k by the eavesdropper with $N = [2, 4, 8, 16]$ are $[0.5, 0.25, 0.0625, 3.91\times10^{-3}]$ and $[0.0625, 3.91\times10^{-3}, 1.53\times10^{-5}, 2.32\times10^{-10}]$ for one



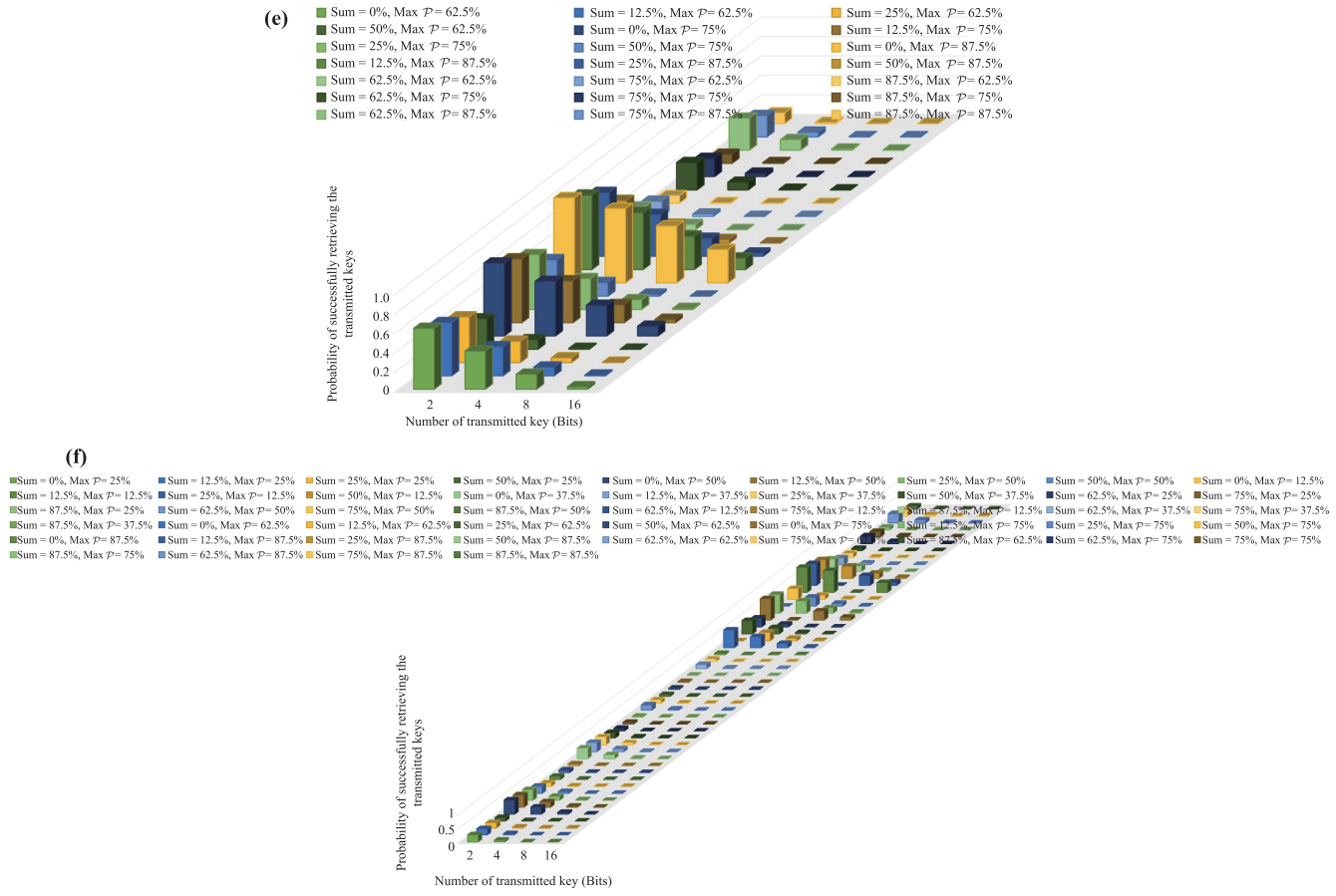


Fig. 4 Two-way channel substitution fraudulent attack security analysis for one user: **(a)** Two-way channel substitution fraudulent attack between QAS and one user with two operations Θ_1, Θ_2 and two supportive particles $\mathcal{E}$, μ. **(b)** Relation between the possibility of the eavesdropper to positively retrieve the transferred keys $\mathcal{P}_e^r$, $N = [2, 4, 8, 16]$ and $Sum = [0, 12.5, 25, 50]\%$ calculated by $\mathcal{P}_e^r = \left[\frac{1}{4}(\sqrt{8 \times Sum - 16 \times Sum^2} + 1)(1 - Sum)\right]^{N/2}$. **(c)** Relation between $\mathcal{P}_e^r$ and N when $\mathcal{P}_e^m = [12.5, 25, 37.5, 50]\%$ and $Sum = [0, 12.5, 25, 50]\%$. **(d)** Relation between $\mathcal{P}_e^r$ and N when $\mathcal{P}_e^m = [12.5, 25, 37.5, 50]\%$ and $Sum = [62.5, 75, 87.5]\%$. **(e)** Relation between $\mathcal{P}_e^r$ and N when $\mathcal{P}_e^m = [62.5, 75, 87.5]\%$ and $Sum = [0, 12.5, 25, 37.5, 50, 62.5, 75, 87.5]\%$. **(f)** Combined relations for **(c–e)**.

user and $[0.35, 1.25 \times 10^{-1}, 1.56 \times 10^{-2}, 2.44 \times 10^{-4}]$ and $[1.56 \times 10^{-2}, 2.44 \times 10^{-4}, 5.96 \times 10^{-8}, 3.6 \times 10^{-15}]$ for two users. The highest values are uniquely obtained when $\mathcal{P}_e^m$ and Sum are equal to $[50, 0]\%$, so the attacker can acquire the highest possible information about the transferred keys J_k. Moreover, the lowest value that the attacker can retrieve for the information about the transferred keys J_k are $[2.32 \times 10^{-10}]$ and $[3.6 \times 10^{-15}]$ for one and two users, which correspond when the values of $\mathcal{P}_e^m$ and Sum are equal to $[12.5, 50]\%$ (See Supplementary Information parts 14 and 17 for the detailed computations of the relation between $\mathcal{P}_e^r$ and N when $\mathcal{P}_e^m = [12.5, 25, 37.5, 50]\%$ and $Sum = [0, 12.5, 25, 50]\%$ for one and two users, respectively.).

From Figs. 4(e), (f), (d), and (e), we can deduce that when the number of transferred key bits N becomes greater, the probability of obtaining J_k is reduced and tends to zero. Thus, the attacker will not detect a vast amount of information, which can be neglected and eliminated by regularly updating the key among the QAS, u_A and u_B. In this case, the attacker's knowledge of the old key will be ineffective.

4 Conclusion

In the present contribution, we have studied the authentication process among N users in a centralized quantum communication environment via entanglement. We have observed that the security analysis of the authentication processes of our protocol — contrary to various kinds of attacks — verifies that it is unconditionally secure and that the attacker will not expose any information about the transmitted key in the case of directly analyzing the

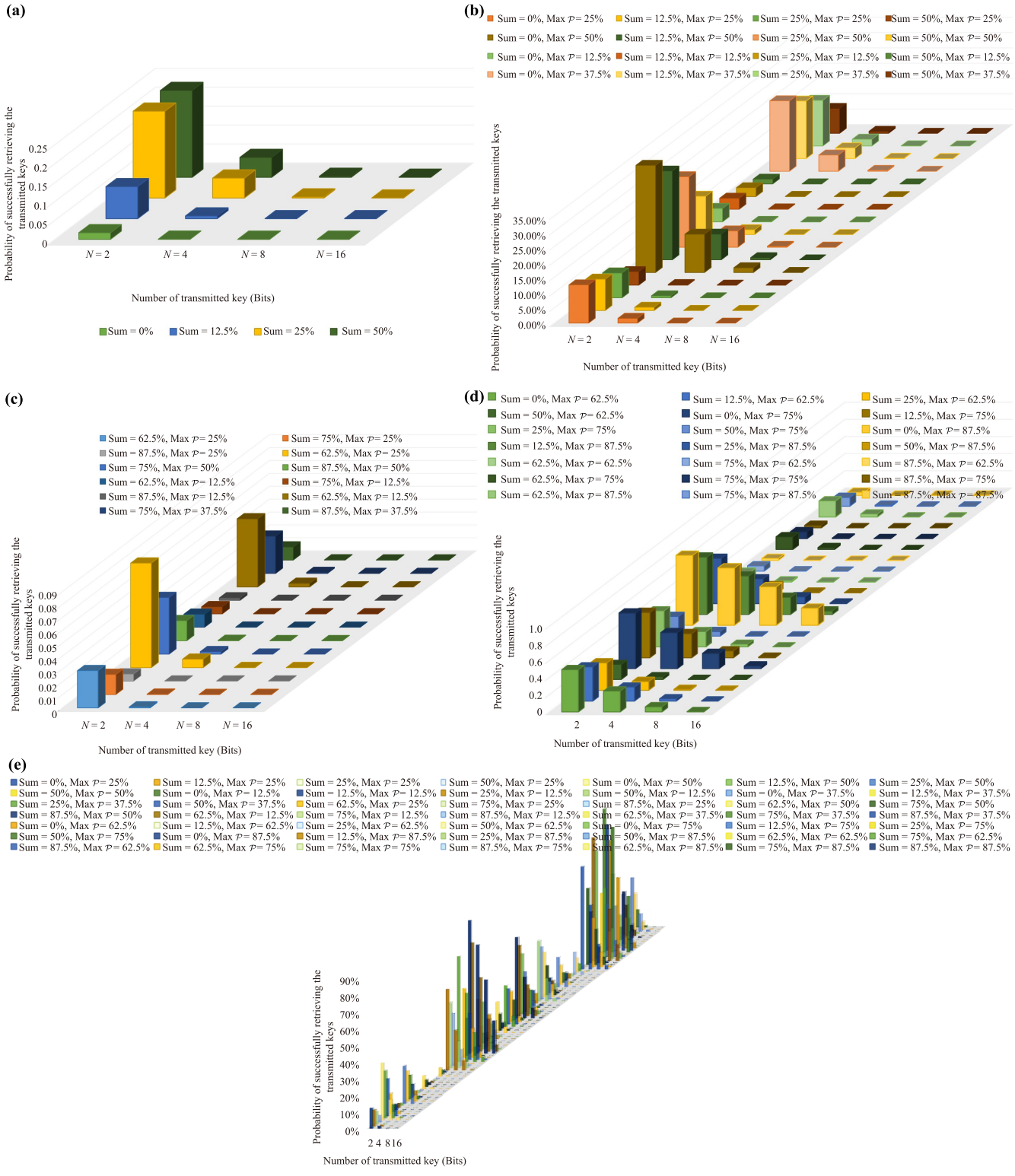


Fig. 5 Two-way channel substitution fraudulent attack security analysis for two users: **(a)** Relation between the probability of the eavesdropper to retrieve the transferred keys $\mathcal{P}_e^r$, $N = [2, 4, 8, 16]$ and $Sum = [0, 12.5, 25, 50]\%$ calculated by $\mathcal{P}_e^r = \left[\frac{1}{4}(\sqrt{16 \times Sum - 16 \times Sum^2 - 3} + 2)(1 - Sum)\right]^{3N/4}$. **(b)** Relation between $\mathcal{P}_e^r$ and N when $\mathcal{P}_e^m = [12.5, 25, 37.5, 50]\%$ and $Sum = [0, 12.5, 25, 50]\%$. **(c)** Relation between $\mathcal{P}_e^r$ and N when $\mathcal{P}_e^m = [12.5, 25, 37.5, 50]\%$ and $Sum = [62.5, 75, 87.5]\%$. **(d)** Relation between $\mathcal{P}_e^r$ and N when $\mathcal{P}_e^m = [62.5, 75, 87.5]\%$ and $Sum = [0, 12.5, 25, 37.5, 50, 62.5, 75, 87.5]\%$. **(e)** Combined relations for **(b–d)**.

transmitted particles over the conveyed channel, from the quantum authentication server to the disjoint user, and vice versa. Moreover, as the number of transferred key bits N becomes larger and the number of users for transmitting the information is increased, the probability of effectively obtaining the transmitted authentication keys is reduced to zero. The nature of our advantage over other protocols is not due to the multipartite non-locality and entanglement content of the generalized GHZ states. Instead, it is the manner, in which these states distribute the information in all steps of the protocol among the quantum server and the users makes our proposed protocol highly successful.

Acknowledgements J. Batle acknowledges fruitful discussions with Joana Rosselló, Maria del Mar Batle and Regina Batle.

Electronic Supplementary Material Supplementary information is available in the online version of this article at https://doi.org/10.1007/s11467-017-0717-3 and is accessible for authorized users.

References and notes

1. C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Theor. Comput. Sci.* 560, 7 (2014)
2. M. Nielsen and I. Chuang, Quantum Computation and Quantum Information, Cambridge: Cambridge University Press, 2000
3. G. H. Zeng, Quantum Cryptology, Beijing: Science Press, 2006
4. G. Assche, Quantum Cryptography and Secret-Key Distillation, Cambridge: Cambridge University Press, 2006
5. M. S. Sharbaf, Quantum Cryptography: A New Generation of Information Technology Security System, Sixth International Conference on Information Technology. Nevada, USA, IEEE, pp 1644–1648, April, 2009
6. W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, *Nature* 299(5886), 802 (1982)
7. A. Poppe, M. Peev, and O. Maurhart, Outline of the SECOQC quantum-key distribution network in Vienna, *Int. J. Quant. Inf.* 06(02), 209 (2008)
8. M. Peev, et al., The SECOQC quantum key distribution network in Vienna, *New J. Phys.* 11(075001), 1367 (2009)
9. C. Elliott, Building the quantum network, *New J. Phys.* 4, 46 (2002)
10. C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, Current status of the DARPA quantum network, *Quantum Information and Computation* 5815, 138 (2005)
11. A. F. Metwaly, M. Z. Rashad, F. A. Omara, and A. A. Megahed, Architecture of multicast centralized key management scheme using quantum key distribution and classical symmetric encryption, *Eur. Phys. J. Spec. Top.* 223(8), 1711 (2014)
12. A. Farouk, M. Zakaria, A. Megahed, and F. A. Omara, A generalized architecture of quantum secure direct communication for N disjointed users with authentication, *Sci. Rep.* 5(1), 16080 (2015)
13. M. Naseri, M. A. Raji, M. R. Hantehzadeh, A. Farouk, A. Boochani, and S. Solaymani, A scheme for secure quantum communication network with authentication using GHZ-like states and cluster states controlled teleportation, *Quantum Inform. Process.* 14(11), 4279 (2015)
14. K. Boström and T. Felbinger, Deterministic Secure Direct Communication Using Entanglement, *Phys. Rev. Lett.* 89(18), 187902 (2002)
15. F. Deng, G. Long, and X. Liu, Two-step quantum direct communication protocol using the Einstein–Podolsky–Rosen pair block, *Phys. Rev. A* 68(4), 042317 (2003)
16. M. Lucamarini and S. Mancini, Secure deterministic communication without entanglement, *Phys. Rev. Lett.* 94(14), 140501 (2005)
17. A. Zhu, Y. Xia, Q. Fan, and S. Zhang, Secure direct communication based on secret transmitting order of particles, *Phys. Rev. A* 73(2), 022338 (2006)
18. H. Lee, J. Lim, and H. Yang, Quantum direct communication with authentication, *Phys. Rev. A* 73(4), 042305 (2006)
19. T. Wang, Q. Wen, and F. Zhu, Controlled quantum secure direct communication with quantum encryption, *Int. J. Quant. Inf.* 6, 543 (2008)
20. C. Wang, F. Deng, Y. Li, X. Liu, and G. Long, Quantum secure direct communication with high dimension quantum superdense coding, *Phys. Rev. A* 71(4), 044305 (2005)
21. T. Gao, F. L. Yan, and Z. X. Wang, A simultaneous quantum secure direct communication scheme between the central party and other M parties, *Chin. Phys. Lett.* 22(10), 2473 (2005)
22. C. Wang, F. Deng, and G. Long, Multi-step quantum secure direct communication using multi-particle Green–Horne–Zeilinger state, *Opt. Commun.* 253(1–3), 15 (2005)
23. J. Wang, Q. Zhang, and C. Tang, Quantum secure direct communication based on order rearrangement of single photons, *Phys. Lett. A* 358(4), 256 (2006)
24. C. Qing-Yu, and L. Bai-Wen, Deterministic secure communication without using entanglement, *Chin. Phys. Lett.* 21(4), 601 (2004)
25. Q. Y. Cai, Eavesdropping on the two-way quantum communication protocols with invisible photons, *Phys. Lett. A* 351(1–2), 23 (2006)

26. G. L. Long, F. Deng, C. Wang, X. Li, K. Wen, and W. Wang, Quantum secure direct communication and deterministic secure quantum communication, *Front. Phys. China* 2(3), 251 (2007)
27. G. Q. He, J. Zhu, and G. Zeng, Quantum secure communication using continuous variable EPR correlations, *Phys. Rev. A* 73, 1 (2006)
28. Y. Chang, C. Xu, S. Zhang, and L. Yan, Controlled quantum secure direct communication and authentication protocol based on five-particle cluster state and quantum one-time pad, *Chin. Sci. Bull.* 59(21), 2541 (2014)
29. C. Yan, Z. Shi-Bin, and Y. Li-Li, A Bidirectional Quantum Secure Direct Communication Protocol Based on Five-Particle Cluster State, *Chin. Phys. Lett.* 30(9), 090301 (2013)
30. W. Li, J. Chen, X. Wang, and C. Li, Quantum Secure Direct Communication Achieved by Using Multi-Entanglement, *Int. J. Theor. Phys.* 54(1), 100 (2015)
31. J. Wang, Q. Zhang, and C. J. Tang, Multiparty controlled quantum secure direct communication using Greenberger–Horne–Zeilinger state, *Opt. Commun.* 266(2), 732 (2006)
32. X.- M. Xiu, L. Dong, Y.- J. Gao, and F. Chi, Quantum secure direct communication using six-particle maximally entangled states and teleportation, *Commum. Theor. Phys.* 51(3), 429 (2009)
33. P. Yadav, R. Srikanth, and A. Pathak, Two-step orthogonal-state-based protocol of quantum secure direct communication with the help of order-rearrangement technique, *Quantum Inform. Process.* 13(12), 2731 (2014)
34. X. Li and H. Barnum, Quantum authentication using entangled states, *Int. J. Found. Comput. Sci.* 15(04), 609 (2004)
35. N. Zhou, G. Zeng, W. Zeng, and F. Zhu, Cross-center quantum identification scheme based on teleportation and entanglement swapping, *Opt. Commun.* 254(4–6), 380 (2005)
36. D. R. Kuhn, A quantum cryptographic protocol with detection of compromised server, *Quantum Inf. Comput.* 5(7), 551 (2005)
37. X. Wen, Y. Liu, and N. Zhou, Secure quantum telephone, *Opt. Commun.* 275(1), 278 (2007)
38. M. Naseri, Eavesdropping on secure quantum telephone protocol with dishonest server, *Opt. Commun.* 282(16), 3375 (2009)
39. Y. Sun, Q. Y. Wen, F. Gao, and F. C. Zhu, Improving the security of secure quantum telephone against an attack with fake particles and local operations, *Opt. Commun.* 282(11), 2278 (2009)
40. D. Zhang and X. Li, Quantum authentication using orthogonal product states, in: Third International Conference on Natural Computation, ICNC 2007, Vol. 4, pp 608–612, IEEE
41. B. S. Shi, J. Li, J. M. Liu, X. F. Fan, and G. C. Guo, Quantum key distribution and quantum authentication based on entangled state, *Phys. Lett. A* 281(2–3), 83 (2001)
42. T. Wei, C. W. Tsai, and T. Hwang, Comment on quantum key distribution and quantum authentication based on entangled state, *Int. J. Theor. Phys.* 50(9), 2703 (2011)
43. P. Huang, J. Zhu, Y. Lu, and G. H. Zeng, Quantum identity authentication using Gaussian-modulated squeezed states, *Int. J. Quant. Inf.* 9(2), 701 (2011)
44. C. W. Tsai, T. S. Wei, and T. Hwang, One-way quantum authenticated secure communication using rotation operation, *Commum. Theor. Phys.* 56(6), 1023 (2011)
45. H. X. Ma, P. Huang, W. S. Bao, and G. H. Zeng, Continuous-variable quantum identity authentication based on quantum teleportation, *Quantum Inform. Process.* 15(6), 2605 (2016)
46. N. Penghao, C. Yuan, and L. Chong, Quantum authentication scheme based on entanglement swapping, *Int. J. Theor. Phys.* 55(1), 302 (2016)
47. M. Naseri, Revisiting quantum authentication scheme based on entanglement swapping, *Int. J. Theor. Phys.* 55(5), 2428 (2016)
48. G. J. Simmons, Message Authentication without secrecy: A secure communications problem uniquely solvable by asymmetric encryption techniques, 12th IEEE Annual Electronics and Aerospace Conference, Washington, USA, IEEE, pp 661–662, December, 1979
49. G. J. Simmons, Authentication theory/coding theory, Advances in Cryptology–Proceedings of Crypto 84, Paris, France, 196, (pp 411–431), Heidelberg: Springer, 1984
50. A. S. Holevo, Statistical problems in quantum physics, in: Proceedings of the second Japan-USSR Symposium on probability theory, 330, 104–119 (1973)
51. A. S. Holevo, The capacity of the quantum channel with general signal states, *IEEE Trans. Inf. Theory* 44(1), 269 (1998)
52. A. K. Ekert, Quantum cryptography based on Bell's theorem, *Phys. Rev. Lett.* 67(6), 661 (1991)
53. C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels, *Phys. Rev. Lett.* 70(13), 1895 (1993)
54. F. G. Deng and G. L. Long, Bidirectional quantum key distribution protocol with practical faint laser pulses, *Phys. Rev. A* 70(1), 012311 (2004)
55. N. Gisin and S. Massar, Optimal quantum cloning machines, *Phys. Rev. Lett.* 79(11), 2153 (1997)
56. A. Peres, Separability criterion for density matrices, *Phys. Rev. Lett.* 77(8), 1413 (1996)
57. F. Giraldi and P. Grigolini, Quantum entanglement and entropy, *Phys. Rev. A* 64(3), 032310 (2001)

58. D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu, Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein–Podolsky–Rosen channels, *Phys. Rev. Lett.* 80(6), 1121 (1998)

59. M. Hillery, V. Bužek, and A. Berthiaume, Quantum secret sharing, *Phys. Rev. A* 59(3), 1829 (1999)

60. M. A. Nielsen, Conditions for a class of entanglement transformations, *Phys. Rev. Lett.* 83(2), 436 (1999)

61. R. A. Bertlmann and A. Zeilinger (Eds.), Quantum (un) Speakables: From Bell to Quantum Information, Springer Science & Business Media 2013

62. A. Aspect, J. Dalibard, and G. Roger, Experimental test of Bell's inequalities using time-varying analyzers, *Phys. Rev. Lett.* 49(25), 1804 (1982)

63. L. F. Wei, Y. X. Liu, M. J. Storcz, and F. Nori, Macroscopic Einstein–Podolsky–Rosen pairs in superconducting circuits, *Phys. Rev. A* 73(5), 052307 (2006)

64. J. S. Huang, C. H. Oh, and L. F. Wei, Testing tripartite Mermin inequalities by spectral joint measurements of qubits, *Phys. Rev. A* 83(6), 062108 (2011)

65. J. Uffink, Quadratic Bell inequalities as tests for multipartite entanglement, *Phys. Rev. Lett.* 88(23), 230406 (2002)

66. Z. Zhao, Y. A. Chen, A. N. Zhang, T. Yang, H. J. Briegel, and J. W. Pan, Experimental demonstration of five-photon entanglement and open-destination teleportation, *Nature* 430(6995), 54 (2004)

67. D. Leibfried, E. Knill, S. Seidelin, J. Britton, R. B. Blakestad, J. Chiaverini, D. B. Hume, W. M. Itano, J. D. Jost, C. Langer, R. Ozeri, R. Reichle, and D. J. Wineland, Creation of a six-atom "Schrödinger cat" state, *Nature* 438(7068), 639 (2005)

68. C. Y. Lu, X. Q. Zhou, O. Gühne, W. B. Gao, J. Zhang, Z. S. Yuan, A. Goebel, T. Yang, and J. W. Pan, Experimental entanglement of six photons in graph states, *Nat. Phys.* 3(2), 91 (2007)

69. Y. Xia, P. Lu, and Y. Zeng, Effective protocol for preparation of N-photon Greenberger–Horne–Zeilinger states with conventional photon detectors, *Quantum Inform. Process.* 11(2), 605 (2012)

70. S. Y. Hao, Y. Xia, J. Song, and N. B. An, One-step generation of multiatom Greenberger–Horne–Zeilinger states in separate cavities via adiabatic passage, *Journal of the Optical Society of America B* 30(2), 468 (2013)

71. Y. F. Huang, B.H. Liu, L. Peng, Y.H. Li, L. Li, C.F. Li, and G.C. Guo, Experimental generation of an eight-photon Greenberger–Horne–Zeilinger state, *Nat. Commun.* 2, 546 (2011)

72. A. Metwaly, M. Z. Rashad, F. A. Omara, and A. A. Megahed, Architecture of Point to Multipoint QKD Communication Systems (QKDP2MP). In 8th International Conference on Informatics and Systems (INFOS), Cairo, pp NW 25–31, IEEE, May, 2012

73. A. Farouk, F. Omara, M. Zakria, and A. Megahed, Secured IPsec multicast architecture based on quantum key distribution, in: The International Conference on Electrical and Bio-medical Engineering, Clean Energy and Green Computing, pp 38–47 (2015). The Society of Digital Information and Wireless Communication.

74. M. M. Wang, W. Wang, J. G. Chen, and A. Farouk, Secret sharing of a known arbitrary quantum state with noisy environment, *Quantum Inform. Process.* 14(11), 4211 (2015)

75. M. Naseri, S. Heidari, M. Baghfalaki, N. Fatahi, R. Gheibi, J. Batle, A. Farouk, and A. Habibi, A new secure quantum watermarking scheme, *Optik* 139, 77 (2017)

76. J. Batle, O. Ciftja, M. Naseri, M. Ghoranneviss, A. Farouk, and M. Elhoseny, Equilibrium and uniform charge distribution of a classical two-dimensional system of point charges with hard-wall confinement, *Phys. Scr.* 92(5), 055801 (2017)

77. H. Geurdes, K. Nagata, T. Nakamura, and A. Farouk, A note on the possibility of incomplete theory, arXiv: 1704.00005 (2017)

78. J. Batle, A. Farouk, M. Alkhambashi, and S. Abdalla, Multipartite correlation degradation in amplitude-damping quantum channels, *J. Korean Phys. Soc.* 70(7), 666 (2017)

79. J. Batle, M. Naseri, M. Ghoranneviss, A. Farouk, M. Alkhambashi, and M. Elhoseny, Shareability of correlations in multiqubit states: Optimization of nonlocal monogamy inequalities, *Phys. Rev. A* 95(3), 032123 (2017)

80. J. Batle, A. Farouk, M. Alkhambashi, and S. Abdalla, Entanglement in the linear-chain Heisenberg antiferromagnet $Cu(C_4H_4N_2)(NO_3)_2$, *Eur. Phys. J. B* 90(3), 49 (2017)

81. J. Batle, M. Alkhambashi, A. Farouk, M. Naseri, and M. Ghoranneviss, Multipartite non-locality and entanglement signatures of a field-induced quantum phase transition, *Eur. Phys. J. B* 90(2), 31 (2017)

82. K. Nagata, T. Nakamura, J. Batle, S. Abdalla, and A. Farouk, Boolean approach to dichotomic quantum measurement theories, *J. Korean Phys. Soc.* 70(3), 229 (2017)

83. M. Abdolmaleky, M. Naseri, J. Batle, A. Farouk, and L. H. Gong, Red–Green–Blue multi-channel quantum representation of digital images, *Optik* 128, 121 (2017)

84. A. Farouk, M. Elhoseny, J. Batle, M. Naseri, and A. E. Hassanien, A proposed architecture for key management schema in centralized quantum network, in: Handbook of Research on Machine Learning Innovations and Trends, pp 997–1021, IGI Global, 2017

85. N. R. Zhou, J. F. Li, Z. B. Yu, L. H. Gong, and A. Farouk, New quantum dialogue protocol based on continuous-variable two-mode squeezed vacuum states, *Quantum Inform. Process.* 16(1), 4 (2017)

86. J. Batle, M. Abutalib, S. Abdalla, and A. Farouk, Persistence of quantum correlations in a XY spin-chain environment, *Eur. Phys. J. B* 89(11), 247 (2016)

87. J. Batle, M. Abutalib, S. Abdalla, and A. Farouk, Revival of Bell nonlocality across a quantum spin chain, *Int. J. Quant. Inf.* 14(07), 1650037 (2016)

88. J. Batle, C. R. Ooi, A. Farouk, M. Abutalib, and S. Abdalla, Do multipartite correlations speed up adiabatic quantum computation or quantum annealing? *Quantum Inform. Process.* 15(8), 3081 (2016)

89. J. Batle, A. Bagdasaryan, A. Farouk, M. Abutalib, and S. Abdalla, Quantum correlations in two coupled superconducting charge qubits, *Int. J. Mod. Phys. B* 30(19), 1650123 (2016)

90. J. Batle, C. R. Ooi, M. Abutalib, A. Farouk, and S. Abdalla, Quantum information approach to the azurite mineral frustrated quantum magnet, *Quantum Inform. Process.* 15(7), 2839 (2016)

91. J. Batle, C. R. Ooi, A. Farouk, and S. Abdalla, Nonlocality in pure and mixed n-qubit X states, *Quantum Inform. Process.* 15(4), 1553 (2016)

92. J. Batle, C. R. Ooi, A. Farouk, M. Abutalib, and S. Abdalla, Do multipartite correlations speed up adiabatic quantum computation or quantum annealing? *Quantum Inform. Process.* 15(8), 3081 (2016)

93. A. F. Metwaly, M. Z. Rashad, F. A. Omara, and A. A. Megahed, Architecture of multicast network based on quantum secret sharing and measurement, *International Research Journal of Engineering and Technology* 02(03), 2336 (2015)