Lim et al. *EPJ Quantum Technology* (2023) 10:35
https://doi.org/10.1140/epjqt/s40507-023-00193-y

EPJ Quantum Technology
a SpringerOpen Journal

RESEARCH Open Access

Quantum authentication method based on key-controlled maximally mixed quantum state encryption

Na-Hee Lim[1,2†], Ji-Woong Choi[1†], Min-Sung Kang[3], Hyung-Jin Yang[4] and Sang-Wook Han[1,2*]

*Correspondence: swhan@kist.re.kr
[1]Center for Quantum Information, Korea Institute of Science and Technology (KIST), Seoul, 02792, Republic of Korea
[2]Division of Nano and Information Technology, Korea Institute of Science and Technology School, Korea University of Science and Technology, Seoul, 02792, Republic of Korea
Full list of author information is available at the end of the article
†Equal contributors

Abstract

Quantum authentication is a fundamental first step that ensures secure quantum communication. Although various quantum authentication methods have been proposed recently, their implementation efficiency is limited. This paper proposes a key-controlled maximally mixed quantum state encryption (MMQSE) method using only a single qubit, unitary operation, minimized quantum transmissions, and a single qubit measurement, which improves implementation feasibility and operation efficiency. We applied it to representative quantum authentication applications, namely, quantum identity and message authentication. The security of our authentication schemes was verified by analyzing the relationship between the integral ratio of Uhlmann's fidelity and probability of successful eavesdropping. Moreover, we demonstrate the higher authentication efficiency of the proposed scheme in a real quantum-channel noise environment. The upper bound of the valid noise rate was quantified using the integral ratio of Uhlmann's fidelity in a noise environment. Finally, the optimal number of authentication sequences was estimated.

Keywords: Quantum identity authentication; Quantum message authentication; Unitary operation; Uhlmann's fidelity

1 Introduction

Modern cryptography has been threatened by the explosive development of quantum-computing technology that can implement quantum algorithms such as Shor's [1–3]. Quantum cryptography is a representative alternative technology [4–7] providing data security based on physical laws such as the superposition of quantum states, irreversibility of quantum measurement, no-cloning theorem, and the uncertainty principle. In the field of quantum cryptography, quantum authentication is the first and most fundamental process in secure communication. Its representative applications include quantum identity authentication (QIA) and quantum message authentication (QMA). First, QIA ensures the legitimacy of the identity by verifying that the claimant possesses secret information [8, 9]. The key technological element for QIA is the use of time variant parameters to ensure timeliness or uniqueness. Since Dušek et al. proposed a QIA scheme in 1999 that combines the BB84 quantum key distribution with identity authentication [10], various QIA

© The Author(s) 2023. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

schemes have been proposed [11–21]. Second, QMA ensures the origin and integrity of the message by validating quantum message authentication code (QMAC) [8, 9]. QMA is performed using an encoded quantum message state called a quantum message authentication code (QMAC). Beginning with a proposal by Curty et al. in 2002 [22], various QMA scheme studies have been proposed [23–25]. Furthermore, QMA can be extended to quantum signatures with the addition of non-repudiation [26–32].

The above quantum authentication methods have successfully proposed a secure authentication process. However, most require complicated resources such as entangled states, CNOT operation, Bell state measurement (BSM), swap test, and multiple quantum transmissions [19, 33–42]. This paper proposes a key-controlled maximally mixed quantum state encryption (MMQSE) method for quantum authentication schemes. It enables the easy encryption and decryption of quantum states using pre-shared secret keys between users with single qubit preparation, unitary operation, single qubit measurement, and minimized quantum transmissions [21, 43]. We applied the key-controlled MMQSE method to design QIA and QMA schemes that are secure, convenient, and easy to implement. The proposed QIA uses cryptographic challenge-response protocols to prove its identity as a verifier without revealing the secret [9]. The proposed QIA and QMA schemes are practical because they require only a single operation on a single quantum state and a single measurement [44]. Moreover, QIA and QMA were efficiently performed with only two and one quantum transmissions, respectively. As Uhlmann's fidelity is a convenient analytical tool for quantifying the distance between quantum states, we analyzed the security of the proposed scheme by relating the integral ratio of Uhlmann's fidelity to the probability of successful eavesdropping. We proved the security of the proposed QIA scheme against impersonation and intercept-and-resend attacks. In addition, we proved the security of our QMA scheme by analyzing the message origin and the impossibility of forgery. Furthermore, we demonstrated the integral ratio of the Uhlmann's fidelity in a real quantum channel noise environment without eavesdropping and calculated the upper bound of the valid noise rate. We then used it to estimate the optimal number of authentication sequences.

The remainder of this paper is organized as follows. Section 2 introduces the primary concept of the key-controlled MMQSE method for the physical realization of quantum authentication. Section 3 proposes QIA schemes based on the key-controlled MMQSE method and analyzes their security. Section 4 proposes QMA schemes based on the key-controlled MMQSE method and analyzes their security. Finally, Sect. 5 analyzes the authentication efficiency for the noise and compares the proposed quantum authentication schemes with an existing scheme.

2 Key-controlled maximally mixed quantum state encryption

For quantum cryptography, we designed a key-controlled MMQSE method for the physical realization of quantum authentication. Additionally, using the proposed method, a legitimate user with a secret key can easily decrypt the quantum state, whereas an eavesdropper, who does not know the secret key, finds it difficult to decrypt a quantum state. The key-controlled MMQSE method comprises three phases: quantum state preparation, unitary operation, and quantum state measurement.

In the quantum state preparation phase, users pre-share a secret key and prepare an appropriate quantum state according to the secret key $\hat{k}_{AB}$; $\hat{k}_{AB} = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$

is the rotation axis of the single qubit rotation operator. θ and ϕ are the polar and azimuthal angles of the rotation axis in Bloch sphere, respectively; it is also represented as $\hat{k}_{AB} = (\theta, \phi)$ in this paper. Subsequently, we consider the arbitrary quantum state $|\Psi\rangle = \cos(\alpha/2)|0\rangle + e^{i\beta}\sin(\alpha/2)|1\rangle$, where α and β are the polar and azimuthal angles of quantum state $|\Psi\rangle$ in the Bloch sphere, respectively. In the key-controlled MMQSE method, quantum state $|\Psi(\alpha,\beta)\rangle$ has the following constraint depending on the secret key $\hat{k}_{AB}(\theta,\phi)$:

$$\left|\cos\left(\frac{\alpha}{2}\right)\cos\left(\frac{\theta}{2}\right) + e^{i(\phi-\beta)}\sin\left(\frac{\alpha}{2}\right)\sin\left(\frac{\theta}{2}\right)\right|^2 = \frac{1}{2}. \tag{1}$$

Second, for the unitary operation phase, consider an arbitrary unitary operator $U = e^{i\Phi}\mathcal{R}_{\hat{k}_{AB}}(\Theta)$, where Φ is the global phase and $\mathcal{R}_{\hat{k}_{AB}}(\Theta) = \cos(\Theta/2)I_2 + i\sin(\Theta/2)(\hat{k}_{AB}\cdot\overrightarrow{\sigma})$ is the rotation operator with rotation angle Θ, rotation axis $\hat{k}_{AB}$, and Pauli vector $\overrightarrow{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$. If $\Phi = 2m\pi$ (m: integer) and $\Theta = \pi/2$, the unitary operator U can be expressed as the rotation operator $V = \mathcal{R}_{\hat{k}_{AB}}(\pi/2)$. Consequently, using Eq. (1), the results of unitary operation for $|\Psi\rangle$ and $|\Psi\rangle_\perp$ becomes

$$\begin{aligned} |R\rangle &= V|\Psi\rangle = \mathcal{R}_{\hat{k}_{AB}}\left(\frac{\pi}{2}\right)|\Psi\rangle, \\ |L\rangle &= V|\Psi\rangle_\perp = \mathcal{R}_{\hat{k}_{AB}}\left(-\frac{\pi}{2}\right)|\Psi\rangle. \end{aligned} \tag{2}$$

The counterclockwise rotated quantum state $|R\rangle$ and the clockwise rotated quantum state $|L\rangle$ are orthogonal, because $|\Psi\rangle$ and $|\Psi\rangle_\perp = \sin(\alpha/2)|0\rangle - e^{i\beta}\cos(\alpha/2)|1\rangle$ are orthogonal. From the point of view of an eavesdropper, $|R\rangle$ and $|L\rangle$ are arbitrary quantum states, and $\hat{k}_{AB}(\theta,\phi)$ is an arbitrary rotation axis. Hence, the density matrix ρ_E for Eq. (2) becomes

$$\rho_E = \int_{\phi=0}^{2\pi}\int_{\theta=0}^{\pi}\Pr(\theta,\phi)\mathcal{R}_{\theta,\phi}\left(\frac{\pi}{2}\right)\rho\mathcal{R}^\dagger_{\theta,\phi}\left(\frac{\pi}{2}\right)d\theta\,d\phi = \frac{I}{2}, \tag{3}$$

where the probability density function $\Pr(\theta,\phi) = (\int_{\phi=0}^{2\pi}\int_{\theta=0}^{\pi} d\theta\,d\phi)^{-1} = (2\pi^2)^{-1}$ for a uniform distribution in the Bloch sphere; $\rho = \int_\beta\int_\alpha \Pr(\alpha,\beta)|\psi(\alpha,\beta)\rangle\langle\psi(\alpha,\beta)|\,d\alpha\,d\beta$ is an ensemble of pure states $|\psi(\alpha,\beta)\rangle$ with probability density function

$$\Pr(\alpha,\beta) = \left(\int_{\beta=0}^{2\pi}\int_{\alpha=0}^{\pi} d\alpha\,d\beta\right)^{-1} = \left(2\pi^2\right)^{-1}.$$

As shown in Eq. (3), the density matrix of the quantum state $|R\rangle$ or $|L\rangle$ is a maximally mixed state. Therefore, an eavesdropper who does not know the secret key cannot obtain any information from the quantum state of Eq. (2).

Finally, in the quantum state measurement phase, we consider a single qubit measurement $B = \lambda_R B_R + \lambda_L B_L = \lambda_R|R\rangle\langle R| + \lambda_L|L\rangle\langle L|$, that satisfies $B|R\rangle = \lambda_R|R\rangle$, $B|L\rangle = \lambda_L|L\rangle$, where λ_R and λ_L are eigenvalues of B. The measurement operator B should also satisfy the completeness relation $\sum_m B_m^\dagger B_m = I$, $(m = R, L)$. Then, $|R\rangle$ and $|L\rangle$ can be completely measured by B. Therefore, only legitimate users who know the secret key can obtain accurate measurement results. For example, in Fig. 1, the key-controlled $|\Psi\rangle$, $|R\rangle$, and $|L\rangle$ are represented geometrically in the Bloch sphere when the secret key is $\hat{k}_{AB} = (\pi/4, 0)$. The orange

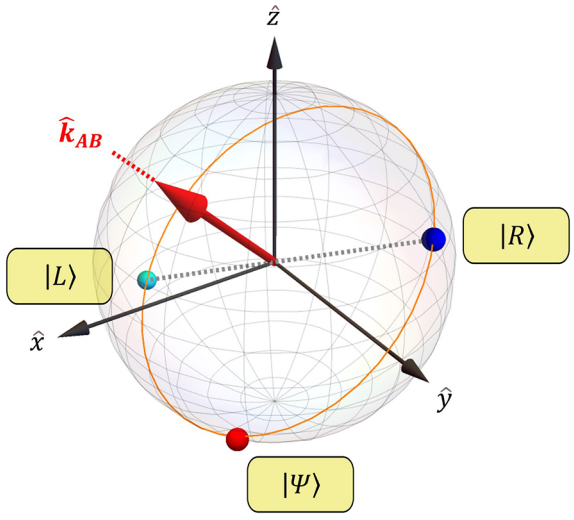

Figure 1 Geometric representation of the key-controlled $|\Psi\rangle$, $|R\rangle$, and $|L\rangle$ in the Bloch sphere. The red arrow represents the secret key $\hat{k}_{AB} = (\pi/4, 0)$ and the red sphere represents a specific $|\Psi\rangle$ among all possible points represented by the orange solid line. The blue and cyan spheres represent $|R\rangle$ and $|L\rangle$ generated by the rotation operator $\mathcal{R}_{\hat{k}_{AB}}$

solid line represents a specific $|\Psi\rangle$ satisfying Eq. (1). If $|\Psi\rangle$ is a red sphere on the orange solid line, $|R\rangle$ and $|L\rangle$ generated by the rotation operator $\mathcal{R}_{\hat{k}_{AB}}$ are represented by the blue and cyan spheres, respectively.

The key-controlled MMQSE method encrypts the single qubit $|\Psi\rangle$ generated in the quantum state preparation phase using the rotation operator V in the unitary operation phase and decrypts it using single qubit measurement B in the quantum state measurement phase. By applying the key-controlled MMQSE method to the quantum authentication schemes, legitimate users can easily encrypt and decrypt the quantum states, and eavesdropping is impossible. Specifically, it provides a security service of confidentiality that allows only legitimate users to encrypt and decrypt completely using the rotation axis corresponding to the secret key. In addition, from the user perspective, $|R\rangle$ and $|L\rangle$ in Eq. (2), encrypted using a fixed rotation angle $\pi/2$, are known quantum states perpendicular to each other. Therefore, they can be easily decrypted using the single qubit measurement. However, from the eavesdropper perspective, eavesdropping on quantum states is fundamentally difficult because $|R\rangle$ and $|L\rangle$ are maximally mixed states, as shown in Eq. (3). Therefore, we designed QIA and QMA schemes that are feasible and efficient for implementation based on single qubit, single qubit rotation operator, and single qubit measurement using the proposed method. This process is described in detail in the following sections.

3 Quantum identity authentication scheme based on the key-controlled MMQSE method

3.1 Quantum identity authentication scheme

The schematic representation of QIA based on the key-controlled MMQSE method is given in Fig. 2. Verifier Bob confirms the legitimacy of the claimant Alice and the existence of an illegal third party. The scheme consists of three phases: preparation, identity authentication, and verification.

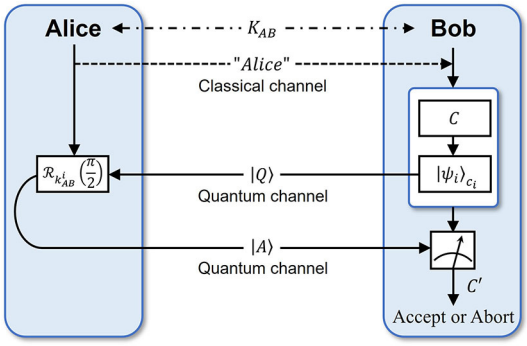

Figure 2 Schematic representation of QIA. When Alice requests authentication, Bob generates a challenge qubit and sends it to Alice. Alice then generates a legitimate response qubit and sends it to Bob to complete the identity authentication process

3.1.1 Preparation phase

Alice and Bob pre-share the secret key sequence $K_{AB} = (k_{AB}^1, k_{AB}^2, \ldots, k_{AB}^i, \ldots, k_{AB}^N)$, where $k_{AB}^i \in \{\hat{n}_1, \hat{n}_2, \ldots, \hat{n}_j, \ldots, \hat{n}_O\}$, N is the number of authentication sequences, O is the number of rotation axes, and $\hat{n}_j = (\sin\theta_j \cos\phi_j, \sin\theta_j \sin\phi_j, \cos\theta_j)$ is the rotation axis of the single qubit rotation operator. θ_j and ϕ_j are the polar and azimuthal angles of the rotation axis, respectively, also represented as $\hat{n}_j = (\theta_j, \phi_j)$ in this study. The size of the secret key is $|k_{AB}^i| = \log_2 O$ and that of the secret key sequence is $|K_{AB}| = N \log_2 O$. K_{AB} determines the rotation axis of the rotation operators and generates the challenge qubits. Subscripts A and B represent Alice and Bob, respectively. Once Alice requests authentication, Bob randomly generates classical bits $C = (c_1 \| c_2 \| \cdots \| c_i \| \cdots \| c_N)$, where $c_i \in \{0, 1\}$. Subsequently, Bob generates a sequence of N challenge qubits $|Q\rangle = \bigotimes_{i=1}^N |Q\rangle_i = \bigotimes_{i=1}^N |\psi_i\rangle_{c_i}$, where authentication qubit $|\psi_i\rangle = \cos(\alpha_i/2)|0\rangle + e^{i\beta_i} \sin(\alpha_i/2)|1\rangle$. If c_i =0, then $|\psi_i\rangle_0 = |\psi_i\rangle$; else, $|\psi_i\rangle_1 = |\psi_i\rangle_\perp$. Here, the pairs of angles (α_i, β_i) and (θ_j, ϕ_j) satisfy the condition of Eq. (1). At this point, $|Q\rangle_i$ can be considered a time-variant parameter used to ensure the uniqueness or timeliness of the QIA scheme.

3.1.2 Identity authentication phase

Bob sends $|Q\rangle$ to Alice. Subsequently, Alice generates a sequence of N response qubits $|A\rangle = \bigotimes_{i=1}^N |A\rangle_i$, $|A\rangle_i \in \{|R\rangle_i, |L\rangle_i\}$ to send to Bob by applying the single qubit rotation operators $\mathcal{R}_{k_{AB}^i}(\pi/2)$ to $|Q\rangle_i$ as $|R\rangle_i = \mathcal{R}_{k_{AB}^i}(\pi/2)|\psi_i\rangle$ or $|L\rangle_i = \mathcal{R}_{k_{AB}^i}(\pi/2)|\psi_i\rangle_\perp = \mathcal{R}_{k_{AB}^i}(-\pi/2)|\psi_i\rangle$, where $|R\rangle_i$ and $|L\rangle_i$ are orthogonal.

3.1.3 Verification authentication phase

Bob performs the single qubit measurement on $|A\rangle$ using measurement operator $B = |R\rangle_{ii}\langle R| - |L\rangle_{ii}\langle L|$; for convenience, λ_R is 1 and λ_L is −1. Because only Bob has a secret key and time-varying parameter, he can obtain the measurement outcome $C' = (c_1' \| c_2' \| \cdots \| c_i' \| \cdots \| c_N')$. If Bob's measurement outcome is $|R\rangle_i$, $c_i' = 0$; else if the measurement outcome is $|L\rangle_i$, $c_i' = 1$. Finally, Bob compares C and C' to confirm Alice's identity. If $C = C'$, Alice's identity is successfully authenticated. Otherwise, Bob aborts the identity authentication process.

3.2 Security analysis

Suppose Eve (eavesdropper) is intended to pass the verification process without being detected or obtain the secret key information. Eve can eavesdrop, pretending to be claimant Alice (impersonation attack) or intercept information in the middle of the quantum channel (intercept-and-resend attack).

First, we analyze Eve's impersonation attack to pass the verification process without being detected. We present a security analysis of the proposed QIA scheme using Uhlmann's fidelity. Fidelity is a measure of the distance between the quantum states [45]. Given two quantum states ρ and σ, the fidelity is defined to be $F(\rho,\sigma) \equiv \mathrm{tr}\sqrt{\rho^{1/2}\sigma\rho^{1/2}}$. Let $|\Psi\rangle$ and $|\Phi\rangle$ be any purification of ρ and σ, then the fidelity is the maximum value of $|\langle\Psi|\Phi\rangle|$ for any purification $|\Psi\rangle$ and $|\Phi\rangle$ using Uhlmann's theorem: $F(\rho,\sigma) = \max_{|\Psi\rangle,|\Phi\rangle} |\langle\Psi|\Phi\rangle|$. Assuming that both $\rho = |\psi\rangle\langle\psi|$ and $\sigma = |\phi\rangle\langle\phi|$ are pure state, the fidelity is represented as $F(\rho,\sigma) = |\langle\psi|\phi\rangle|$. If $|\psi\rangle$ and $|\phi\rangle$ are orthogonal, then fidelity is 0. If $|\psi\rangle$ and $|\phi\rangle$ are the same, then fidelity is 1. For Eve to pass the verification process, it is necessary to estimate the secret key K_{AB} or generate a legitimate response qubit $|A\rangle$. Most simply, Eve can estimate some secret key information by measuring the challenge qubit $|Q\rangle_i$ transmitted by Bob because the secret key information (θ_j,ϕ_j) imposes constraints on the challenge qubit information (α_i,β_i), as shown in Eq. (1). However, (θ_j,ϕ_j) is a function of (α_i,β_i), and even if Eve knows a specific (α_i,β_i), the secret key cannot be estimated because there are multiple combinations of (θ_j,ϕ_j) satisfying Eq. (1). Moreover, Eve does not know whether the qubit transmitted in the sequence is $|\psi\rangle$ or $|\psi\rangle_\perp$ by the time-varying parameters R, which only Bob knows. Therefore, quantum state measurement using the above method causes quantum state collapse. Eve cannot generate the correct quantum state to transmit to Bob based on the irreversibility of quantum state measurements and the no-cloning theory. Bob then knows of Eve's existence in the quantum channel and aborts the authentication process. Thus, Eve encodes the received challenge qubits using a self-generated arbitrary rotation operation as an optimized impersonation attack and transmits them to Bob. When $c_i = 0$ in the ith sequence, the fidelity between legitimate response qubit $|A\rangle_i = \mathcal{R}_{k_{AB}^i}(\pi/2)|\psi_i\rangle$ and response qubit estimated by Eve $|A_E\rangle_i = \mathcal{R}_{E^i}(\pi/2)|\psi_i\rangle$ is as follows:

$$F = \left|{}_i\langle A|A_E\rangle_i\right| = \left|\langle\psi_i|\mathcal{R}^\dagger_{k_{AB}^i}(\pi/2)\mathcal{R}_{E^i}(\pi/2)|\psi_i\rangle\right|. \tag{4}$$

Here, subscript E refers to Eve, and components of $E^i = (\theta_E,\phi_E)$ represent polar and azimuthal angles, respectively. Eve randomly selects the rotation axis E^i to generate $|A_E\rangle_i$. Since challenge qubits $|\psi_i\rangle$ are randomly selected by Bob to follow Eq. (1), the average fidelity for all possible challenge qubits is as given in Fig. 3.

As shown in Fig. 3, when $|A\rangle_i = \mathcal{R}_{k_{AB}^i}(\pi/2)|\psi_i\rangle$ and $|A_E\rangle_i = \mathcal{R}_{E^i}(\pi/2)|\psi_i\rangle$ are orthogonal, the fidelity is zero. Then, the estimated E^i is orthogonal to $k_{AB}^i = (\pi/4,0)$. In addition, the closer they are to each other, the closer their fidelity is to 1, implying that E^i and k_{AB}^i have the same components. If fidelity is 0, that is $E^i = (3\pi/4,\pi)$, then Eve fails to pass the verification process. Therefore, as the integral ratio of the average fidelity approaches 1, the QIA scheme cannot guarantee security against Eve's impersonation attack. In Fig. 3, the integral ratio of the average fidelity for all E^i values that Eve can select is 0.6555. As the number of authentication sequence N increases, integral ratio of the average fidelity gradually approaches 0, as shown in Fig. 4. Specifically, when N is 2, 5, 10, and 20, the integral ratio of the average fidelity is 0.5000, 0.3073, 0.1979, and 0.1229, respectively. When

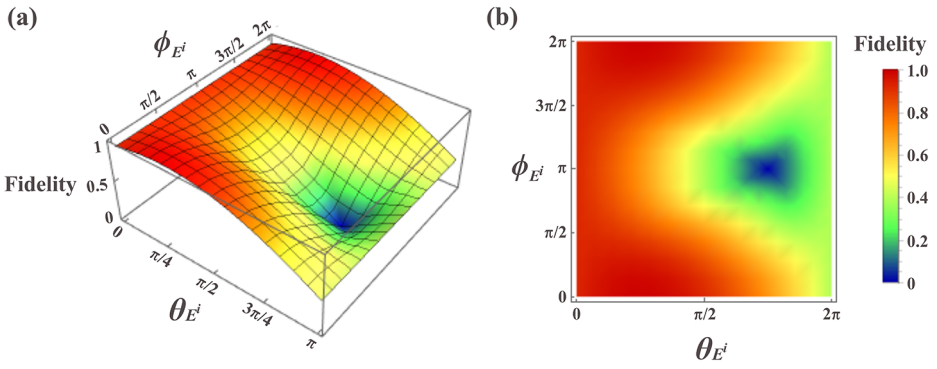

Figure 3 Average Uhlmann's fidelity between legitimate response qubit $|A\rangle_i = \mathcal{R}_{k_{AB}^i}(\pi/2)|\psi_i\rangle$ and response qubit estimated by Eve $|A_E\rangle_i = \mathcal{R}_{E^i}(\pi/2)|\psi_i\rangle$ on (a) 3D and (b) 2D contour plot, where $k_{AB}^i = (\pi/4, 0)$. θ_{E^i} and ϕ_{E^i} are the polar and azimuthal angles of the secret key E^i estimated by Eve, respectively

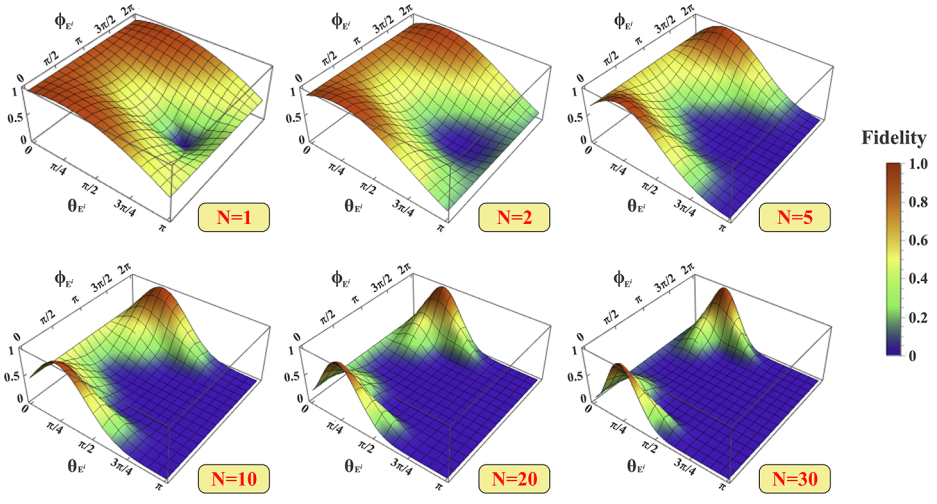

Figure 4 Average fidelity when the number of identity authentication sequences N is 1, 2, 5, 10, 20, and 30 on 3D; the integral ratio in this plot is 0.6555, 0.5000, 0.3073, 0.1979, 0.1229, and 0.0920, respectively

N increases to 30, the ratio becomes 0.0920. Therefore, as N increases, Eve cannot pass the verification process, and the proposed QIA scheme ensures security against impersonation attacks.

Next, we analyzed the security of the secret key of the proposed QIA scheme by analyzing Eve's intercept-and-resend attack to obtain secret key information. Similar to the impersonation attack, Eve cannot estimate the exact secret key information by measuring the challenge qubits from Bob. Therefore, Eve attempts to estimate the secret key while intercepting Alice and Bob. Eve first stores the challenge qubit $|Q\rangle$ sent by Bob and then transmits $|0\rangle$ to Alice to extract the secret key information. Subsequently, Eve applies the unitary operator corresponding to the secret key estimated by Alice's response qubit $|A'\rangle_i = \mathcal{R}_{k_{AB}^i}(\pi/2)|0\rangle$ to the stored challenge qubit. Thus, Eve can obtain fidelity between $|0\rangle$ state and $|A'\rangle_i$ with secret key information: $F = |\langle 0|A'\rangle_i| = |\langle 0|\mathcal{R}_{k_{AB}^i}(\pi/2)|0\rangle| = |1 - i\cos\theta_j|/\sqrt{2}$. Assuming that the same secret key is used for each sequence, θ_j seems to be known, but the key is different for each sequence. Furthermore, the polar angle θ_j of

the secret key can be estimated, but not the azimuth angle ϕ_j. When $c_i = 0$, the probability of estimating the exact secret key is related to fidelity as follows:

$$\begin{aligned}
\frac{\int F\,dv}{\int dv} &= \frac{1}{4\pi}\iint_{\theta_{E^i},\phi_{E^i}} \left|\langle\psi_i|\mathcal{R}_{k^i_{AB}}(\pi/2)\mathcal{R}_{E^i}(\pi/2)|\psi_i\rangle\right| \sin\theta_{E^i}\,d\theta_{E^i}\,d\phi_{E^i} \\
&= \frac{1}{4\pi}\iint_{\theta_{E^i},\phi_{E^i}} \sqrt{\left|\langle\psi_i|\mathcal{R}_{E^i}(\pi/2)\mathcal{R}_{k^i_{AB}}(\pi/2)|\psi_i\rangle\right|\left|\langle\psi_i|\mathcal{R}_{k^i_{AB}}(\pi/2)\mathcal{R}_{E^i}(\pi/2)|\psi_i\rangle\right|} \\
&\quad \times \sin\theta_{E^i}\,d\theta_{E^i}\,d\phi_{E^i} \\
&= \frac{1}{4\pi}\iint_{\theta_{E^i},\phi_{E^i}} \sqrt{\left|{}_i\langle R_E|R\rangle\langle R|R_E\rangle_i\right|} \sin\theta_{E^i}\,d\theta_{E^i}\,d\phi_{E^i} \\
&= \frac{1}{4\pi}\iint_{\theta_{E^i},\phi_{E^i}} \sqrt{\left|{}_i\langle R_E|B_R^\dagger B_R|R_E\rangle_i\right|} \sin\theta_{E^i}\,d\theta_{E^i}\,d\phi_{E^i} \\
&= \frac{1}{4\pi}\iint_{\theta_{E^i},\phi_{E^i}} \sqrt{p_R(\theta_{E^i},\phi_{E^i})} \sin\theta_{E^i}\,d\theta_{E^i}\,d\phi_{E^i} \\
&= \sqrt{P_R}. \qquad (5)
\end{aligned}$$

Here, $|R_E\rangle_i = \mathcal{R}_{E^i}(\pi/2)|\psi_i\rangle$ is estimated by Eve. If the state in the verification phase is $|R_E\rangle_i$ before measurement, then the probability that the result $|R\rangle_i$ occurs is P_R for all possible secret key information estimated by Eve; $p_R(\theta_{E^i},\phi_{E^i})$ is the probability of estimating the exact secret key at a specific value $(\theta_{E^i},\phi_{E^i})$, where $0 \le \theta_{E^i} \le \pi$, and $0 \le \phi_{E^i} < 2\pi$. Therefore, for all secret keys E^i estimated by Eve, the square of the probability that the result is $|R\rangle_i$ is the integral ratio of fidelity. The probability that Eve succeeds in the intercept-and-resend attack can be calculated as the integral ratio of fidelity: $(\int F\,dv/\int dv)^2$. As the authentication sequence N is performed several times, the probability of Eve's success decreases, $(\int F\,dv/\int dv)^{2N}$. Thus, the probability of Eve being detected is

$$P_{\text{fail}} = 1 - (P_R)^N = 1 - \left(\int F\,dv/\int dv\right)^{2N}. \qquad (6)$$

As shown in Fig. 5, when N is 17, $P_{\text{fail}} = 0.999999$; hence, the probability of Eve being detected is $P_{\text{fail}} \approx 1$.

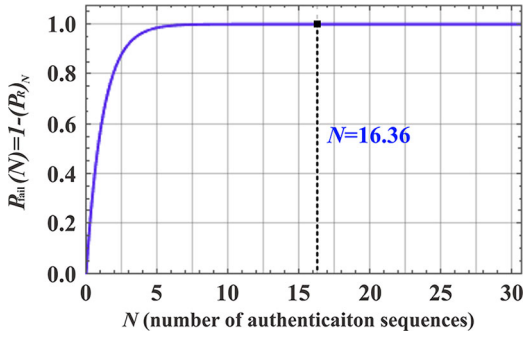

Figure 5 Probability P_{fail} of Eve being detected increases as the number of authentication sequence N increases. If $N \ge 16.36$, $P_{\text{fail}} \ge 0.999999$ is satisfied

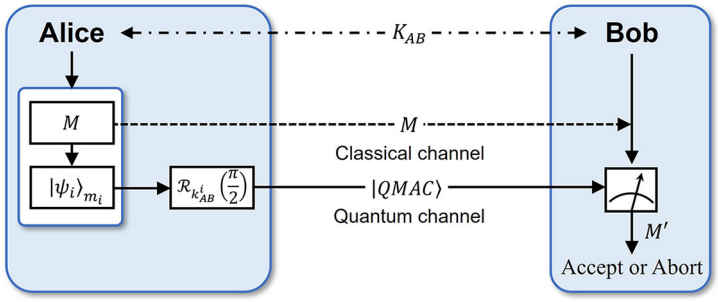

Figure 6 Schematic representation of QMA. Alice generates a QMAC corresponding to the message and sends them to Bob. Bob verifies the QMAC using the message to complete the message authentication process

4 Quantum message authentication scheme based on the key-controlled MMQSE method

4.1 Quantum message authentication scheme

The schematic representation of QMA using the key-controlled MMQSE method is given in Fig. 6. In the QMA scheme, verifier Bob confirms the integrity of the message and authenticates the origin of the message from sender Alice. The proposed QMA scheme consists of three phases: preparation, message authentication, and verification.

4.1.1 Preparation phase

Alice and Bob pre-share the secret key K_{AB} as in the proposed QIA scheme. Then, Alice generates the message $M = (m_1 \| m_2 \| \cdots \| m_i \| \cdots \| m_N)$, where $m_i \in \{0, 1\}$. Subsequently, Alice generates the initial quantum state $\bigotimes_{i=1}^{N} |\psi_i\rangle_{m_i}$, where $|\psi_i\rangle = \cos(\alpha_i/2)|0\rangle + e^{i\beta_i}\sin(\alpha_i/2)|1\rangle$. If m_i =0, then $|\psi_i\rangle_0 = |\psi_i\rangle$; else $|\psi_i\rangle_1 = |\psi_i\rangle_\perp$, where $|\psi_i\rangle_\perp$ is orthogonal to $|\psi_i\rangle$. As in the QIA schemes, the pair of angles (α_i, β_i) and secret key angles (θ_j, ϕ_j) satisfy the condition of Eq. (1). Furthermore, with specific values $\alpha_i = 2\arctan(\sin\theta_j + \sqrt{1 + \sin^2\theta_j})$ and $\beta_i = \phi_j + \theta_j$, the quantum states are completely dependent on the secret key information.

4.1.2 Message authentication phase

Alice generates a sequence of N QMAC, $|\text{QMAC}\rangle = \bigotimes_{i=1}^{N} |\text{QMAC}\rangle_i$, by applying the single qubit rotation operator $\mathcal{R}_{k_{AB}^i}(\pi/2)$ to the initial quantum states as $|\text{QMAC}\rangle_i = \mathcal{R}_{k_{AB}^i}(\pi/2)|\psi_i\rangle_{m_i}$. If $m_i = 0$, $|\text{QMAC}\rangle_i = |R\rangle_i = \mathcal{R}_{k_{AB}^i}(\pi/2)|\psi_i\rangle$ else $|\text{QMAC}\rangle_i = |L\rangle_i = \mathcal{R}_{k_{AB}^i}(\pi/2)|\psi_i\rangle_\perp = \mathcal{R}_{k_{AB}^i}(-\pi/2)|\psi_i\rangle$. $|R\rangle_i$ and $|L\rangle_i$ are orthogonal. Subsequently, Alice transmits M and $|\text{QMAC}\rangle$ to Bob.

4.1.3 Verification phase

Bob performs a single qubit measurement to $|\text{QMAC}\rangle$ using the measurement operator $B = |R\rangle_{ii}\langle R| - |L\rangle_{ii}\langle L|$. Because Bob has the secret key K_{AB}, he can obtain the measurement outcome M'. If Bob's measurement outcome is $|R\rangle_i$, $m_i' = 0$. However, if the measurement outcome is $|L\rangle_i$, $m_i' = 1$. Finally, Bob verifies Alice's message by comparing M and M'. If $M = M'$, the message M is authenticated; else, Bob aborts the message authentication process.

4.2 Security analysis

In the proposed QMA scheme, Eve intends to disturb the message origin authentication and contaminates the message integrity without being detected. Thus, Eve causes confusion about the origin of the message by generating a quantum message that only legitimate users can create (security of the message origin). Alternatively, Eve forgeries the message to induce incorrect message delivery (impossibility of forgery).

First, we analyze the security of the message origin, in which Eve generates illegal quantum messages to cause confusion about the origin of the message, and show a security analysis of the proposed QMA scheme using fidelity. Eve attempts to cause confusion about the message origin using arbitrary classical messages $M_E = (m_{E^1} \| m_{E^2} \| \cdots \| m_{E^i} \| \cdots \| m_{E^N})$, where $m_{E^i} \in \{0,1\}$, and QMAC $|\mathrm{QMAC_E}\rangle = \bigotimes_{i=1}^{N} \mathcal{R}_{E^i}(\pi/2)|\psi_{E^i}\rangle_{m_{E^i}}$ pairs because only legitimate users know the secret key. When $m_{E^i} = 0$ in the ith sequence, the fidelity between legitimate quantum message $|\mathrm{QMAC}\rangle_i = \mathcal{R}_{k_{AB}^i}(\pi/2)|\psi_i\rangle$ and Eve's quantum message $|\mathrm{QMAC_E}\rangle_i = \mathcal{R}_{E^i}(\pi/2)|\psi_{E^i}\rangle$ is as follows:

$$F = \left|{}_i\langle \mathrm{QMAC}|\mathrm{QMAC_E}\rangle_i\right| = \left|\langle\psi_i|\mathcal{R}^{\dagger}_{k_{AB}^i}(\pi/2)\mathcal{R}_{E^i}(\pi/2)|\psi_{E^i}\rangle\right|. \tag{7}$$

Eve generates the initial quantum state $|\psi_{E^i}\rangle = \cos(\alpha_{E^i}/2)|0\rangle + e^{i\beta_{E^i}}\sin(\alpha_{E^i}/2)|1\rangle$ with specific value $\alpha_{E^i} = 2\arctan(\sin\theta_{E^i} + \sqrt{1+\sin^2\theta_{E^i}})$ and $\beta_{E^i} = \phi_{E^i} + \theta_{E^i}$ using secret key information $E^i = (\theta_{E^i}, \phi_{E^i})$ estimated by Eve. Therefore, Eve's initial quantum states are completely dependent on the $E^i = (\theta_{E^i}, \phi_{E^i})$. The fidelity of QMAC is shown in Fig. 7.

When $m_i = 0$, i.e., $|\mathrm{QMAC}\rangle_i = |R\rangle_i$, the range of the polar angle of the $|\mathrm{QMAC}\rangle_i$ is from $\pi/4$ to $\pi/2$. However, since there is no E^i where $|\mathrm{QMAC_E}\rangle_i$ is orthogonal to $|\mathrm{QMAC}\rangle_i$ corresponding to $k_{AB}^i = (\pi/4, 0)$, the fidelity cannot be 0 in Fig. 7. If $E^i = (\pi/4, 0)$ and k_{AB}^i are the same, then the fidelity is 1. In Fig. 7, even if E^i is different from the actual secret key, the fidelity can be 1 when $|\mathrm{QMAC_E}\rangle_i = |\mathrm{QMAC}\rangle_i$. However, Eve's probability of manipulating and selecting such a scenario is almost 0. Therefore, assuming that Eve knows the classical message m_i that Alice wants to send, the fidelity integral ratio for all E^i that Eve can select is 0.7517. As in QIA, as the number of authentication sequence N increases, the quantum message is represented by the product state $|\mathrm{QMAC_E}\rangle = \bigotimes_{i=1}^{N}|\mathrm{QMAC_E}\rangle_i = \bigotimes_{i=1}^{N}\mathcal{R}_{E^i}(\pi/2)|\psi_{E^i}\rangle$, and the fidelity integral ratio gradu-

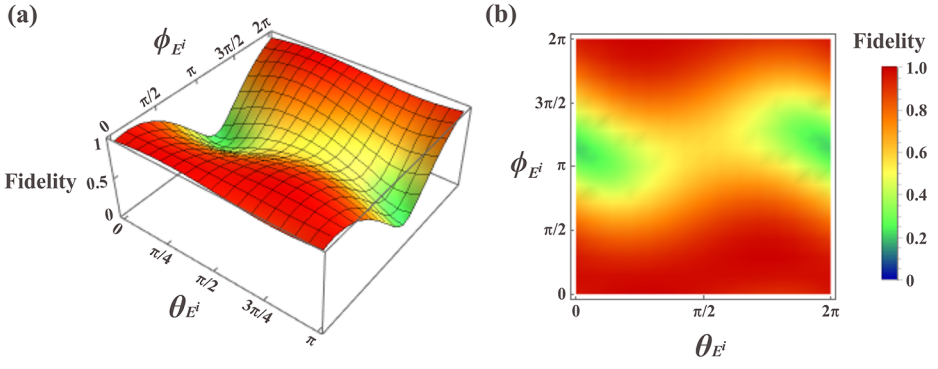

Figure 7 Fidelity between legitimate QMAC $|\mathrm{QMAC}\rangle_i = \mathcal{R}_{k_{AB}^i}(\pi/2)|\psi_i\rangle$ and Eve's QMAC $|\mathrm{QMAC_E}\rangle_i = \mathcal{R}_{E^i}(\pi/2)|\psi_{E^i}\rangle$ on (a) 3D, and (b) 2D contour plot. θ_{E^i} and ϕ_{E^i} are the polar and azimuthal angles of the secret key E^i estimated by Eve, respectively

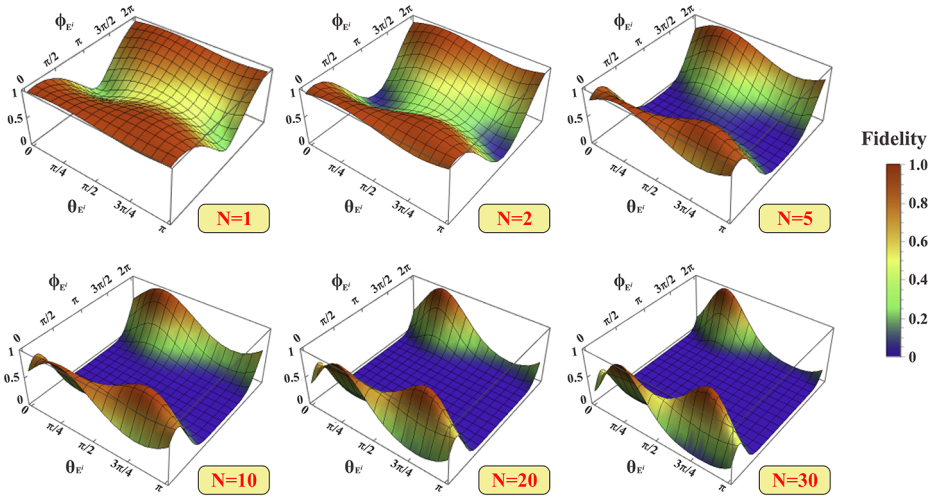

Figure 8 Fidelity when the number of message authentication sequences N is 1, 2, 5, 10, 20, and 30 on 3D; the integral ratio in this plot is 0.7517, 0.6020, 0.3895, 0.2641, 0.1730, and 0.1314, respectively

ally approaches zero, as shown in Fig. 8. Specifically, when N is 2, 5, 10, and 20, the fidelity integral ratio is 0.6020, 0.3895, 0.2641, and 0.1730, respectively. When N increases to 30, the fidelity integral ratio becomes 0.1314. Therefore, as N increases, Eve cannot send the intended message and is not authenticated as the legitimate user Alice. Thus, the proposed QMA scheme ensures the security of the message origin.

Next, we analyze the security of the proposed QMA scheme using Eve's forgery strategy that attempts to violate the integrity of the message and QMAC pair. Eve's purpose is to forge the message and QMAC pair owned by Alice to pass the verification process undetected. Eve flips the bit of message M, and applies an arbitrary unitary operator U_{E^i} to $|\text{QMAC}\rangle_i$. The forged QMAC $|\text{QMAC}_E\rangle_i$ in which Eve applies U_{E^i} to $|\text{QMAC}\rangle_i$ is as follows:

$$\begin{aligned} |\text{QMAC}_E\rangle_i &= U_{E^i}|\text{QMAC}\rangle_i \\ &= U_{E^i}\mathcal{R}_{k_{AB}^i}(\pi/2)|\psi_i\rangle. \end{aligned} \tag{8}$$

Eve performs message authentication using the forged message M_E and QMAC $|\text{QMAC}_E\rangle_i$. For example, we consider the case of rotation axis $k_{AB}^i = (0,0)$ and initial quantum state $|\psi_i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Then, $|\text{QMAC}\rangle_i \in \{|R\rangle_i, |L\rangle_i\}$ that Alice transmits to Bob is as follows:

$$|\text{QMAC}\rangle_i = \begin{cases} |R\rangle_i = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \\ |L\rangle_i = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle). \end{cases} \tag{9}$$

Eve flips the message bit and applies the unitary operator $U_{E^i} = \mathcal{R}_{\hat{Z}}(\pi)$ to $|\text{QMAC}\rangle_i$ for the forgery sequence. If $m_i = 0$, Eve forges message bit to $m_{E^i} = 1$ and $|\text{QMAC}\rangle_i$ to $|\text{QMAC}_E\rangle_i = \mathcal{R}_{\hat{Z}}(\pi)|R\rangle_i = |L_E\rangle_i$. Figure 9 presents Eve's forgery for message and QMAC pair using $U_{E^i} = \mathcal{R}_{\hat{Z}}(\pi)$ when the secret key is $k_{AB}^i = (0,0)$.

For Eve to succeed in forgery, $E^i = k_{AB}^i$ must be satisfied. We consider a universal quantum NOT gate (U-NOT) that evolves any arbitrary quantum state $|\psi\rangle$ into $|\psi\rangle_\perp$. If Eve

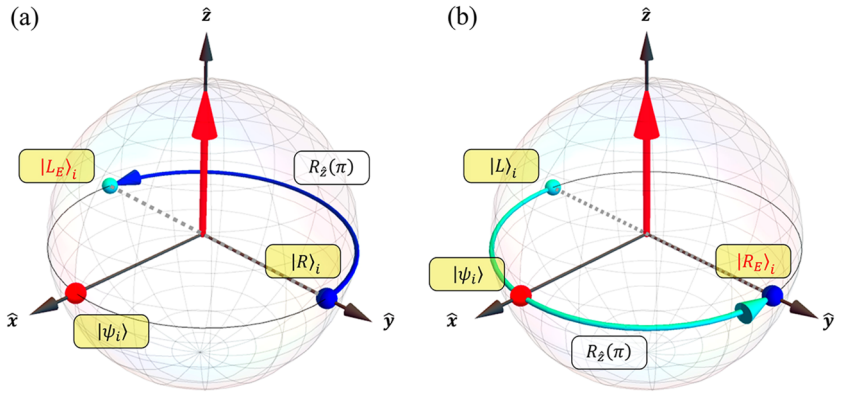

Figure 9 Eve's forged message and QMAC pair using $U_{E^i} = \mathcal{R}_{\hat{Z}}(\pi)$ when the secret key is $k^i_{AB} = (0,0)$. (a) Eve forges QMAC $|R\rangle_i$ to $|L_E\rangle_i$ when $m_i = 0$. (b) Eve forge QMAC $|L\rangle_i$ to $|R_E\rangle_i$ when $m_i = 1$

flips the message bit and performs U-NOT instead of U_{E^i} in Eq. (8), in forgery for any rotation axis k^i_{AB} will be successful. However, being an antiunitary operator, the U-NOT gate can only partially be implemented [46–48]. If Eve attempts forgery using a gate approximated to the U-NOT gate, the probability of evolving $|\psi\rangle$ into $|\psi\rangle_\perp$ is 2/3. Thus, the probability of Eve being detected is

$$P_{\text{fail}} = 1 - (2/3)^N. \tag{10}$$

As shown in Eq. (10), when N is 14, P_{fail} reaches 0.999999, indicating that the probability of Eve being detected is approximately 1. Therefore, in practice, Eve's forgery of messages and QMAC pairs are impossible.

5 Performance

This section compares the proposed quantum authentication schemes with previously proposed schemes. Subsequently, we demonstrate that the proposed schemes are robust to noise through several important noise cases. In addition, we calculated the point where the probability of Eve being detected and the probability of success in a secure authentication process in a noisy environment are optimal for the number of sequences.

5.1 Comparison

We compared the proposed quantum authentication schemes with previously proposed schemes. Most previously proposed schemes were designed without considering the feasibility of implementing factors such as quantum sources, quantum operations, quantum measurements, and the number of quantum transmissions. First, quantum authentication schemes based on entangled states, such as the Bell or GHZ states, are difficult to generate and maintain [34–36]. It is difficult to generate and maintain high quality entangled states using spontaneous parametric down-conversion [49–51]. Second, most methods implement quantum operations, such as the controlled operation of two or more qubits, probabilistically [37–39]. Even the antiunitary operations are practically impossible to implement [46–48]. Third, quantum measurements, such as the swap test and BSM, cannot be completely implemented using linear optics [40–42, 52]. The swap test is only probabilistically implemented, and the BSM based on linear optics cannot measure the Bell state

Table 1 Comparison between the proposed and existing QIA schemes

	CMQIA [16]	QIA [21]	DSQC QIA [17]	Our scheme
Method	Password	Challenge-response	Password	Challenge-response
Quantum source	2N GHZ-like states	2N single qubits	2N Bell states	N single qubits
Quantum operation	N Pauli operation	4N single rotation operation	N CNOT operation, 2N Pauli operation	N single rotation operation
Measurement	2N single qubit measurement, 2N Bell state measurement	N swap test	N single qubit measurement, 2N Bell state measurement	N single qubit measurement
Number of quantum transmission	4N times	4N times	2N times	2N times
Decoy state	O	O	O	X

Table 2 Comparison between the proposed and existing QMA schemes

	QMA [22]	QR QMA [23]	QMA [25]	Our scheme
Quantum source	2N single qubits, N Bell states	N single qubits	2N single qubits	N single qubits
Quantum operation	2N single unitary operation	2N controlled operation, N/2 swap operation	4N single rotation operation, 2N single Pauli operation	N single rotation operation
Measurement	N single qubit measurement	N single qubit measurement	N swap test	N single qubit measurement
Number of quantum transmission	N times	N times	3N times	N times
Decoy state	△	O	X	X

△: Not used, but required to verify the security of quantum channels

$|\Phi^{\pm}\rangle$. Finally, noise on the quantum channel reduces the efficiency of quantum authentication schemes as the number of quantum transmissions increases. Conversely, because our QIA and QMA schemes are based on the key-controlled MMQSE method, they are feasible and efficient for implementation. In the proposed method, the single qubits and single qubit measurement corresponding to the secret key facilitate the quantum state preparation and measurement process. Single qubit rotation operators for encryption are simpler to implement than multi qubit or antiunitary operations. Moreover, our schemes are robust to noise because the number of quantum transmissions is less [44], and highly efficient because the sequences used as decoy qubits can also be used as authentication qubits [21, 43]. Decoy qubits added for protocol security are difficult to implement in practice, and no research has been published on their implementation to date. Tables 1 and 2 compare the quantum sources, quantum operations, quantum measurements, and the number of quantum transmissions between the proposed and conventional quantum authentication schemes.

In Table 1, our QIA scheme uses N single qubits as the quantum source, compared to the control mutual quantum entity authentication scheme using 2N GHZ-like states proposed by Kang et al. in 2018 [16]. Our QIA scheme applies only N rotation operators and performs only 2N quantum transmissions, compared with the quantum identification scheme with many quantum operations and quantum transmissions proposed by Choi et al. in 2020 [21]. Our QIA scheme performs single qubit measurement instead of two or

more qubits measurement, such as the BSM used in the scheme proposed by Dutta et al. in 2022 [17]. In Table 2, compared with the simple QMA scheme proposed by Curty et al. in 2002 [22], our QMA scheme uses N single qubits. Finally, in Table 2, compared with the QMA schemes proposed by Bartkiewicz et al. in 2014 [23] and Kang et al. in 2021 [25], our QMA scheme has fewer operations and quantum transmissions and does not use the swap test.

5.2 Analysis of noise environment

The proposed schemes are robust to noise because the number of quantum transmissions is less than that of other schemes. Even without eavesdropping, we analyze the authentication efficiency for noises in the quantum channels using fidelity. There are several important examples of noise in a quantum channel: bit flip noise, phase flip noise, bit-phase flip noise, and depolarizing noise. In noisy environments, noise causes authentication errors even in the absence of eavesdroppers. The fidelity integral ratio without noise is 1. As noise increases gradually, the fidelity integral ratio decreases. However, when there was no noise and only eavesdropping in the channel, the fidelity integral ratios were 0.6555 and 0.7517 in QIA and QMA, respectively. Therefore, the valid upper bound for the bit flip noise rate (ϵ_b), phase flip noise rate (ϵ_p), bit-phase flip error rate (ϵ_{b+p}), and depolarizing noise rate (ϵ_d) is calculated for the security of the proposed schemes [45].

The simulation results in Fig. 10 indicate that QIA, which performs quantum transmission twice, is more affected by noise than QMA, which performs quantum transmission once. Figure 10(a) shows that in QIA, the integral ratio of the average fidelity decreases similarly for all noises but is slightly more sensitive to bit-phase flip noise, represented by red lines and dots. The upper bound of the valid noise rate not exceeding the integral ratio of the average fidelity 0.6555 when Eve eavesdrops is $\epsilon_b \leq 5.79\%$, $\epsilon_p \leq 5.79\%$, $\epsilon_{b+p} \leq 5.78\%$, and $\epsilon_d \leq 5.79\%$; the corresponding integral ratio of the average fidelity for each upper bound of the valid noise rate are 0.6556, 0.6557, 0.6557, and 0.6557, respectively. Figure 10(b) shows that in the QMA, the slope of the fidelity integral ratio decreases differently. The slope decreases more rapidly for bit flip noise than in others. This is because the polar angle range of the $|\text{QMAC}\rangle_i = |R\rangle_i$ state used in the simulation is set to $\pi/4 \sim \pi/2$; if bit flip noise occurs in the $|R\rangle_i$ state, the result is closer to the $|L\rangle_i$ state rather than $|R\rangle_i$ state unconditionally. Therefore, the probability that the fidelity is closer to zero increases and the integral ratio of fidelity decreases more rapidly. The upper bound of the

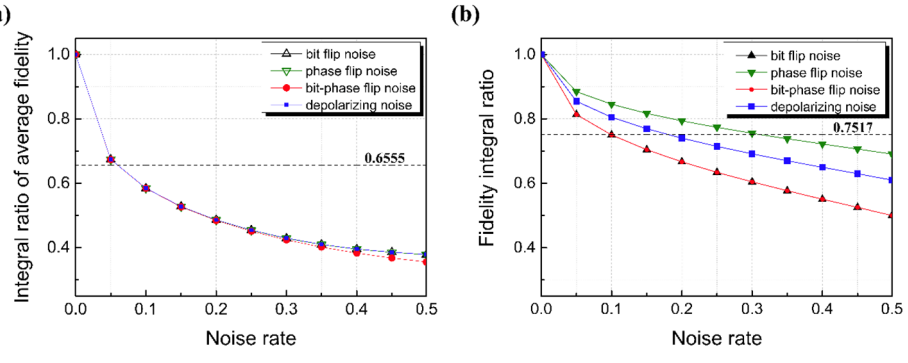

Figure 10 In the proposed QIA and QMA schemes (a) average fidelity integral ratio, and (b) fidelity integral ratio to noise rate

valid noise rate not exceeding the fidelity integral ratio of 0.7517 when Eve eavesdrops is $\epsilon_b \leq 9.83\%$, $\epsilon_p \leq 30.90\%$, $\epsilon_{b+p} \leq 9.83\%$, and $\epsilon_d \leq 17.90\%$; the corresponding fidelity integral ratios in each upper bound of the valid noise rate are 0.7518, 0.7521, 0.7518, and 0.7518.

If the noise rate of the quantum channel is higher than the upper bound of the valid noise rate, security of the proposed scheme cannot be guaranteed because it is impossible to determine whether the authentication error is due to noise in the quantum channel or eavesdropping by Eve. In addition, as the number of transmissions increases, the noise rate increases. This reduces the integral ratio of fidelity and increases authentication errors. Quantum authentication schemes with many transmissions are not robust to noise because the upper bound of the valid noise rate increases. Therefore, the proposed quantum authentication schemes are efficient and secure because they reduce the number of quantum transmissions.

Furthermore, we can also calculate the upper bound of the valid noise rate in various types of noisy environments. For example, if bit flip, phase flip, and bit-phase flip noise occur simultaneously with the different probabilities p_1, p_2, and p_3, respectively. Subsequently, the noise operator for two or more types of noise at the same time in the quantum channel can be expressed as follows:

$$E_{\text{mix}} = \sqrt{1-(p_1+p_2+p_3)}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} + \sqrt{p_1}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} + \sqrt{p_2}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} + \sqrt{p_3}\begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}. \tag{11}$$

In Eq. (11), depolarizing noise occurs when $p_1 = p_2 = p_3$. Using Eq. (11), QIA and QMA fidelity can be expressed with respect to the noise operator E_{mix}, and according to Eq. (5), the (average) fidelity integral ratio can be calculated. Finally, the upper bound of the valid noise ratio can also be expressed as a function of probabilities p_1, p_2, and p_3, after which it can be analyzed in a more straightforward manner.

In the proposed QIA scheme, when the number of authentication sequences $N = 17$, the probability of Eve being detected is $P_{\text{fail}} \approx 1$, i.e., a user can complete a secure authentication process against Eve. Therefore, even in a noisy environment, at least $N = 17$ authentication sequences must be performed for secure authentication. Similarly, in the QMA scheme, $N \geq 25$ must be applied. Quantitatively, the probability of success in a secure authentication process in a noisy environment is $P_{\text{QIA}|\epsilon}(N) = \sum_{r=0}^{1} {}_N C_r p^r (1-p)^{N-r}$ and $P_{\text{QMA}|\epsilon}(N) = \sum_{r=0}^{2} {}_N C_r p^r (1-p)^{N-r}$, which depends on the valid noise rate ϵ. r is the number of times noise occurring in the total sequence N and depends on the valid noise rate. In quantum cryptography systems, the quantum bit error rate is typically less than 3%, and depends on the system form, distance, and environment and is particularly affected by channel noise [53–56]. Therefore, we assume that the noise p of the quantum channel occurs at 3%. Specifically, in the QIA scheme, for the quantum states passing through the quantum channels to be robust to noise, noise should not occur more than twice in the 17 sequences. Therefore, even in noisy environments, the probability of success in a secure authentication process $P_{\text{QIA}|\epsilon}(N)$ is 90.91%. Similarly, in the QMA scheme, $P_{\text{QMA}|\epsilon}(N)$ is 96.20% when the number of authentication sequences N is 25. As the sequence increases, the quantum state is frequently exposed to noise. Thus, the probability

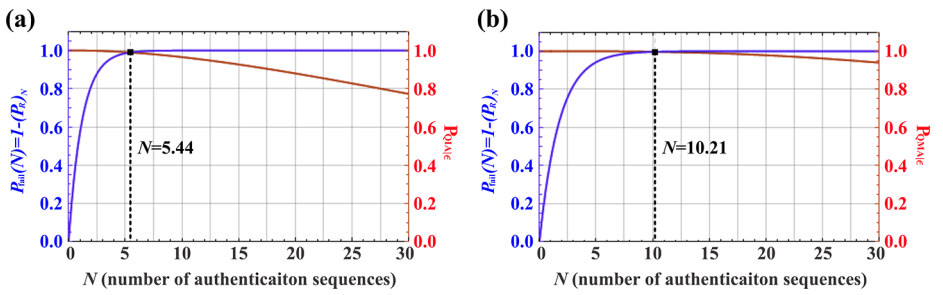

Figure 11 Optimal number of authentication sequences between the probability of Eve being detected $P_{\text{fail}}(N)$ and probability of success in a secure authentication process in a noise environment; $P_{\text{QIA}|\epsilon}(N) = \sum_{r=0}^{1} {}_N C_r p^r (1-p)^{N-r}$, $P_{\text{QMA}|\epsilon}(N) = \sum_{r=0}^{2} {}_N C_r p^r (1-p)^{N-r}$ (a) QIA and (b) QMA schemes

of success in a secure authentication process decreases. Figure 11 shows the optimal point between the probability of Eve being detected and the probability of success in a secure authentication process in a noisy environment for the number of authentication sequences. Therefore, the most optimal number of sequences is when $N = 6$ in QIA and $N = 11$ in QMA. Here, the probability of Eve being detected is $P_{\text{fail}}(N = 6) = 0.9937$ in the QIA and $P_{\text{fail}}(N = 11) = 0.9981$ in the QMA.

6 Conclusion

We propose a key-controlled MMQSE method that uses only a single qubit operation with remarkable advantages in terms of implementation. First, the rotation operator corresponding to single qubit operation can be easily implemented by combining half- and quarter-wave plates in linear optics. Second, because the rotation angle of the rotation operator is fixed, legitimate users possessing the secret key can easily decrypt it using only a single qubit measurement. Third, using a single qubit instead of an entangled state makes generating and maintaining quantum sources easy. We apply this to the QIA and QMA schemes and confirm the legitimacy of an identity or message by performing a single qubit operation. They provide unconditional security because of the arbitrary rotation axis corresponding to the pre-shared secret information. This implies that the security of a quantum channel can be verified without decoy qubits. Furthermore, our schemes are robust to noise because they perform fewer quantum transmissions in real quantum-channel noise environments.

We analyzed the security of the proposed quantum authentication scheme using Uhlmann's fidelity against various eavesdropper attacks. We demonstrated the relationship between the integral ratio of the Uhlmann's fidelity and the probability of successful eavesdropping. Using the QIA scheme, we proved the security of our scheme against impersonation and intercept-and-resend attacks. We estimate the probability of successful eavesdropping by Eve as the fidelity integral ratio and demonstrate that the probability of Eve being detected is almost 1 when the number of authentication sequences is 17. We prove the security of our QMA scheme by analyzing the message origin and the impossibility of forgery using the fidelity integral ratio. In addition, the probability of Eve forging the message and QMAC pair is almost zero when the number of authentication sequences is 14.

Subsequently, we show that our schemes improve efficiency compared to previously proposed schemes in terms of quantum sources, quantum operations, quantum measure-

ments, and quantum transmissions. The proposed schemes are robust to noise because the number of quantum transmissions required is less compared to other schemes. We demonstrate the integral ratio of the Uhlmann's fidelity to the noise rate in the proposed QIA and QMA schemes, even without eavesdropping. We also calculated the upper bound of the valid noise ratio, which did not exceed the fidelity integral ratio when Eve eavesdropped. In the QIA scheme, the upper bound of the valid noise is $\epsilon_b \leq 5.79\%$, $\epsilon_p \leq 5.79\%$, $\epsilon_{b+p} \leq 5.78\%$, and $\epsilon_d \leq 5.79\%$. In the QMA scheme, the upper bound of the valid noise rate is $\epsilon_b \leq 5.79\%$, $\epsilon_p \leq 5.79\%$, $\epsilon_{b+p} \leq 5.78\%$, and $\epsilon_d \leq 5.79\%$. Furthermore, the optimal number of sequences determined was $N = 6$ in QIA and $N = 11$ in QMA. Therefore, we demonstrated QIA and QMA schemes that are secure, convenient, and feasible using the key-controlled MMQSE method.

Acknowledgements
The authors would like to thank the editor and anonymous reviewers for their valuable suggestions.

Funding
This work was supported by the National Research Foundation of Korea (NRF) (2021M1A2A2043892, 2022M3K4A1097119), Institute for Information and Communications Technology Promotion (IITP) (2020-0-00890), the Commercializations Promotion Agency for R&D Outcomes (2022SCPO_B_0210), KREONET Advanced Research Program Grant from KISTI, and KIST research program (2E31531, 2E32801).

Availability of data and materials
The datasets used and analyzed during the current study are available from the corresponding author on reasonable request.

Declarations

Competing interests
The authors declare no competing interests.

Author contributions
S.-W.H. planned and supervised the research. N.-H.L. and J.-W.C. designed protocols. J.-W.C., M.-S.K., and H.-J.Y. analyzed the security of protocols; all authors contributed to analysis and discussion of the performances. N.-H.L., J.-W.C. and S.-W.H. wrote the manuscript with input from all authors.

Author details
[1]Center for Quantum Information, Korea Institute of Science and Technology (KIST), Seoul, 02792, Republic of Korea. [2]Division of Nano and Information Technology, Korea Institute of Science and Technology School, Korea University of Science and Technology, Seoul, 02792, Republic of Korea. [3]Korean Intellectual Property Office (KIPO), Government Complex Daejeon Building 4, 189, Cheongsa-ro, Seogu, Daejeon, 35208, Republic of Korea. [4]Department of Physics, Korea University, Sejong, 30019, Republic of Korea.

Received: 16 May 2023 Accepted: 1 September 2023 Published online: 13 September 2023

References

1. Shor PW, editor. Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th annual symposium on foundations of computer science. Los Alamitos: IEEE; 1994.
2. Shor PW. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Rev. 1999;41(2):303–32.
3. Arute F, Arya K, Babbush R, Bacon D, Bardin JC, Barends R et al. Quantum supremacy using a programmable superconducting processor. Nature. 2019;574(7779):505–10.
4. Bennett CH, Brassard G. Ekert AK. Quantum cryptography. Sci Am. 1992;267(4):50–7.
5. Lo H-K, Chau HF. Unconditional security of quantum key distribution over arbitrarily long distances. Science. 1999;283(5410):2050–6.
6. Shor PW, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. Phys Rev Lett. 2000;85(2):441.
7. Gisin N, Ribordy G, Tittel W, Zbinden H. Quantum cryptography. Rev Mod Phys. 2002;74(1):145.
8. Forouzan BA, Mukhopadhyay D. Cryptography and network security. New York: McGraw-Hill; 2015.
9. Menezes AJ, Van Oorschot PC, Vanstone SA. Handbook of applied cryptography. Boca Raton: CRC Press; 2018.
10. Dušek M, Haderka O, Hendrych M, Myška R. Quantum identification system. Phys Rev A. 1999;60(1):149.
11. Ljunggren D, Bourennane M, Karlsson A. Authority-based user authentication in quantum key distribution. Phys Rev A. 2000;62(2):022305.
12. Zeng G, Zhang W. Identity verification in quantum key distribution. Phys Rev A. 2000;61(2):022303.
13. Mihara T. Quantum identification schemes with entanglements. Phys Rev A. 2002;65(5):052326.

14. Zhang Z, Zeng G, Zhou N, Xiong J. Quantum identity authentication based on ping-pong technique for photons. Phys Lett A. 2006;356(3):199–205.
15. Yang Y-G, Wang H-Y, Jia X, Zhang H. A quantum protocol for (t, n)-threshold identity authentication based on Greenberger-Horne-Zeilinger states. Int J Theor Phys. 2013;52:524–30.
16. Kang M-S, Heo J, Hong C-H, Yang H-J, Han S-W, Moon S. Controlled mutual quantum entity authentication with an untrusted third party. Quantum Inf Process. 2018;17(7):1–15.
17. Dutta A, Pathak A. Controlled secure direct quantum communication inspired scheme for quantum identity authentication. Quantum Inf Process. 2022;22(1):13.
18. Chen G, Wang Y, Jian L, Zhou Y, Liu S. Quantum identity authentication based on the extension of quantum rotation. EPJ Quantum Technol. 2023;10(1):1.
19. Hong C, Heo J, Jang JG, Kwon D. Quantum identity authentication with single photon. Quantum Inf Process. 2017;16(10):236.
20. Zawadzki P. Quantum identity authentication without entanglement. Quantum Inf Process. 2019;18(1):1–12.
21. Choi J-W, Kang M-S, Heo J, Hong C, Yoon C-S, Han S-W et al. Quantum challenge-response identification using single qubit unitary operators. Phys Scr. 2020;95(10):105104.
22. Curty M, Santos DJ, Pérez E, García-Fernández P. Qubit authentication. Phys Rev A. 2002;66(2):022301.
23. Bartkiewicz K, Černoch A, Lemr K. Using quantum routers to implement quantum message authentication and Bell-state manipulation. Phys Rev A. 2014;90(2):022335.
24. Kang M-S, Choi Y-H, Kim Y-S, Cho Y-W, Lee S-Y, Han S-W et al. Quantum message authentication scheme based on remote state preparation. Phys Scr. 2018;93(11):115102.
25. Kang M-S, Kim Y-S, Choi J-W, Yang H-J, Han S-W. Experimental quantum message authentication with single qubit unitary operation. Appl Sci. 2021;11(6):2653.
26. Zeng G, Keitel CH. Arbitrated quantum-signature scheme. Phys Rev A. 2002;65(4):042312.
27. Li Q, Chan WH, Long D-Y. Arbitrated quantum signature scheme using Bell states. Phys Rev A. 2009;79(5):054307.
28. Zhang L, Sun H-W, Zhang K-J, Jia H-Y. An improved arbitrated quantum signature protocol based on the key-controlled chained CNOT encryption. Quantum Inf Process. 2017;16:1–15.
29. Hong C, Jang J, Heo J, Yang H-J. Quantum digital signature in a network. In: Quantum information processing. vol. 19. 2020. p. 1–21.
30. Yoon CS, Kang MS, Lim JI, Yang HJ. Quantum signature scheme based on a quantum search algorithm. Phys Scr. 2014;90(1):015103.
31. Kang M-S, Hong C-H, Heo J, Lim J-I, Yang H-J. Quantum signature scheme using a single qubit rotation operator. Int J Theor Phys. 2015;54:614–29.
32. Yoon CS, Hong CH, Kang MS, Choi J-W, Yang HJ. Quantum asymmetric key crypto scheme using Grover iteration. Sci Rep. 2023;13(1):3810.
33. Pirandola S, Andersen UL, Banchi L, Berta M, Bunandar D, Colbeck R et al. Advances in quantum cryptography. Adv Opt Photonics. 2020;12(4):1012–236.
34. Pan J-W, Chen Z-B, Lu C-Y, Weinfurter H, Zeilinger A, Żukowski M. Multiphoton entanglement and interferometry. Rev Mod Phys. 2012;84(2):777.
35. Wang X-L, Chen L-K, Li W, Huang H-L, Liu C, Chen C et al. Experimental ten-photon entanglement. Phys Rev Lett. 2016;117(21):210502.
36. Bozzio M, Vyvlecka M, Cosacchi M, Nawrath C, Seidelmann T, Loredo JC et al. Enhancing quantum cryptography with quantum dot single-photon sources. npj Quantum Inf. 2022;8(1):104.
37. Ralph T, Resch K, Gilchrist A. Efficient Toffoli gates using qudits. Phys Rev A. 2007;75(2):022313.
38. Uskov DB, Kaplan L, Smith AM, Huver SD, Dowling JP. Maximal success probabilities of linear-optical quantum gates. Phys Rev A. 2009;79(4):042326.
39. Zeuner J, Sharma AN, Tillmann M, Heilmann R, Gräfe M, Moqanaki A et al. Integrated-optics heralded controlled-NOT gate for polarization-encoded qubits. npj Quantum Inf. 2018;4(1):13.
40. Welte S, Thomas P, Hartung L, Daiss S, Langenfeld S, Morin O et al. A nondestructive Bell-state measurement on two distant atomic qubits. Nat Photonics. 2021;15(7):504–9.
41. Kim Y-H, Kulik SP, Shih Y. Quantum teleportation of a polarization state with a complete Bell state measurement. Phys Rev Lett. 2001;86(7):1370.
42. Garcia-Escartin JC, Chamorro-Posada P. Swap test and Hong-Ou-Mandel effect are equivalent. Phys Rev A. 2013;87(5):052330.
43. Kang M-S, Choi H-W, Pramanik T, Han S-W, Moon S. Universal quantum encryption for quantum signature using the swap test. Quantum Inf Process. 2018;17:1–11.
44. Huang Z, He Z, Ye Y, Sheng X. Quantum state sharing under noisy environment. Int J Theor Phys. 2021;60:1254–60.
45. Nielsen MA, Chuang I. Quantum computation and quantum information. American Association of Physics Teachers; 2002.
46. Bužek V, Hillery M, Werner RF. Optimal manipulations with qubits: universal-NOT gate. Phys Rev A. 1999;60(4):R2626.
47. Bužek V, Hillery M, Werner F. Universal-NOT gate. J Mod Opt. 2000;47(2–3):211–32.
48. De Martini F, Bužek V, Sciarrino F, Sias C. Experimental realization of the quantum universal NOT gate. Nature. 2002;419(6909):815–8.
49. Kwiat PG, Mattle K, Weinfurter H, Zeilinger A, Sergienko AV, Shih Y. New high-intensity source of polarization-entangled photon pairs. Phys Rev Lett. 1995;75(24):4337.
50. Lerch S, Bessire B, Bernhard C, Feurer T, Stefanov A. Tuning curve of type-0 spontaneous parametric down-conversion. J Opt Soc Am B. 2013;30(4):953–8.
51. Boyd RW. Nonlinear optics. San Diego: Academic Press; 2020.
52. Choi J-W, Kang M-S, Park CH, Yang H-J, Han S-W. Measurement-device-independent mutual quantum entity authentication. Quantum Inf Process. 2021;20(4):1–16.
53. Park CH, Woo MK, Park BK, Lee MS, Kim Y-S, Cho Y-W et al. Practical plug-and-play measurement-device-independent quantum key distribution with polarization division multiplexing. IEEE Access. 2018;6:58587–93.
54. Park CH, Woo MK, Park BK, Kim Y-S, Baek H, Lee S-W et al. 2 × N twin-field quantum key distribution network configuration based on polarization, wavelength, and time division multiplexing. npj Quantum Inf. 2022;8(1):48.

55. Nadlinger D, Drmota P, Nichol B, Araneda G, Main D, Srinivas R et al. Experimental quantum key distribution certified by Bell's theorem. Nature. 2022;607(7920):682–6.
56. Wang S, Yin Z-Q, He D-Y, Chen W, Wang R-Q, Ye P et al. Twin-field quantum key distribution over 830-km fibre. Nat Photonics. 2022;16(2):154–61.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Submit your manuscript to a SpringerOpen journal and benefit from:

► Convenient online submission
► Rigorous peer review
► Open access: articles freely available online
► High visibility within the field
► Retaining the copyright to your article

Submit your next manuscript at ► springeropen.com