applied sciences

MDPI

Article

Experimental Quantum Message Authentication with Single Qubit Unitary Operation

Min-Sung Kang [1,2], Yong-Su Kim [1,3], Ji-Woong Choi [1,4], Hyung-Jin Yang [4] and Sang-Wook Han [1,3,*]

[1] Center for Quantum Information, Korea Institute of Science and Technology (KIST), Seoul 02792, Korea; mskang81@korea.kr (M.-S.K.); yong-su.kim@kist.re.kr (Y.-S.K.); jodol007@kist.re.kr (J.-W.C.)
[2] Korean Intellectual Property Office (KIPO), Government Complex Daejeon Building 4, 189, Cheongsa-ro, Seo-gu, Daejeon 35208, Korea
[3] Division of Nano and Information Technology, Korea Institute of Science and Technology School, Korea University of Science and Technology, Seoul 02792, Korea
[4] Department of Physics, Korea University, Sejong 30019, Korea; yangh@korea.ac.kr
* Correspondence: swhan@kist.re.kr; Tel.: +82-31-546-7474

Abstract: We have developed a quantum message authentication protocol that provides authentication and integrity of an original message using single qubit unitary operations. Our protocol mainly consists of two parts: quantum encryption and a correspondence check. The quantum encryption part is implemented using linear combinations of wave plates, and the correspondence check is performed using Hong–Ou–Mandel interference. By analyzing the coincidence counts of the Hong–Ou–Mandel interference, we have successfully proven the proposed protocol experimentally, and also showed its robustness against an existential forgery.

Keywords: quantum message authentication; quantum three-pass protocol; Gao's forgery; swap test

check for updates

Citation: 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*, 2653. https://doi.org/10.3390/app11062653

Academic Editors: Maria Bondani, Alessia Allevi and Stefano Olivares

Received: 28 February 2021
Accepted: 13 March 2021
Published: 16 March 2021

1. Introduction

Modern cryptography provides four functions, namely, confidentiality, authentication, integrity, and nonrepudiation [1,2]. Therefore, as a substitution candidate for next-level secure cryptography, quantum cryptography should also have the ability to offer these four functions. Remarkable progress has been made in the area of confidentiality because the quantum key distribution (QKD) protocol that provides confidentiality has been considerably improved [3–6]. QKD aims to enable communication partners, e.g., Alice and Bob, to share secret keys and ultimately perform a one-time pad communication. Those protocols provide unconditional confidentiality based on the principle that an arbitrary unknown quantum state cannot be copied and that quantum measurement is irreversible [7–10]. On the other hand, many researchers have also studied how to use these secret keys in quantum message authentication [11–13], arbitrated quantum signature [14–19], or quantum digital signature [20–29], providing authentication, integrity, and non-repudiation.

In this paper, we introduce a simple and practical quantum message authentication protocol with a quantum three-pass protocol [30–33] and a quantum encryption scheme [19,34]. This protocol is a lightweight to simplify the implementation by removing an arbitrator from our proposed quantum signature protocol [19]. Here, the quantum three-pass protocol is the quantum version of Shamir's three-pass protocol [1,35], and quantum encryption scheme is to prevent existential forgery, called Gao's forgery. More specifically, the core elements of the proposed protocol, such as the quantum three-pass protocol and the quantum encryption scheme, are implemented with only single qubit unitary operators. In other words, these can be implemented easily by using linear combinations of wave plates [36,37]. Additionally, the swap test that checks the correspondence of the original message and quantum message authentication code (QMAC) can be implemented using a Hong–Ou–Mandel interferometer [38–40]. In advance, as the Hong-Ou-Mandel interferometer is a destructive swap test [40], more resources are needed to implement a controlled swap test.

In Section 2, we briefly explain the concept of the proposed scheme. Section 3 presents a security analysis of the proposed protocol for Alice's private key, the forgery of QMAC pair, and the origin authentication of quantum message. Section 4 describes the experimental setup and measurement results. We conducted three experiments with the proposed protocol. First, we implemented a quantum three pass protocol, which is a method of conveying information in the proposed quantum message authentication. Second, we implemented a quantum encryption scheme with a single qubit unitary operator to prevent forgery. Finally, we confirmed that the QMAC pair with the quantum encryption scheme is robust to Gao's forgery. In Section 5, after a thorough discussion that includes the possibility of expanding the scheme to quantum signature and quantum entity authentication, we present the conclusions of this work.

2. Quantum Message Authentication Protocol

Quantum message authentication, which is similar to conventional message authentication, should provide message integrity and origin authentication. What differentiates quantum message authentication from conventional message authentication [41,42] is that the former uses quantum states $|0\rangle$ and $|1\rangle$ as a message represented by a sequence of "0" and "1" bits. In addition, using arbitrary quantum states as a message enables more information to be delivered at once [43,44]. Moreover, there is a significant difference that is described below. In modern cryptography, asymmetric key cryptography easily provides message integrity, message origin authentication, and nonrepudiation. Unfortunately, a quantum asymmetric key cryptosystem based on the quantum trapdoor one-way function do not exist, making the design of quantum authentication and quantum signature protocols difficult. To overcome this difficulty, we propose a new quantum message authentication protocol based on Shamir's three-pass protocol [1,35]. Shamir's three pass protocol has the advantage that two parties, e.g., Alice and Bob, can share information without exposing their own private keys. In the implementation, the central idea is that the commutative property [19] of exponential operation in Shamir's three-pass protocol is implemented using single-qubit rotation operators consisting of linear combinations of wave plates. To our knowledge, this is the first time a quantum message authentication protocol has been proposed using the quantum three-pass protocol, though other applications of the quantum three-pass protocol, such as direct communication [32], quantum key distribution [30], and quantum signature [19], have been proposed theoretically. Figure 1 schematically shows the quantum message authentication protocol that we implemented. Our quantum message authentication protocol consists of preparation, quantum message authentication, and verification phase.

2.1. Preparation Phase

In the preparation phase, Alice and Bob pre-share secret key sequences $K_{AB} = \left(k_{AB}^1, k_{AB}^2, \ldots, k_{AB}^N\right)$ and $K_H = \left(k_H^1, k_H^2, \ldots, k_H^N\right)$ that determine which single-qubit operation is chosen. The sequences $K_{AB} = \left(k_{AB}^1, k_{AB}^2, \ldots, k_{AB}^N\right)$ and $K_H = \left(k_H^1, k_H^2, \ldots, k_H^N\right)$ are a classical bit sequence with the size of $2N$ and N respectively, where $k_{AB}^i \in \{00, 01, 10, 11\}$, $k_H^i \in \{0, 1\}$. The secret keys k_{AB}^i and k_H^i correspond to the Pauli operators $\sigma_{k_{AB}^i} \in \{I, \sigma_x, \sigma_y, \sigma_z\}$ and the operator $H^{k_H^i} \in \{H^0 = I, H^1 = H\}$. Here, operator is a linear combination of the Pauli operators $\{I, \sigma_x, \sigma_y, \sigma_z\}$ and unitary operator $H^\dagger H = HH^\dagger = I$.

$$H = \left(I - i\sigma_x - i\sigma_y - i\sigma_z\right)/2 \tag{1}$$

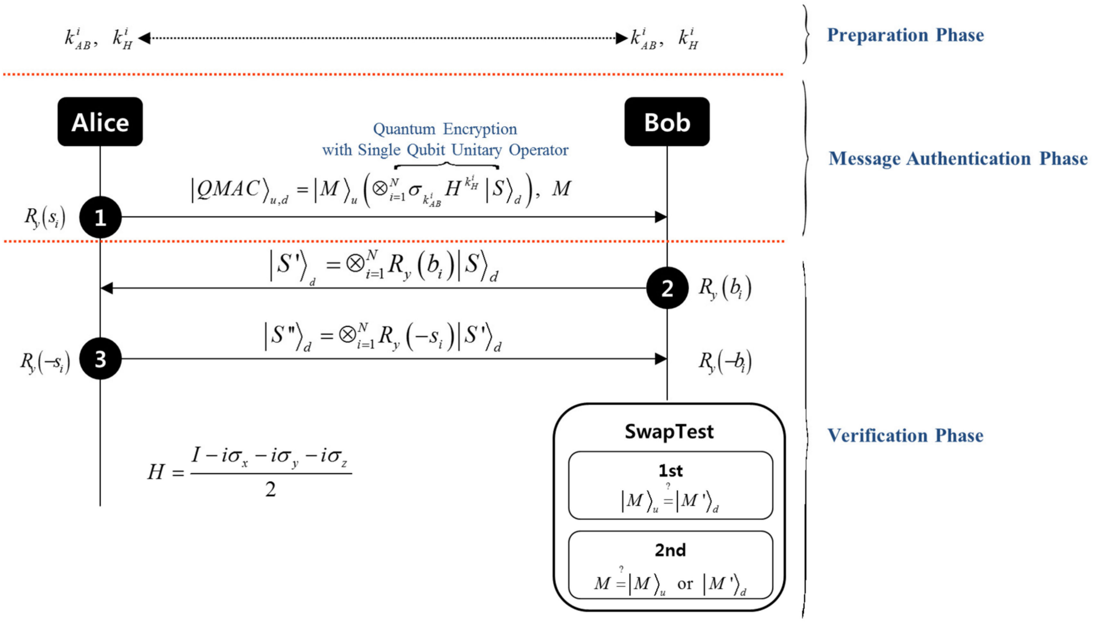
$k^i_{AB},\ k^i_H$
$k^i_{AB},\ k^i_H$
Preparation Phase
Alice
Bob
Quantum Encryption with Single Qubit Unitary Operator
$|QMAC\rangle_{u,d} = |M\rangle_u \left(\otimes^N_{i=1}\sigma_{k^i_{AB}} H^{k^i_H}|S\rangle_d\right),\ M$
$R_y(s_i)$
1
Message Authentication Phase
$|S'\rangle_d = \otimes^N_{i=1} R_y(b_i)|S\rangle_d$
2
$R_y(b_i)$
$|S''\rangle_d = \otimes^N_{i=1} R_y(-s_i)|S'\rangle_d$
$R_y(-s_i)$
3
$R_y(-b_i)$
$H = \frac{I - i\sigma_x - i\sigma_y - i\sigma_z}{2}$
SwapTest
1st
$|M\rangle_u \overset{?}{=} |M'\rangle_d$
2nd
$M \overset{?}{=} |M\rangle_u$ or $|M'\rangle_d$
Verification Phase

Figure 1. Basic structure of the quantum message authentication protocol based on quantum three-pass protocol. Similar to quantum three-pass protocol, which transmits bits three times, our protocol performs three quantum state transmissions. After three attempts of quantum state transmission, Bob finally acquires quantum message states $|M\rangle_u = \otimes_{i=1}^{N} R_y(m_i)|\varphi\rangle_u^i$ and $|M'\rangle_d = \otimes_{i=1}^{N} R_y(m_i)|\varphi\rangle_d^i$. He then uses a swap test twice to confirm the similarity of the two arbitrary quantum states $|M\rangle_u$, $|M'\rangle_d$ and bit message sequence M. K_{AB} and K_H denote the secret key sequences that Alice and Bob previously shared. S is the private key sequence that only Alice knows, and B is the one known only to Bob.

2.2. *Quantum Message Authentication Phase*

The quantum message authentication phase is composed of two stages: quantum message generation, QMAC generation, and quantum encryption. In the quantum message generation stage, Alice generates a quantum message state pair

$$|M\rangle_u|M\rangle_d = \left[\otimes_{i=1}^{N} R_y(m_i)|\varphi\rangle_u^{(i)}\right]\left[\otimes_{i=1}^{N} R_y(m_i)|\varphi\rangle_d^{(i)}\right] \tag{2}$$

by applying a single qubit rotation operator

$$R_y(m_i) = \begin{pmatrix} cos\frac{m_i}{2} & -sin\frac{m_i}{2} \\ sin\frac{m_i}{2} & cos\frac{m_i}{2} \end{pmatrix}, \tag{3}$$

where $M = (m_1, m_2,\ m_3,\ \ldots,\ m_N)$ is a rotation angle sequence, $0^\circ \le m_i \le 360^\circ$, and $|\varphi\rangle_u^{(i)}|\varphi\rangle_d^{(i)}$ are the logical states $|0\rangle|0\rangle$ or $|1\rangle|1\rangle$, corresponding to horizontally polarized photons $|H\rangle|H\rangle$ and vertically polarized photons $|V\rangle|V\rangle$, respectively. The superscript (i) denotes the i th qubit, and subscripts u and d denote up and down, corresponding to the up-line and down-line, respectively, of the experimental setup used for our protocol. The rotation angle sequence $M = (m_1, m_2,\ m_3,\ \ldots,\ m_N)$ is a bit message sequence, and we assume that it has already been published in public as in the case of a contract or an official document. The reason for publishing M is to prevent Alice from attempting to forge using a modulated QMAC pair, which is discussed in detail in Section 3.2 impossibility of forgery.

In the QMAC generation stage, Alice encrypts the quantum message pair $|M\rangle_u|M\rangle_d$ of Equation (2) by using a single qubit rotation operator $R_y(s_i)$;

$$|M\rangle_u|S\rangle_d = |M\rangle_u\left[\otimes_{i=1}^{N} R_y(s_i)|M\rangle_d\right] = \left[\otimes_{i=1}^{N} R_y(m_i)|\varphi\rangle_u^{(i)}\right]\left[\otimes_{i=1}^{N} R_y(s_i)R_y(m_i)|\varphi\rangle_d^{(i)}\right]. \tag{4}$$

Here, $S = (s_1, s_2, s_3, \ldots, s_N)$ is a rotation angle sequence, $0^\circ \leq s_i \leq 360^\circ$. In addition, S is a private key known only to Alice. Furthermore, we call $|M\rangle_u |S\rangle_d$ to a QMAC state pair.

In the quantum encryption stage, Alice applies quantum encryption $\sigma_{k^i_{AB}} H^{k^i_H}$ to the QMAC state pair $|M\rangle_u |S\rangle_d$ of Equation (4);

$$|M\rangle_u \left[\otimes_{i=1}^{N} \sigma_{k^i_{AB}} H^{k^i_H} |S\rangle_d \right]. \tag{5}$$

Here, $|M\rangle_u \left[\otimes_{i=1}^{N} \sigma_{k^i_{AB}} H^{k^i_H} |S\rangle_d \right]$ is an encrypted QMAC state pair, and then she sends it to Bob. This quantum encryption is an essential function for verifying that the entity sending the QMAC pair is Alice and for protecting against forgery.

The rotation angles m_i and s_1 are the elements of the finite discrete variable set. For applying them to real protocols, Alice and Bob must preset the range of the finite discrete variable set and pre-decide how to divide the set range. For example, if Alice and Bob split the rotation angle from 0° to 360° in intervals of 10°, then the finite discrete variable set becomes $\{0^\circ, 10^\circ, 20^\circ, \ldots, 350^\circ\}$. Here, the size of the discrete variable set is determined by the performance of the experimental apparatus. Therefore, as the performance of experimental apparatus improves, the size of the discrete variable set increases. Increasing the size of the discrete variable set means that the rotation angle can be subdivided, and this can lead to authenticating more information compared with using the four states of the BB84 protocol. On the other hand, If the performance of the experimental apparatus is poor, the size of the discrete variable set decreases. Then, the rotation angle cannot be subdivided, and information that can be authenticated decreases. Additionally, in this situation, if the communication members use the subdivided rotation angles to such an extent that the experimental apparatus cannot distinguish, detecting the malicious behavior of Eve is impossible.

2.3. Verification Phase

The verification phase is divided into five stages: "quantum decryption", "Bob's encryption", "QMAC recovery", "Bob's decryption", and "swap test". In Stage 1, for quantum decryption, Bob uses secret key sequences K_{AB} and K_H, which were pre-shared with Alice to decrypt the encrypted QMAC state pair $|M\rangle_u \left[\otimes_{i=1}^{N} \sigma_{k^i_{AB}} H^{k^i_H} |S\rangle_d \right]$ in Equation (5), received from Alice to obtain the QMAC state pair $|M\rangle_u |S\rangle_d$ of Equation (4). In Stage 2, Bob's encryption, Bob generates his own private key sequence $B = (b_1, b_2, \ldots, b_N)$ and re-encrypts quantum state $|S\rangle_d = \otimes_{i=1}^{N} R_y(s_i) |M\rangle_d$ with it to obtain quantum state $|S'\rangle_d = \otimes_{i=1}^{N} R_y(b_i) |S\rangle_d$. Then, he sends $|S'\rangle_d$ to Alice while keeping the other quantum message state $|M\rangle_u$. In Stage 3, QMAC recovery, Alice uses her own private key sequence S to apply rotation operator $\otimes_{i=1}^{N} R_y(-s_i)$ to quantum state $|S'\rangle_d$ and sends quantum state $|S''\rangle_d = \otimes_{i=1}^{N} R_y(-s_i) |S'{}_d$ to Bob. In Stage 4, Bob's decryption, Bob uses his own private key sequence B and applies rotation operator $\otimes_{i=1}^{N} R_y(-b_i)$ to quantum state $|S''\rangle_d$ to obtain quantum message state $|M'\rangle_d = \otimes_{i=1}^{N} R_y(-b_i) |S''\rangle_d$. Because the proposed quantum message authentication based on the quantum three-pass protocol operates Alice's private key s_i, there is a need for a method to verify the encrypted QMAC pair described thus far. This is an important element that the proposed protocol can guarantee the origin of quantum message. In addition, to avoid counterfeiting, it is assumed that quantum encryption such as $\sigma_{k^i_{AB}} H^{k^i_H}$ in Equation (5) is applied to Alice and Bob in every process of exchanging quantum states.

In the final stage, Bob performs the swap test [42,45] twice to verify the QMAC state pair. In the first swap test, Bob verifies whether quantum message state $|M\rangle_u$ and quantum message state $|M'\rangle_d$ are the same. If the test result reveals that $|M\rangle_u$ and $|M'\rangle_d$ agree, Bob accepts QMAC state pair $|M\rangle_u |S\rangle_d$ sent by Alice. Otherwise, he does not accept it. In the second swap test, Bob generates quantum state $|M''\rangle$ corresponding to the public bit message sequence M and verifies that it matches quantum message state $|M\rangle_u$ or $|M'\rangle_d$.

If the test result reveals that ($|M''\rangle$, $|M\rangle_u$) or ($|M''\rangle$, $|M'\rangle_d$) agree, then the integrity of QMAC state pair $|M\rangle_u|S\rangle_d$ is verified completely. For the second swap test, it is noted that the first swap test requires a non-demolition swap test. Figure 2 shows the swap test in the circuit, and the result of inputting

$$|m_i\rangle_u = R_y(m_i)|\varphi\rangle_u^{(i)} \tag{6}$$

and

$$|m_i'\rangle_d = R_y(m_i')|\varphi\rangle_d^{(i)} \tag{7}$$

in the second and third lines of the circuit is expressed as follows:

$$\frac{1}{\sqrt{2}}|0\rangle_{ancilla}\left[\frac{1}{\sqrt{2}}\left(|m_i\rangle_u|m_i'\rangle_d + |m_i'\rangle_u|m_i\rangle_d\right)\right] + \frac{1}{\sqrt{2}}|1\rangle_{ancilla}\left[\frac{1}{\sqrt{2}}\left(|m_i\rangle_u|m_i'\rangle_d - |m_{i\,u}'|m_i\rangle_d\right)\right]. \tag{8}$$

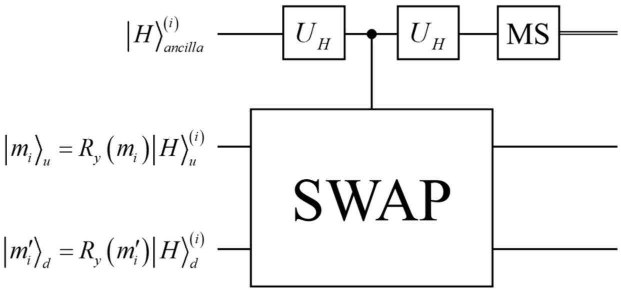
$|H\rangle_{ancilla}^{(i)}$
U_H
U_H
MS
$|m_i\rangle_u = R_y(m_i)|H\rangle_u^{(i)}$
$|m_i'\rangle_d = R_y(m_i')|H\rangle_d^{(i)}$
SWAP

Figure 2. Circuit of the quantum swap test. "SWAP" indicates a swap gate, and U_H represents a Hadamard gate. "MS" represents quantum measurement, and the single lines and the double line represent the quantum channel and classical channel, respectively.

If $|m_i\rangle_u$ and $|m_i'\rangle_d$ agree, the above equation becomes $|0\rangle_{ancilla}\left[\frac{1}{\sqrt{2}}\left(|m_i\rangle_u|m_i'\rangle_d + |m_i'\rangle_u|m_i\rangle_d\right)\right]$, which makes the measurement outcome of the ancilla state to always be $|0\rangle$. However, if $|m_i\rangle_u$ and $|m_i'\rangle_d$ do not agree, the measurement outcome becomes $|0\rangle$ with a probability $\left(1+\varepsilon^2\right)/2$ or becomes $|1\rangle$ with a probability $\left(1+\varepsilon^2\right)/2$, where $\varepsilon = |{}_d\langle m_i'|m_i\rangle_u|$ and $0 \le \varepsilon \le 1$. Therefore, if the swap test result of the measurement is $|1\rangle$, we know that $|m_i\rangle_u$ and $|m_i'\rangle_d$ are different. If the result is $|1\rangle$, we cannot guarantee that $|m_i\rangle_u$ and $|m_i'\rangle_d$ are the same. The parameter ε is determined by the arbitrary quantum state components $|m_i\rangle_u$ of Equation (6) and $|m_i'\rangle_d$ of Equation (7). If the two rotation angles m_i and m_i' are the same, i.e., $m_i = m_i'$, then the value of parameter ε is 1. On the other hand, if the difference between m_i and m_i' is 180°, i.e., $m_i = m_i' \pm 180°$, then the parameter ε is 0. As a result, according to rotation angles m_i and m_i', the parameter ε has a value between 0 and 1, $0 \le \varepsilon \le 1$. Further, the probability of failure in the verification phase is the total error probability P_e for N qubits as follows:

$$P_e \le \otimes_{i=1}^{N}\left[\left(1+|{}_d\langle m_i'|m_i\rangle_u|^2\right)/2\right] \tag{9}$$

Therefore, it is expected that the swap test will work well even though the quantum state sequence is finite. Hence, the probability of failure in the verification phase becomes lower, approaching P_e as the size of the quantum state sequence N becomes considerably larger [42,45]. For an arbitrary $|m_i\rangle_u$, a random choice for $|m_i'\rangle_d$ on the $R_y\left(m_i'\right)$—rotation circle, the average of ε^2 is $1/2$. In this case, the upper bound of the total error probability P_e is $(3/4)^N$. If the size of the quantum state sequence is 15, then the upper bound of the total error probability P_e is only approximately 1.3%. Therefore, it is expected that the swap test will work well even though the quantum state sequence is finite.

3. Security Analysis

3.1. Security of Alice's Private Key

Eve, including Bob, may try to obtain Alice's private key. Especially, as described in Section 2.3, malicious Bob may try to know Alice's private key sequence $S = (s_1, s_2,\ s_3,\ \ldots,\ s_N)$, which consists of the degrees of rotation about $\hat{y}$-axis from $|S\rangle_d = \otimes_{i=1}^{N} R_y(s_i)|M\rangle_d$ in Equation (4). However, the security of Alice's private key sequence S is guaranteed by Holevo's theorem, as follows [19,32]:

$$I(x, S) \leq V(\rho) \leq H(S) \tag{10}$$

Here, $H(S)$ is the Shannon entropy of the sequence of arbitrary rotation angle s_i, $V(\rho)$ is the von Neumann entropy of mixed state ρ that Eve can acquire through the arbitrary measurement of the quantum state $|S\rangle_d = \otimes_{i=1}^{N} R_y(s_i)|M\rangle_d$, and $I(x, S)$ is the mutual information between arbitrary rotation s_i and measurement outcomes x. As we can see in Equation (10), the amount of mutual information about the arbitrary rotation angle sequence S that Bob acquires using measurement outcomes x is limited, and thus, it is impossible for Eve to obtain the information of S. Based on the same principle, the security of Bob's private key sequence $B = (b_1, b_2,\ b_3,\ \ldots,\ b_N)$ is guaranteed.

3.2. Impossibility of Forgery

Many quantum message authentication and signature protocols use quantum encryption implemented by Pauli operators to ensure message integrity and message origin authentication. A QMAC pair (or quantum signature pair), which is composed of a quantum message and an encrypted quantum message, checks the forgery and modulation of the QMAC pair (or quantum signature pair) using a swap test [34]. As described in Section 2.3, Bob validates the original quantum message state $|M\rangle_u$ and the recovered quantum message state $|M'\rangle_d$ from the QMAC state pair of Equation (4) using the swap test. Bob can be sure that $|M\rangle_u$ and $|M'\rangle_d$ are the same quantum state from the outcomes of the swap test. However, it is not known whether they match the original message M. Because of the limitations of this swap test, the proposed protocol can be falsified in two ways.

The first falsification method is that Alice creates a modulated QMAC pair

$$I(x, S) \leq V(\rho) \leq H(S) \tag{11}$$

with the two same quantum states $\left|\widetilde{M}\right\rangle_u$ and $\left|\widetilde{M'}\right\rangle_d$ that do not correspond to the original message M and sends it to Bob. In this case, Bob cannot detect Alice's malicious behaviour even if he verifies that the two quantum states $\left|\widetilde{M}\right\rangle_u$ and $\left|\widetilde{M'}\right\rangle_d$ are the same from the QMAC pair by using the swap test. To prevent this, Alice must disclose message M. Additionally, Bob needs an additional process to validate $|M''\rangle$, which is converted to a quantum state, and $|M\rangle_u$ or $|M'\rangle_d$ by using the swap test.

Second, Eve can try Gao's forgery to apply Pauli operators to a QMAC pair [34,46]. Recently, Gao et al. showed that even if an adversary applies the arbitrary Pauli operator to the QMAC pair (or quantum signature pair), the swap test could not detect it because of the commutation relation of Pauli operators [46]. This is called Gao's forgery, and it can be considered as an existential forgery [34] of modern cryptosystems because it randomly forges QMAC pairs (or quantum signature pairs), which are arbitrary quantum states. The posing of this security problem by Gao et al. was a major turning point in the study of quantum message authentication (or quantum signature) protocols. In 2011, Choi et al. proposed the (I, H)- or (U, V)-type quantum encryption scheme to cope with Gao's forgery [47,48]. In 2013, Zhang et al. pointed out that the encryption scheme of Choi et al. was still insecure against Gao's forgery, and instead they proposed the key-controlled-"I" quantum one-time pad or key-controlled-"T" quantum one-time pad [49,50] as an alternative. The four unitary operators of the controlled-I quantum one-time pad are $W_{00} = (\sigma_x + \sigma_z)/\sqrt{2}$, $W_{01} = (\sigma_y + \sigma_z)/\sqrt{2}$, $W_{10} = (I + i\sigma_x - i\sigma_y + i\sigma_z)/\sqrt{2}$, and $W_{10} = (I + i\sigma_x + i\sigma_y + i\sigma_z)/\sqrt{2}$. However, the encryption scheme of Zhang et al. is not easy to implement with simple hardware. In contrast, we propose a quantum encryption scheme with a single qubit unitary operation by randomly using unitary operator H, which can be easily implemented by controlling wave plates and an authentication protocol. Therefore, the proposed protocol is robust against an existential forgery. Section 4.3 in Ref. [22] shows that unitary operators can be used randomly to prevent Gao's forgery. The detailed implementation of our experimental setup and the testing results of the quantum three-pass protocol and security against Gao's forgery are described in Section 4. Finally, to prevent Gao's forgery in the proposed protocol, the quantum encryption scheme should be applied to all processes in which Alice and Bob exchange quantum states.

3.3. Origin Authentication of Quantum Message

To clarify the origin of the quantum message, the proposed quantum message authentication operates by using not only the secret key pre-shared by Alice and Bob but also Alice's private key. In general, message authentication guarantees the origin of message authentication by using a secret key previously shared by Alice and Bob. At this time, as the user who can create a message authentication code (MAC) pair can be Alice or Bob, the origin of the message may become unclear. On the other hand, in the proposed protocol, Alice generates a QMAC pair $|M\rangle_u |S\rangle_d$ of Equation (4) by using a private key sequence $S = (s_1, s_2, s_3, \ldots, s_N)$ known only to her; thus, the possibility of such a dispute is very low.

4. Experiment Setup and Measurement Results

Figure 3a shows the implementation setup of our proposed quantum message authentication protocol. With this setup, we have experimentally proved that the proposed QMAC is robust against existential forgery. Each stage is implemented with a linear combination of wave plates; that is, the y-axis rotation operator $R_y(\theta)$, the unitary operator H, and the Pauli operators are implemented by combinations of half-wave plates (HWPs) and quarter-wave plates (QWPs). Figure 3b schematically shows a possible forgery attack that Eve can try. Eve can attempt a forgery attack using the same Pauli operators $\sigma_{e_i} = \sigma_{e'_i}$ [46], or she can attempt a forgery attack using different Pauli operators $\sigma_{e_i} \neq \sigma_{e'_i}$ [49,50]. We define these two approaches as an original and improved Gao's Forgeries, respectively. To prevent Gao's forgeries, we need to choose unitary operator H randomly. We explain this in detail at the end of this section.

We assume that Alice and Bob have already pre-shared the secret key sequences in the preparation phase. For the message authentication phase, we implemented message generation, QMAC generation, and quantum encryption using wave plates on Alice's side. To create correlated photon pairs, Type-I spontaneous parametric down-conversion (SPDC) photon pairs were generated in a beta barium borate (BBO) crystal pumped by a multimode diode laser with a 408-nm wavelength. The SPDC photon pairs have the same H-polarization and an 816-nm wavelength. The photon pairs are emitted with a noncollinear angle of 3.3°. One of the photons goes through only the rotation operator for message generation, and the other experiences the sequence of operations from message generation through the quantum encryption scheme with a single qubit unitary operator. Then, they are delivered to Bob. For the verification phase, one photon is kept on Bob's side, and the other photon experiences quantum decryption and Bob's encryption implemented by the wave plate, after which Bob sends it to Alice. Alice then decrypts it by using QMAC recovery. In our experiment, we installed the QMAC recovery stage between Bob's encryption and Bob's decryption for convenience of implementation; it is marked by yellow shading in Figure 3a. Finally, after Bob's decryption, the swap test that verifies the agreement of the two photon sequences is performed using the Hong–Ou–Mandel interferometer. The Hong–Ou–Mandel dip confirms the similarity between the two photons, which is the last step of the implementation of the proposed quantum message authentication protocol.

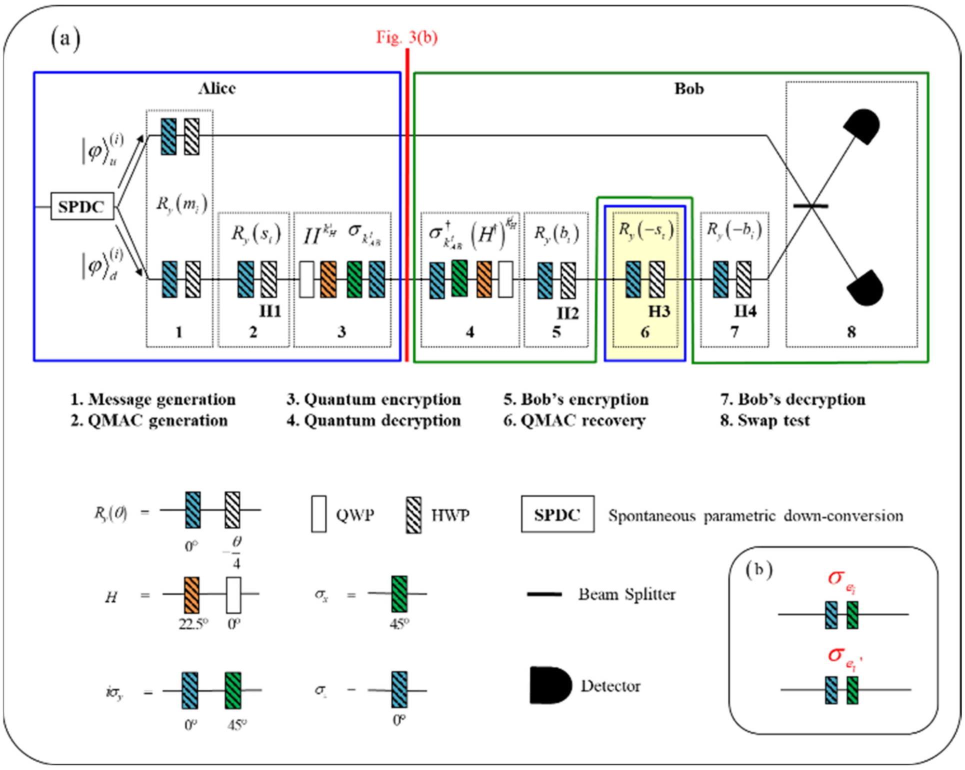

Figure 3. Schematic representation of the experimental setup for the quantum message authentication protocol and an existential forgery. (**a**) Quantum message authentication protocol: the blue box represents Alice's operation, and the green box represents Bob's operation. m_i is the rotation angle that indicates message. ${k^i}_{AB}$, ${k^i}_H$, s_i, and b_i are the same as in Figure 1. (**b**) Existential forgery: Eve can attempt forgery on the quantum message authentication code (QMAC) state pair using Pauli operators when Alice transmits the encrypted QMAC state pair to Bob.

In other words, the realization of the quantum three-pass protocol, quantum encryption scheme, and the robustness of Gao's forgery can be confirmed by the Hong–Ou–Mandel Dip. Hong–Ou–Mandel interference is the same as the destructive swap test [40]. Because the destructive swap test does not have an ancilla qubit unlike the controlled swap test, the two quantum states that are compared are directly measured and collapsed. For this reason, we performed only the first swap test in the two swap tests shown in Figure 1. To implement the second swap test in Figure 1 using Hong–Ou–Mandel interference, there is a need for more resources (e.g., single photons and wave plates) than the current experimental setup. There are other ways to implement a second swap test by using an experimental controlled swap gate that was recently implemented [51].

We tested the feasibility of our protocol with the experimental setup for the case without Gao's forgery. First, we verified that the quantum three-pass protocol (Figure 3) was working correctly. As shown in Figure 4a, when the half-wave plate H1′s angle $s_i/4$ is -120°, the coincidence count reaches its minimum at the half-wave plate H3′s angles $-s_i/4 = 30^{\circ}, 120^{\circ}$ as expected. This indicates that Alice generates the QMAC state by applying rotation operator $R_y(-120^{\circ})$ and then uses rotation operator $R_y(-120^{\circ} \pm \pi n/2)$ to recover the QMAC state, where n is an integer, because the period of the half-wave plate is $\pi/2$. The red plots represent the averages of the coincidence counts over one second. In Figure 4b, we recognize that Bob's encryption and decryption also work well. When the half-wave plate H2′s angle $b_i/4$ is -60°, the Hong–Ou–Mandel dip occurs at the half-wave plate H4′s angles $-b_i/4 = 60^{\circ}, 150^{\circ}$. Bob uses rotation operator $R_y(-60^{\circ})$ to re-encrypt the QMAC state, and then he decrypts the re-encrypted QMAC state by applying rotation operator $R_y(60^{\circ} \pm \pi n/2)$, where n is an integer. In Figure 4, the experimental data are the average of 10 measurements per 10 s.

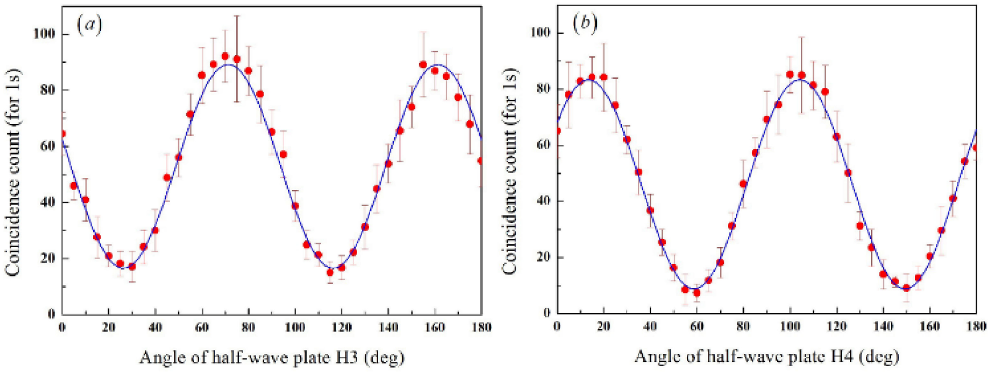

Figure 4. Coincidence counts of the quantum three-pass protocol. The red plots indicate the average of the coincidence counts for one second. The red bars indicate the standard deviation of the coincidence counts for each point. The blue solid line indicates the sine curve fitted to the data. (**a**) Test for QMAC generation and recovery. (**b**) Test for Bob's encryption and decryption.

During this time, the averages of single counts were $27,000$ and $27,000$, respectively, and coincidence windows are 5 ns; the maximum value of the coincidence counts after accidental coincidences were removed was 127, and the minimum value was 2.

Second, we tested the quantum encryption and decryption. If Alice and Bob are proper users who previously shared secret key sequences K_{AB} and K_H then the quantum message states $|M\rangle_u$ and $|M'\rangle_d$ should be identical. Bob can check the correspondence of these states using the Hong–Ou–Mandel interferometer [38,39]. Figure 4 shows the experimental results for Alice's quantum encryption and Bob's quantum decryption. P_c is the coincidence probability of Hong–Ou–Mandel interference, and $\overline{P}_c = 1 - P_c$ represents the probability of two quantum message states matching. Figure 5a,b represents whether operator H exists or not, respectively. Although theoretically, the red blocks on the diagonal in both cases should be 100%, experimentally they are greater than 82% and 76%, respectively. On the other hand, the blue blocks off the diagonal, when Alice and Bob share different secret keys k^i_{AB} and k^i_H, $|M\rangle_u$ and $|M'\rangle_d$ have different quantum states, and the respective probabilities are less than 41% and less than 46%. Considering that theoretically $\overline{P}_c$ can only have less than 50%, the measurement results prove that our scheme works well. From these results, we can conclude that the encryption operates properly because $\overline{P}_c$ is greater than 76% in the case of the same operators and $\overline{P}_c$ is less than 46% in the case of different operators regardless of the existence of operator H. The above theoretical values are derived from the success probability $\epsilon^2 = \left|{}_d\langle\psi'_i|\psi_i\rangle_u\right|^2$ of the swap test, with $|\psi_i\rangle_u = U_i R_y(m_i)|0\rangle^{(i)}_u$, $|\psi'_i\rangle_d = U'_i R_y(m_i)|0\rangle^{(i)}_d$, $U_i, U'_i \in \{I,\ \sigma_x, \sigma_y, \sigma_z,\ H,\ \sigma_x H, \sigma_y H, \sigma_z H\}$, and $m_i = 135^{\circ}$. Errors in the experiment shown in Figure 5 could be due to an inherent error of the swap test, birefringence in the beam splitter, and/or systematic errors in the wave-plate setting [38,39,42,45].

From the measurement results given in Figures 4 and 5, we have demonstrated that our implementation succeeds in realizing the proposed protocol. Although there are some errors due to unavoidable imperfections of the realization, our practical implementation still performs message integrity and message origin authentication successfully only if our protocol is applied to multiple bits sequentially and analyzed statistically.

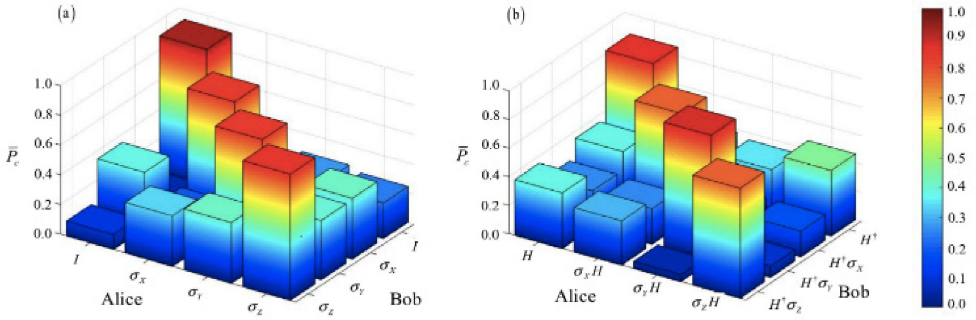

Figure 5. P_c is the coincidence probability of the quantum encryption scheme with a single qubit unitary operator for quantum message authentication. $\overline{P}_c = 1 - P_c$ represents the probability of two quantum message states being matched. In (**a**), $\overline{P}_c$ corresponds to the quantum encryption scheme with a single qubit unitary operator that Alice and Bob can select when secret key k_H^i of Alice and Bob is zero. In (**b**), $\overline{P}_c$ corresponds to every type of quantum encryption with single qubit unitary operator that Alice and Bob can select when secret key k_H^i of Alice and Bob is one. In this experiment, message m_i was set to 135°.

Gao et al. demonstrated the possibility of existential forgery in the case of quantum message authentication that includes a swap test [34,46,48]. In other words, if the QMAC state pair that Alice generates is not encrypted, Alice cannot detect Eve's intervention. In the quantum encryption $\sigma_{k_{AB}^i} H^{k_H^i}$ in Equation (5), the secret key $k_{AB}^i \in \{00,\ 01,\ 10,\ 11\}$ and $k_H^i \in \{0,\ 1\}$ correspond to the Pauli operator $\sigma_{k_{AB}^i} \in \{I,\ \sigma_x,\ \sigma_y,\ \sigma_z\}$ and the operator $H^{k_{AB}^i} \in \{I,\ H\}$ of quantum encryption with a single qubit unitary operator, respectively. The two bits information $e_i \in \{00,\ 01,\ 10,\ 11\}$ corresponds to the Pauli operator $\sigma_{e_i} \in \{I,\ \sigma_x,\ \sigma_y,\ \sigma_z\}$ for Gao's Attack. For example, if $k_{AB}^i = 01, k_H^i = 0$, an encrypted QMAC state pair is

$$|M\rangle_u\left[\sigma_{01}H^0|S\rangle_d\right] = |M\rangle_u\left[\sigma_{\mathrm{x}}|S\rangle_d\right] \tag{12}$$

In addition, the forged QMAC state pair by Eve's Pauli operator $\sigma_{10}(= \sigma_{\mathrm{y}})$ is

$$\sigma_{10}|M\rangle_u\left[\sigma_{10}\sigma_{01}H^0|S\rangle_d\right] = \sigma_{\mathrm{y}}|M\rangle_u\left[\sigma_{\mathrm{y}}\sigma_{\mathrm{x}}|S\rangle_d\right] \tag{13}$$

The forged QMAC state pair of Equation (13) transforms into the following state after a decryption process:

$$\sigma_{10}|M\rangle_u\left[\left(H^\dagger\right)^0\sigma_{01}\sigma_{10}\sigma_{01}H^0|S\rangle_d\right] = \sigma_{\mathrm{y}}|M\rangle_u\left[\sigma_{\mathrm{x}}\sigma_{\mathrm{y}}\sigma_{\mathrm{x}}|S\rangle_d\right] = \sigma_{\mathrm{y}}|M\rangle_u\left[-\sigma_{\mathrm{y}}|S\rangle_d\right]. \tag{14}$$

Assuming that $|M\rangle_u$ and $|S\rangle_d$ of Equation (14) are the same, Eve succeeded in attacking because the Pauli operator σ_{y} remained in the first and second qubits of Equation (14). This is the first method to forge the quantum message code or quantum signature pair proposed by Gao et al. [34,46,48].

As another example, if $k_{AB}^i = 01, k_H^i = 1$, an encrypted QMAC state pair is

$$|M\rangle_u\left[\sigma_{01}H^1|S\rangle_d\right] = |M\rangle_u\left[\sigma_{\mathrm{x}}H|S\rangle_d\right]. \tag{15}$$

The forged QMAC state pair by Eve's Pauli operator $\sigma_{10}(= \sigma_{\mathrm{y}})$ is

$$\sigma_{10}|M\rangle_u\left[\sigma_{10}\sigma_{01}H^1|S\rangle_d\right] = \sigma_{\mathrm{y}}|M\rangle_u\left[\sigma_{\mathrm{y}}\sigma_{\mathrm{x}}H|S\rangle_d\right]. \tag{16}$$

The forged QMAC state pair transforms into the following state after a decryption process:

$$\sigma_{10}|M\rangle_{\mathrm{u}}\left[\left(H^{\dagger}\right)^{1}\sigma_{01}\sigma_{10}\sigma_{01}H^{1}|S\rangle_{\mathrm{d}}\right] = \sigma_{\mathrm{y}}|M\rangle_{u}\left[H^{\dagger}\sigma_{\mathrm{x}}\sigma_{\mathrm{y}}\sigma_{\mathrm{x}}H|S\rangle_{d}\right] = \sigma_{\mathrm{y}}|M\rangle_{1}\left[-\sigma_{\mathrm{x}}|S\rangle_{2}\right] \quad (17)$$

Despite the assumption that $|M\rangle_u$ and $|S\rangle_d$ of Equation (17) are the same, Eve's attack is unsuccessful. The reason is that the Pauli operators σ_{y} and σ_{x} remained in the first and second qubits of Equation (17), respectively. This is the (I, H)-type quantum encryption proposed to overcome Gao's forgery [47]. Zhang et al., however, showed that the (I, H)-type quantum encryption is not secure for improved Gao's forgery [49,50]. We [19,34] overcome the original Gao's forgery [46] or the improved Gao's forgery [49,50] with quantum encryption $\sigma_{k^i_{AB}}H^{k^i_H}$, which randomly uses operator H. Here, the number of all possible cases of quantum encryption $\sigma_{k^i_{AB}}H^{k^i_H} \in \{I, \sigma_{\mathrm{x}}, \sigma_{\mathrm{y}}, \sigma_{\mathrm{z}}, H, \sigma_{\mathrm{x}}H, \sigma_{\mathrm{y}}H, \sigma_{\mathrm{z}}H\}$ is 8. Furthermore, except $\sigma_{e_i} = I$, there are three possible ways that Eve can attack with σ_{e_i}. Therefore, there are a total of 24 forgery cases using the Pauli operator σ_{e_i} in the encrypted QMAC state pair $|M\rangle_u\left[\sigma_{k^i_{AB}}H^{k^i_H}|S\rangle_d\right]$ of Equation (5) in the manuscript, Table 1 lists these 24 cases, and Figure 6 shows the results of the experiment with the existential forgery using the Pauli operator for 12 cases in Table 1.

Table 1. A total of 24 forgery cases using the Pauli operator $e_i \in \{\sigma_x, \sigma_y, \sigma_z\}$ in the encrypted QMAC state pair $|M\rangle_u\left[\sigma_{k^i_{AB}}H^{k^i_H}|S\rangle_d\right]$. Here, $\sigma_{e_i} \in \{\sigma_x, \sigma_y, \sigma_z\}$, $\sigma_{k^i_{AB}} \in \{I, \sigma_x, \sigma_y, \sigma_z\}$, and $H^{k^i_H} \in \{I, H\}$. We assume that the quantum states $|M\rangle_u$ and $|S\rangle_d$ are the same. The yellow shade represents the case where the operator σ_z is not used for quantum encryption or Gao's forgery.

$H^{k^i_H}$	$\sigma_{k^i_{AB}}$	σ_{e_i}	Up(u) Qubit	Down(d) Qubit
$H^0 = I$	$\sigma_{00} = \mathrm{I}$	$\sigma_{01} = \sigma_x$	$\sigma_{\mathrm{x}}|M\rangle_u$	$\sigma_{\mathrm{x}}|S\rangle_d$
		$\sigma_{10} = \sigma_y$	$\sigma_{\mathrm{y}}|M\rangle_u$	$\sigma_{\mathrm{y}}|S\rangle_d$
		$\sigma_{11} = \sigma_z$	$\sigma_{\mathrm{z}}|M\rangle_u$	$\sigma_{\mathrm{z}}|S\rangle_d$
	$\sigma_{01} = \sigma_x$	$\sigma_{01} = \sigma_x$	$\sigma_{\mathrm{x}}|M\rangle_u$	$\sigma_{\mathrm{x}}\sigma_{\mathrm{x}}\sigma_{\mathrm{x}}|S\rangle_d = \sigma_{\mathrm{x}}|S\rangle_d$
		$\sigma_{10} = \sigma_y$	$\sigma_{\mathrm{y}}|M\rangle_u$	$\sigma_{\mathrm{x}}\sigma_y\sigma_{\mathrm{x}}|S\rangle_d = -\sigma_y|S\rangle_d$
		$\sigma_{11} = \sigma_z$	$\sigma_{\mathrm{z}}|M\rangle_u$	$\sigma_{\mathrm{x}}\sigma_{\mathrm{z}}\sigma_{\mathrm{x}}|S\rangle_d = -\sigma_{\mathrm{z}}|S\rangle_d$
	$\sigma_{10} = \sigma_y$	$\sigma_{01} = \sigma_x$	$\sigma_{\mathrm{x}}|M\rangle_u$	$\sigma_y\sigma_x\sigma_y|S\rangle_d = -\sigma_{\mathrm{x}}|S\rangle_d$
		$\sigma_{10} = \sigma_y$	$\sigma_{\mathrm{y}}|M\rangle_u$	$\sigma_y\sigma_y\sigma_y|S\rangle_d = \sigma_y|S\rangle_d$
		$\sigma_{11} = \sigma_z$	$\sigma_{\mathrm{z}}|M\rangle_u$	$\sigma_y\sigma_z\sigma_y|S\rangle_d = -\sigma_z|S\rangle_d$
	$\sigma_{11} = \sigma_z$	$\sigma_{01} = \sigma_x$	$\sigma_{\mathrm{x}}|M\rangle_u$	$\sigma_z\sigma_x\sigma_z|S\rangle_d = -\sigma_x|S\rangle_d$
		$\sigma_{10} = \sigma_y$	$\sigma_{\mathrm{y}}|M\rangle_u$	$\sigma_z\sigma_y\sigma_z|S\rangle_d = -\sigma_y|S\rangle_d$
		$\sigma_{11} = \sigma_z$	$\sigma_{\mathrm{z}}|M\rangle_u$	$\sigma_z\sigma_z\sigma_z|S\rangle_d = \sigma_z|S\rangle_d$
$H^1 = H$	$\sigma_{00} = \mathrm{I}$	$\sigma_{01} = \sigma_x$	$\sigma_{\mathrm{x}}|M\rangle_u$	$H^{\dagger}\sigma_x H|S\rangle_d = \sigma_z|S\rangle_d$
		$\sigma_{10} = \sigma_y$	$\sigma_{\mathrm{y}}|M\rangle_u$	$H^{\dagger}\sigma_y H|S\rangle_d = \sigma_x|S\rangle_d$
		$\sigma_{11} = \sigma_z$	$\sigma_{\mathrm{z}}|M\rangle_u$	$H^{\dagger}\sigma_z H|S\rangle_d = \sigma_y|S\rangle_d$
	$\sigma_{01} = \sigma_x$	$\sigma_{01} = \sigma_x$	$\sigma_{\mathrm{x}}|M\rangle_u$	$H^{\dagger}\sigma_{\mathrm{x}}\sigma_x\sigma_{\mathrm{x}}H|S\rangle_d = \sigma_{\mathrm{z}}|S\rangle_d$
		$\sigma_{10} = \sigma_y$	$\sigma_{\mathrm{y}}|M\rangle_u$	$H^{\dagger}\sigma_{\mathrm{x}}\sigma_y\sigma_{\mathrm{x}}H|S\rangle_d = -\sigma_x|S\rangle_d$
		$\sigma_{11} = \sigma_z$	$\sigma_{\mathrm{z}}|M\rangle_u$	$H^{\dagger}\sigma_{\mathrm{x}}\sigma_{\mathrm{z}}\sigma_{\mathrm{x}}H|S\rangle_d = -\sigma_y|S\rangle_d$
	$\sigma_{10} = \sigma_y$	$\sigma_{01} = \sigma_x$	$\sigma_{\mathrm{x}}|M\rangle_u$	$H^{\dagger}\sigma_y\sigma_x\sigma_y H|S\rangle_d = -\sigma_z|S\rangle_d$
		$\sigma_{10} = \sigma_y$	$\sigma_{\mathrm{y}}|M\rangle_u$	$H^{\dagger}\sigma_{\mathrm{y}}\sigma_y\sigma_{\mathrm{y}}H|S\rangle_d = \sigma_x|S\rangle_d$
		$\sigma_{11} = \sigma_z$	$\sigma_{\mathrm{z}}|M\rangle_u$	$H^{\dagger}\sigma_{\mathrm{y}}\sigma_{\mathrm{z}}\sigma_{\mathrm{y}}H|S\rangle_d = -\sigma_y|S\rangle_d$
	$\sigma_{11} = \sigma_z$	$\sigma_{01} = \sigma_x$	$\sigma_{\mathrm{x}}|M\rangle_u$	$H^{\dagger}\sigma_{\mathrm{z}}\sigma_x\sigma_{\mathrm{z}}H|S\rangle_d = -\sigma_z|S\rangle_d$
		$\sigma_{10} = \sigma_y$	$\sigma_{\mathrm{y}}|M\rangle_u$	$H^{\dagger}\sigma_{\mathrm{z}}\sigma_y\sigma_{\mathrm{z}}H|S\rangle_d = -\sigma_x|S\rangle_d$
		$\sigma_{11} = \sigma_z$	$\sigma_{\mathrm{z}}|M\rangle_u$	$H^{\dagger}\sigma_{\mathrm{z}}\sigma_{\mathrm{z}}\sigma_{\mathrm{z}}H|S\rangle_d = \sigma_y|S\rangle_d$

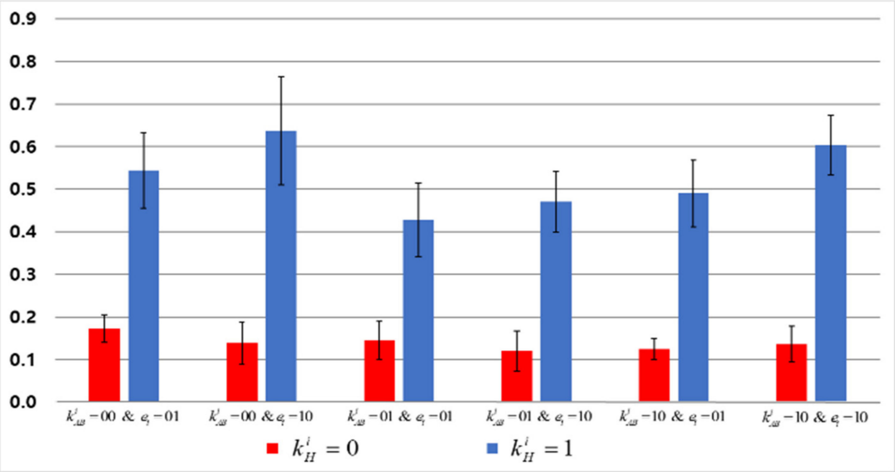

Figure 6. Coincidence probability by existential forgery. Red bars denote the case where Eve attempts original Gao's Forgery when operator H is not used in the quantum encryption scheme $\left(k^i_H = 0\right)$. The blue bars show the case of attempting improved Gao's Forgery when operator H is used in the quantum encryption scheme $\left(k^i_H = 1\right)$. P_c is the coincidence probability. The black bars indicate the standard deviation of the coincidence counts for 1 s. k^i_{AB} is the same as in Figure 1. $e_i \in \{00, 01, 10, 11\}$ corresponds to the Pauli operator $\sigma_{e_i} \in \{I, \sigma_x, \sigma_y, \sigma_z\}$ that Eve uses to attempt Gao's Forgery 1.

5. Conclusions and Discussion

We have proposed a new quantum message authentication protocol including quantum encryption for improving security against an existential forgery. Additionally, a practical implementation of the proposed protocol has been developed and its robustness against existential forgery has been verified experimentally. It consists of wave plates and the Hong–Ou–Mandel interferometer. The measurement results for each function—QMAC generation and recovery, Bob's encryption and decryption, and quantum encryption and decryption—successfully show the feasibility of robustness against Gao's forgeries.

The system loss and the optical channel loss, etc., should be considered when applying our protocol to real implementation. Let us assume that Alice and Bob use the single photon detector with 20% efficiency and are connected by 30-km single-mode fiber with 0.2 dB/km loss. In a result, the total efficiency becomes 0.08% because the qubits are pass through total 100 km, and if the QMAC pairs are generated at 100 MHz, Bob can receive 8×10^4 pairs/s. As we mentioned in Section 2, the size of the quantum state sequence should be more than 15. Therefore, Alice must generate at least 1.9×10^4 QMAC pairs, i.e., $\left(1.9 \times 10^4\right) \times 0.08\% = 15$ that is quite implementable number, and send them to Bob to ensure this accuracy of the swap test.

Our protocol can be used as an arbitrated quantum signature protocol if a trusted center (TC) is added in the communication channel used by Alice and Bob [19]. In addition, if freshness property is added to our protocol, it can be used for quantum entity authentication as well [1,52]. In conclusion, we have proposed the base technology for a complete quantum cryptosystem that provides confidentiality, authentication, integrity, and nonrepudiation.

Author Contributions: M.-S.K. conceived the main idea. M.-S.K. wrote the manuscript. M.-S.K. and Y.-S.K. developed the experimental setup and performed the experiment. M.-S.K., Y.-S.K., J.-W.C., H.-J.Y. and S.-W.H. analyzed the results. S.-W.H. supervised the whole project. All authors reviewed the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: Korea Institute of Science and Technology (2E30620); National Research Foundation of Korea (2019 M3E4A107866011, 2019M3E4A1079777, 2019R1A2C2 006381); Institute for Information and Communications Technology Promotion (2020-0-00947, 2020-0-00972).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Menezes, A.J.; Van Oorschot, P.C.; Vanstone, S.A. *Handbook of Applied Cryptography*; CRC Press: Boca Raton, FL, USA, 1997.
2. Stinson, D.R. *Cryptography*; Chapman & Hall/CRC: Boca Raton, FL, USA, 2006.
3. Bennett, C.H. Quantum crytography. In Proceedings of the International Conference on Computers, Systems & Signal Processing, Bangalore, India, 10–12 December 1984; pp. 175–179.
4. Bennett, C.H. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **1992**, *68*, 3121–3124. [CrossRef]
5. Fuchs, C.A.; Gisin, N.; Griffiths, R.B.; Niu, C.-S.; Peres, A. Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy. *Phys. Rev. A* **1997**, *56*, 1163. [CrossRef]
6. Scarani, V.; Acin, A.; Ribordy, G.; Gisin, N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.* **2004**, *92*, 057901. [CrossRef]
7. Brassard, G.; Crépeau, C. 25 years of quantum cryptography. *ACM Sigact News* **1996**, *27*, 13–24. [CrossRef]
8. Lo, H.K.; Chau, H.F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **1999**, *283*, 2050–2056. [CrossRef] [PubMed]
9. Shor, P.W.; Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **2000**, *85*, 441–444. [CrossRef]
10. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145. [CrossRef]
11. Curty, M.; Santos, D.J. Quantum authentication of classical messages. *Phys. Rev. A* **2001**, *64*. [CrossRef]
12. Barnum, H.; Crépeau, C.; Gottesman, D.; Smith, A.; Tapp, A. Authentication of quantum messages. In Proceedings of the 43rd Annual IEEE Symposium on the Foundations of Computer Science, Vancouver, BC, Canada, 19 November 2002; pp. 449–458.
13. Kang, M.S.; Choi, Y.H.; Kim, Y.S.; Cho, Y.W.; Lee, S.Y.; Han, S.W.; Moon, S. Quantum message authentication scheme based on remote state preparation. *Phys. Scr.* **2018**, *93*. [CrossRef]
14. Zeng, G.; Keitel, C.H. Arbitrated quantum-signature scheme. *Phys. Rev. A* **2002**, *65*, 042312. [CrossRef]
15. Lee, H.; Hong, C.; Kim, H.; Lim, J.; Yang, H.J. Arbitrated quantum signature scheme with message recovery. *Phys. Lett. A* **2004**, *321*, 295–300. [CrossRef]
16. Li, Q.; Chan, W.; Long, D.-Y. Arbitrated quantum signature scheme using Bell states. *Phys. Rev. A* **2009**, *79*, 054307. [CrossRef]
17. Zou, X.; Qiu, D. Security analysis and improvements of arbitrated quantum signature schemes. *Phys. Rev. A* **2010**, *82*, 042325. [CrossRef]
18. Yoon, C.S.; Kang, M.S.; Lim, J.I.; Yang, H.J. Quantum signature scheme based on a quantum search algorithm. *Phys. Scr.* **2014**, *90*, 015103. [CrossRef]
19. 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*, 614–629. [CrossRef]
20. Gottesman, D.; Chuang, I. Quantum digital signatures. *arXiv* **2001**, arXiv:quant-ph/0105032.
21. Clarke, P.J.; Collins, R.J.; Dunjko, V.; Andersson, E.; Jeffers, J.; Buller, G.S. Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light. *Nat. Commun.* **2012**, *3*. [CrossRef] [PubMed]
22. Collins, R.J.; Donaldson, R.J.; Dunjko, V.; Wallden, P.; Clarke, P.J.; Andersson, E.; Jeffers, J.; Buller, G.S. Realization of Quantum Digital Signatures without the Requirement of Quantum Memory. *Phys. Rev. Lett.* **2014**, *113*. [CrossRef] [PubMed]
23. Dunjko, V.; Wallden, P.; Andersson, E. Quantum Digital Signatures without Quantum Memory. *Phys. Rev. Lett.* **2014**, *112*. [CrossRef]
24. Wallden, P.; Dunjko, V.; Kent, A.; Andersson, E. Quantum digital signatures with quantum-key-distribution components. *Phys. Rev. A* **2015**, *91*. [CrossRef]
25. Amiri, R.; Wallden, P.; Kent, A.; Andersson, E. Secure quantum signatures using insecure quantum channels. *Phys. Rev. A* **2016**, *93*. [CrossRef]
26. Donaldson, R.J.; Collins, R.J.; Kleczkowska, K.; Amiri, R.; Wallden, P.; Dunjko, V.; Jeffers, J.; Andersson, E.; Buller, G.S. Experimental demonstration of kilometer-range quantum digital signatures. *Phys. Rev. A* **2016**, *93*. [CrossRef]
27. Yin, H.L.; Fu, Y.; Chen, Z.B. Practical quantum digital signature. *Phys. Rev. A* **2016**, *93*. [CrossRef]
28. Collins, R.J.; Amiri, R.; Fujiwara, M.; Honjo, T.; Shimizu, K.; Tamaki, K.; Takeoka, M.; Sasaki, M.; Andersson, E.; Buller, G.S. Experimental demonstration of quantum digital signatures over 43 dB channel loss using differential phase shift quantum key distribution. *Sci. Rep.* **2017**, *7*. [CrossRef]
29. Yin, H.L.; Fu, Y.; Liu, H.; Tang, Q.J.; Wang, J.; You, L.X.; Zhang, W.J.; Chen, S.J.; Wang, Z.; Zhang, Q.; et al. Experimental quantum digital signature over 102 km. *Phys. Rev. A* **2017**, *95*. [CrossRef]
30. Chan, K.W.C.; El Rifai, M.; Verma, P.; Kak, S.; Chen, Y. Multi-photon quantum key distribution based on double-lock encryption. In Proceedings of the CLEO: QELS_Fundamental Science, San Jose, CA, USA, 10–15 May 2015; p. FF1A.3.
31. Kak, S. A three-stage quantum cryptography protocol. *Found. Phys. Lett.* **2006**, *19*, 293–296. [CrossRef]

32. Nikolopoulos, G.M. Applications of single-qubit rotations in quantum public-key cryptography. *Phys. Rev. A* **2008**, *77*, 032348. [CrossRef]
33. Yang, L.; Wu, L.-A.; Liu, S. Quantum three-pass cryptography protocol. In Proceedings of the Quantum Optics in Computing and Communications, Shanghai, China, 13 September 2002; pp. 106–112.
34. 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*. [CrossRef]
35. Massey, J.L.; Omura, J.K. Method and Apparatus for Maintaining the Privacy of Digital Messages Conveyed by Public Transmission. US4567600A, 28 January 1986.
36. Clarke, R.B.M.; Kendon, V.M.; Chefles, A.; Barnett, S.M.; Riis, E.; Sasaki, M. Experimental realization of optimal detection strategies for overcomplete states. *Phys. Rev. A* **2001**, *64*. [CrossRef]
37. Hecht, E.J.I. *Optics*, 4th ed.; Addison-Wesley: San Francisco, CA, USA, 2002; Volume 3, p. 2.
38. Horn, R.T.; Babichev, S.; Marzlin, K.-P.; Lvovsky, A.; Sanders, B.C. Single-qubit optical quantum fingerprinting. *Phys. Rev. Lett.* **2005**, *95*, 150502. [CrossRef]
39. Massar, S. Quantum fingerprinting with a single particle. *Phys. Rev. A* **2005**, *71*, 012310. [CrossRef]
40. Garcia-Escartin, J.C.; Chamorro-Posada, P. Swap test and Hong-Ou-Mandel effect are equivalent. *Phys. Rev. A* **2013**, *87*, 052330. [CrossRef]
41. Curty, M.; Lutkenhaus, N. Comment on "arbitrated quantum-signature scheme". *Phys. Rev. A* **2008**, *77*. [CrossRef]
42. Zeng, G.H. Reply to "Comment on 'Arbitrated quantum-signature scheme'". *Phys. Rev. A* **2008**, *78*. [CrossRef]
43. Riebe, M.; Haffner, H.; Roos, C.F.; Hansel, W.; Benhelm, J.; Lancaster, G.P.T.; Korber, T.W.; Becher, C.; Schmidt-Kaler, F.; James, D.F.V.; et al. Deterministic quantum teleportation with atoms. *Nature* **2004**, *429*, 734–737. [CrossRef] [PubMed]
44. Nielsen, M.A.; Chuang, I.L. *Quantum Computation and Quantum Information*; Cambridge University Press: Cambridge, UK, 2000.
45. Buhrman, H.; Cleve, R.; Watrous, J.; de Wolf, R. Quantum fingerprinting. *Phys. Rev. Lett.* **2001**, *87*. [CrossRef] [PubMed]
46. Gao, F.; Qin, S.J.; Guo, F.Z.; Wen, Q.Y. Cryptanalysis of the arbitrated quantum signature protocols. *Phys. Rev. A* **2011**, *84*. [CrossRef]
47. Choi, J.W.; Chang, K.Y.; Hong, D. Security problem on arbitrated quantum signature schemes. *Phys. Rev. A* **2011**, *84*. [CrossRef]
48. Kang, M.S.; Hong, C.H.; Heo, J.; Lim, J.I.; Yang, H.J. Comment on "Quantum Signature Scheme with Weak Arbitrator". *Int. J. Theor. Phys.* **2014**, *53*, 1862–1866. [CrossRef]
49. Zhang, K.J.; Qin, S.J.; Sun, Y.; Song, T.T.; Su, Q. Reexamination of arbitrated quantum signature: The impossible and the possible. *Quantum Inf. Process.* **2013**, *12*, 3127–3141. [CrossRef]
50. Zhang, K.-J.; Zhang, W.-W.; Li, D. Improving the security of arbitrated quantum signature against the forgery attack. *Quantum Inf. Process.* **2013**, *12*, 2655–2669. [CrossRef]
51. Ono, T.; Okamoto, R.; Tanida, M.; Hofmann, H.F.; Takeuchi, S. Implementation of a quantum controlled-SWAP gate with photonic circuits. *Sci. Rep.* **2017**, *7*. [CrossRef] [PubMed]
52. Hong, C.H.; Heo, J.; Jang, J.G.; Kwon, D. Quantum identity authentication with single photon. *Quantum Inf. Process.* **2017**, *16*. [CrossRef]