Multi-Stage Quantum Secure Direct Communication Using Secure Shared Authentication Key

Nur Ziadah Harun ^{1,2}, Zuriati Ahmad Zukarnain ^{1,*}, Zurina Mohd Hanapi ¹ and Idawaty Ahmad ¹

¹ Faculty of Computer Science and Information Technology, University Putra Malaysia, Serdang 43400, Selangor, Malaysia; GS46865@student.upm.edu.my (N.Z.H.); zurinamh@upm.edu.my (Z.M.H.); idawaty@upm.edu.my (I.A.)

² Department of Information Security and Web Technology, Faculty of Computer Science and Information Technology, University Tun Hussein Onn Malaysia, Parit Raja 86400, Malaysia

* Correspondence: zuriati@upm.edu.my

Received: 29 July 2020; Accepted: 22 August 2020; Published: 9 September 2020

Abstract: The security of Quantum Secure Direct Communication (QSDC) and its authentication procedure based on multiple stages is analyzed. The security analysis shows that the process of authentication is required to be done three times based on the usage of unitary transformation that is only known between Alice and Bob. In the proposed protocol, a secure quantum handshake is utilized to share the secret polarization angle and an authentication key at the initial stage of authentication over the quantum channel. The symmetry key is used in this work to protect user data communication within the QSDC protocol, where the same secret key is used to encrypt and decrypt the message. This work adopts the information travel time (ITT) by allowing the sender to detect any interference from third parties. In addition, the operation of the Pauli-X quantum gate increases Eve's difficulty in stealing the information. The information transmitted is then continued by sending photons once in the quantum channel, which improves the efficiency without losing the message's security. In addition, to securely transfer the stream of messages, the proposed protocol is operated in single-stage, and the authentication is applied bit-by-bit, thus reducing the transmission time. Security checks are carried out along the data transmission process. Compared to previous protocols, this new initial authentication protocol has remarkable advantages since it does not require public communication to pre-share the authentication key and secret angles before the onset of the transmission, therefore, reducing the communication cost. Moreover, the secret authentication key and polarization angles are updated after a number of bits are sent to increase the security level. The verification process is also conducted to ensure the symmetry of the sender and receiver. The analyses presented herein demonstrate that the proposed authentication protocol is simple and secure in order to ensure the legitimacy of the users.

Keywords: authentication key; half-wave plate; superposition state; unitary transformation

1. Introduction

Quantum Secure Direct Communication (QSDC) protocol is one of the quantum cryptography concepts that securely transmits the message directly in the quantum channel, where all the information deals with the quantum state. QSDC promotes a high level of protocol security by instantly transmitting the message directly to the quantum channel. Long and Liu introduced the first QSDC protocol in 2002, which securely and directly transmitted the secret message without using a key in advanced [1]. The modified version of the basic QSDC protocol has been introduced, which are (Einstein–Podolsky–Rosen) EPR QSDC [2] and single-photon QSDC. EPR QSDC utilized the block of

EPR pairs as carriers to directly transmit information, while single photon QSDC combined a one-time pad protocol with the secret message [3].

The security requirement in QSDC is stricter compared to Quantum Key Distribution (QKD) since an eavesdropper must not uncover the transmitted messages. Like QKD, QSDC is divided into three approaches: Quantum entanglement [4], single-photon [5,6], and multiple photons [7]. All of the QSDC protocols consist of four parts: Authentication, encoding, the transformation of quantum properties, and decoding, as illustrated in Figure 1. QSDC starts with the authentication process to verify the identity of Alice and Bob. After the successful authentication process, Alice embeds the sensitive information using the proposed QSDC encoding procedure and sends the secret message over the quantum channel. To encode the information, various properties of photons can be employed such as phase, polarization, EPR quantum correlation pairs, wavelength, or quadrature components of squeezed state of light [8]. Bob will then retrieve the contents of the secret message through the proposed decoding process.

Figure 1. The framework of general Quantum Secure Direct Communication (QSDC) protocol.

One of the biggest limitations of QSDC is the low transfer rate in the long-distance quantum channel [7,9]. To overcome this limitation, a concept of multi-photon was proposed by Subhash Kak [10], namely the three-stage protocol that can directly share the message over the multi-stages of the quantum channel using a rotational change in polarization. The multi-photon provides security features without the involvement of the key distribution step, and no entanglement is required. In the multi-photon protocol, photons act as the carrier to carry the quantum information by polarizing their quantum properties, i.e., $|0\rangle$ and $|1\rangle$.

Given the advantages of multi-photon QSDC, it remains a challenge to enforce QSDC authentication on behalf of each entity. Throughout quantum communication, a good authentication component is essential to ensure the legitimacy of users. Moreover, the participants in the communication must be authenticated to secure the transmitted message from the man-in-the-middle (MITM) attack [11,12]. The problem of today's authentication is the complex environment of networks. A network administrator, therefore, finds it very difficult to apply a consistent set of authentication, quality of service, and security schemes that are safe from security breaches and comply with regulations [13].

Unlike our previous work [14] that focused on increasing the transmission rates by reducing the transmission time in multi-photon over multi-stage protocol, here, the issue of authentication is focused. The aim of this paper is, therefore, to recommend a secure way to share the initial secret angle and authentication key between users over a multi-stage quantum channel. In this work, the symmetry key is applied to secure the user's data communications in QSDC protocol, where the same secret key is used to encrypt and decrypt the message. Therefore, the secret key must be exchanged securely over the communication channel, thus that the sender and receiver are symmetry on both sides. To solve the problem of initial communication in the authentication phase, a quantum handshake protocol is proposed to share Alice's secret angle and the authentication key [15]. In addition, an update function of the secret angle and the authentication key is proposed based on a mutually agreed algorithm.

The proposed protocol in this paper sends multi-photon over the single-stage and implements bit-by-bit authentication to defend against a MITM attack. It should be noted that Alice is a trusted party that does not mislead the information. This protocol will significantly improve the existing multi-photon works of references [7,9] that need to share the secret angle at the onset of the transmission over the secret channel. This protocol significantly improves communication efficiency without losing security. The main contributions of this work are as follows:

- (1) The secret angle and authentication key are generated by Alice, and no third party is involved in the process to enhance the confidentiality of the communication. Thus, no pre-shared authentication key and initial secret angle are exchanged between Alice and Bob at the onset of the communication, which occurs in public channels.
- (2) The secret angles and the authentication key are updated using a mutually agreed algorithm after a number of bits sent to increase the security level.
- (3) The QSDC protocol is operated in single-stage, and the authentication is applied bit-by-bit, thus reducing the transmission time, and the security check is done along with the data transmission process.

The remainder of this paper is organized as follows. In Section 2, the importance of the authentication procedure in QSDC is discussed. Related works are presented in Section 3, while Section 4 presents the secure shared authentication key protocol. Section 5 shows the example of the proposed protocol. Section 6 discusses the performance analysis, while Section 7 provides the implementation issues of the proposed protocol. Finally, the conclusion of this paper is summarized in Section 8.

2. The Importance of Authentication for QSDC

The authentication procedure is significant to avoid the legitimate parties' identities being impersonated by an eavesdropper that contributes to the leak of secret messages. In order to avoid eavesdroppers' attacks, existing quantum cryptography protocols typically require a third-party authentication for Alice and Bob to initiate the communication. However, some drawbacks may occur when a third party is involved in the communication. Third-party authentication is typically based on the classical cryptography assumptions that utilize computational complexity. Another problem noted is Eve can still attack the quantum communication channels after Alice and Bob are authenticated to circumvent the third party authentication, leaving such attack undetected as revealed in reference [16]. This type of attack is called the Intercept-Resend attack, which will be discussed later in this paper.

Thus, to overcome the aforementioned problem, the authentication process should be performed during the quantum data communication process. It is important to ensure that the parties involved in the protocol are whom they are supposed to be; this is what we call identity authentication. In addition, the data origin authentication can be done on a bit-by-bit basis to eliminate the possibility that Eve attacks the quantum channel after Alice and Bob are authenticated. This step is important to ensure that the data originate from the right sender and is received by the right receiver. The important part of the authentication is to share the authentication key between Alice and Bob to allow the recognition process [16]. The authentication key is important to avoid a MITM attack launched by Eve, who is pretending to be Alice and Bob at the same time. The authentication key must not be revealed to Eve and needs to be shared secretly between Alice and Bob before the process of authentication has started. This process is done in the initial part of the authentication by sharing the sender's secret angle and the authentication key since pre-shared is not suitable to be adapted because it deals with the public channel.

In quantum communication, it is essential to reduce the level of complexity and, at the same time, maintain the security of the system against eavesdropping attacks. However, a direct link between Alice and Bob will significantly be affected where an eavesdropper can overhear, jam, or spoof the communication between them [17]. Recent work by [18] showed that an eavesdropper might span into multiple smart attackers that can overhear the secure message depending on their location

between the transmitter and the receiver. In addition, the investigation by reference [19] proved that an attacker might use several transmitter antennas to increase the attack rate. It can be concluded that the eavesdroppers can utilize various types of attacks to intercept secret messages. Thus, the improvement of data and transmission secrecy is an urgent issue to be solved in the communication area.

3. Related Works

In the last few years, several authentication protocols for multiphoton QSDC have been proposed. The main objective of those approaches was to ensure that the messages are delivered securely to the legitimate parties. This section reviews several multiphoton QSDC's authentication approaches over multi-stage to validate the parties involved in quantum communication, discussing their basic concepts, and describing their advantages and drawbacks.

In reference [20], a single-stage protocol was proposed to transmit the photon in a stage using secret unitary transformation. The security strength of this protocol relies on the secret value of the polarization angle, θ , and it must be secret along with the communication between Alice and Bob. Otherwise, the security of this protocol cannot be compromised anymore when the eavesdropper is able to get the value of θ . This protocol assumes that there is another protocol operated, such as a trusted certificate exchanged before the secure transmission begins. The authors in [9] presented a secure quantum communication over a single-stage, hereafter called it a Braided Single Stage protocol. The idea of Braided Single Stage protocol is to overcome the drawback of the three-stage protocol by reducing the overhead to encode the photons. Later, the IV Three-stage protocol [7] was proposed based on the adoption of an Initialization Vector (IV) to be a one-time pad key as the extra dimension of security for the three-stage protocol.

All of the mentioned approaches utilized the three-stage protocol to handle the authentication process in the first phase by sharing the initial value of secret polarization angle θ (e.g., 0° , 25° , 50° , ..., 180°) that is predetermined among users. The set is usually exchanged via a secret channel [21,22] over the public channel or using face to face communication. However, the technique of exchanging the secret angle is omitted. Besides, the reviewed multi-photon approaches only assumed that the sender and receiver to be mutually trusted parties, and they are already authenticated to each other [7,23]. The usage of the authentication key that is only known by legal parties is able to provide secrecy in the authentication of QSDC [16,24,25]. Hence, combining the unitary transformation with the authentication key has become an appropriate strategy to construct high-level security of the cryptographic protocol. Therefore, an important question in this research is how to share the secret angle and authentication key securely in the quantum channel? Most of the authentication schemes are based on pre-shared secret information, which is not so practical for the initial communication of trusted parties [15]. To mitigate these issues, a secure shared authentication key (SSAK) is proposed in this paper. The SSAK protocol shares the secret angle and authentication key using the quantum handshake mechanism. The main objective of the proposed SSAK protocol is to improve the efficiency of authentication and reduce the communication cost by avoiding public channel usage.

4. Secure Shared Authentication Key (SSAK) Protocol

This section presents the proposed SSAK protocol. The SSAK protocol focuses on the idea of sharing a secret angle and an authentication key between Alice and Bob over a multi-stage quantum channel. In the proposed protocol, an Information Travel Time (ITT) or Time Stamp technique associated with the data [26] is adopted to detect the presence of eavesdroppers in the initial authentication procedure. In the condition, Eve is located midway between Alice and Bob, the ITT is obviously different due to the fact that the distances between Alice and Bob are greater than the distance between Alice and Eve as well as Eve and Bob. However, in the case of Eve located far away from Alice and Bob, the ITT would be doubled and shows a sign of eavesdroppers' attack. Thus, when quantum particles pass through optical polarization devices on the sender's site, and an eavesdropper is present in the communication to read the photon, the response by the receiver might induce abnormal timing

information. Moreover, this work utilizes the Pauli-X quantum gate to increase the difficulty for Eve to steal the information. Theoretically, a wire of transmission carries a qubit of information, and the quantum gate will take that qubit as an input. Here, the function of the quantum gate is to perform the unitary transformation on this qubit and produce a new state of qubit as an output. Pauli-X gate is also known as a bit flip operator that is responsible for altering the qubit state by flipping bit 0 to 1 and vice versa. Based on previous research, the quantum gate provides many benefits such as being easy-to-use as the information related to the operators is not necessarily shared between the parties, has less precision requirement compared to in arbitrary rotation such as half-wave plate (HWP), and provides accurate measurement [27].

The details of the proposed protocol can be described in three phases: Initial authentication, secure message sharing, and security checking. Figure 2 shows the whole process of the proposed SSAK protocol.

Figure 2. Procedure of the secure shared authentication key (SSAK) protocol.

4.1. Initial Authentication Procedure

Alice is the party that supposedly sends a message to Bob. For Alice, it is extremely important to ensure the messages are only received by the authenticated user who is Bob. However, Bob faces difficulties when he receives the message; he does not know whether it comes from Alice or an eavesdropper. The initial part of authentication is important to verify the party that initiates the communication. Therefore, in this paper, a novel quantum handshake for sharing initial secret angle and authentication key, which is utilized before the quantum communication session is proposed. The objective of the proposed protocol is to allow Alice to identify herself to Bob and Bob can prove that Alice is a legitimate party. Note that operator $E_K[\cdot]$ and $D_K[\cdot]$ operators in Figure 2 are defined as encrypt and decrypt operations with key K .

The steps of the proposed protocol are discussed below:

1. First item, Alice prepares a private orthogonal state ψ_0 and generates a random quantum state θ_A using a random number generator. Based on the decimal value of θ_A , she prepares five binary digits and do Pauli-X quantum gate operation to produce θ_A' . She then encrypts θ_A with ψ_0 to produce the quantum state ψ_1 . The *TimeStamp* is set to $t_A(1) = 0$.
2. Second item, Bob generates a random quantum state θ_B using a random number generator and encrypts it with the received quantum state ψ_1 and produces ψ_2 . The *TimeStamp* is set to $t_B(1) = 2$.
3. Third item, Alice decrypts the received ψ_2 with $(-\theta_A)$ to generate ψ_3 and sends it back to Bob. At this stage, Alice is able to extract θ_B . Alice will verify the *TimeStamp* after she gets the photon replied by Bob. Alice starts to analyze the difference between the sending and receiving time. If Alice gets *TimeStamp* $\neq 4$, an eavesdropper is detected and she will terminate the communication. Otherwise, the communication will be continued. Then, the *TimeStamp* is set to 4.
4. Bob applies $(-\theta_B)$ to obtain the ψ_0 and successfully extracted ψ_0 . Bob gets the value of θ_A and converts it into five binary digits. He then does the Pauli-X quantum gate operation to generate new value of θ_B . Next, he encrypts it with the received quantum state ψ_0 to produce quantum state ψ_4 and sends it to Alice.
5. Alice authenticates Bob by comparing and analysing θ_B using measurement. If the value is correct, she will then send the authentication key $\Phi_{initial}$ that is generated using a random number generator. The $\Phi_{initial}$ is then encrypted with the θ_B that she had extracted in step 3 to produce ψ_5 and passed it back to Bob. If the value is different, the communication will be terminated and needs to be restarted.
6. Bob couples the receiving ψ_5 with $(-\theta_B)$, to get the authentication key Φ .

After the authentication is successfully completed, Alice will start to convert the string of bit message into the photons and directly sends it to Bob using the initial secret polarization angle ($\theta_{initial}$) and authentication key ($\Phi_{initial}$).

4.2. Secure Message Sharing Procedure

It is assumed that Alice and Bob have the same secret angle and authentication key that they shared in the initial stage of authentication in Section 4.1. Suppose that Alice's secret message X is a series of classical bit of 0 and 1 in order, $X(x_i, x_{i+1} \dots x_n)$.

1. Alice encrypts her secret message x_i by generating a state with a linear polarization using a 0° polarizer as bit 0 or using 90° polarizer as bit 1 to get θ_X .
2. Quantum state θ_X is then coupled with initial θ_A and sent along with the initial authentication key Φ by Alice. The combination of θ_X , θ_A and Φ generates ψ_A are sent to Bob.
3. Bob receives the quantum state ψ_A and couples it with $(-\theta_A)$ and $(-\Phi)$ obtains information X_i .
4. Alice and Bob frame the received bits and convert the last n bits to integer value N , given by

$$N = \sum_{i=k-n+1}^k b_i \times 2^i \quad (1)$$

where k is the number of transmitted keys, b is the sequence of the transmitted bits (i.e., the bits $b_{k-n+1}, \dots, b_k$) using the last n bits to generate the new angle θ .

5. Alice and Bob compute new value of θ and Φ , given by

$$\theta_{Next} = \frac{N\pi}{2^k} + \theta_{initial} \quad (2)$$

$$\Phi_{Next} = \frac{N\pi}{2^k} + \Phi_{initial} \quad (3)$$

4.3. Security Checking Procedure

Alice and Bob will check the authenticity between them by performing a measurement. By doing so, if there is no eavesdropper, Alice will be ensured that she received the same value as Bob, given by

$$(\theta_{Next} \cdot \Phi_{Next}) \times (-\theta_{Next} - \Phi_{Next}) = I \quad (4)$$

where “ $\cdot$ ” is the multiplication operator and I is the identity matrix. If there is an eavesdropper, in the case of Alice’s result is not the same with Bob, then Alice will announce to Bob to abort the communication, where

$$(\theta_{Next} \cdot \Phi_{Next}) \times (-\theta_{Next} - \Phi_{Next}) \neq I \quad (5)$$

5. Example of the Proposed Protocol

Let us illustrate an example of the proposed protocol and describe the three parts of secure QSDC, which is the initial authentication procedure, message sharing procedure, and security phase procedure. The implementation of proposed SSAK has been tested using a simulation developed via Python programming language. Python is chosen due to its capabilities to simulate the quantum state in superposition via mathematical form. The pseudo-code of SSAK protocol is detailed in Algorithm 1.

5.1. Initial Authentication Procedure

The initial authentication procedure is explained as follows:

1. Suppose that Alice prepares a photon $\psi_0 = |0\rangle$ and generates a random secret angle, $\theta_A = 1^\circ$. Based on the decimal value of θ_A , she converts it into binary digits $|00001\rangle$ and employs Pauli-X quantum gate operation to produce $|11110\rangle$. She converts it back to decimal value, $\theta_A' = 30^\circ$. The new value will be used as the security check for the next procedure. She starts to encrypt $X = |0\rangle$ using θ_A and produce quantum state ψ_1 . The *TimeStamp* is set to $t_A(1) = 0$.
2. Bob generates a random secret angle $\theta_B = 15^\circ$ and encrypts it with the received quantum state ψ_1 and produces ψ_2 . The *TimeStamp* is set to $t_B(1) = 2$.
3. Alice decrypts the received ψ_2 with $-\theta_A$ to generate ψ_3 and sends it back to Bob. At this stage, Alice gets $\theta_B = 15^\circ$. Alice will verify the *TimeStamp* = 4 after she gets the photon replied by Bob. If Alice gets the *TimeStamp* $\neq 4$, an eavesdropper is detected, and she will terminate the communication. Otherwise, the communication will be continued. The *TimeStamp* is set to $t_A(2) = 4$.
4. Bob applies $-\theta_B$ to obtain $\psi_0 = |0\rangle$. He gets the value of $\theta_A = 1^\circ$ and converts it into the binary digits $|00001\rangle$. Using the Pauli-X quantum gate, he gets $|11110\rangle$, and he converts it back into decimal value and generates $\theta_B = 30^\circ$. He then encrypts it with the received quantum state $\psi_0 = |0\rangle$ to produce quantum state ψ_4 and sends it to Alice. The *TimeStamp* is set to $t_B(2) = 6$.
5. Alice authenticates Bob by comparing and analyzing θ_B using measurement. If $\theta_B = \theta_A'$, she sends the initial authentication key $\Phi_{initial} = 20^\circ$ that is generated using a random number generator and encrypts it with $\theta_B = 30^\circ$. If $\theta_B \neq \theta_A'$, the communication will be terminated and need to be restarted.
6. Finally, Bob couples the receiving ψ_5 with $\theta_B = 30^\circ$ to get the authentication key $\Phi_{initial}$.
7. It can be concluded that the security of the proposed scheme depends entirely on the initial authentication procedure, where the eavesdropping check and identity authentication are implemented at the same time.

5.2. Message Sharing Procedure

In this section, the implementation of SSAK protocol over free space optics using passive optical components is discussed. Figure 3 shows the setup of the implementation.

Figure 3. Implementation of secure shared authentication key protocol over Free Space Optic (FSO).

Alice will have three half-wave plates (HWPs) in her possession while Bob will have two HWPs. A linearly polarized laser is used as the photon source in our implementation [28]. At the beginning of the protocol, Alice generates a state with a 0° linear polarization using a 0° polarizer. The polarization procedure is to encrypt the classical bits using the photons to produce the quantum bit (qubit). After the classical bits are encrypted to the photons, she will apply a transformation using HWP-1 at the angle θ and apply her second HWP-2 at angle θ_A , which results in the superposition state, $|\psi\rangle$. The superposition states carry the secret message that will be shared between Alice and Bob in quantum manners [27]. The rotation of HWP operation is represented as

$$M_{HWP}(\theta) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos(4\theta) & \sin(4\theta) & 0 \\ 0 & \sin(4\theta) & -\cos(4\theta) & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \quad (6)$$

where

$$0^\circ < \theta < 45^\circ \quad (7)$$

It is noted that HWP-1 at the angle θ is the authentication key set from 0° to 45° , coupled with information X to make the protocol more secure. Alice then applies the transformation associated with the encoded bit using HWP-3 that will be set at an angle $\theta_X = 0^\circ$ in the case of bit 0 being sent or $\theta_X = 45^\circ$ if bit 1 is being sent.

$$\begin{aligned} \text{Message } X &\Rightarrow \text{bits} \in \{0, 1\}^n \\ \{0, 1\}^n &\Rightarrow \begin{cases} |0\rangle, |S_{out} = M_{HWP}(0^\circ) \times S_{in} \\ |1\rangle, |S_{out} = M_{HWP}(45^\circ) \times S_{in} \end{cases} \end{aligned} \quad (8)$$

where S_{in} is the Stokes parameter's sequence of the input light that is illustrated as

$$S_{in} = \begin{bmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad (9)$$

while S_{out} is the Stokes parameter's sequence of the output light

$$S_{out} = \begin{bmatrix} S'_0 \\ S'_1 \\ S'_2 \\ S'_3 \end{bmatrix} \quad (10)$$

$$S_{out} = M_{HWP} \times S_{in} \quad (11)$$

The light polarization angle after passing through the HWP can be measured [28,29] by

$$\theta = \cos^{-1} \frac{S_{in}[1:3] \cdot S_{out}[1:3]}{\|S_{in}[1:3]\| \times \|S_{out}[1:3]\|} \quad (12)$$

where “ $\cdot$ ” is the multiplication operator and $\|\cdot\|$ is the norm operator.

Alice will send the optical beam containing the message to Bob, who will first pass it through his first HWP (HWP-4). Then he will remove his transformation using a HWP-5 sets at the angle θ_A . Bob will receive a beam polarizer at either 0° or 90° and pass it through a polarization beam splitter. The detectors will detect whether it is bit 0 or bit 1.

A basic description of the proposed protocol is discussed here. First, the message that is translated into the binary code is encrypted into a single particle called a quantum bit or qubit. The quantum bit is then transmitted from Alice to Bob using the proposed protocol as follows.

1. Suppose that Alice prepares a photon. Alice wants to send the first qubit, $|0\rangle$, the qubit is then encrypted to the photons using the first agreed angle from the first procedure, $\theta_A = 30^\circ$. Alice prepares photons based on Equation (9) and encrypts it using the rotation of HWP based on Equation (6).

$$\begin{aligned} \varphi_1 &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos(4(30)) & \sin(4(30)) & 0 \\ 0 & \sin(4(30)) & -\cos(4(30)) & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \times \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \\ &= \begin{bmatrix} 1 \\ -0.5 \\ 0.8660254 \\ 0 \end{bmatrix}. \end{aligned} \quad (13)$$

2. Alice encrypts the φ_1 with the authentication key, which is previously shared in the initial authentication procedure, $\Phi = 20^\circ$.

$$\begin{aligned} \varphi_2 &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos(4(20)) & \sin(4(20)) & 0 \\ 0 & \sin(4(20)) & -\cos(4(20)) & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \times \begin{bmatrix} 1 \\ -0.5 \\ 0.8660254 \\ 0 \end{bmatrix} \\ &= \begin{bmatrix} 1 \\ 0.76604444 \\ -0.64278761 \\ 0 \end{bmatrix}. \end{aligned} \quad (14)$$

3. Alice then applies the transformation associated with the encoded bit. In the case of bit 0 is being sent, the angle is set at $\theta_X = 0^\circ$ or $\theta_X = 45^\circ$ if bit 1 is being sent.

$$\begin{aligned}\varphi_3 &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos(4(0)) & \sin(4(0)) & 0 \\ 0 & \sin(4(0)) & -\cos(4(0)) & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0.76604444 \\ -0.64278761 \\ 0 \end{bmatrix} \\ &= \begin{bmatrix} 1 \\ 0.76604444 \\ 0.64278761 \\ 0 \end{bmatrix}.\end{aligned}\quad (15)$$

4. Bob receives φ_3 and decrypts it by rotating it back with the angle $-\theta_A$.

$$\begin{aligned}\varphi_4 &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos(4(-30)) & \sin(4(-30)) & 0 \\ 0 & \sin(4(-30)) & -\cos(4(-30)) & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \times \begin{bmatrix} 1 \\ 0.76604444 \\ 0.64278761 \\ 0 \end{bmatrix} \\ &= \begin{bmatrix} 1 \\ -0.5 \\ -0.8660254 \\ 0 \end{bmatrix}.\end{aligned}\quad (16)$$

5. Bob receives φ_4 and decrypts it by rotating it back using the angle of authentication key Φ_A . Bob receives the original message.

$$\begin{aligned}\varphi_5 &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos(4(-20)) & \sin(4(-20)) & 0 \\ 0 & \sin(4(-20)) & -\cos(4(-20)) & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \times \begin{bmatrix} 1 \\ -0.5 \\ -0.8660254 \\ 0 \end{bmatrix} \\ &= \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}.\end{aligned}\quad (17)$$

5.3. Security Check Procedure

After φ_5 is delivered successfully, the process continues with the remaining qubits using the same procedure. Alice and Bob will check the authenticity between them by comparing Alice's and Bob's secret rotations using Equation (4).

$$\begin{aligned}Auth_{AB} &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0.76604444 & -0.64278761 & 0 \\ 0 & 0.64278761 & 0.76604444 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0.76604444 & 0.64278761 & 0 \\ 0 & -0.64278761 & 0.76604444 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.\end{aligned}\quad (18)$$

Algorithm 1 SSAK protocol

```

1: Notation:
2:  $\text{TimeStamp} \leftarrow$  calibration using time synchronization/time stamp
3:  $\theta \leftarrow$  is the secret polarization angle
4:  $f(\text{Pauli}-X) \leftarrow$  is a function bit flip operator using Pauli-X gate
5: 1. Initialization authentication procedure
6:  $\varphi_{i...n} \leftarrow$  is the random string message of (0,1)
7:  $R(\theta) \leftarrow$  is the rotation of HWP using Equation (6)
8:  $|\varphi_{i...n}\rangle \leftarrow$  is the photon associate with  $\varphi_{i...n}$ 
9: Alice prepares a photon using Equation (8)
10: Alice converts the decimal of  $\theta$  into binary and does Pauli-X operation
11:  $\theta' \leftarrow f(\text{Pauli}-X)$ 
12: Alice initializes the authentication by sharing secret polarization
13:  $R(\theta_A)|\varphi_0\rangle = |\varphi_1\rangle$ 
14:  $\text{TimeStamp} = 0$ 
15:  $R(\theta_B)|\varphi_1\rangle = |\varphi_2\rangle$ 
16:  $\text{TimeStamp} = 2$ 
17:  $R(-\theta_A)|\varphi_2\rangle = |\varphi_3\rangle$ 
18:  $\text{TimeStamp} = 4$ 
19: if  $\text{TimeStamp} \neq 4$  then
20:     detect Eve and terminate communication
21: elif
22:      $R(-\theta_B)|\varphi_3\rangle = |\varphi_0\rangle$ 
23:      $\text{TimeStamp} = 6$ 
24: end if
25: Bob analyzed the result
26: Determine the value of  $\theta_A$  using Equation (12) and the corresponding bit
27:  $\theta_A' \leftarrow f(\text{Pauli}-X)$ 
28: Generate new  $\theta_B$ 
29:  $R(\theta_B)|\varphi_0\rangle = |\varphi_4\rangle$ 
30: Alice compares and analyses new  $\theta_B$  according to her previous calculation, verifies Bob and sends authentication key
31: Determine the new value of  $\theta_B$  using Equation (12) and the corresponding bit
32: if  $R(\theta_A') \neq R(\theta_B)$  then
33:     detect Eve and terminate communication
34: elif
35:     Alice sends authentication key using  $\theta_B$  to Bob
36:      $R(\theta_B)|\Phi\rangle = |\varphi_5\rangle$ 
37: end if
38: Bob gets authentication key
39:  $R(-\theta_B)|\varphi_5\rangle = |\Phi\rangle$ 
40: 2. Message sharing procedure of bit sequence, B
41:  $B \leftarrow$  A bit sequence
42:  $\text{len}(B) \leftarrow$  is the length of bit sequence B is set to 8 photons per block
43: Alice prepares photons based on Equation (8), encrypts it using  $\theta_A$  and  $\Phi$ .
44: Notation:
45:  $f(B, \theta, \Phi) \leftarrow$  is the function that returns the updated secret polarization angle and authentication key for every block of photon (8 photons per block)
46: for  $i$  ( $\theta, \Phi$ ) in enumerate ( $f(B, \theta, \Phi)$ ) do
47:     for  $j = 1$  in range  $B$  do
48:         Transmission of photon using single-stage
49:         if  $i * B + j \geq \text{len}(B)$  then
50:             break transmission;
51:         end if
52:     end for
53: end for
54: Alice and Bob checks for authenticity
55: if  $(\theta_A \cdot \Phi) \times (-\theta_A \cdot -\Phi) = I$  then
56:     Alice and Bob are authenticated
57: else
58:     detect Eve and terminate communication
59: end if

```

6. Performance Analysis

6.1. Mutual Authentication

It has been found that the authentication procedure in the IV Three-stage and Braided Single Stage protocol is unidirectional, which means that only Alice can authenticate Bob. In this work, a mutual authentication procedure is presented by applying the unitary transformation in the process of authentication. Mutual authentication between legal parties is necessary to avoid an eavesdropper stealing the secret message. Mutual authentication requires the parties to prove their identity with each other in the communication. Therefore, the mutually agreed algorithm of the authentication keys is changed every eight bits of transactions. The keys are updated based on every last n bit photons to prevent the message from leaking. The frequent change of the authentication key has helped to enhance the level of security, but a longer time is needed to change the polarization angle due to the limitations of the mechanical components [28].

As discussed in the previous section, the transformation needs to be commutative in which the rotation is only known to the parties that apply them [30]. Therefore, in the case where Alice and Bob are not mutually authenticated, Equation (5) is fulfilled, where $\theta_A \cdot \Phi$ is the polarization at Alice that acts as encryption angle, $-\theta_A \cdot -\Phi$ is the polarization at Bob that acts as decryption angle and I is the identity matrix, as shown in Equation (18). As shown in Figure 4, the sender and receiver authentication controllers provide an authentication function by the evaluation of information sent by both parties [16]. Besides, the controller also monitors the bit error rate of the received photons. For instance, Alice and Bob can check the legitimacy of each other by comparing their polarizations. If the result is not equal to I , the failed authentication alarm will be triggered, and the procedure would be stopped. The procedure needs to start over again.

Figure 4. The implementation of the sender and receiver side authentication controller.

6.2. Low Cost and Low Complexity

Table 1 shows that the previous protocols, IV Three-stage and Braided Single Stage, use the public channel to share the initial secret angle between Alice and Bob, therefore, making the secret angle vulnerable to attacks. The proposed protocol, on the other hand, uses the quantum channel to share the initial angle and the authentication key. Thus it is hard for the attacker to obtain the value since the quantum state is implemented from the beginning of the procedure. It makes the authentication of the users simpler without sharing the secret polarization angle and authentication key onset of the protocol. Similar to previous protocols, there is no need for a third party to verify the authentication in the proposed protocol. Despite the IV Three-stage protocol that used four variables [7] during the message sharing, the proposed authentication only consists of three variables, which are θ_X , θ_A , and Φ . It shows that the consumption of photonic devices is less compared to the previous protocols.

Table 1. Performance comparison between three-stage variants and proposed authentication protocol.

Protocol	IV Three-Stage	Braided Single Stage	Proposed Protocol
1. Public Communication (pre-shared angle)	Yes	Yes	No
2. Authentication key	Yes	No	Yes
3. No. of HWP for information exchange	7	5	5
4. Information exchange stage	3 times	1 times	1 times
5. Quantum communication complexity of authentication	$Q^*(f_I) = \Omega(3n + 3IV)$	$Q^*(f_I) = \Omega(3n)$	$Q(f_I) = 5n$

Instead of the classical authentication, which is based on the computational complexity of certain mathematical problems, quantum authentication utilizes quantum mechanics, which provides absolute security [15,16,31]. Thus, to evaluate the quantum authentication protocol, quantum communication complexity measurement was conducted. Quantum communication complexity can be defined as the amount of communications carried out between the parties to accomplish information distribution tasks [32]. The protocol that uses quantum and classical resources to authenticate users is denoted by $Q^*(f_I)$, while the protocol that fully uses quantum channel to authenticate users is denoted by $Q(f_I)$, where Q is the quantum communication complexity and f_I is the identity authentication [32,33]. It can be seen from Table 1 that the IV Three-stage and Braided Single Stage protocol require a classical channel (Ω) to share a set of polarization states predetermined amongst them for authentication functionalities [30]. For the IV Three-stage protocol, a three-stage transformation over the quantum channel (n) is required to perform the authentication process between the parties and to exchange the initialization vector that acts as an authentication key. Due to no authentication key in the Braided Single Stage [9], the three-stage transformation is only used for authentication tasks. Indeed, the proposed protocol does not need a predetermined polarization state before the effective authentication process starts. The secret polarization angle and authentication key can be shared in a fully quantum channel within five stages. It can be considered a good quantum authentication protocol if a minimum number of communications are held between parties. In order to make the authentication process more secure and efficient, classical communication is not necessary.

6.3. Security Analysis

Security analysis is the critical assessment standard for any quantum protocol to ensure that the proposed protocol is secure against any eavesdropper attacks. The security of the proposed QSDC authentication protocol relies not only on the quantum non-cloning theorem and the quantum uncertainty principle of the secret message to prevent an unconditional attack, but the quantum state is also applied to the authentication key that secures the messages. The security analysis is explained in detail herein.

6.3.1. Man-in-the-Middle Attack

Due to the two secret polarization angles, the attacker must know the value of θ_A and Φ at the same time. However, it is very difficult for the attacker to guess the exact value due to the secure handshake mechanism that has been conducted to share that value between Alice and Bob. If the Φ and the quantum states θ_X are exposed to Eve during transmission, she has no means to understand the value of Φ or X . Even if Alice sends multiple photons with the same polarization, Eve cannot obtain the useful information since different values of authentication keys are generated for each block of the bit transfer. Bob is able to decode the information X if he possesses the correct θ_A and Φ . Hence, Eve cannot pretend to be Alice or Bob if she does not know the authentication key. As shown in Figure 4, Alice and Bob will compare the bits to determine if a MITM attack has been launched. For example, Eve may disturb the message by interrupting the quantum channel several times, and this situation will lead to the re-initialization of the communication between the legitimate parties. If an interception

occurs, Alice and Bob will immediately detect it, and Eve will never get the original message. If the bit error rate is high, this means that Eve's attack has been started as the quantum states are disturbed. Thus, if the error rate is higher than the threshold, the transmission will be canceled. During the MITM attack, Eve will impersonate Alice and Bob to extract information. Eve does not know the value of θ_A and Φ to send a fake sequence of messages prepared by herself to Bob because Alice and Bob share the $\theta_{initial}$ and $\Phi_{initial}$ by utilizing a quantum handshake scheme. The possible cases on how the proposed protocol defends MITM attacks are discussed here.

- Case 1: Eve has no knowledge of the $\theta_{initial}$ or the $\Phi_{initial}$, thus she is incapable of getting anything about the secret message. Thus, the proposed protocol is secure against MITM attack. As stated in Section 5, Eve needs to guess 45 possibilities of angle for each qubit transmitted. Eve can predict the true angle for $\theta_{initial}$ and $\Phi_{initial}$ with the probability $p = \frac{1}{45} \times \frac{1}{45} = \frac{1}{2025}$.
- Case 2: Eve succeeds in guessing the $\theta_{initial}$. However, Eve does not get any useful information about the message since she does not know $\Phi_{initial}$.

In order to investigate the impact of Eve's information on the secret angles of the SSAK and the benchmark protocol, a random character from 5 to 25 with random message generation is selected. The messages are shared over the QSDC protocol. The simulations have been tested using Python programming language. Figure 5 shows an average of 30 simulation runs for each data point. The leakage angle in average, $Leak_{AB}$ can be calculated as:

$$Leak_{AB} = \frac{LeakAngle}{SecretAngle} \quad (19)$$

where $LeakAngle$ is the number of angles that are successfully recovered by Eve and $SecretAngle$ is the number of secret angles agreed by Alice and Bob.

Figure 5. The implementation of the sender and receiver side authentication controller.

As shown in Figure 5, the average covered angle by Eve is 0% in the proposed protocol. This means that Eve does not have any clue to guess the true angles, Φ and θ simultaneously. Therefore, Eve has completely no knowledge about the polarized photon that represents the message. However, in benchmark protocols (IV Three-stage and Braided Single Stage), as the number of bits increases, Eve still has chances to guess the secret angle by 2% on average. The line plotted in the graph shows the maximum average covered angles by Eve after 30 simulation runs for the benchmark protocol. It can be seen that Eve is able to guess up to 7% of the secret angles in the lowest number of characters shared.

6.3.2. Intercept/Resend Attack

After Alice encodes the photons, Eve attempts to steal the photons and substitutes them with fake photons prepared in advance. In the proposed SSAC protocol, Alice shares the secret θ and Φ securely with Bob that is only known to them. Eve cannot measure the intercepted photons correctly because she cannot know the right value of θ and Φ . Eve's ability to obtain useful information is limited because the quantum states are transmitted in the quantum mechanical property, which means that the states are the non-orthogonal. The authentication keys and polarization states of photons are used to generate the non-orthogonal quantum states. It shows that the security relies on the no-cloning theorem, which means no one can make a copy of any unknown non-orthogonal states. Besides, when Eve tries to measure the superposition states during the transformation phase, the result could be any non-orthogonal state. Thus, no information regarding the polarization angle is detected. Assuming that Eve managed to intercept the transmitted photons from Alice, Eve will resend the photons to Bob after doing a measurement. However, Eve cannot break the protocol because she does not know the polarization angles and authentication keys set by Alice and Bob. Let us assume that Alice transmits a quantum state of $|\varphi\rangle$, i.e., $|1\rangle$ in 45° polarization angle and encrypts it using the authentication key. Then, Eve tries to intercept them. Eve will fail to get the $|\varphi\rangle$ since she does not possess the secret polarization angle and the authentication key. In the proposed protocol, Eve needs to guess two secret angles in high precision. Eve can be detected if her polarization angle is not the same as Alice and Bob keys' possession. Since this protocol applies bit-by-bit authentication, Eve cannot spend a long time analyzing the statistics of a large number of photons that she gets during her attack, or she will be exposed. Consequently, Eve's attack can be exposed as Alice's and Bob's measurements on the fake bit are not identical to the original one. Moreover, Eve cannot gain any profit from this attack.

6.3.3. Beam Splitting Attack

In this attack, Eve will locate the beam splitter between Alice and Bob to collect the photons illegally. Without being detected at Bob, Eve will get the probability of 50% of the correct photons. However, this attack is not possible against the proposed protocol. Even if Eve is able to collect the fraction of the transmitted photons without being detected by Bob, it is very difficult to find the secret polarization angles since the angle will never be disclosed publicly. In addition, the angles of polarization will be updated after a number of photons using the mutually agreed secret algorithm to maintain the level of secrecy and to obtain unconditional security [7,28]. Apart from that, the newly updated keys will prevent information related to the keys and messages from being sniffed by an eavesdropper.

7. Implementation Issues of the Proposed Protocol

The security of the protocol proposed is based on how hard it is for an eavesdropper to construct the authentication key and secret angle that Alice and Bob exchange. Eve has to find Alice's secret information using a probability of up to $\frac{1}{2025}$ by intercepting their communications. The ease of implementation is one of the key factors in the design of QSDC. It can be observed that there are no entangled states, which are difficult to implement in the proposed protocol. The performance analysis showed that the proposed protocol is low-cost, and it can be implemented with today's technology using optical devices, as discussed in Section 4. As discussed in the literature, the proposed work intends to secure the information against an eavesdropper's attack. In the real implementation of the QSDC protocol, several practical issues need to be considered other than security issues. The practical issues that will impact the implementation of quantum communication are the noise and error in the quantum channel. Besides, photon loss may occur in the large communication distance due to the features of quantum mechanics [34]. The channel loss will lead to photon loss, which results in the secret information loss due to the information been encoded into individual photons. In addition, an eavesdropper could hide her presence in the channel noise and take the advantages to gain a certain

amount of information [6]. Thus, a quantum error correction is necessary during transmission via a noisy channel.

8. Conclusions

This work implements a secure mutual authentication to ensure the legitimacy of users without any involvement of the third party. Unlike the most well-known QSDC protocols that rely on a slight classical communication to share the pre-shared authentication key at the onset of communication, the proposed protocol fully utilizes the quantum channel to share the secret angle and authentication key at the initial stage of authentication. Firstly, the proposed scheme is enhanced with ITT implementation by allowing the sender to detect any disturbance by the third party. When quantum particles pass through optical polarization devices at the sender's site, and an eavesdropper is present in the communication to read the photon, the response by the receiver might induce additional time. Secondly, Pauli-X quantum gate operation is employed where the received qubit is flipped according to the numerical secret rotation angle to increase the difficulty for Eve to steal the information. The proposed protocol can be concluded that public communication or public states are not used to transmit a secret message or verify the parties. The security of the proposed scheme is discussed in the context of eavesdropping attacks during initial authentication and transmission of messages. Security analysis of initial authentication and transmission of messages has shown that the eavesdropper is unable to reveal any information about the authentication key or the transmitted message. That is because Alice only knows the secret angle of polarization and authentication key, and this is successfully shared with Bob through the quantum channel without being exposed to Eve.

The authentication is also prepared before the message is exchanged, and bit-by-bit checks are performed during quantum communication. The security analysis demonstrates that the suggested quantum authentication scheme is secure against most of the well-known attacks. There is no chance Eve could impersonate either Alice or Bob. In the proposed protocol, we only considered two parties involved in the communication. Recently, the authors of [35] proposed an effective way to share the authentication key among three parties using a single photon in polarization and spatial-mode degree of freedom. Following their work, we will study the authentication parts of three-party on multi-stage using unitary transformation of QSDC in the future. The problem of photon loss in the real implementation of the QSDC protocol has been studied in our work [14]. Therefore, the implementation of practical QSDC in a realistic environment of high information loss and noise using the proposed protocol should be focused on in our future research.

Author Contributions: Investigation, N.Z.H.; Methodology, N.Z.H.; Supervision, Z.A.Z., Z.M.H. and I.A.; Validation, Z.A.Z., Z.M.H. and I.A.; Writing—original draft, N.Z.H.; Writing—review & editing, Z.A.Z., Z.M.H. and I.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research is sponsored by University Putra Malaysia.

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

References

1. Long, G.L.; Liu, X.S. Theoretically efficient high-capacity quantum-key-distribution scheme. *Phys. Rev. A* **2002**, *65*, 1–3. [\[CrossRef\]](#)
2. Deng, F.; Long, G.L.; Liu, X. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. *Phys. Rev. A* **2003**, *68*, 1–6. [\[CrossRef\]](#)
3. Deng, F.-G.; Long, G.L. Secure direct communication with a quantum one-time pad. *Phys. Rev. A* **2004**, *052319*, 1–4. [\[CrossRef\]](#)
4. Li, J.; Pan, Z.; Sun, F.; Chen, Y.; Wang, Z.; Shi, Z. Quantum secure direct communication based on dense coding and detecting eavesdropping with four-particle genuine entangled state. *Entropy* **2015**, *17*, 6743–6752. [\[CrossRef\]](#)
5. Chang, Y.; Xu, C.X.; Zhang, S.; Yan, L.L. Quantum secure direct communication and authentication protocol with single photons. *Chin. Sci. Bull.* **2013**, *58*, 4571–4576. [\[CrossRef\]](#)

6. Hu, J.Y.; Yu, B.; Jing, M.Y.; Xiao, L.T.; Jia, S.T.; Qin, G.Q.; Long, G.L. Experimental quantum secure direct communication with single photons. *Light Sci. Appl.* **2016**, *5*, 1–5. [\[CrossRef\]](#)
7. Rifai, M.E.; Chan, K.W.C.; Verma, P.K. Multi-stage quantum secure communication using polarization hopping. *Secur. Commun. Netw.* **2015**, *8*, 4333–4342. [\[CrossRef\]](#)
8. Alizo, M.T.D. Soft Processing Techniques for Quantum Key Distribution Applications, Politecnico di Torino Porto. Ph.D. Thesis, Politecnico di Torino, Torino, Italy, 2012.
9. Darunkar, B.; Verma, P. The braided single-stage protocol for quantum secure communication. In Proceedings of the SPIE, Quantum Information and Computation XII, Baltimore, MD, USA, 22 May 2014; Volume 9123, pp. 1–8.
10. Kak, S. A three-stage Quantum Cryptography protocol. *Found. Phys. Lett.* **2006**, *19*, 293–296. [\[CrossRef\]](#)
11. Chang, Y.; Zhang, S.; Yan, L.; Li, J. Deterministic secure quantum communication and authentication protocol based on three-particle W state and quantum one-time pad. *Chin. Sci. Bull.* **2014**, *59*, 2835–2840. [\[CrossRef\]](#)
12. El-latif, A.A.A.; Abd-el-atty, B.; Hossain, M.S.; Samir, E.; Ghoneim, A. Secure Quantum Steganography Protocol for Fog Cloud Internet of Things. *IEEE Access* **2018**, *6*, 10332–10340. [\[CrossRef\]](#)
13. Wu, L. Reconfigurable Optical Networks And Multi-Photon Quantum Cryptography. Ph.D. Thesis, University of Houston, Houston, TX, USA, 2015.
14. Harun, N.Z.; Zukarnain, Z.A.; Hanapi, Z.M.; Ahmad, I. Hybrid M-Ary in Braided Single Stage Approach for Multiphoton Quantum Secure Direct Communication Protocol. *IEEE Access* **2019**, *7*, 22599–22612. [\[CrossRef\]](#)
15. Li, Y.; Zhang, P.; Huang, R. Lightweight Quantum Encryption for Secure Transmission of Power Data in Smart Grid. *IEEE Access* **2019**, *7*, 36285–36293. [\[CrossRef\]](#)
16. Chen, Y. Methods And Apparatuses For Authentication In Quantum Key Distribution And/Or Quantum Data Communication. U.S Patent 20180048466A1, 15 February 2018.
17. Lai, X.; Fan, L.; Lei, X.; Li, J.; Yang, N.; Karagiannidis, G.K. Distributed Secure Switch-and-Stay Combining over Correlated Fading Channels. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 2088–2101. [\[CrossRef\]](#)
18. Xu, Y.; Xia, J.; Wu, H.; Fan, L. Q-Learning Based Physical-Layer Secure Game Against Multiagent Attacks. *IEEE Access* **2019**, *7*, 49212–49222. [\[CrossRef\]](#)
19. Li, C.; Zhou, W.; Yu, K.; Fan, L.; Xia, J. Enhanced Secure Transmission Against Intelligent Attacks. *IEEE Access* **2019**, *7*, 53596–53602. [\[CrossRef\]](#)
20. Thomas, J.H. Variations on Kak's Three Stage Quantum Cryptography Protocol. *arXiv* **2007**, 1–7, arXiv:0706.2888.
21. Li, Q.; Le, D.; Wu, X.; Niu, X.; Guo, H. Efficient bit sifting scheme of post-processing in quantum key distribution. *Quantum Inf. Process.* **2015**, *14*, 3785–3811. [\[CrossRef\]](#)
22. Iwakoshi, T. On problems in security of quantum key distribution raised by Yuen. *Quantum Inf. Sci. Technol. III* **2017**, 1044203, 3. [\[CrossRef\]](#)
23. Chen, Y.; Kak, S.; Verma, P.K.; Macdonald, G.; El Rifai, M.; Punekar, N. Multi-photon tolerant secure quantum communication—From theory to practice. *IEEE Int. Conf. Commun.* **2013**, 2111–2116. [\[CrossRef\]](#)
24. Huang, W.; Xu, B.-J.; Duan, J.-T.; Liu, B.; Su, Q.; He, Y.-H.; Jia, H.-Y. Authenticated Quantum Key Distribution with Collective Detection using Single Photons. *Int. J. Theor. Phys.* **2016**, *55*, 4238–4256. [\[CrossRef\]](#)
25. Li, C.M.; Yu, K.F.; Kao, S.H.; Hwang, T. Authenticated semi-quantum key distributions without classical channel. *Quantum Inf. Process.* **2016**, *15*, 2881–2893. [\[CrossRef\]](#)
26. Kak, S. Authentication Using Piggy Bank Approach to Secure Double-Lock Cryptography. *arXiv* **2014**, 1–8, arXiv:1411.3645.
27. Abushgra, A.; Elleithy, K. A Shared Secret Key Initiated by EPR Authentication and Qubit Transmission Channels. *IEEE Access* **2017**, 17753–17763. [\[CrossRef\]](#)
28. Darunkar, B.A. Multi-Photon Tolerant Quantum Key Distribution Protocols For Secured Global Communication. Ph.D. Thesis, University Of Oklahoma, Norman, OK, USA, 2017.
29. Darunkar, B.; Punekar, N.; Verma, P.K. Secure Satellite Communication Using Multi-Photon tolerant quantum communication protocol. In Proceedings of the Quantum Communications and Quantum Imaging XIII, San Diego, CA, USA, 1 September 2015; Volume 9615, p. 961509.
30. Verma, P.K.; El Rifai, M.; Chan, K.W.C. *Multi-Photon Quantum Secure Communication*; Springer: Singapore, 2019; ISBN 9789811086175.

31. Liu, Z.H.; Chen, H.W.; Liu, W.J. Information Leakage Problem in Efficient Bidirectional Quantum Secure Direct Communication with Single Photons in Both Polarization and Spatial-Mode Degrees of Freedom. *Int. J. Theor. Phys.* **2016**, *55*, 4681–4686. [[CrossRef](#)]
32. Ghilen, A.; Belmabrouk, H.; Bouallegue, R. Classification of quantum authentication protocols and calculation of their complexity. In Proceedings of the 15th International Conference on Sciences and Techniques of Automatic Control & Computer Engineering, Hammamet, Tunisia, 21–23 December 2014; pp. 169–173.
33. Guedes, E.B.; de Assis, F.M. An Approach To Evaluate Quantum Authentication Protocols. In Proceedings of the Congresso Brasileiro de Inteligência Computacional, Fortaleza, Brazil, 8–11 November 2011; pp. 1–8.
34. Wang, L.; Ma, W. Controlled quantum secure communication protocol with single photons in both polarization and spatial-mode degrees of freedom. *Mod. Phys. Lett. B* **2016**, *30*, 1650051. [[CrossRef](#)]
35. Wang, L.L.; Ma, W.P.; Wang, M.L.; Shen, D.S. Three-party Quantum Secure Direct Communication with Single Photons in both Polarization and Spatial-mode Degrees of Freedom. *Int. J. Theor. Phys.* **2016**, *55*, 2490–2499. [[CrossRef](#)]

© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).