Cryptanalysis of quantum secure direct communication protocol with mutual authentication based on single photons and Bell states

NAYANA DAS\(^{(a)}\) and GOUTAM PAUL\(^{(b)}\)

\(^{(a)}\)Applied Statistics Unit, Indian Statistical Institute - Kolkata 700108, India
\(^{(b)}\)Cryptology and Security Research Unit, R. C. Bose Centre for Cryptology and Security, Indian Statistical Institute Kolkata 700108, India

Abstract – Recently, Yan et al. proposed a quantum secure direct communication (QSDC) protocol with authentication using single photons and Einstein-Podolsky-Rosen (EPR) pairs (Yan L. et al., Comput. Mater. Contin., 63 (2020) 1297). In this work, we show that the above QSDC protocol is secure neither against intercept-and-resend attack, nor against impersonation attack. With any of these two types of attacks, an eavesdropper can recover the full secret message. We also propose a suitable modification of this protocol, which not only defeats the above attacks, but also resists all other common attacks. Thus, our modified protocol provides an improvement over the existing one in terms of security.

Introduction. – Quantum cryptography is an application of quantum mechanics in the field of cryptography, which provides unconditional security based on the laws of physics. In 1984, Bennett and Brassard proposed the first quantum cryptographic protocol. This is based on quantum key distribution (QKD) and is known as the BB84 QKD [1]. Since then various types of QKD protocols have been proposed [2–8].

Quantum secure direct communication (QSDC) is another direction of quantum cryptography, which offers secure communication without any shared key [3,9–27]. In QSDC protocols, the sender encodes the secret message into some qubits by using a predefined encoding rule and sends those qubits to the receiver. After the necessary security checks, the receiver can get the secret message. A few interesting generalizations of QSDC protocols are quantum dialogue or bidirectional QSDC [28,29], multiparty QSDC [30,31] and so on.

If QSDC or any quantum cryptographic protocol is not properly designed, it gives a chance to an eavesdropper to impersonate an authorized party. For this concern, each legitimate party should verify the authenticity of other parties, which requires quantum authentication protocols [32,33]. The first QSDC protocol with authentication was proposed in 2006 [34], and thereafter many researchers are working in this domain [35,36].

There are multiple quantum cryptographic protocols, which are proven to be insecure against various familiar attacks, such as intercept-and-resend attack [37,38], impersonation attack [39,40], Denial-of-Service attack [41,42], man-in-the-middle attack [43,44], entangle-measure attack [42,45], Trojan horse attack [46,47], etc. These are all active attacks, i.e., an eavesdropper has access to the communicated qubits in the quantum channel between the legitimate parties, and actively participates in the protocol. Inactive attacks can also cause information leakage problems in some communication protocols [48,49].

In 2020, Yan et al. have presented a QSDC protocol based on single photons and EPR pairs, which also realizes mutual authentication [50]. For simplicity, throughout this paper, we call this QSDC protocol as YZCSS protocol, based on the authors’ initials. In this protocol, the sender Alice prepares qubit pairs corresponding to the secret message and her authentication identity. She sends all the qubits to the receiver Bob, who uses his authentication identity to get the secret message. However, in this article, we show that the YZCSS protocol is not secure against intercept-and-resend attack and impersonation attack. If an eavesdropper performs any one of these attacks, then it can get the complete secret message, i.e., the entire
message is compromised. Moreover, for impersonation attack, the legitimate parties cannot detect the presence of the eavesdropper. Furthermore, we present a modification of the YZCSS protocol to improve its security, where we assume that the classical channel is authenticated, and we achieve authentication of the quantum channel within our protocol. The rest of the paper is organized as follows: in the next section, we briefly describe the YZCSS protocol, then we discuss the security flaws of the same protocol. Thereafter an improved version of the protocol is presented and, finally, we conclude with our result.

**Brief review of the YZCSS protocol**. In this section, we describe the YZCSS protocol. There are two parties, namely, Alice and Bob with their corresponding identities $ID_A$ and $ID_B$ respectively, where $ID_A, ID_B \in \{0,1\}^N$. Alice wants to send a secret message $M \in \{0,1\}^N$ to Bob by using single photons and Bell states, where the Bell states (EPR pairs) are defined as: $|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$, $|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$. The steps of the protocol are as follows:

1) Alice and Bob have their previously shared identities $ID_A$ and $ID_B$, they used some QKD to exchange $ID_A$ and $ID_B$. Alice prepares two sequences of two-qubit states $S_M$ and $S_A$ corresponding to the message $M$ and her own identity $ID_A$, each sequence contains $N$ qubit pairs. For $1 \leq i \leq N$, let the $i$-th bit of $M$ (or $ID_A$ or $ID_B$) be $M_i$ (or $ID_{A,i}$ or $ID_{B,i}$) and the $i$-th qubit of $S_M$ (or $S_A$) be $S_{M,i}$ (or $S_{A,i}$). She prepares the qubits by using the following rule:

- a) if $M_i$ (or $ID_{A,i}$) = 0, then $S_{M,i}$ (or $S_{A,i}$) = $|01\rangle$ or $|10\rangle$ with equal probability,
- b) if $M_i$ (or $ID_{A,i}$) = 1, then $S_{M,i}$ (or $S_{A,i}$) = $|\Phi^+\rangle$ or $|\Phi^-\rangle$ with equal probability.

The qubit pairs of the sequence $S_A$ are called decoy states. Now Alice inserts these decoy states into the sequence $S_M$ according to the following rule:

- a) if $ID_{B,i} = 0$, then she inserts $S_{A,i}$ before $S_{M,i}$,
- b) if $ID_{B,i} = 1$, then she inserts $S_{A,i}$ after $S_{M,i}$.

Let the new sequence be $S$ containing $2N$ qubit pairs. Then Alice sends $S$ to Bob using a quantum channel. Let us show an example.

**Example 1.** Let $M = 10110$, $ID_A = 01011$ and $ID_B = 01001$. Then $S_M = \{|\Phi^+\rangle, |01\rangle, |\Phi^+\rangle, |\Phi^-\rangle, |01\rangle\}$, $S_A = \{|10\rangle, |\Phi^+\rangle, |\Phi^-\rangle, |01\rangle, |\Phi^+\rangle\}$ and $S = \{|01\rangle, |\Phi^+\rangle, |10\rangle, |\Phi^-\rangle, |\Phi^-\rangle, |\Phi^+\rangle, |01\rangle, |\Phi^-\rangle, |10\rangle, |\Phi^+\rangle\}$.

2) After Bob receives $S$, he knows the exact positions of the decoy photons corresponding to his identity $ID_B$. Bob measures those decoy photons in proper bases according to $ID_A$. If $ID_{A,i} = 0$, then he chooses $Z \times Z$ basis, where $Z = \{|0\rangle, |1\rangle\}$, thus $Z \times Z = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, and if $ID_{A,i} = 1$, then he chooses the Bell basis $= \{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$ to measure $S_{A,i}$. Bob also measures the qubit pairs of $S_M$ in $Z \times Z$ basis or Bell basis randomly. He notes the measurement results.

3) Bob asks Alice to announce the initial states of the qubit pairs of $S_A$ for security check. They compare the initial states and the measurement results of the decoy photons and calculate the error rate. If the error rate exceeds some pre-defined threshold value, then they terminate the protocol, else they continue.

4) Bob gets all the secret message bits from the measurement results of the qubit pairs of $S_M$. The relations between the measurement results and the secret message bits are given in table 1. To check the integrity of the secret message Alice and Bob publicly compare some parts of the message. The authors of [50] have shown that the YZCSS protocol is secure against various kinds of attacks, such as impersonation attack, intercept-and-resend attack, man-in-the-middle attack, entangle-measure attack. However, in the next section, we show that an eavesdropper can design a strategy that allows her to effectively execute the intercept-and-resend attack. A similar argument follows for the impersonation attack as well, making this protocol insecure against these two attacks.

**Security loophole of the YZCSS protocol.** We now show that the YZCSS protocol discussed in the previous section is not secure against intercept-and-resend attack and impersonation attack, an eavesdropper (Eve) can get the whole secret message $M$ and Alice’s authentication identity $ID_A$ by adopting these attacks.

**Intercept-and-resend attack.** In this attack strategy, when Alice sends the quantum states to Bob, Eve intercepts those from the quantum channel, she measures the states and resends those to Bob. However, to attack the YZCSS protocol, Eve follows a special strategy while resending the quantum states to Bob. The process of the attack is as follows.

| $M_i$ | $S_{M,i}$ | Basis chosen by Bob | Measurement result of Bob | Decoded secret bit |
|-------|-----------|---------------------|--------------------------|--------------------|
| 0     | $|01\rangle$ | $Z \times Z$ basis   | $|01\rangle$             | 0                  |
|       | $|\Psi^+\rangle$ or $|\Psi^-\rangle$ | Bell basis         | 0                      |                    |
| 1     | $|01\rangle$ | $Z \times Z$ basis   | $|10\rangle$             | 0                  |
|       | $|\Psi^+\rangle$ or $|\Psi^-\rangle$ | Bell basis         | 0                      |                    |
| 0     | $|\Phi^+\rangle$ | $Z \times Z$ basis   | $|00\rangle$ or $|11\rangle$ | 1                  |
|       | Bell basis   | $|\Phi^+\rangle$      | 1                      |                    |
| 1     | $|\Phi^-\rangle$ | $Z \times Z$ basis   | $|00\rangle$ or $|11\rangle$ | 1                  |
|       | Bell basis   | $|\Phi^-\rangle$      | 1                      |                    |

| Table 1: Different cases of the YZCSS protocol |
Crypanalysis of QSDC with authentication based on single photons and Bell states

Table 2: Rule of construction of $m$ by Eve.

| Basis chosen by Eve | Eve’s measurement result | Bit guessed by Eve |
|---------------------|--------------------------|--------------------|
| $Z \times Z$ basis  | (01) or (10)             | 0                  |
|                     | (00) or (11)             | 1                  |
| Bell basis          | $|\Psi^+\rangle$ or $|\Psi^-\rangle$ | 0                  |
|                     | $|\Phi^+\rangle$ or $|\Phi^-\rangle$ | 1                  |

1) Eve intercepts the sequence $S$ and measures each two-qubit state randomly in $Z \times Z$ basis or Bell basis and notes down the measurement results. For $1 \leq i \leq 2N$, if she chooses $Z \times Z$ basis to measure the $i$-th qubit pair of $S$ and the measurement result is either (01) or (10), then she simply sends this state to Bob. But if the measurement result is either (00) or (11), Eve definitely knows that she chose the wrong basis and the initial state was either $|\Phi^+\rangle$ or $|\Phi^-\rangle$. Then she randomly prepares $|\Phi^+\rangle$ or $|\Phi^-\rangle$ and sends it to Bob. Similarly if Eve chooses the Bell basis and gets $|\Phi^+\rangle$ or $|\Phi^-\rangle$, then she sends them. Otherwise, she randomly sends (01) or (10) to Bob.

2) Eve constructs a $2N$-bit string $m$ from the measurement results by using table 2.

3) Eve splits the $2N$-bit string $m = m_1 m_2 \ldots m_{2N}$ into $N$ number of 2-bit strings $M_1, M_2, \ldots, M_N$, and for $1 \leq i \leq N$, $M_i = m_{2i-1} m_{2i}$. Now from the construction procedure of the sequence $S$, Eve exactly knows that each $M_i$ contains the $i$-th bit of the secret message $M$ and the $i$-th bit of Alice’s authentication identity $ID_A$. If both the bits of $M_i$ are equal, i.e., $M_i = bb$, where $b \in \{0, 1\}$, then she concludes $M_i = b$ and $ID_{A,i} = b$. Again if $M_i = bb$, where $b = \text{bit complement of } b$, then she waits for Alice’s announcement about the initial states of the decoy photons. If Alice announces (01) or (10), then Eve concludes $ID_{A,i} = 0$ and $M_i = 1$, otherwise she concludes $ID_{A,i} = 1$ and $M_i = 0$. Thus Eve can successfully attack the protocol and gets the complete secret message.

Now Alice and Bob can detect this intercept-and-resend attack at the time of security check, but it has no impact on the attack result as one of the main requirement of a QSDC protocol is “the secret messages which have been encoded already in the quantum states should not leak even though an eavesdropper may get hold of channel” [10].

Impersonation attack. By analyzing the YZCSS protocol, we find that the authentication procedure of this QSDC protocol is unidirectional, i.e., only Bob can verify Alice’s identity. Here we show how Eve impersonates Bob to acquire the secret message of Alice. The process is as follows:

1) Alice prepares the sequence $S$ and sends it to Eve.

2) After receiving $S$, Eve measures all the qubit pairs randomly in $Z \times Z$ or Bell basis and generates a $2N$-bit string $m$ from the measurement results by using table 2.

3) Eve asks Alice to declare the initial state of the decoy photons and, from this information, she gets the whole secret message (by using the same process as in step 3) of the intercept-and-resend attack).

In this case, Alice cannot detect Eve, or in other words, only one-way authentication is possible in the YZCSS protocol. Moreover, without knowing the exact position of the decoy photons, Eve can get the whole secret message. Let us take an example of this attack.

Example 2. Let $M = 10110$, $ID_A = 01011$ and $ID_B = 01001$. Then $S_M = \{|\Phi^+\rangle, |01\rangle, |\Phi^+\rangle, |01\rangle\}$, $S_A = \{|0\rangle, |\Phi^-\rangle, |01\rangle, |\Phi^+\rangle\}$ and $S = \{|0\rangle, |\Phi^+\rangle, |01\rangle, |\Phi^-\rangle, |01\rangle, |\Phi^+\rangle, |01\rangle, |\Phi^-\rangle, |01\rangle, |\Phi^+\rangle\}$.

1) Eve has the sequence $S$.

2) Let $B = \{Z, Z, Bell, Z, Bell, Bell, Bell, Bell, Z, Z, Bell\}$ be a sequence of bases which Eve chooses to measure the qubit pairs of $S$.

3) Let the sequence of measurement results be $\{|0\rangle, |\Phi^-\rangle, |11\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |11\rangle, |01\rangle, |\Phi^+\rangle\}$.

4) Then $m = 01011010101$ and $M_1 = 01, M_2 = 01, M_3 = 11, M_4 = 01, M_5 = 01$. Eve concludes $M_5 = 1$ and $ID_{A,3} = 1$.

5) Alice announces $S_A = \{|10\rangle, |\Phi^-\rangle, |01\rangle, |\Phi^+\rangle\}$ and then Eve concludes

   $-ID_{A,1} = 0, \quad M_1 = 1; \quad -ID_{A,4} = 0, \quad M_4 = 1; \quad -ID_{A,2} = 1, \quad M_2 = 0; \quad -ID_{A,5} = 1, \quad M_5 = 0.$

   Thus Eve gets the whole secret message $M = 10110$.

Another problem with the YZCSS protocol is that the lengths of the authentication identities of Alice and Bob are equal to the length of the secret message. Since the identities are previously shared, Alice can send a fixed-length message to Bob, which is a disadvantage of this protocol. In the next section, we propose a remedy to these security problems of the YZCSS protocol.

Authentication and proposed modification. - In this section, first we describe how authentication is performed, and then our modified protocol, followed by its security analysis.

Authentication. There are two types of authentication in cryptography, one is a user or identity authentication, and another is message authentication. The first process is used to check the authenticity of the users of the protocol, and the second process is to check the integrity of the transmitted information. Here in our protocol, we use both classical and quantum channels and

48001-p3
Table 3: Channel authentication (assumptions and achievements).

| Type of the channel | User authentication | Message authentication |
|---------------------|---------------------|------------------------|
| Classical           | yes                 | yes                    |
| Quantum             | no                  | yes                    |

assume that the classical channel is authenticated. That means, both user and message authentications are assumed for the classical channel, or in other words, we can say that an eavesdropper can eavesdrop the information but cannot modify it. Here the concept of public announcement [1] is used in our protocol. For the quantum channel we do not assume any authentication, but both the user authentication and message authentication are incorporated with the modified protocol (see table 3 for more details).

Our modified protocol. Now we discuss how to modify this YZCSS protocol so that it can provide mutual authentication and stand against the intercept-and-resend attack. In the original protocol, the length of ID$_A$ and ID$_B$ are equal to the length of the message, which may vary. However, in our improved version, we fix the length of ID$_A$ and ID$_B$ and the length is $k$. Here we use some techniques of the authentication protocol proposed by Fei et al. [40]. Our modified protocol is given below:

1) Qubits preparation to encode secret message:

a) Alice and Bob have their previously shared $k$-bit identities ID$_A$ and ID$_B$, where ID$_A$ and ID$_B$ are unknown to everybody other than Alice and Bob.

b) Suppose Alice has an $n$-bit secret message $m$ which she wants to send to Bob through a quantum channel. She chooses $c$ random check bits and inserts those in random positions of $m$. Let the new message string be $M$ of length $N = n + c$.

c) Alice prepares a sequence of $N$ qubit pairs $S_M$ corresponding to her $N$-bit message $M$. For $1 \leq i \leq N$, let the $i$-th pair of $S_M$ be $S_{M,i} = (S_{M,i}^1, S_{M,i}^2)$ and she prepares $S_{M,i}$ by using the following rule (w.p. with probability):

$$S_{M,i} = \begin{cases} 
|01\rangle \text{ w.p. } \frac{1}{2}, & \text{if } M_i = 0, \\
|\Phi^+\rangle \text{ or } |\Phi^-\rangle \text{ w.p. } \frac{1}{2}, & \text{if } M_i = 1.
\end{cases}$$

(1)

d) Alice takes one qubit from each qubit pair $S_{M,i}$ to form an ordered qubit sequence $Q^1_M = \{S_{M,1}^1, S_{M,2}^1, \ldots, S_{M,N}^1\}$. The remaining partner qubits of $S_{M,i}$ compose another qubit sequence $Q^2_M = \{S_{M,1}^2, S_{M,2}^2, \ldots, S_{M,N}^2\}$.

e) Alice prepares the first sequence of decoy photons $S_A$, for authentication, corresponding to her own identity ID$_A$ as follows: for $1 \leq i \leq k$,

$$S_{A,i} = \begin{cases} 
|0\rangle \text{ or } |1\rangle \text{ w.p. } \frac{1}{2}, & \text{if } ID_{A,i} = 0, \\
|+\rangle \text{ or } |−\rangle \text{ w.p. } \frac{1}{2}, & \text{if } ID_{A,i} = 1,
\end{cases}$$

(2)

where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|−\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Now she inserts these decoy states into the first sequence $Q^1_M$ according to the following rule: for $1 \leq i \leq k$,

i) if ID$_{B,i} = 0$, then she inserts $S_{A,i}$ before $Q_{M,\lambda-\lambda+1}$;

ii) if ID$_{B,i} = 1$, then she inserts $S_{A,i}$ after $Q^1_{M,\lambda}$,

where $\lambda = \lfloor N/k \rfloor$, $|x|$ is the greatest integer not greater than $x$ and $k \leq N$. Let the first sequence become $S$ containing $N + k$ qubits. For better understanding, let us show an example.

Example 3. Let $M = 1011010$, ID$_A = 011$ and ID$_B = 010$.

i) $S_M = \{|\Phi^+\rangle, |01\rangle, |\Phi^+\rangle, |01\rangle, |\Phi^+\rangle, |10\rangle\}$ and let the $i$-th pair of $S_M$ be $(S_{M,1}^1, S_{M,1}^2)$.

ii) $Q^1_M = \{S_{M,1}^1, S_{M,2}^1, \ldots, S_{M,7}^1\}$, $Q^2_M = \{S_{M,1}^2, S_{M,2}^2, \ldots, S_{M,7}^2\}$.

iii) $S_A = \{|0\rangle, |−\rangle, |−\rangle\}$.

iv) $\lambda = \lfloor 7/3 \rfloor = 2$.

v) $S = \{|0\rangle, S_{M,1}^1, S_{M,2}^1, S_{M,3}^1, S_{M,4}^1, S_{M,5}^1, S_{M,6}^1, S_{M,7}^1\}$.

f) She also prepares a second set of decoy photons $D_A$ randomly from $\{(0), |1\rangle, |+\rangle, |−\rangle\}$ and inserts them in random positions of $S$. Let the new sequence be $S'$.

2) First sequence of qubits transmission: Alice sends the new sequence $S'$ to Bob using a quantum channel. She keeps the sequence $Q^1_M$ with her.

3) Security check: After Bob receives $S'$, Alice announces the positions and the bases of the second set of decoy photons. Bob measures those decoy photons and they calculate the error rate in the channel by comparing the measurement results with the initial states. If the error rate is low, then they continue the protocol, otherwise they terminate this.
4) Authentication procedure:

a) Bob knows the exact positions of the decoy photons of $S_A$ corresponding to his identity $ID_B$. He measures those decoy photons in proper bases according to $ID_A$. If $ID_{A,i} = 0$, then he chooses the $Z$ basis and if $ID_{A,i} = 1$, then he chooses the $X = \{|+,|\rangle\} \rangle$ basis to measure $S_{A,i}$.

b) For $1 \leq i \leq k$, Alice and Bob construct a $k$-bit string $info(S_A)$ such that, if $S_{A,i} = |0\rangle$ or $|+\rangle$, then $info(S_{A,i}) = 0$, else $info(S_{A,i}) = 1$.

c) They randomly choose $k/2$ (approximate) positions and Alice announces the values of the corresponding bits of $info(S_A)$. Bob compares these values with his corresponding measurement results to authenticate Alice’s identity. Similarly, Bob announces the remaining bits of $info(S_A)$ for his identity authentication. If any of them finds intolerable error rate, then he or she aborts this protocol.

5) Second sequence of qubits transmission: Alice prepares a third set of decoy photons $D_A'$ randomly from $\{|0\rangle,|1\rangle,|+\rangle,|\rangle\rangle\}$ and inserts them into random positions of $Q_A$. Let the new sequence be $S''$ and she sends the new sequence $S''$ to Bob using a quantum channel.

6) Security check: After Bob receives $S''$, Alice announces the positions and the bases of the third set of decoy photons. Bob measures those decoy photons and they calculate the error rate in the channel by comparing the measurement results with the initial states. If the error rate is low, then they continue the protocol, otherwise, they terminate this protocol.

7) Message decoding:

a) Bob discards all the decoy photons and gets back the sequences $Q_{M}'$ and $Q_{M}''$.

b) He measures the qubit pairs of $S_M$ in $Z \times Z$ basis or Bell basis randomly and notes the measurement results.

c) Bob gets all the secret message bits from the measurement results of the qubit pairs of $S_M$. The relations between the measurement results and the secret message bits are given in table 1.

d) To check the integrity of the secret message, Alice and Bob publicly compare values of the random check bits. Bob discards these check bits from $M$ and gets back $m$.

Note that, though quantum memories are still at the early development stage, many state-of-the-art quantum communication protocols use quantum memory [3,10,11,49,51–53]. Here in this work we also follow a similar approach. The possible realizations of quantum memory are discussed in [13,54].

Security analysis of the modified protocol. We now show that our modified protocol is secure against some common attacks. First, we discuss the intercept-and-resend attack and the impersonation attack as the original YZCSS protocol was proven to be insecure against these two attacks. Then we also discuss Denial-of-Service attack, man-in-the-middle attack, entangle-measure attack and Trojan horse attack.

1) Intercept-and-resend attack: Let Eve intercept the sequence $S'$ from the quantum channel. Since $S'$ contains only the first qubit of each pair of qubits corresponding to the secret message bits, it is impossible for Eve to gain any information by measuring those qubits. At most Eve can do is to measure the qubits of $S'$ on $Z$ or $X$ basis and resend those measured qubits to Bob. In that case, she does not get any useful information about the secret message, and Alice and Bob also detect her and terminate the protocol at the time of security checking (Step 3 of the modified protocol). Let the second set of decoy photons $D_A$ contain $l$ number of qubits.

We now calculate the probability that Alice and Bob can detect Eve. Let the $i$-th qubit of $D_A$ be $d_i$ prepared in basis $B_i \in \{Z,X\}$, and suppose Eve chooses the basis $B_i'$ to measure $d_i$ and gets $d_i'$. At the time of security checking, Bob measures $d_i'$ in $B_i$ and gets the result $d_i''$. Thus the winning probability of Eve for the $i$-th decoy qubit is

$$\Pr(d_i'' = d_i) = \Pr(d_i'' = d_i | B_i = B_i') \Pr(B_i = B_i') + \Pr(d_i'' = d_i | B_i \neq B_i') \Pr(B_i \neq B_i')$$

$$= \frac{1}{2} \{\Pr(d_i'' = d_i | B_i = B_i') + \Pr(d_i'' = d_i | B_i \neq B_i')\}$$

$$= \frac{1}{2} \left(1 + \frac{1}{2}\right) = \frac{3}{4}.$$ 

Thus the probability that Alice and Bob can detect the existence of Eve is $1 - \left(\frac{3}{4}\right)^l > 0$.

Again if Eve intercepts the sequence $S''$ from the quantum channel in the second phase of transmission, then also she cannot get any information about $M$ as $S''$ contains only one qubit of each qubit pair. In this case, also Alice and Bob detect her with probability $1 - \left(\frac{3}{4}\right)^{l'} > 0$, where $l'$ is the number of decoy qubits in the set $D_A'$, and terminate the protocol at the time of the second security checking (step 6) of the modified protocol.

2) Impersonation attack: In the YZCSS protocol, only Alice announces the exact states of the decoy photons corresponding to $ID_A$ and Bob compares them with his measurement results to check the authenticity of Alice. In the modified version, both Alice and Bob have to announce the information about the initial states of the decoy
 photons of $S_A$, they do not announce the exact states to keep $ID_A$ secret. If Eve impersonates any one of Alice and Bob, then the other one can detect her and aborts this protocol. Let Eve impersonate Alice, then in the authentication procedure (step 4) Eve has to construct a k-bit string as $inf_j^o(S_A)$. Then she needs to announce the bit values of $inf_j^o(S_A)$ for k/2 positions jointly chosen by Bob and her. Since Eve does not know the positions of the qubits corresponding to $ID_A$, she just randomly guesses the bit values of $inf_j^o(S_A)$. Thus, the winning probability of Eve is $(1/2)^{k/2}$ and hence Bob can detect her with probability $1 - (1/2)^{k/2} > 0$. Similarly, when Eve impersonates Bob, Alice can detect her with probability $1 - (1/2)^{k/2} > 0$.

3) Denial-of-Service (DoS) attack: The motivation of Eve, for adopting the DoS attack, is to tamper with the secret message [41]. Let Eve capture the sequence $S'$ (or $S''$) and apply a certain unitary operation $U$ to each qubit of $S'$. However, this action will be detected by the legitimate parties at the security checking procedure in step 3), and as a result, Alice and Bob terminate this protocol. Since the Pauli matrices $I$, $\sigma_x$, $\sigma_y$ and $\sigma_z$ form a basis for the space of all $2 \times 2$ Hermitian matrices [55], $U$ can be expressed as a linear combination of these basis vectors. Let $U = w_1I + w_2\sigma_x + w_3\sigma_y + w_4\sigma_z$ where $\sum_{j=1}^4 w_j^2 = 1$ as $U$ is unitary. Now we calculate the winning probability of Eve for each decoy qubit $d$ in $D_A$ (or $d$ in $D'_A$). First, we individually calculate the winning probabilities $p_1$, $p_2$, $p_3$ and $p_4$ of Eve if she applies the Pauli matrices $I$, $\sigma_x$, $\sigma_y$ and $\sigma_z$, respectively. We obtain $p_1 = 1$, as $I$ applied on $d$ does not change its state; $p_2 = 1/2$, as $\sigma_x$ changes the state of a decoy qubit $d$ only if $d \in \{0\}$; $p_3 = 0$, as $\sigma_y$ always changes the state of a decoy qubit; and $p_4 = 1/2$, as $\sigma_z$ changes the states of qubits in $X$-basis. Therefore the winning probability of Eve is $p = \sum_{j=1}^4 p_j w_j^2 < 1$, unless $U = I$ (which is equivalent to no attack by Eve). Hence in the security check processes (step 3) and step 6) of the modified protocol) Alice and Bob find this eavesdropping with probability $1 - p^2 > 0$ (or with $1 - p^2 > 0$).

4) Man-in-the-middle attack: When Alice sends the sequence $S'$ (or $S''$) to Bob, Eve intercepts $S'$ (or $S''$) and keeps this with her. She prepares another set of qubits $T'$ (or $T''$) and sends it to Bob. In this case, Alice and Bob can also realize the existence of Eve and abort the protocol in step 3) (or step 6) and terminate the protocol. We now calculate the detection probability of Eve when she intercepts $S'$. Let the i-th decoy qubit of $D_A$ be $d_i$ and suppose it is the j-th qubit of $S'$. Also let Eve prepare $t_j$ as the j-th qubit of $T'$. Let the preparation bases of $d_i$ and $t_j$ be $B_1$ and $B_2$, respectively. In the security check process, Bob measures $t_j$ in basis $B_1$ and gets $t'_j$. Thus the winning probability of Eve for the i-th decoy qubit is as follows:

$$\Pr(t'_j = d_i) = \Pr(t'_j = d_i | B_1 = B_2) \Pr(B_1 = B_2)$$

Hence Alice and Bob detect Eve with probability $1 - (1/2)^{k/2} > 0$. A similar argument follows for the second transmission phase also.

5) Entangle-measure attack: In order to steal partial information, Eve may apply this attack [56]. She first intercepts the qubits of the sequence $S'$ and prepares some ancillary state $|E\rangle$, then applies a unitary $U_E$ to the joint states of qubits of $S'$ and $|E\rangle$ such that the composite system becomes entangled. Let the i-th decoy state in $D_A$ be $d_i$ and after applying $U_E$ suppose it becomes $d'_i$. However, the effects of the unitary operation $U_E$ on the second set of decoy photons are as follows:

$$U_E[0]|E\rangle = \alpha_0|0\rangle|E_{00}\rangle + \beta_0|1\rangle|E_{01}\rangle, U_E[1]|E\rangle = \alpha_1|0\rangle|E_{10}\rangle + \beta_1|1\rangle|E_{11}\rangle.$$ (3)

Since $U_E$ is unitary, we must have

$$|\alpha_0|^2 + |\beta_0|^2 = 1, |\alpha_1|^2 + |\beta_1|^2 = 1, \alpha_0 \alpha_1^* + \beta_0 \beta_1^* = 0.$$ (4)

Thus when the decoy state $d_i$ is in $Z$ basis, the error rate is $e = |\beta_0|^2 = |\alpha_1|^2$. Further, we get $U_E[\pm]|E\rangle = \frac{1}{\sqrt{2}}(|+\rangle|E_{\pm+}\rangle + |\pm\rangle|E_{\pm-}\rangle)$, where

$$|E_{++}\rangle = \frac{1}{\sqrt{2}}(\alpha_0|E_{00}\rangle + \beta_0|E_{01}\rangle + \alpha_1|E_{10}\rangle + \beta_1|E_{11}\rangle),$$

$$|E_{+-}\rangle = \frac{1}{\sqrt{2}}(\alpha_0|E_{00}\rangle - \beta_0|E_{01}\rangle + \alpha_1|E_{10}\rangle - \beta_1|E_{11}\rangle),$$

$$|E_{-+}\rangle = \frac{1}{\sqrt{2}}(\alpha_0|E_{00}\rangle + \beta_0|E_{01}\rangle - \alpha_1|E_{10}\rangle - \beta_1|E_{11}\rangle),$$

$$|E_{--}\rangle = \frac{1}{\sqrt{2}}(\alpha_0|E_{00}\rangle - \beta_0|E_{01}\rangle - \alpha_1|E_{10}\rangle + \beta_1|E_{11}\rangle).$$

Thus if the decoy state $d_i$ is prepared in $X$ basis, then Bob measures the first qubit $d'_i$ of the entangled state $U_E[+]|E\rangle$ or $U_E[-]|E\rangle$ in $X$ basis. Therefore he gets the correct result with probability 1/2, and hence the error rate is 1/2. Hence from the error rate introduced by Eve in the communication process, Alice and Bob detect this eavesdropping in step 3). Furthermore, if Eve applies this attack on the second stage of transmission, then also in a similar way Alice and Bob can detect her.

6) Trojan horse attack: Both the YZCSS protocol and its modified version are one-way quantum communication protocols, i.e., only Alice prepares qubits and sends them to Bob. Thus these protocols have immunity to the Trojan horse attack.
**Conclusion.** — In this paper, we analyze the security of QSDC protocols with authentication (YZCSS protocol) and demonstrate that this protocol is vulnerable to two specific attacks, namely, intercept-and-resend attack and impersonation attack. An eavesdropper adopting any one of these two attacks gets the whole secret message. The authentication process in the YZCSS protocol is unidirectional, which causes the impersonation attack. To address these concerns, we propose a modification of the YZCSS protocol, where a mutual authentication process is suggested, and the modified protocol resists the intercept-and-resend attack. We also prove that it is secure against several familiar attack strategies.

**REFERENCES**

[1] BENNETT C. H. and BRASSARD G., *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE) 1984.
[2] EKER T A. K., *Phys. Rev. Lett.*, 67 (1991) 661.
[3] LONG G.-L. and LIU X.-S., *Phys. Rev. A*, 65 (2002) 032302.
[4] LI J. et al., *Sci. Rep.*, 6 (2016) 28767.
[5] BENNETT C. H., *Phys. Rev. Lett.*, 68 (1992) 3121.
[6] LUCAMARINI M. and MANCINI S., *Phys. Rev. Lett.*, 94 (2005) 140501.
[7] BENNETT C. H. et al., *J. Cryptol.*, 5 (1992) 3.
[8] TANG Z. et al., *Phys. Rev. Lett.*, 112 (2014) 190503.
[9] BOSTROM K. and FELBRINGER T., *Phys. Rev. Lett.*, 89 (2002) 187902.
[10] DENG F.-G. et al., *Phys. Rev. A*, 68 (2003) 042317.
[11] DENG F.-G. and LONG G. L., *Phys. Rev. A*, 69 (2004) 052319.
[12] HU J.-Y. et al., *Light: Sci. Appl.*, 5 (2016) e16144.
[13] ZHANG W. et al., *Phys. Rev. Lett.*, 118 (2017) 220501.
[14] ZHOU L. et al., *Sci. Bull.*, 65 (2020) 12.
[15] CHEN S.-S. et al., *Sci. China Phys. Mech. Astron.*, 61 (2018) 090312.
[16] ZOU Z.-K. et al., *EPL*, 131 (2020) 40005.
[17] WU X.-D. et al., *Quantum Inf. Process.*, 19 (2020) 354.
[18] LIU L. et al., *Quantum Inf. Process.*, 19 (2020) 404.
[19] LI T. and LONG G.-L., *New J. Phys.*, 22 (2020) 063017.
[20] HU J.-Y. et al., *EPL*, 129 (2020) 10004.
[21] PAN D. et al., *Phys. Rev. Lett.*, 8 (2020) 1522.
[22] LI T. et al., *EPL*, 131 (2020) 60001.
[23] WU J. et al., *Quantum Eng.*, 1 (2019) e26.
[24] GAO Z. et al., *EPL*, 125 (2019) 40004.
[25] ZHOU Z. et al., *Sci. China Phys. Mech. Astron.*, 63 (2020) 230362.
[26] HE R. et al., *EPL*, 127 (2019) 50006.
[27] DAS N. et al., *Int. J. Theor. Phys.*, 60 (2021) 4044.
[28] NGUYEN B. A., *Phys. Lett. A*, 328 (2004) 6.
[29] DAS N. and PAUL G., *Int. J. Quantum Inf.*, 18 (2020) 2050038.
[30] GAO T. et al., *J. Phys. A: Math. Gen.*, 38 (2005) 5761.
[31] DAS N. and PAUL G., *Quantum Inf. Comput.*, 21 (2021) 0203.
[32] CURTY M. and SANTOS D. J., *Phys. Rev. A*, 64 (2001) 062309.
[33] LEE H. et al., *arXiv preprint, arXiv:quant-ph/0510144* (2005).
[34] LEE H. et al., *Phys. Rev. A*, 73 (2006) 042305.
[35] DAI L. et al., *Chin. Phys. Lett.*, 27 (2010) 050306.
[36] ZAWADZKI P., *Quantum Inf. Process.*, 18 (2019) 7.
[37] QIN S.-J. et al., *Opt. Commun.*, 283 (2010) 1566.
[38] CHANG C.-H. et al., *Quantum Inf. Process.*, 14 (2015) 3515.
[39] ZHANG Z.-J. et al., *Phys. Rev. A*, 75 (2007) 026301.
[40] FEI G. et al., *Chin. Phys. Lett.*, 28 (2011) 020303.
[41] CAI Q.-Y., *arXiv preprint, arXiv:quant-ph/0402052* (2004).
[42] LIU Z.-H. et al., *Quantum Inf. Process.*, 13 (2014) 1345.
[43] PEEV M. et al., *Int. J. Quantum Inf.*, 3 (2005) 225.
[44] LIN T.-H. et al., *Int. J. Theor. Phys.*, 52 (2013) 3199.
[45] FEI G. et al., *Chin. Phys. Lett.*, 25 (2008) 1561.
[46] DENG F.-G. et al., *Phys. Rev. A*, 72 (2005) 044302.
[47] GISIN N. et al., *Phys. Rev. A*, 73 (2006) 022320.
[48] GAO F. et al., *Phys. Lett. A*, 372 (2008) 3333.
[49] DAS N. and PAUL G., *Sci. Bull.*, 65 (2020) 2048.
[50] YAN L. et al., *Comput. Mater. Contin.*, 63 (2020) 1297.
[51] JIN X.-R. et al., *Phys. Lett. A*, 354 (2006) 67.
[52] NIE P.-H. et al., *Sci. Bull.*, 63 (2018) 1345.
[53] ZHU A.-D. et al., *Phys. Rev. A*, 73 (2006) 022338.
[54] JIANG N. et al., *npj Quantum Inf.*, 5 (2019) 1.
[55] NIELSEN M. A. and CHUANG I., *Quantum Computation and Quantum Information* (Cambridge University Press) 2002.
[56] GISIN N. et al., *Rev. Mod. Phys.*, 74 (2002) 145.