Optics Communications 282 (2009) 3375–3378

Contents lists available at ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

Eavesdropping on secure quantum telephone protocol with dishonest server

Mosayeb Naseri *

Islamic Azad University, Kermanshah Branch, Kermanshah, Iran

ARTICLE INFO

Article history:
Received 4 January 2009
Received in revised form 18 March 2009
Accepted 5 May 2009

PACS:
03.67.Hk
03.65.Ud

Keywords:
Quantum telephone
Quantum communication
Quantum cryptography

ABSTRACT

The crucial issue of quantum communication protocol is its security. In this paper, we show that in secure quantum telephone protocol proposed by Wen et al. [X. Wen et al., Opt. Commun. 275 (2007) 278–282] the dishonest server can obtain full information of the communication with zero risk of being detected.

1. Introduction

Quantum key distribution (QKD) is an ingenious application of quantum mechanics, in which two remote legitimate users (Alice and Bob) establish a shared secret key through the transmission of quantum signals and use this key to encrypt (decrypt) the secret messages [1–3]. Since BB84 scheme, the first quantum key distribution scheme first proposed by Bennett and Brassard in 1984 [1], quantum key distribution has attracted much attention of the researchers [2–5]. Quantum secure direct communication (QSDC) [6–9] is a branch of quantum cryptography, which allows the sender to transmit directly the secret message (not a random key) to the receiver in a deterministic and secure manner. Quantum secret sharing (QSS) [10,11] is another important application of quantum mechanics, which allows a secret to be shared among many participants in such a way that only the authorized groups can reconstruct it. Bostrm and Felbinger [12] put forward a ping–pong QSDC scheme by using Einstein–Podolsky–Rosen (EPR) pairs. Based on the idea of a ping–pong QSDC scheme, Nguyen [13] proposed a quantum dialogue scheme by using EPR pairs. However, an eavesdropper who adopts the intercept-and-resend attack strategy can steal the secret messages without being detected. A quantum telephone protocol including the dialing process and the talking one has been proposed by Wen et al. in 2007 [14]. In this protocol in the dialing process, with their respective secret keys, the legitimate communicators, Alice and Bob, can pass the authentication by Charlie acting as a telephone company. In the talking process, Charlie provides the authenticated Alice and Bob with a quantum channel sequence, on which Alice and Bob can communicate with each other directly by virtue of some encoding operations.

In this paper we show that in secure quantum telephone protocol, the dishonest server can obtain full information of the communication with zero risk of being detected. Here a fake entangled photons eavesdropping (FEP) scheme is presented, which reveals that the protocol is insecure under the dishonest server's fake entangled photons eavesdropping attack. This paper is organized as follows.

In the next section, we discuss the brief description of the secure quantum telephone protocol. A fake entangled photons eavesdropping (FEP) scheme is presented in Section 3. Finally, in Section 4, some conclusions and discussion are presented.

2. Secure quantum telephone

Let us start with the brief description of the secure quantum telephone protocol of Wen et al. [14].

The protocol is separated in two processes, dialing process and talking one. If Bob wants to call Alice privately, he asks Charlie (telephone server) to provide quantum channels. Once Alice and Bob have passed Charlie's authentication, they can talk with each other in the quantum talking process.

In dialing process, Bob asks Charlie to provide quantum channels between Alice and him. On receiving Bob's request, Charlie

* Tel.: +98 9183300026; fax: +98 8317243181.
E-mail address: sepehr1976@yahoo.com

0030-4018/$ - see front matter © 2009 Published by Elsevier B.V.
doi:10.1016/j.optcom.2009.05.012

prepares an ordered set of N qubits authentication sequences $B = [P_1(B), P_2(B), \ldots, P_N(B)]$ to identify Bob and an ordered set of N qubits authentication sequences $A = [P_1(A), P_2(A), \ldots, P_N(A)]$ to identify Alice, where $B(A)$-authentication sequence used to identify Bob(Alice) is prepared using bases $(B_z = |1\rangle, |0\rangle)$ or $(B_x = |+\rangle, |-\rangle)$ according to the telephone key $ID_B(ID_A)$. If the ith value of $ID_B(ID_A)$ is 1, Charlie prepares the ith qubit of the $B(A)$-authentication sequence using the bases $(|1\rangle, |0\rangle)$; or else, he prepares it using the bases $(|+\rangle, |-\rangle)$.

To verify Bob's and Alice's identity, Charlie sends the B-authentication sequence and A-authentication sequence to Bob and Alice. As the legitimate users Bob and Alice know their ID_B and ID_A sequences, therefore, they can accurately choose bases B_z or B_x to measure B-authentication sequence and A-authentication sequences according to their ID_B and ID_A sequences; so Charlie can check their measuring results. If their results are the same as those prepared by Charlie, their authentications are succeeded and Charlie provides quantum channels to them and the talking process begins. If not, he informs Bob and denies the service requested by Bob.

If the authentication to Alice and Bob has succeeded in the quantum dialing process, the talking process begins. In the talking process, if Alice has a secret message consisting of $2M$ secret classical bits $\{(i_1, j_1), (i_2, j_2), \ldots, (i_n, j_n), \ldots, (i_M, j_M)\}$, where $(i_n, j_n \in (0, 1))$, and Bob has another secret $2M$ secret classical bit message $\{(k_1, l_1), (k_2, l_2), \ldots, (i_n, j_n), \ldots, (k_M, l_M)\}$, where $(k_n, l_n \in (0, 1))$, Charlie prepares a random sequence of M Bell states $(|\psi_1\rangle_{ht}, |\psi_2\rangle_{ht}, \ldots\ldots, |\psi_M\rangle_{ht})$ as M quantum channels from the following four Bell states:

$$|\phi^{(\pm)}\rangle_{ht} = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)_{ht}, \quad |\psi^{(\pm)}\rangle_{ht} = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)_{ht}. \tag{1}$$

After preparing random sequence of M Bell states, to each quantum channel $|\psi_n\rangle_{ht}$, Charlie keeps one photon, qubit h_n (home photon) in his hands, and sends the other photon, qubit t_n (travel photon) to Bob.

Once Bob receives qubit t_n, he encodes his secret bits (k_n, l_n) by applying $C^t_{k^t_n, l_n}$ on it. Where $C^t_{k^t_n, l_n}$ denotes the following four transformations:

$$C^t_{00} = I^t = |0\rangle\langle 0| + |1\rangle\langle 1|, \quad C^t_{01} = \sigma^t_x = |0\rangle\langle 1| + |1\rangle\langle 0|,$$
$$C^t_{10} = i\sigma^t_y = |0\rangle\langle 1| - |1\rangle\langle 0|, \quad C^t_{11} = \sigma^t_z = |0\rangle\langle 0| - |1\rangle\langle 1|, \tag{2}$$

where the operation of these four kinds of transformations is presented in Table 1, which shows the relationship between the initial Bell states, the final Bell states and the corresponding operator $C_{x^t_n, y_n}$ applied on the travel qubit, where the initial states of the quantum channel are given in the row, four kinds of transformations are given in the column and the he final states of the quantum channel appear in the box.

After Bob's encoding operation, he pings the encoded qubit t_n to Alice. Then Alice encodes her secret bits (i_n, j_n) by performing the transformation $C^t_{i^t_n j_n}$ on the encoded qubit t_n received from Bob, and pongs it back to Bob.

After Bob's and Alice's encoding operations, the state of quantum channels become $|\psi_{x_n, y_n}\rangle_{ht}$, where:

Table 1
The relationship between the initial Bell states, the final Bell states and the corresponding operator $C^t_{x_n, y_n}$ applied on the travel qubit.

Quantum channel	$\|\psi^+\rangle$	$\|\psi^-\rangle$	$\|\phi^+\rangle$	$\|\phi^-\rangle$
$C^t_{0,0}$	$\|\psi_{0,0}\rangle = \|\psi^+\rangle$	$\|\psi_{0,0}\rangle = \|\psi^-\rangle$	$\|\psi_{0,0}\rangle = \|\phi^+\rangle$	$\|\psi_{0,0}\rangle = \|\phi^-\rangle$
$C^t_{0,1}$	$\|\psi_{0,1}\rangle = \|\phi^+\rangle$	$\|\psi_{0,1}\rangle = \|\phi^-\rangle$	$\|\psi_{0,1}\rangle = \|\psi^+\rangle$	$\|\psi_{0,1}\rangle = \|\psi^-\rangle$
$C^t_{1,0}$	$\|\psi_{1,0}\rangle = \|\phi^-\rangle$	$\|\psi_{1,0}\rangle = \|\phi^+\rangle$	$\|\psi_{1,0}\rangle = \|\psi^-\rangle$	$\|\psi_{1,0}\rangle = \|\psi^+\rangle$
$C^t_{1,1}$	$\|\psi_{1,1}\rangle = \|\phi^+\rangle$	$\|\psi_{1,1}\rangle = \|\psi^+\rangle$	$\|\psi_{1,1}\rangle = \|\psi^-\rangle$	$\|\psi_{1,1}\rangle = \|\phi^+\rangle$

$$|\psi_{x_n, y_n}\rangle_{ht} = C_{i^t_n j_n} C^t_{k_n, l_n} |\psi_n\rangle_{ht}. \tag{3}$$

When Bob receives qubit t_n from Alice, he requests Charlie for the qubit h_n of initial quantum channels $|\psi_n\rangle_{ht}$. Once receiving Bob's request, Charlie sends qubit h_n to him and publicly announces the initial Bell state of the quantum channel $|\psi_n\rangle_{ht}$. So Bob performs a Bell measurement on the entangled two qubits with the result in state $|\psi_{x_n, y_n}\rangle_{ht}$, and decodes Alice's bits as $(i_n = |x_n - k_n|, j_n = |y_n - l_n|)$. Also he publicly announces the results of his measurements, (x_n, y_n), to Alice, and lets her to decode his secret bits as $(k_n = |x_n - i_n|, l_n = |y_n - j_n|)$.

In order to detect eavesdropping, Alice and Bob may publish some of their bits to estimate the quantum bit error rate. For this, after receiving qubit t_n from Alice, Bob can switch to the control mode, i.e., measures the final state of some quantum channels $|\psi_n\rangle$, and publicly reveals (k_n, l_n) and (x_n, y_n) and asks Alice to publicly reveal (i_n, j_n) to check the eavesdropping. If both $(k_n = |x_n - i_n|, l_n = |y_n - j_n|)$ hold, there would be no eavesdropping.

In the original paper, it is explicitly stated (Ref. [14] p. 279 first column third paragraph) that Charlie is not necessarily trusted and it is claimed that he has no chance to overhear the content of dialogue. Unfortunately, it will be shown in the next section that in the secure quantum telephone protocol the dishonest server, Charlie, can obtain full information of the communication with zero risk of being detected.

3. Eavesdropping on secure quantum telephone protocol with dishonest server

In this section fake entangled photons eavesdropping (FEP) scheme is presented, in which, the dishonest server can gain full information of the communication without being detected. Consider the talking process of the nth bit string. Our attack scheme can be described as follows.

In talking process, when Bob sends the travel photon to Alice after his encoding operation, in line B to A, the dishonest server, Charlie, captures this photon and performs a Bell measurement on qubits, t_n and h_n with the results in state $|\psi_{k,l}\rangle$, where the values of k, l rely on the initial state and the final state of the quantum channel, as presented in Table 1. So Charlie can draw Bob's encoding message easily. After drawing Bob's message, Charlie prepares a fake EPR pair in the state $|\psi_n\rangle_{h't'} = |\psi_{k,l}\rangle_{h't'}$ and instead of the photon t_n, sends Alice the photon t'_n. So Alice will take photon t'_n for photon t_n, then she encodes her secret bits on photon t'_n and sends it back to Bob.

For a second eavesdropping try, in line A to B, Charlie can capture this photon and make a Bell-state measurement on the photons h''_n, t'_n, to obtain all the information about the operations done by Alice. Then he prepares another fake EPR pair in the state $|\psi_n\rangle_{h''t''} = |\psi_{x,y}\rangle_{h''t''}$ and keeps one photon, qubit h''_n in his laboratory, and sends the other photon, qubit t''_n to Bob. On the other hand, when Bob requests Charlie for the qubit h_n of quantum channel $|\psi_n\rangle_{ht}$, he sends him a qubit h''_n of quantum state $|\psi_{x,y}\rangle_{h''t''}$. So Bob will take qubit h''_n for the initial home qubit h_n and finally performs a Bell measurement on encoded fake entangled state $|\psi_{x,y}\rangle_{h''t''}$ for the state $|\psi_{x,y}\rangle_{ht}$. In this way, it is needless to say that, Charlie's eavesdropping introduces no errors in the outcomes of the measurements done by Bob and Alice and cannot be detected.

As an example, for the sake of simplicity for the talking process of the nth bit string, suppose that Bob wants to send bits (1,0) secretly to Alice and also Alice wants to send bits (0,1) to Bob.

If the authentication to Alice and Bob succeeds in the quantum dialing process, Charlie will prepare a random Bell state as a quantum channel from the four Bell states (1). Suppose Charlie provides the quantum channel $|\psi_n\rangle_{ht} = |\psi^+\rangle_{ht}$. Then Charlie keeps qubit h_n with him and sends qubit t_n to Bob. So Bob encodes his secret bits