Optik 125 (2014) 624–627

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

Quantum key distribution with several intercepts and resend attacks with partially non-orthogonal basis states

Mustapha Dehmani, Hamid Ez-Zahraouy*, Abdelilah Benyoussef

Laboratoire de Magnétisme et de Physique des Hautes Energies, Faculté des Sciences, Université Mohammed V-Agdal, Rabat, Morocco

ARTICLE INFO

Article history:
Received 10 February 2013
Accepted 22 June 2013

Keywords:
Quantum cryptography
Intercepts and resend attacks
Non-orthogonal basis states
Information
Security

ABSTRACT

The effect of partially non-orthogonal basis states for several intercept and resend attacks of the Bennett–Brassard cryptographic protocol has been studied. The quantum error and the mutual information are computed for arbitrary angles η of the non-orthogonal basis states. It is found that the secure information depend strongly on the angle η, the probability of intercepts and resend attack and the number of eavesdropper. Besides, it is found that for any eavesdroppers number $N \geq 2$, the protocol is more secured for $(\pi/2) < \eta < (3\pi/2)$, while for $N = 1$, the protocol is more secured for $\eta = \pi/2$ or $3\pi/2$ which correspond to the totally orthogonal basis states.

1. Introduction

In practice, all the protocols of quantum cryptography using photon as carriers of information, because they are relatively easy to produce, easy to handle and travel (very) quickly in optical fibers, while suffering little attenuation. There are as many protocols as properties on which encode information: polarization, amplitude, phase, frequency and time. Historically, the first protocol to be implemented is called BB84 [1].

The information is encoded in the polarization of single photons, choosing two non-independent polarization bases for safety.

This protocol has undergone several variants [2,3], and has been implemented many times. E91, another protocol [4], designed by Artur Ekert, uses entangled states EPR polarization-encoded and was developed independently of BB84. Both protocols are generally considered the founding protocols of quantum cryptography. Other protocols use highly attenuated laser states, while performing a discrete measure (detectors or photon counters). Examples include protocols DPS (differential phase shift) [5], where the information is encoded in the successive phases of the pulses, but also the protocols to frequency coding [6–8], and protocols to temporal coding [9,10].

The quantum key distribution with several intercepts and resend attacks [11] and cloning attack [12] with orthogonal bases is studied in previous work. Also the channel effect on the quantum key distribution with several intercept and resend attacks is studied [13].

Moreover, for the SARG04 key-distribution protocol, an optimal attack of eavesdropper on the transmitted key is explicitly constructed for arbitrary angles between the basis states [14], and quantum key distribution in a single photon regime with non-orthogonal basis states is recently presented by Kronberg and Molotkov [15] where an explicit optimal attack on the distributed key has been constructed.

Our aim in this paper is to study both effects partially non-orthogonal basis states and the multiple sequential intercept and resend attacks on the security of the BB84 quantum key distribution protocol.

The paper is organized as follows. The protocol is detailed in Section 2. Section 3 is devoted to the results and discussion, while Section 4 is reserved for the conclusion.

2. The protocol

2.1. The model

We consider a set of two bases states a and b:

$$|0_a\rangle = \begin{pmatrix} \cos\left(\frac{\eta}{2}\right) \\ \sin\left(\frac{\eta}{2}\right) \end{pmatrix}, \quad |1_a\rangle = \begin{pmatrix} \cos\left(\frac{\eta}{2}\right) \\ -\sin\left(\frac{\eta}{2}\right) \end{pmatrix} \quad \text{and} \quad |0_b\rangle = \begin{pmatrix} \frac{\sqrt{2}}{2} \\ -\frac{\sqrt{2}}{2} \end{pmatrix}, \quad |1_b\rangle = \begin{pmatrix} \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} \end{pmatrix} \tag{1}$$

* Corresponding author.
E-mail address: ezahamid@fsr.ac.ma (H. Ez-Zahraouy).

0030-4026/$ – see front matter © 2013 Elsevier GmbH. All rights reserved.
http://dx.doi.org/10.1016/j.ijleo.2013.06.099

$$|0_a\rangle = \cos\left(\frac{\eta}{2}\right)|0\rangle + \sin\left(\frac{\eta}{2}\right)|1\rangle, \quad |1_a\rangle = \cos\left(\frac{\eta}{2}\right)|0\rangle - \sin\left(\frac{\eta}{2}\right)|1\rangle \tag{2}$$

$$|0_b\rangle = \frac{\sqrt{2}}{2}|0\rangle - \frac{\sqrt{2}}{2}|1\rangle, \quad |1_b\rangle = \frac{\sqrt{2}}{2}|0\rangle + \frac{\sqrt{2}}{2}|1\rangle \tag{3}$$

In all the following we consider that those involved in communication operate using the bases $\{|0_a\rangle, |1_a\rangle\}$ and $\{|0_b\rangle, |1_b\rangle\}$. It is clear that $\langle 0_a|1_a\rangle = \cos\eta$ and $\langle 0_b|1_b\rangle = 0$.

Alice sends a sequence of photons to Bob while choosing randomly to send 1 or 0 by using one of the bases from a set of the bases $\{|0_a\rangle, |1_a\rangle\}$ and $\{|0_b\rangle, |1_b\rangle\}$. Bob measures each photon by selecting random between two polarization analyzers. Between them are several eavesdroppers, which intercept some photons with probabilities ω_i, measure the polarization by choosing randomly an arbitrary base which one is characterized by η_i. At the photons place which they do not measure, they put randomly 0 or 1 in their chains of bits. Then, Alice and Bob exchange in a traditional way the bases which they used; they remove in their chain of bits those exchanged in different bases. For studying the security of information exchanged between two honest parties Alice and Bob, we introduce the notion of mutual information and in this way we calculate the mutual information between Alice and Bob and the mutual information between Alice and every eavesdropper.

2.2. The mutual information

The direct reconciliation information between Alice and Bob is governed by the mutual information $I(A, B)$ given by:

$$I(A, B) = 1 + P_{AB}(0/0)\mathrm{Log}_2(P_{AB}(0/0)) + P_{AB}(1/0)\mathrm{Log}_2(P_{AB}(1/0)) \tag{4}$$

$P_{AB}(x_B/x_A)$ is the conditional probability that Bob receives a photon polarized ($x_B = 0;1$) with respect that Alice sends a photon polarized ($x_A = 0;1$)

This probability is given by:

$$P_{AB}(0/0) = P_{AB}(1/1) = \sum_{k=0}^{n}\frac{2^{n-k}+1}{2^{n-k+1}} \times \sum_{i_1,\ldots,i_k=1,n}\prod_{j=1}^{k}(1-\omega_{i_j}\sin^2(\eta_{i_j}))\prod_{l=k+1}^{n}\omega_{i_l}\sin^2(\eta_{i_l}) \tag{5}$$

$$P_{AB}(0/1) = P_{AB}(1/0) = 1 - P_{AB}(0/0) \tag{6}$$

While the mutual information $I(A, E_m)$ between Alice and the mth eavesdropper E_m is written as:

$$I(A, E_m) = 1 + P_{AE_m}(0/0)\mathrm{Log}_2(P_{AE_m}(0/0)) + P_{AE_m}(1/0)\mathrm{Log}_2(P_{AE_m}(1/0)) \tag{7}$$

where, $P_{AE_m}(x_{E_m}/x_A)$ is the conditional probability that the eavesdropper copies a photon polarized ($x_{E_m} = 0;1$) using an arbitrary bases characterized by η_m with respect that Alice sends a photon polarized ($x_A = 0;1$)

$$P_{AE_m}(0/0) = P_{AE_m}(1/1) = \frac{1-(\omega_m/2)(1+\cos(\eta_m))}{2} + \sum_{k=0}^{m-1}\frac{2^{m-k}+1}{2^{m-k+1}}\sum_{i_1,\ldots,i_k=1,m-1}\prod_{j=1}^{k}\left(1-\omega_{i_j}\left(\frac{1+\cos(\eta_{i_j})}{2}\right)\right)\prod_{l=k+1}^{m}\omega_{i_l}\left(\frac{1+\cos(\eta_{i_l})}{2}\right) \tag{8}$$

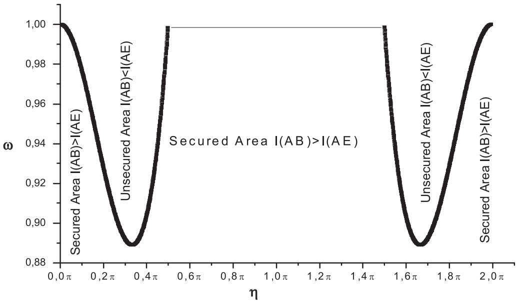

Fig. 1. Phase diagram in the space (η, ω) showing the transition between secured and unsecured information.

$$P_{AE_m}(0/1) = P_{AE_m}(1/0) = 1 - P_{AE_m}(0/0) \tag{9}$$

In the case of many eavesdroppers the lost information between Alice and Bob corresponds to the maximum information copied by the entire eavesdroppers:

$$I(A, E) = \underset{i=1,m}{\mathrm{Max}}[I(A, E_i)] \tag{10}$$

The error rate or the error probability P_{err} is given by [13,16,17]: $(11)P_{err} = \sum_{x_A,x_B}|P_{AB}(x_A, x_B)|_{\omega_i=0} - P_{AB}(x_A, x_B)|_{\omega_i\neq 0}|$

The secret information I_s is an important parameter to study security of a quantum cryptography protocol and it is given by:

$$I_s = I(A, B) - I(A, E) \tag{12}$$

The quantum error Q_{err} is the value of the error probability P_{err} for which $I(A, B) = I(A, E)$. However, for $P_{err} < Q_{err}$, $I(A, E) < I(A, B)$, while for $P_{err} < Q_{err}$, $I(A, E) > I(A, B)$.

In the particular case, where the eavesdropper communicate between them and try to intercept the same photon with identical probability and using an identical base ($\omega_i = \omega$ and $\eta_i = \eta$, for $i = 1, \ldots, N$), Eqs. (5) and (8) become, respectively

$$P_{AB}(0/0) = \frac{1}{2}\left[1 + \left(1 - \frac{\omega}{2}\sin^2(\eta)\right)^N\right] \tag{13}$$

$$P_{AE_m}(0/0) = \frac{1}{2}\left[1 + \frac{\omega}{2}(1+\cos(\eta))\left(1 - \frac{\omega}{2}(1+\cos(\eta))\right)^{m-1}\right] \tag{14}$$

And the error probability is given by:

$$P_{err} = \frac{1}{2}\left(1 - \left(1 - \frac{\omega}{2}\sin^2(\eta)\right)^N\right) \tag{15}$$

3. Results and discussion

In this section we will start with the effect of one eavesdropper and we will examine the mutual information between Alice and Bob $I(A,B)$ and the loosed information $I(A,E)$. It should be noted that the totally orthogonal basis states corresponds to $\eta = \pi/2$ or $3\pi/2$.

The phase diagram (η, ω) presented in Fig. 1 shows the transition line between secured and unsecured area in the presence of one eavesdropper. It is clear that the secure area depends strongly on the basis states angle η and the attack probability ω and if $(\pi/2) < \eta < (3\pi/2)$ the information exchanged between Alice and Bob is secured (i.e. $I(A, B) > I(A, E)$) independently of the attack probability ω.