ADVANCED JOURNAL OF SCIENCE AND ENGINEERING
Winter 2020, Volume 1, Issue 1, Pages 20-26; DOI: https://doi.org/10.22034/AJSE2011020

Original Research Article

https://adv-j-sci-eng.com

A Chaotic Quantum Secure Communication Scheme Based on a Mixed Open System

Nafiseh Hematpour[1,✉], Sodeif Ahadpour[1], Sohrab Behnia[2]

Received: April 21, 2020 / *Accepted*: April 28, 2020 / *Published Online*: April 30, 2020

ABSTRACT. A system of a particle kicked by a Gaussian beam is studied. A description of the chaotic behavior of this system is presented. The suitability of the model for cryptography is demonstrated by applying the Einstein-Podolsky-Rosen correlations and calculating the entanglement parameter. Based on this model, we introduce a quantum secure communication protocol. By using the Shannon information theory about the detailed analysis of the Gaussian cloner attack strategy about this system, we demonstrate that the system is both safe and reliable. The results show that the proposed algorithm improves the problem of failure of encryption, such as small key space and level of security.

Keywords: Chaos; Quantum cryptography; Secure communication; Quantum key distribution; Discrete variable.

INTRODUCTION

Quantum cryptography, which is also known as Quantum key distribution, is a state of the art approach that represents the features of quantum mechanics to guarantee the safe exchange of secret keys. The laws of quantum mechanics govern fundamental particle physics. At atomic scales, the fundamental particles lack precise location and speed. The famous Heisenberg uncertainty principle states that any observer who wishes to obtain location information loses speed information. This is a fundamental limitation and has nothing to do with the observer's technology. The first application of quantum information theory introduced in the mid-twentieth century was proposed by Wiesner.[1] As a benefit, the quantum cryptography could supply a secure communication way.[2-8] The security is assured by the laws of quantum mechanics.[1, 2, 5, 9] Many Quantum Key Distribution (QKD) systems that are dependent on a Discrete Variable (DV) are exhibited.[10] In this system, an encoded binary bit into a quantum state is sent by the sender (Alice) to the receiver (Bob). In this case, the decoded bit value by Bob cannot be concluded for Alice. This attribute means that the system is deterministic, which is very important for assuring the security of this protocol. However, the deterministic estate results in a loss of qubits. Most recently, many quantum secure communications based on continuous variables have been proposed.[11, 12] We now want to propose a new deterministic quantum communication system, dependent on DV entanglement state or non-orthogonal state.[13-15] These systems clearly increase the value efficiency of quantum communication schemes by applying the technique of ping-pong of photons.16 We introduce a quantum secure communication system dependent upon the correlation of the DV (Discrete Variable).[17] There are two principles for examining the cryptography on a discrete kicked Hamiltonian system: 1) this Hamiltonian is super sensitive to primary condition, i.e., it has a chaotic function; 2) the cryptographic function of this Hamiltonian has a high degree of safety, that the smallest change regarding the input from Alice can lead to the detection of Eve. Therefore, Eve is practically impossible because of the reason we had mentioned and also owing to the right below.[18-21] This system can be used as a QKD system and quantum encryption to send a message. The discrete Gaussian modulation used on

✉ Corresponding author.
E-mail address: n_hematpour@uma.ac.ir (N. Hematpour)

[1] Department of Physics, University of Mohaghegh Ardabili, Ardabil, Iran

[2] Department of Physics, Urmia University of Technology, Urmia, Iran

the DV carrier increases the competence of the quantum secret communication noticeably.[5] The security of the system against the general Gaussian-cloner eavesdropping attack is illustrated using Shannon's information theory.[22-24] The paper continues as follows: our model system is proposed, then we will propose an algorithm and calculate entanglement parameter F for a mixed open system. Furthermore, we are going to study security analysis by using the Shannon's information theory. Finally, we provide the obtained conclusions.

MATERIALS AND METHODS

Models

We start with the Hamiltonian of a particle kicked by a Gaussian potential:

$$H = \frac{p^2}{2m} - K'T\exp(-\frac{x^2}{2\Delta^2})\Sigma_n\delta(t-nT), \quad (1)$$

Classical equations of motion read:

$$\frac{dp}{dt} = -\frac{\partial H}{\partial x} = -K'T\frac{x}{\Delta^2}\exp(-\frac{x^2}{2\Delta^2})\Sigma_n\delta(t-nT), \quad (2)$$

$$\frac{dx}{dt} = \frac{\partial H}{\partial p} = \frac{p}{m}, \quad (3)$$

by considering:

$$\overline{x} = \frac{x}{\Delta}, \overline{t} = \frac{t}{T}, \overline{p} = \frac{pT}{m\Delta} \text{ and } k = \frac{K'T^2}{m\Delta^2}$$

The dimensionless motion equations are as follows[25-28]:

$$\begin{cases} \dot{\overline{p}} = -K\overline{x}\exp(-\frac{\overline{x}^2}{2})\Sigma_n\delta(\overline{t}-n), & (A1) \\ \dot{\overline{x}} = \overline{p}. & (A2) \end{cases}$$

Integration of eq. (A1) from n to (n + 1) and substitution the solution of (A1) into (A2):

$$\dot{x} = p(n) - Kx(n)\exp(-\frac{x(n)^2}{2}), \quad (4)$$

We integrate of eq. (4) from t= n to t= (n+1), and insert x(n) = x, x(n+1) = x_{n+1}, p(n) = p_n and p(n + 1) = p, and obtain:

$$\begin{cases} p_{n+1} = p_n - Kx_n\exp(-\frac{x_n^2}{2}), \\ x_{n+1} = x_n + p_n - Kx_n\exp(-\frac{x_n^2}{2}). \end{cases} \quad (5)$$

Where K is a parameter that determines "how chaotic" the map is. Fig. (1) and Fig. (2) depict the phase space for the particle kicked by a Gaussian beam Hamiltonian. The first property of this map is reflection symmetry; (x, p) → (-x, -p). This property of this map is used to calculate the main periodic orbits.[25, 21]

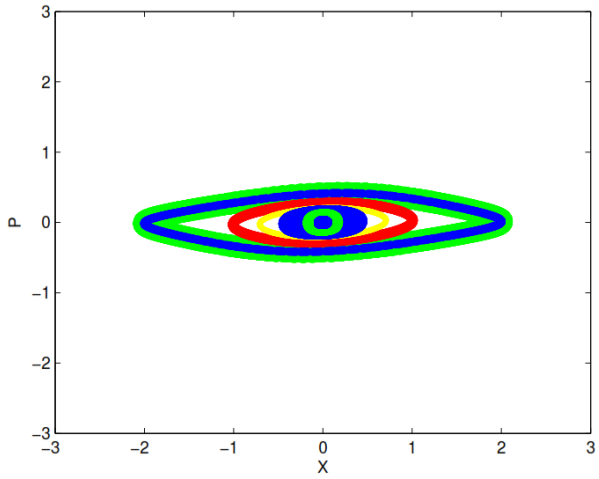

Fig. 1: Plot of the phase space for fixed parameters of "K". The curves are the level sets of the particle kicked by a Gaussian beam Hamiltonian, eq. (5). The different colors correspond to trajectories beginning from different initial conditions.

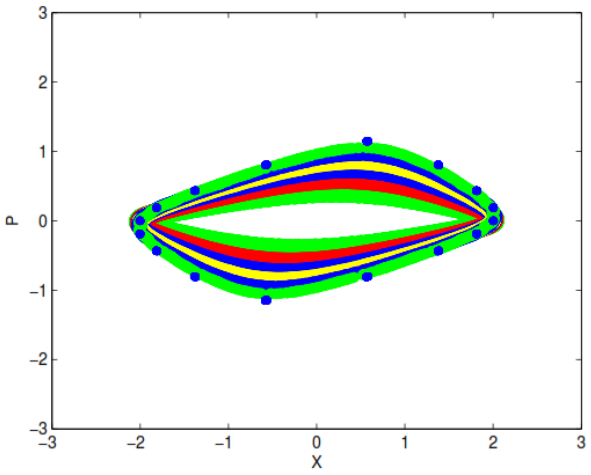

Fig. 2: Plot of the phase space for differential parameters of "K". The curves are the level sets of the particle kicked by a Gaussian beam Hamiltonian, eq. (5). The different colors correspond to trajectories beginning from fixed initial condition.

Encryption of Algorithm Based on the Standard Map

If we imagine (p_1, x_1) as two inputs for cryptography system, therefore, (p_2, x_2) are considered as outputs of the first cryptographic cycle. So if we implement secondary iterate in second cryptography cycle n = 2; therefore, (p_3, x_3) is taken into account as outputs of the secondary cryptography cycle. We obtain:

$$M: \begin{cases} p_2 = p_1 - Kx_1 exp(-\frac{x_1^2}{2}) \\ x_2 = x_1 + p_2 \end{cases} \quad (6)$$

$$M: \begin{cases} p_3 = p_2 - Kx_2 exp(-\frac{x_2^2}{2}) \\ x_3 = x_2 + p_3 \end{cases} \quad (7)$$

We have:

$$\begin{cases} \delta p = p_3 + \gamma_p p_2 \\ \delta x = x_3 - \gamma_x x_2 \end{cases} \quad (8)$$

where γ_x and γ_p are coefficients for giving minimum variance, respectively.

Using eq. (6) to obtain minimum variance $\triangle_x^2$ and $\triangle_p^2$:

$$\begin{cases} \triangle_x^2 = <(\delta x)^2> - <\delta x>^2 \\ \triangle_p^2 = <(\delta p)^2> - <\delta p>^2 \end{cases} \quad (9)$$

A minimum variance occurs for a particular quantity of γ.

$$\triangle_x^2 = <(\delta x)^2> - <\delta x>^2 = <(x_3 - \gamma x_2)^2> - <(x_3 - \gamma x_2)>^2 \quad (10)$$
$$\triangle_x^2 = \triangle^2 x_3 + \gamma^2 \triangle^2 x_2 - 2\gamma < x_3 x_2 >$$

and:

$$\triangle_p^2 = <(\delta p)^2> - <\delta p>^2 = <(p_3 + \gamma p_2)^2> - <(p_3 + \gamma p_2)>^2 \quad (11)$$
$$\triangle_p^2 = \triangle^2 p_3 + \gamma^2 \triangle^2 p_2 + 2\gamma < p_3 p_2 >$$

Derivative of $\triangle_x^2$ and $\triangle_p^2$ with respect to γ, we obtain:

$$\frac{d\triangle_x^2}{d\gamma} = 0 \quad (12)$$
$$\gamma_{min} = \frac{< x_3 x_2 >}{\triangle^2 x_2}$$

and:

$$\frac{d\triangle_p^2}{d\gamma} = 0 \quad (13)$$
$$\gamma_{min} = -\frac{< p_3 p_2 >}{\triangle^2 p_2}$$

By defining the important parameter F_a, which is both a criterion for the entanglement of two systems and the necessary condition for cryptography, we want to show that $F_a < 1$ is an essential condition for cryptography.

$$F_a = (\triangle_x^2)(\triangle_p^2) \quad (14)$$

See Appendix A for details of calculating parameter F_a. We obtain:

$$F_a = \frac{9K^4}{4e^2} + \frac{18K^4}{e^3} \quad (15)$$

By considering eq. (20) we can illustrate that in this model cryptography creation depends on F_a, in which $K < 1$.

$$\begin{cases} K = 0.1 \Rightarrow F_a = 0.1200966 * 10^{-4} < 1 \\ K = 0.3 \Rightarrow F_a = 2.9184629 * 10^{-3} < 1 \\ K = 0.7 \Rightarrow F_a = 0.2883633 < 1 \\ K = 0.9 \Rightarrow F_a = 0.78798494 < 1 \end{cases} \quad (16)$$

According to the following formula:

$$\begin{cases} x_{out1} = \sqrt{G\eta} x_3 + \sqrt{(G-1)\eta} x_7 + \sqrt{1-\eta} x_9 = X_{10} \\ p_{out1} = \sqrt{G\eta} p_3 - \sqrt{(G-1)\eta} p_7 + \sqrt{1-\eta} p_9 = P_{10} \end{cases} \quad (17)$$

We can use eq. (22), to calculate Minimum variance $\triangle^2 X_{eve}$ and $\triangle^2 P_{eve}$. Given the assumptions $G = 1$ and $\eta = 1$ (Eve absent), we obtain parameter F_b (See Appendix A).

$$F_b = (\triangle^2 X_{eve})(\triangle^2 P_{eve})$$

$$F_b = \frac{3\Sigma^2 K^4}{4e^2} + \frac{6\Sigma^2 K^4}{e^3}$$

Alice reports to Bob both of the measurement results. Bob is estimated F_b parameter.

Protocol

Such a suggested system can be used for random distribution to convey messages utilizing different input parameters. The protocol steps are as follows. step1. *Step 1*. Alice modulates on two inputs with states x_1, p_1 by using mapping, M:

$$M: \begin{cases} p_{n+1} = p_n - K x_n exp(-\frac{x_n^2}{2}) \\ x_{n+1} = x_n + p_{n+1} \end{cases}$$

Therefore, these two combinations create two new states after the first iteration, two new states are x_2, p_2, which are input states for second iterate state. When that parameter has K, states x_3 with p_3 are correlated and this correlation increases with K coefficient.

Step 2. Alice can calculate parameter F_a between x_3, p_3 according to the equation mentioned above on the previous page. Alice writes the results of the measurement. F_a is a way to detect Eve after the end of the transmission. Although the states of x_3, p_3 have been sent to Bob.

Step 3. Bob applies the third iterate to receive a state of x_3, p_3. State x_3, p_3 is similar to x_4, p_4, when Eve is absent. After the end of the operation, Bob measures both of the x_4 or p_4 in output mode of x_{12}, p_{12}.

Step 4. Alice reports Bob the results of both measurements. Bob estimates parameter F_b. If $F_b > F_a$ then, Eve exists, and if $F_b = F_a$, Eve absent.

RESULTS AND DISCUSSION

Quantum cryptography security is an important issue. The proposed system security is reviewed by Shannon

Information Theory. To illustrate the security and detection of eavesdropping, the secret information rate $\triangle I$ and entanglement parameter F are used, respectively. The secret information rate is the only Alice-Bob connection in Quantum Key Distribution.

$$\triangle I = I(\alpha,\beta) - I(\alpha,\varepsilon)$$

$I(\alpha,\beta)$ and $I(\alpha,\varepsilon)$ are the mutual information between Alice and Bob and the mutual information of Alice and Eve, respectively.

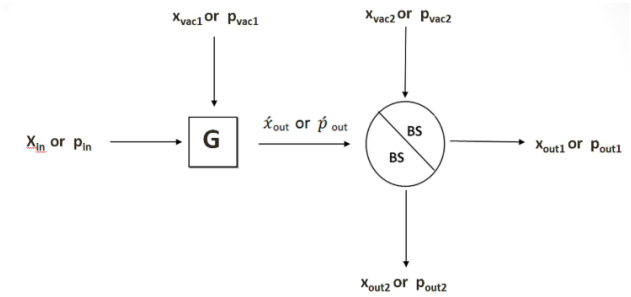

Fig. 3: Schematic demonstration of a quantum secure communication scheme based on Discrete Variable of the particle kicked by a Gaussian beam. LA: linear amplifier. BS: beam splitter. G: the gain of LA. η: the transmission coefficient of BS. The Arabic numerals denote the mode.

Fundamental of General Gaussian Cloner

To describe the general Gaussian cloner, different parts of it, including Liner Amplifier (LA) and Beam Splitter (BS), must be examined. If x_3 or p_3 and x_7 or p_7 are input LA, one of outputs is obtained as follows:

$$\acute{x}_{out} = \sqrt{G}x_3 + \sqrt{G-1}x_7$$

or

$$\acute{p}_{out} = \sqrt{G}p_3 - \sqrt{G-1}p_7$$

where $G > 1$ is the power of LA and $\acute{x}_{out}$ or $\acute{p}_{out}$ and x_9 , or p_9 are two inputs for BS. If $G = 1$, the Gaussian cloner is reduced to the beam splitter. [29, 30]

The Gaussian cloner outputs are listed below:

$$\begin{cases} x_{out1} = \sqrt{G\eta}x_{in} + \sqrt{(G-1)\eta}x_{vac1} + \sqrt{1-\eta}x_{vac2} = X_{10} \\ p_{out1} = \sqrt{G\eta}p_{in} - \sqrt{(G-1)\eta}p_{vac1} + \sqrt{1-\eta}p_{vac2} = P_{10} \\ x_{out2} = \sqrt{\eta}x_{vac2} - \sqrt{G(1-\eta)}x_{in} + \sqrt{(1-\eta)(G-1)}x_{vac1} = X_{11} \\ p_{out2} = \sqrt{\eta}p_{vac2} - \sqrt{G(1-\eta)}p_{in} + \sqrt{(1-\eta)(G-1)}p_{vac1} = P_{11} \end{cases} \quad (18)$$

By using eq. (22), one may investigate the outputs of the Gaussian cloner (Fig. 3).

Secret Information Rate

The secret key can be provided by Alice and Bob with classical error correlation and privacy enhancement techniques when $\triangle I > 0$. To achieve $I(\alpha,\beta)$, $I(\alpha,\varepsilon)$ according to Shannon information theory, the probability distribution of X and P is considered in all states. Assuming that the Gaussian cloner was used by Eve to eavesdrop on the quantum channel[31,32], we will continue the discussion.

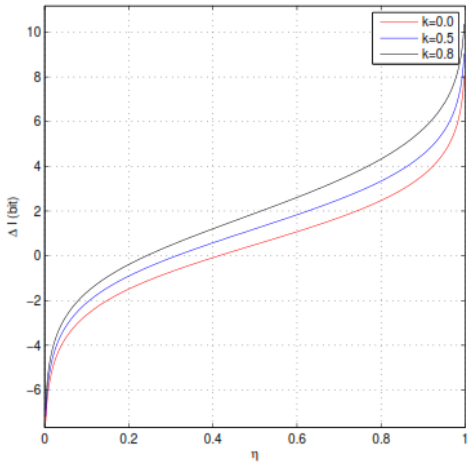

Fig. 4: The dependence of ΔI on η in the QKD process ($\Sigma = 10$; $\sigma = 1$; and $k = 0.1$).

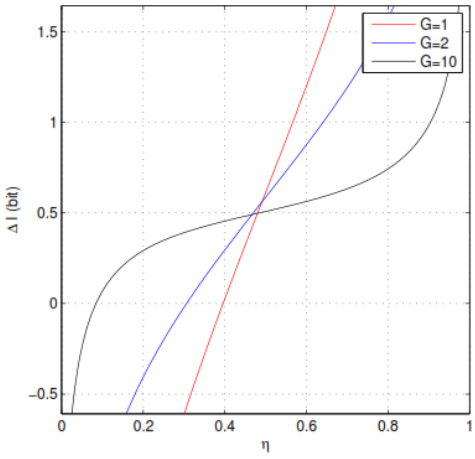

Fig. 5: The dependence of ΔI on η in the QKD process ($\Sigma = 10$; $\sigma = 1$; and G = 1).

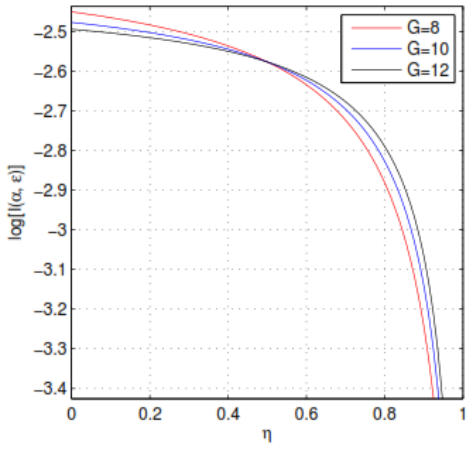

Fig. 6: Schematic The dependence of $I(\alpha,\epsilon)$ on η in the quantum encryption process. The parameters are $\Sigma = 10$; $\sigma = 30$; and $k = 0.1$.

We have:

$$\begin{cases} x_{out1} = \sqrt{G\eta}x_3 + \sqrt{(G-1)\eta}x_7 + \sqrt{1-\eta}x_9 = X_{10} \\ p_{out1} = \sqrt{G\eta}p_3 - \sqrt{(G-1)\eta}p_7 + \sqrt{1-\eta}p_9 = P_{10} \\ x_{out2} = \sqrt{\eta}x_9 - \sqrt{G(1-\eta)}x_3 + \sqrt{(1-\eta)(G-1)}x_7 = X_{11} \\ p_{out2} = \sqrt{\eta}p_9 - \sqrt{G(1-\eta)}p_3 + \sqrt{(1-\eta)(G-1)}p_7 = P_{11} \end{cases} \quad (19)$$

In the equation above, the random variables follow Gaussian distribution.

$$\begin{cases} x_3 \quad and \quad p_3 = N(0, \Sigma^2) \\ x_i \quad and \quad p_i = N(0, \sigma^2) \end{cases} \quad (20)$$

With $i = 7, 9$, that is vacuum state. Now, Bob applies x_4 or p_4 to receive state X_{10} or P_{10}. States X_{10} or P_{10} is similar to x_3 or p_3, when Eve is absent in the quantum channel.[32]

$$\begin{cases} X_{12} = x_4 = x_3 + p_4 \\ P_{12} = p_4 = p_3 - Kx_3 exp(-\frac{x_3^2}{2}) \end{cases} \quad (21)$$

According to eq. (9), we can obtain the variances of X_{11} and P_{11}.

$$\triangle^2 X_{11} = \eta < {x_9}^2 > + G(1-\eta) < {x_3}^2 > + (G-1)(1-\eta) < {x_7}^2 >$$

$$\triangle^2 P_{11} = \eta < {p_9}^2 > + G(1-\eta) < {p_3}^2 > + (G-1)(1-\eta) < {p_7}^2 >$$

We have to calculate the variance:

$$\begin{cases} \triangle^2 X_{11} = \eta\sigma^2 + G(1-\eta)\Sigma^2 + (G-1)(1-\eta)\sigma^2 \\ \triangle^2 P_{11} = \eta\sigma^2 + G(1-\eta)\Sigma^2 + (G-1)(1-\eta)\sigma^2 \end{cases} \quad (22)$$

The variance of the signal distribution of measuring either X or P is:

$$M = G(1-\eta)\Sigma^2 \quad (23)$$

For noise, the variance is calculated as follows:

$$N = \eta\sigma^2 + (G-1)(1-\eta)\sigma^2 = \sigma^2[\eta + (G-1)(1-\eta)] \quad (24)$$

From the above equations for Alice and Eve, we calculate the signal-to-noise ratio:

$$\gamma_{\alpha\varepsilon} = \frac{M}{N} \quad (25)$$

The Additive White Gaussian Noise (AWGN) channel capacity is obtained by considering Shannon's information theory[33, 13, 34] as follows:

$$I = \frac{1}{2}\log_2(1+\gamma) \quad (26)$$

In the above equation, the signal-to-noise ratio and variance of the signal and the variance of the noise are shown with $\gamma = \frac{\Sigma^2}{\sigma^2}$, $\Sigma^2$and σ^2, respectively.
Given the Gaussian distribution signal and the AWGN channel and the mutual information channel capacity, the mutual information between Alice and Eve is obtained as follows:

$$I(\alpha, \varepsilon) = \frac{1}{2}\log_2(1+\gamma_{\alpha\varepsilon}) \quad (27)$$

By calculating the variance of the signal distribution for the system, the following equation is obtained:

$$P = G\eta\Sigma^2[2 + K^2 exp(-\Sigma^2 G\eta) - 2Kexp(\frac{-\Sigma^2 G\eta}{2})]$$

The noise variance is calculated as follows:

$$Q = \sigma^2[\eta(G-1)+(1-\eta)][2+K^2 exp(-\sigma^2[\eta(G-1)+(1-\eta)]) - 2Kexp(-\frac{\sigma^2[\eta(G-1)+(1-\eta)]}{2})]$$

The signal-to-noise ratio is gotten for Alice and Bob:

$$\gamma_{\alpha\beta} = \frac{P}{Q} \quad (28)$$

The mutual information of these two people can be calculated as follows:

$$I(\alpha, \beta) = \frac{1}{2}\log_2(1+\gamma_{\alpha\beta}) \quad (29)$$

By using eqs. (44) and (45), we acquire the mutual information *I(α, β)* and *I(α, ε)*. Alice and Bob can obtain a secure final key given the classical error correction and privacy amplification provided that *I(α, β) > I(α, ε)* exists. The final key assembled based on the circumstance.[30]

$$\triangle I = I(\alpha, \beta) - I(\alpha, \varepsilon) > 0 \quad (30)$$

In the absence of Eve ($G = 1$ and $\eta = 1$) based on eqs. (45) and (46) we have:

$$I(\alpha, \varepsilon) = 0$$

$$\Delta I = I(\alpha, \beta) = \frac{1}{2}\log_2(1 + \frac{\Sigma^2[2 + K^2 exp(-\Sigma^2) - 2Kexp(-\frac{\Sigma^2}{2})]}{2K}) \quad (31)$$

The quantum channel capacity for Alice and Bob is evaluated by ΔI. The increase in ΔI with Σ^2 in eq. (47) is seen. If $\Delta I > 0$, we obtain a secure key for a QKD scheme. In the remaining text, we consider $\Sigma = 10$; $\sigma = 1$. Figs. 4, 5 are plotted for demonstrating dependence between ΔI and η. In Fig. 4, for larger k at $\Delta I = 0$, η is smaller. It is more appropriate to implement the key distribution, a high degree of entanglement for the CV EPR pair. In Fig. 5, the relevancy of ΔI and η is plotted for different G. η becomes smaller by considering large

G and $\Delta I = 0$. By focusing on the mutual information $I(\alpha, \epsilon)$, we try to know how much information Eve can get through eavesdropping in this quantum encryption algorithm. In Fig. 6 we plot the dependence of $I(\alpha, \epsilon)$on η with $k = 0.1$, $\Sigma = 10$ and $\sigma = 30$ for different G. For example with $G = 10$, when Eve receives thirty percent of the signal, the information $I(\alpha, \epsilon)$are 0.0033 bits. This information is insignificant compared to the mutual information of Bob and Alice. Besides, the security level requested, the parameters k, σ may be selected. Our results are better than those already reported.[22] For $G = 10$ in Fig. 6, extracted information by Eve is 0.00333 bits but in similar condition with our earlier work[22] is 0.1262 bits.

CONCLUSION

We present a quantum secure communication system with the correlation of discrete variable EPR. This method can be used to distribute quantum keys and to transmit many messages whose key is already shared. The Hamiltonian and proposed algorithm mentioned above recuperate some failures of encryption such as small key space and level of security. The security of the proposed method against the Gaussian-cloner attack is illustrated by calculating the secret information rate ΔI and the Shannon mutual information *I(α, ε)*. Also, the DV EPR correlation produced by NOPA provides its physical security. Given the work being done today in the field of Einstein-Podolsky-Rosen (EPR) entanglement,[35] it could be the promise of quantum communication. We can hope that subsequent studies increase encryption speed.

APPENDIX A.

Calculating the Entanglement Parameter

As usual, to calculate Fa we have to find $\triangle_x^2$, $\triangle_p^2$.

$$< x_3x_2 >=< [x_2+p_2-Kx_2exp(-\frac{x_2^2}{2})]x_2 >=< x_2^2 > + < p_2x_2 > -K < x_2^2exp(-\frac{x_2^2}{2}) >$$

$$= 3 - K < x_2^2[1 - \frac{x_2^2}{2} + \frac{x_4^2}{8} - \frac{x_8^2}{48} + ...] >= 3 - 3K\sum \frac{(-1)^n}{n!} * (\frac{3}{2})^n$$

$$< x_3x_2 >= 3 + \frac{6K}{e} \quad (.1)$$

$$\triangle^2 x_2 =< (\triangle x_2)^2 > -< \triangle x_2 >^2 = 3 \quad (.2)$$

and

$$\triangle^2 x_3 =< (\triangle x_3)^2 > -< \triangle x_3 >^2 =< [x_2 + p_2 - Kx_2exp(-\frac{x_2^2}{2})]^2 >$$

$$= 3 + 3K^2\sum \frac{(-1)^n}{n!}(3)^n - 6K\sum \frac{(-1)^n}{n!}(\frac{3}{2})^n$$

$$\triangle^2 x_3 = 3 - \frac{3(K^2)}{2e} + 12\frac{K}{e} \quad (.3)$$

Inserting eqs. (12), (15), (16) and (17) into eq. (10) we obtain

$$\triangle_x^2 = -\frac{3(K^2)}{2e} - 12\frac{K^2}{e^2} \quad (.4)$$

On the other hand, we can calculate $\triangle_p^2$ by using eq. (11).

$$< p_3p_2 >=< p_2 - Kx_2exp(-\frac{x_2^2}{2})p_2 >=< p_2^2 > -K < x_2p_2exp(-\frac{x_2^2}{2}) >= 3$$

because:

$$< x_2p_2 >= 0$$

In addition :

$$\triangle^2 p_2 =< (\triangle p_2)^2 > -< \triangle p_2 >^2 = 3$$

Now, we calculate $\triangle^2 p_3$:

$$\triangle^2 p_3 =< (\triangle p_3)^2 > -< \triangle p_3 >^2 =< p_2 - Kx_2exp(-\frac{x_2^2}{2})^2 >$$

$$= 3 + 3K^2\sum \frac{(-1)^n}{n!}3^n = 3 - \frac{3K^2}{2e}$$

$$\triangle^2 p_3 = 3 - \frac{3K^2}{2e}$$

therefore:

$$\triangle_p^2 = -\frac{3K^2}{2e} \quad (.5)$$

Inserting eqs. (18) and (19) into eq. (14) we obtain:

$$F_a = (\triangle_x^2)(\triangle_p^2) = (-\frac{3K^2}{2e} - 12\frac{K^2}{e^2})(-\frac{3K^2}{2e})$$

then

$$F_a = \frac{9K^4}{4e^2} + \frac{18K^4}{e^3} \quad (.6)$$

In the same way, with respect to the following equations, parameter F_a can be calculated.

$$\begin{cases} \delta P_{eve} = P_{10} + \gamma_p p_3 \\ \delta X_{eve} = X_{10} - \gamma_x x_3 \end{cases} \quad (.7)$$

$$\begin{cases} x_{out1} = \sqrt{G\eta}x_3 + \sqrt{(G-1)\eta}x_7 + \sqrt{1-\eta}x_9 = X_{10} \\ p_{out1} = \sqrt{G\eta}p_3 - \sqrt{(G-1)\eta}p_7 + \sqrt{1-\eta}p_9 = P_{10} \end{cases}$$

$$\triangle^2 X_{eve} =< (\delta X_{eve})^2 > -< \delta X_{eve} >^2$$

$$\triangle^2 P_{eve} =< (\delta P_{eve})^2 > -< \delta P_{eve} >^2$$

$$\triangle^2 X_{eve} =< (X_{10} - \gamma x_3)^2 > - < (X_{10} - \gamma x_3) >^2$$

$$\triangle^2 X_{eve} =< (P_{10} - \gamma p_3)^2 > - < (P_{10} - \gamma p_3) >^2$$

$$\triangle^2 X_{eve} = \triangle^2 X_{10} + \gamma^2\triangle^2 x_3 - 2\gamma < X_{10}x_3 > \quad (.8)$$

$$\triangle^2 P_{eve} = \triangle^2 P_{10} + \gamma^2\triangle^2 p_3 + 2\gamma < P_{10}p_3 > \quad (.9)$$

Now, if we do derivative from $\triangle^2 X_{eve}$, $\triangle^2 P_{eve}$ on γ, we have:

$$\frac{d\triangle^2 X_{eve}}{d\gamma} = 0$$

$$\gamma_{min} = \frac{< X_{10}x_3 >}{\triangle^2 x_3} \quad (.10)$$

and

$$\frac{d\triangle^2 P_{eve}}{d\gamma} = 0$$

$$\gamma_{min} = -\frac{< P_{10}p_3 >}{\triangle^2 p_3} \quad (.11)$$

Now, we want to find $\triangle^2 X_{eve}$, $\triangle^2 P_{eve}$, and then, create their relationship:

$$F_b = (\triangle^2 X_{eve})(\triangle^2 P_{eve}) \quad (.12)$$

$$\triangle^2 X_{eve} = G\eta\Sigma^2 + \eta(G-1)\sigma^2 + (1-\eta)\sigma^2 + G\eta\Sigma^2[1 - Kexp(-\frac{\Sigma^2 G\eta}{2})]^2$$

$$+\gamma^2(3 - \frac{3(K^2)}{2e} + 12\frac{K}{e}) - 2\gamma(\sqrt{G\eta}\Sigma^2 + \sqrt{(G-1)\eta} < x_7x_3 > + \sqrt{1-\eta} < x_9x_3 >)$$

$$\triangle^2 P_{eve} = G\eta\Sigma^2 + \eta(G-1)\sigma^2 + (1-\eta)\sigma^2 + G\eta\Sigma^2[1 - Kexp(-\frac{\Sigma^2 G\eta}{2})]^2$$

$$+\gamma^2(3 - \frac{3K^2}{2e}) + 2\gamma(\sqrt{G\eta}\Sigma^2 - \sqrt{(G-1)\eta} < p_7p_3 > + \sqrt{1-\eta} < p_9p_3 >)$$

When $G = 1$ and $\eta = 1$ (Eve absent), relationship is:

$$F_b = (\triangle^2 X_{eve})(\triangle^2 P_{eve})$$

$$F_b = \frac{3\Sigma^2 K^4}{4e^2} + \frac{6\Sigma^2 K^4}{e^3}$$

REFERENCES

1. Wiesner S. Conjugate coding. ACM Sigact News 1983;15:78-88.
2. Mayers D. Unconditional security in quantum cryptography. J. ACM. 2001;48:351-406.
3. Kogias I, Xiang Y, He Q, Adesso G. Unconditional security of entanglement-based continuous-variable quantum secret sharing. Phys. Rev. A 2017;95:012315.
4. Ahadpour S, Sadra Y. Randomness criteria in binary visibility graph and complex network perspective. Info. Sci. 2012;197:161-176.
5. Chung YF, Wu ZY, Chen TS. Unconditionally secure cryptosystems based on quantum cryptography. Info. Sci. 2008;178:2044-2058.
6. Chong SK, Hwang T. The enhancement of three-party simultaneous quantum secure direct communication scheme with EPR pairs. Optics Commun. 2011;284:515-518.
7. Banerjee A, Pathak A. Maximally efficient protocols for direct secure quantum communication. Phys. Lett. A 2012;376:2944-2950.
8. Xiu XM, Dong L, Gao YJ, Chi F, Ren YP, Liu HW. A revised controlled deterministic secure quantum communication with five-photon entangled state. Optics Commun. 2010;283:344-347.
9. Gisin N, Ribordy G, Tittel W, Zbinden H. Quantum cryptography. Rev. Modern Phys. 2002;74:145-195.
10. Huang P, Zhu J, He G, Zeng G. Study on the security of discrete-variable quantum key distribution over non-Markovian channels. J. Phys. B 2012;45:135501.
11. Chai G, Cao Z, Liu W, Zhang M, Liang K, Peng J. Novel continuous-variable quantum secure direct communication and its security analysis. Laser Phys. Lett. 2019;16:095207.
12. Eriksson TA, Hirano T, Puttnam BJ, Rademacher G, Luís RS, Fujiwara M, Namiki R, Awaji Y, Takeoka M, Wada N, Sasaki M. Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 tbit/s data channels. Commun. Phys. 2019;2:1-8.
13. Lo HK, Chau HF. Unconditional security of quantum key distribution over arbitrarily long distances. Science 1999;283:2050-2056.
14. Boström K, Felbinger T. Deterministic secure direct communication using entanglement. Phys. Rev. Lett. 2002;89:187902.
15. Shor PW, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. 2000;85:441-444.
16. CAI QY. The ping-pong protocol can be attacked without eavesdropping. Phys. Rev. Lett. 2003;91:109801.
17. Diamanti E, Leverrier A. Distributing secret keys with quantum continuous variables: principle, security and implementations. Entropy 2015;17:6072-6092.
18. Han X, Chang X. A chaotic digital secure communication based on a modified gravitational search algorithm filter. Info. Sci. 2012;208:14-27.
19. Lin JS, Huang CF, Liao TL, Yan JJ. Design and implementation of digital secure communication based on synchronized chaotic systems. Dig. Sig. Proc. 2010;20:229-237.
20. Moskalenko OI, Koronovskii AA, Hramov AE. Generalized synchronization of chaos for secure communication: Remarkable stability to noise. Phys. Lett. A 2010;374:2925-2931.
21. Tse KK, Ng RM, Chung HH, Hui SR. An evaluation of the spectral characteristics of converters with chaotic carrier-frequency modulation. IEEE Trans. Ind. Elec. 2003;50:171-182.
22. He G, Zhu J, Zeng G. Quantum secure communication using continuous variable Einstein-Podolsky-Rosen correlations. Phys. Rev. A 2006;73:012314.
23. Reid MD. Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations. Phys. Rev. A 2000;62:062308.
24. Ottaviani C, Pirandola S. General immunity and superadditivity of two-way Gaussian quantum cryptography. Sci. Rep. 2016;6:22225.
25. Krivolapov Y, Fishman S, Ott E, Antonsen TM. Quantum chaos of a mixed open system of kicked cold atoms. Phys. Rev. E 2011;83:016204.
26. Rarity JG, Gorman PM, Tapster PR. Secure key exchange over 1.9 km free-space range using quantum cryptography. Elec. Lett. 2001;37:512-514.
27. Jensen JH. Quantum corrections for chaotic scattering. Phys. Rev. A 1992;45:8530-8535.
28. Badr A, Fahmy A. A proof of convergence for ant algorithms. Info. Sci. 2004;160:267-279.
29. Paul H. Quantum-mechanical long-range correlations generated in optical beam-splitting. Optica Acta 1981;28:1-4.
30. Maurer UM. Secret key by public discussion from common information. IEEE Trans. Info. Theor. 1993;39:733-742.
31. Sun Y, Cao J, Feng G. An adaptive chaotic secure communication scheme with channel noises. Phys. Lett. A 2008;372:5442-5447.
32. Li S, Álvarez G, Chen G, Mou X. Breaking a chaos-noise-based secure communication scheme. Chaos 2005;15:013703.
33. Lucamarini M, Mancini S. Secure deterministic communication without entanglement. Phys. Rev. Lett. 2005;94:140501.
34. Grosshans F, Grangier P. Continuous variable quantum cryptography using coherent states. Phys. Rev. Lett. 2002;88:057902.
35. Wang K, Ding DS, Zhang W, He QY, Guo GC, Shi BS. Experimental demonstration of Einstein-Podolsky-Rosen entanglement in rotating coordinate space. Sci. Bull. 2020;65:280-285.

How to cite this article: Hematpour N, Ahadpour S, Behnia S. A chaotic quantum secure communication scheme based on a mixed open system. Adv. J. Sci. Eng. 2020;1(1):20-26.