THE COORDINATE RATIOS AS A TOOL TO ANALYZE THE INTRUSION BASED ON BUŽEK-HILLERY QUANTUM COPYING MACHINE

Besma Othmani[1], Mohsen Machhout[1], Houcine Mejri[1,2], Hafedh Belmabrouk[1] , Rached Tourki[1]

[1]Laboratoire d'Electronique et Micro Electronique Faculté des Sciences de Monastir, 5000 Monastir, Tunisia

besma.othmani@gmail.com

machhout@yahoo.fr

Hafedh.Belmabrouk@fsm.rnu.tn

rached.tourki@topnet.tn

[2]Unité de Mathématiques Appliquées et Physique Mathématique, Ecole Préparatoire aux Académies Mélitaires
Avenue Maréchal Tito 4029 Sousse, Tunisia

houcinemejri78@yahoo.fr

ABSTRACT

The intrusion based on Bužek-Hillery universal quantum copying machine (UQCM) is investigated. A major problem to the eavesdropper Eve is how to choose the intrusion parameters required by the copying machine in order to take out the maximum of information on the transmitted qubits while making her intrusion as discrete as possible. The present paper attempts to investigate the equatorial and isotropic cloning by means of coordinate ratios. The degree of intrusion is evaluated by means of the ratios of the receiver (Bob) coordinates and the eavesdropper (Eve) coordinates to the sender (Alice) coordinates in the Bloch sphere. The fidelity has been usually used as a criterion to analyze the intrusion. More especially, this fidelity can achieve the value 0.85 for equatorial qubits by using Bužek-Hillery 1→2 machine. Our goal is to study the behavior of these ratios as a function of the intrusion parameters. As has been found, the coordinate ratios of both the receiver and the eavesdropper achieve an optimal value higher than 2/3, in contrast to the isotropic cloning. This can favor the eavesdropping when using equatorial qubits. For isotropic cloning, the maximal intrusion is reached when the coordinate ratios are equal. The optimal values of the intrusion parameters are then evaluated.

KEYWORDS

Eavesdropping, intrusion, quantum copying machines, isotropic cloning, equatorial cloning, coordinate ratios, fidelity

1. INTRODUCTION

Transmission of quantum information has incited extensive fundamental and applied studies during the last decades. In contrast to the classical cryptography, the quantum one provides more security of information due to the no-cloning theorem [1-3]. Indeed, this theorem confirms that arbitrary information cannot be copied identically, but only imperfect copying can be performed. The difficulty of copying an arbitrary quantum state is one of the basic rules governing the

DOI : 10.5121/ijnsa.2012.4112

physics of quantum systems. Quantum machines are designed to study a variety of tasks such as eavesdropping, quantum cryptography and quantum information. The main goal of quantum copying is to produce a copy being as close as possible to the original state while the output qubit state shall be minimally disturbed. To overcome this limitation for the eavesdropping procedure, several quantum copying machines (QCMs) have been proposed [4-6]. The Bužek-Hillery QCM has the advantage to be universal in the sense that the quality of its output does not depend on the input for specific transmitted qubits. Using this machine, the eavesdropper (Eve) wants to take out the maximum of information as possible on the transmitted qubits and makes her intrusion as discrete as possible. The sender (Alice) and the receiver (Bob) are faced with two main problems: the noise effect due to the channel and Eve's intrusion. In the following, our intention will be focused only on the eavesdropping. So, the major difficulty to Alice is how to choose conveniently the initial state in order to minimize the intrusion effects.

The UQCM clones all of the states in the Bloch sphere with the same optimal fidelity [3–5]. Furthermore, studies have also been performed on quantum cloning of phase covariant states [6] or unknown equatorial states [7]. It has been proven that equatorial states can be cloned with an optimal fidelity of 0.85 [9], which is higher than that of UQCM [9]. This is possible when prior information about the qubit state to transmit is available.

Many works were interested in the noise effects of the channel [7]. Quantum purification amplification (QPA) [8-9] and elaboration of quantum machines [10] have been made for this purpose. The quantum transmission was analyzed using the concept of fidelity. Only few reports described the capacity of the channel or the copying machine with use of relative entropy [11]. Furthermore, these studies were restricted to the transmission of particular qubits such as EPR pairs, isotropic cloning or equatorial qubits.

In this paper, we will study in detail the behavior of the coordinate ratios for equatorial and isotropic cloning versus the intrusion parameters of the eavesdropper machine. This study is aimed at determining the maximum value of the coordinate ratios. The paper is organized as follows: after a brief introduction, we present, in section 2, the theoretical formulation of the coordinate ratios based on qubits density matrices. Results will be discussed in section 3. Concluding remarks are summarized presented in section 4.

2. RELATED WORKS

To analyze the action of the quantum copying machine, most interesting is to evaluate the quality of the copy received by Eve in comparison with that sent to Bob. This could presumably be made by investigating the relation between Eve and Bob coordinate states in the Bloch sphere with respect to Alice's. S.Felloni and G.Strini [10], have shown that the maximum coordinates ratio for isotropic cloning by using Buzek and Hillery machine is equal to 2/3. We note that isotropy results in when Alice and Bob use a six-state protocol, that is the measurements being performed along the x, y and z axis of the Bloch sphere. Dealing with the optimal value of the fidelity for equatorial qubits, the problem is to determine the maximum value of the coordinate ratios in this case.

In their article [10], the authors S.Felloni and G.Strini propose to analyze the quantum copying machine of Buzek and Hillery by means of the coordinates ratios for both symmetrical and asymmetrical behaviors, each case related to the cryptographic protocol used by the two communicating parties: in the symmetrical case a six-state protocol requires isotropic cloning of the information transmitted, while in the asymmetrical case the isotropy conditions may be relaxed when a four-state protocol is used.

3. THEORETICAL FORMULATION-DENSITY MATRICES AND BLOCH SPHERE COORDINATES

3.1. Description of the copying machine:

The Bužek-Hillery UQCM is shown in figure 1.

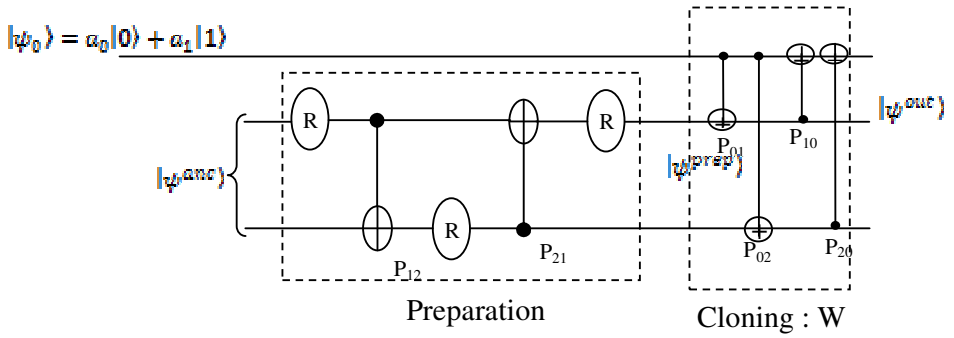


Figure 1. Scheme of the Buzek-Hillery quantum copying machine

It involves two unitary circuits [12]:
-The first circuit contains CNOT and rotation gates and stands for qubits preparation by the eavesdropper (Eve), the ancillary qubits to be considered at the input of preparation circuit are:

$$\left|\psi^{anc}\right\rangle = \alpha|00\rangle + \beta|00\rangle + \gamma|00\rangle + \delta|00\rangle \quad (1)$$

The parameters α, β, γ and δ are assumed to be real and satisfy the normalization condition:

$$\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = 1 \quad (2)$$

Additionally, the choice of these parameters must be appropriate according to the purpose intended by the Eve's intrusion. Preparation of the UQCM for working consists of obtaining from the ancillary $\left|\psi^{anc}\right\rangle$-qubit an entangled state in the form:

$$\left|\psi^{prep}\right\rangle = R_1(\theta_3)\ P_{21}\ R_2(\theta_2)\ P_{12}\ R_1(\theta_1)\ \left|\psi^{anc}\right\rangle \quad (3)$$

with

$$R(\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \text{ and CNOT= } P_{ij}\left|x_i, y_j\right\rangle = \left|x_i, x_i \oplus y_j\right\rangle \quad (4)$$

where $R(\theta)$ and P_{ij} are rotation and CNOT operators respectively and $\oplus$ is the modulus-2 summation .
-The second circuit is the well-known W unitary transformation. It is formed by four CNOT-gates This circuit represents the cloning component.

3.2. Expressions of the density matrices:

The qubit state sent by Alice is:

$$\left|\psi_0\right\rangle = a_0|0\rangle + a_1|1\rangle \quad (5)$$

with

$$|a_0|^2 + |a_1|^2 = 1$$

The parameters a_0 and a_1 may be real or complex.
The qubit state at the input of the cloning circuit is defined as:

$$|\psi^{in}\rangle = a_0\alpha|000\rangle + a_0\beta|001\rangle + a_0\gamma|010\rangle + a_0\delta|011\rangle + a_1\alpha|100\rangle + a_1\beta|101\rangle + a_1\gamma|110\rangle + a_1\delta|111\rangle \quad (6)$$

The unitary transformation W converts the state $|\psi^{in}\rangle$ into the state $|\psi^{out}\rangle = \prod_{i\neq j} P_{ij}|\psi_0\rangle \oplus |\psi^{prep}\rangle$ according to:

$$|\psi^{out}\rangle = a_0\alpha|000\rangle + a_1\gamma|001\rangle + a_1\beta|010\rangle + a_0\delta|011\rangle + a_1\delta|100\rangle + a_0\beta|101\rangle + a_0\gamma|110\rangle + a_1\alpha|111\rangle \quad (7)$$

The quantum copying machine provides two copies of the initial state sent by Alice: one copy is sent to Eve and the other is received by Bob instead of the original intercepted qubit state. A pure qubit state is perfectly characterized by $|\psi^{out}\rangle$. However, mixed states, require the use of the density operator. Such an operator is defined by the projector: $\rho^{out} = \|\psi^{out}\rangle\langle\psi^{out}\|$. The reduced density matrix of Bob is obtained by tracing over Eve's and ancillary qubits: $\rho^{Bob} = tr_{Eve,anc}(\rho^{out})$.

$$\rho^{Bob} = tr_{Eve,anc.}\left(\rho^{out}\right) = \begin{pmatrix} |a_0|^2(\alpha^2+\delta^2)+|a_1|^2(\beta^2+\gamma^2) & 2a_0a_1^*\alpha\delta + 2a_0^*a_1\beta\gamma \\ 2a_0^*a_1\alpha\delta + a_0a_1^*\beta\gamma & |a_0|^2(\beta^2+\gamma^2)+|a_1|^2(\alpha^2+\delta^2) \end{pmatrix} \quad (8)$$

where * denotes the complex conjugate.

Similarly, the reduced density matrix of Eve is obtained by tracing over Bob's qubit and over the ancillary qubit.

$$\rho^{Eve} = tr_{Bob,anc.}\left(\rho^{out}\right) = \begin{pmatrix} |a_0|^2(\alpha^2+\beta^2)+|a_1|^2(\gamma^2+\delta^2) & 2a_0a_1^*\alpha\beta + 2a_0^*a_1\gamma\delta \\ 2a_0^*a_1\alpha\beta + a_0a_1^*\gamma\delta & |a_0|^2(\gamma^2+\delta^2)+|a_1|^2(\alpha^2+\beta^2) \end{pmatrix} \quad (9)$$

The quality of obtained copies has been usually specified by the fidelity F, which is defined as:

$$F_{ij} = \langle\psi_0|\rho_{i,j}^{out}|\psi_0\rangle. \quad (10)$$

3.3. Representation of the reduced matrices on the Bloch sphere

The relationship between a reduced matrix ρ and the corresponding vector $\vec{V}(x,y,z)$ in the Bloch sphere reads

$$\rho = \frac{1}{2}\begin{pmatrix} 1+z & x-iy \\ x+iy & 1-z \end{pmatrix} \tag{11}$$

where $i^2 = -1$. Let us call $\vec{V}_A(x_A, y_A, z_A)$, $\vec{V}_B(x_B, y_B, z_B)$ and $\vec{V}_E(x_E, y_E, z_E)$ the Bloch sphere vectors corresponding to ρ_A, ρ_B and ρ_E respectively. By identification, we obtain the following relations:

$$\begin{cases} x_B = 2(\alpha\delta + \beta\gamma)\, x_A \\ y_B = 2(\alpha\delta - \beta\gamma)\, y_A \\ z_B = (\alpha^2 + \delta^2 - \beta^2 - \gamma^2)\, z_A \end{cases} \quad \text{and} \quad \begin{cases} x_E = 2(\alpha\beta + \gamma\delta)\, x_A \\ y_E = 2(\alpha\beta - \gamma\delta)\, y_A \\ z_E = (\alpha^2 + \beta^2 - \gamma^2 - \delta^2)\, z_A \end{cases} \tag{12}$$

4. RESULTS AND DISCUSSION

The optimal value of the fidelity is 83% for the Bužek-Hillery UQCM machine that is used in the present study. For specific qubits, namely the equatorial qubits, the fidelity may reach the value 85% [13]. In this work, we will investigate the intrusion by means of the ratios of state coordinates in the Bloch sphere. Concerning the coordinate ratios, two cases are considered: the isotropic cloning and the equatorial cloning. The isotropic cloning can occur when Alice and Bob use a six-state protocol that means the detection is carried out along the x-, y- and z-axis in the Bloch sphere. This leads to imposing:

$$\begin{cases} \dfrac{x_B}{x_A} = \dfrac{y_B}{y_A} = \dfrac{z_B}{z_A} \\ \dfrac{x_E}{x_A} = \dfrac{y_E}{y_A} = \dfrac{z_E}{z_A} \end{cases} \tag{13}$$

However, when Alice and Bob use a four-state protocol and Eve knows the measurement axes, the previous condition may be less restrictive. This case is known as equatorial cloning. If the measurement axes are x- and z-axis, the condition of the equatorial cloning reads:

$$\begin{cases} \dfrac{x_B}{x_A} = \dfrac{z_B}{z_A} \\ \dfrac{x_E}{x_A} = \dfrac{z_E}{z_A} \end{cases} \tag{14}$$

4.1. The isotropic cloning

To satisfy the conditions imposed by the isotropic cloning (Eq. 13), it is necessary to have [14]:

$$\begin{cases} \gamma = 0 \\ \beta = \dfrac{1}{2}\left(\alpha - \sqrt{2-3\alpha^2}\right) \\ \delta = \dfrac{1}{2}\left(\alpha + \sqrt{2-3\alpha^2}\right) \\ \dfrac{1}{\sqrt{2}} \le \alpha \le \dfrac{2}{\sqrt{6}} \end{cases} \tag{15}$$

Figure 2 presents the ratios $R_B(\alpha) = \frac{x_B}{x_A} = \frac{y_B}{y_A} = \frac{z_B}{z_A}$ and $R_E(\alpha) = \frac{x_E}{x_A} = \frac{y_E}{y_A} = \frac{z_E}{z_A}$ versus the intrusion parameter α in the case of isotropic cloning.

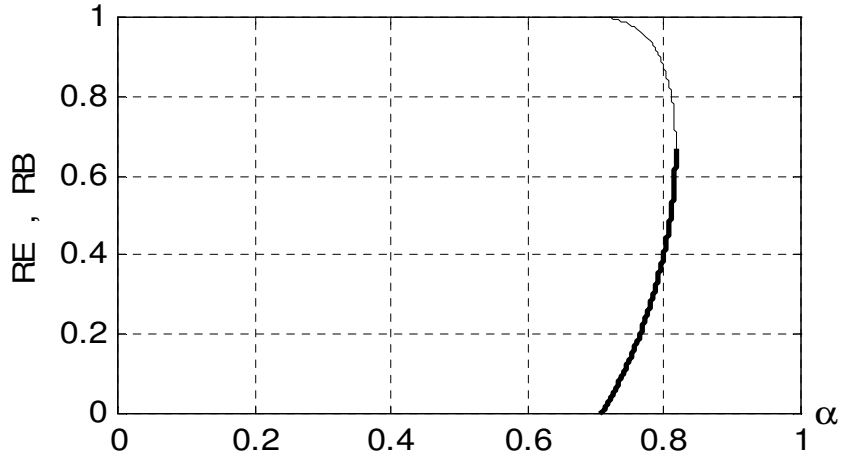


Figure 2. Evolution of the ratios R_B and R_E versus the intrusion parameter α in the case of isotropic cloning

As shown, the maximal intrusion is obtained for $\alpha = 2/\sqrt{6}$ and in this case $R_B = R_E = 2/3$. Therefore, Eve succeeds in making two identical imperfect copies of the original qubit state. Furthermore, she minimizes the perturbation of the qubit received by Bob and at the same time she obtains the maximum of information allowed by the machine for isotropic cloning. The minimum of intrusion is attained at the value $\alpha = 1/\sqrt{2}$. For this case, $R_E = 0$ i.e. there is no-intrusion and so Eve fails in attacking the qubit sent by Alice. These results are in good agreement with those obtained by Felloni and Strini [12]. The ratio $R_{EB} = R_E / R_B$ increases with the parameter α. This proves that the degree of intrusion increases as α increases from $\alpha = 1/\sqrt{2}$ to $\alpha = 2/\sqrt{6}$. It is worth noting, that, in the case of isotropic cloning, the range of α is very narrow ($0.707 \le \alpha \le 0.81$) and for a given value of α, the other parameters β, γ and δ have each one a unique value. This reduces considerably the possibilities of the choice of the intrusion parameters. This problem becomes critical especially in practice due to experimental uncertainties. If we impose for example $R_{EB} \ge 0.8$ in the purpose to have an acceptable intrusion, the range of γ is reduced further. Therefore, the choice of the intrusion parameters becomes more difficult.

In order to enlarge the useful range of the intrusion parameters, we extend this study and consider that the parameters α, β and γ are independent. For a given value of γ, the two other parameters α and β satisfy $\alpha^2 + \beta^2 \leq 1 - \gamma^2$. To stand near the isotropic condition, we assume in the first step $\gamma = 0$. In this case, the coordinate ratios become:

$$\begin{cases} \dfrac{x_B}{x_A} = \dfrac{y_B}{y_A} = 2\alpha\sqrt{1-\alpha^2-\beta^2} \\ \dfrac{z_B}{z_A} = 1 - 2\beta^2 \end{cases} \quad \text{and} \quad \begin{cases} \dfrac{x_E}{x_A} = \dfrac{y_E}{y_A} = 2\alpha\beta \\ \dfrac{z_E}{z_A} = 2(\alpha^2+\beta^2) - 1 \end{cases} \tag{16}$$

In figure 3, we report the contour lines of the coordinate ratios versus the intrusion parameters α and β.

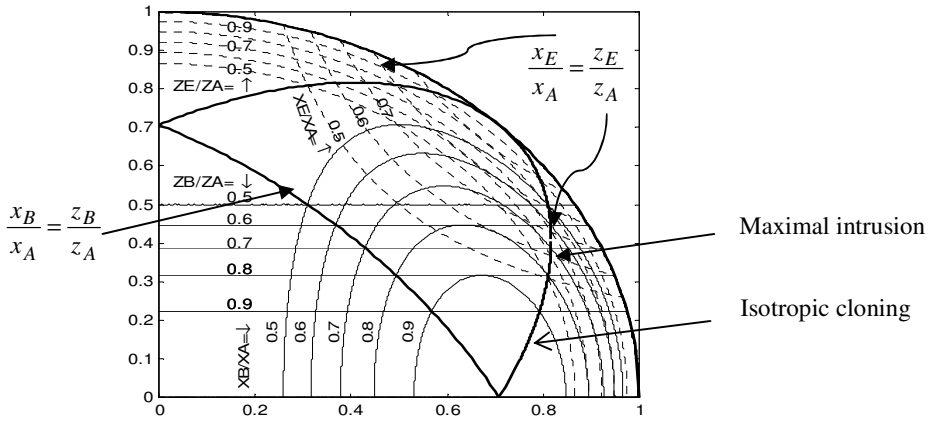


Figure 3. Contour lines of the coordinate ratios versus the intrusion parameters α and β for $\gamma = 0$.

In this figure, the curves corresponding to the condition $x_B / x_A = y_B / y_A = z_B / z_A$ i.e. $\beta = \frac{1}{2}(\alpha \pm \sqrt{2-3\alpha^2})$ or $\beta = \frac{1}{2}(-\alpha + \sqrt{2-3\alpha^2})$ as well as the curve corresponding to the condition $x_E / x_A = y_E / y_A = z_E / z_A$ i.e. $\beta = \frac{1}{2}(\alpha - \sqrt{2-3\alpha^2})$ have been reported. Along the curve $\beta = (\alpha - \sqrt{2-3\alpha^2})/2$ i.e. for isotropic cloning, in progressing from $\alpha = 1/\sqrt{2}$ to $\alpha = 2/\sqrt{6}$, the ratios x_B / x_A and z_B / z_A decrease however the ratios x_E / x_A and z_E / z_A increase. In other words, the degree of intrusion increases as mentioned above. In the vicinity of this curve, we may delimit an area where the isotropy condition is approximately satisfied and at the same time the coordinate ratios remain greater than a threshold value. In this domain, the parameters α and β are independent. This gives to Eve a large domain of possible choice of the intrusion parameters without altering significantly the isotropic condition. Therefore, we may tolerate some uncertainty in the choice of the intrusion parameters α and β.

Similarly, it is obvious that the parameter γ may endure some uncertainty. For this reason, we will calculate again the coordinate ratios with $\gamma \neq 0$. Figure 4 presents the contour lines of the coordinate ratios for $\gamma = 0.02$.

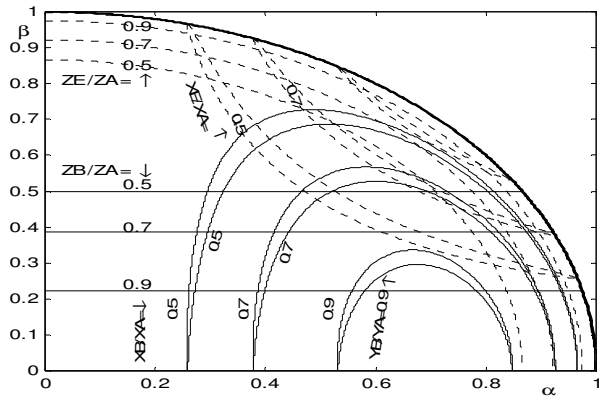


Figure 4. Contour lines of the coordinate ratios versus the intrusion parameters α and β for $\gamma = 0.02$

The coordinate ratios x_B / x_A and y_B / y_A are no longer equal. In the same way, $x_E / x_A \neq y_E / y_A$. The curve related to z_B / z_A does no more intersect those related to coordinate ratios x_B / x_A and y_B / y_A at the same point, for a given value of the ratios. Furthermore, when increasing the intrusion parameter γ, the curves representing x_B / x_A and y_B / y_A deviate more and more from their positions obtained for $\gamma = 0$. The deviation of these curves is symmetrical: the contour lines for a given value of ratio x_B / x_A become more extended while the contour lines for a given value of ratio y_B / y_A contract. This proves that to hold even approximately the isotropy condition, it is necessary to have $\gamma \approx 0$.

We define $S_{xyz}(\gamma)$ the area in the $\alpha - \beta$ plane for a given value of γ where all the coordinate ratios x_B / x_A , y_B / y_A, z_B / z_A, x_E / x_A , y_E / y_A and z_E / z_A exceed a certain value. The threshold will be chosen arbitrarily. In this case, it's fixed at 0.5. This area is normalized with respect to the total area $\pi / 4$.

Figure 5 exhibits the evolution of the normalized area S_{xyz} versus the intrusion parameter γ. The area S_{xyz} has its maximal value for $\gamma = 0$ and it vanishes sharply when increasing γ .

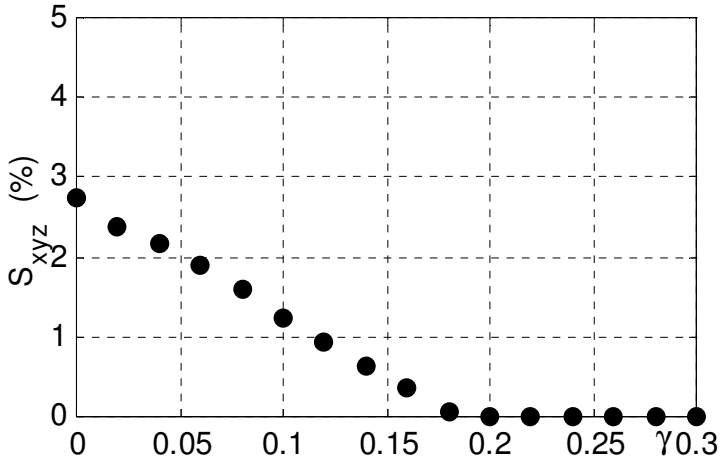


Figure 5. Variation of the area S_{xyz} as a function of the parameter γ

For $\gamma > 0.18$, S_{xyz} is null. In other words, the conditions imposed to the coordinate ratio are no longer satisfied by any couple (α, β). Therefore, for a protocol using six axes protocols, Eve take's advantage in choosing $\gamma = 0$.

From figure 3 we deduce that the area where x_B / x_A, y_B / y_A and z_B / z_A are greater than 0.5 is about 41% of the total area and the area where x_E / x_A, y_E / y_A and z_E / z_A are greater than 0.5 is about 15% of the total area for $\gamma = 0$. Whereas these two zones overlap only in a very small region and their intersection covers only 2.7% of the total area for $\gamma = 0$. Eve should choose the intrusion parameters in this zone.

In conclusion, to reach the maximal degree of intrusion in the case of isotropic cloning, the preparation circuit built by the eavesdropper Eve should have the following parameters $\alpha \approx 0.82$, $\beta \approx \delta \approx 0.41$ and $\gamma \approx 0$. If we tolerate some uncertainties on the coordinate ratios, the useful region is extended in the vicinity of this point.

4.2. The equatorial cloning

To satisfy Eq. 14, it is necessary to have:

$$\beta = \frac{-\gamma + \alpha - \sqrt{2 + 2\alpha\gamma - 3\alpha^2 - 3\gamma^2}}{2} \tag{17}$$

As α increases, the ratio $R_B = \frac{x_B}{x_A} = \frac{z_B}{z_A}$ decreases while the ratio $R_E = \frac{x_E}{x_A} = \frac{z_E}{z_A}$ increases. Thus, the maximal intrusion is obtained when $R_B = R_E$. In this case, the parameters α and γ are related by the relation:

$$\alpha = \frac{\gamma + \sqrt{6 - 8\gamma^2}}{3} \tag{18}$$

The coordinate ratios are then expressed by:

$$R_B = R_E = \frac{2}{3} + \frac{2}{9}\gamma\left[\sqrt{6 - 8\gamma^2} - 8\gamma\right] \tag{19}$$

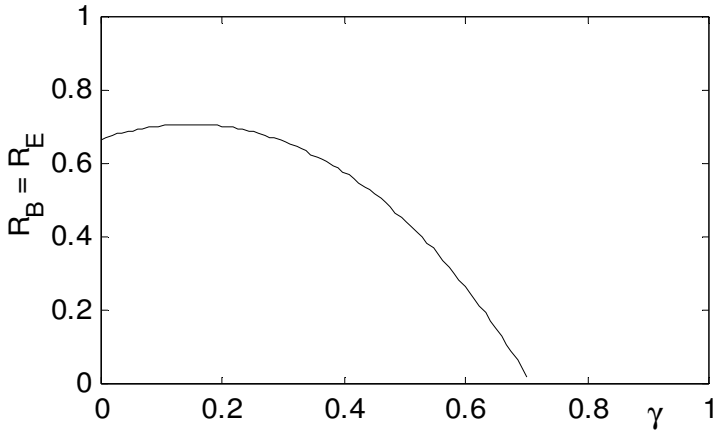


Figure 6. Variation of the ratio $R_B = R_E$ versus the intrusion parameter γ in the case of equatorial cloning.

Figure 6 shows the ratio $R_B = R_E$ calculated versus the intrusion parameter γ in the case of equatorial cloning and when the two ratios are equal, i.e. by using Eq.19. As this plot shows for equatorial cloning, it is not necessary to have $\gamma = 0$ to achieve maximized intrusion. For $\gamma < 0.29$, we have $R_B = R_E > \frac{2}{3}$, which is the value obtained in the case of isotropic cloning. However, for larger values of γ, the ratios decline drastically. Also, it is seen that the maximum value of the ratio is equal to $\frac{\sqrt{2}}{2}$ and is reached for $\gamma = \frac{2-\sqrt{2}}{4} \approx 0.15$ .On the other hand, we have calculated the coordinates ratio $R_B = R_E$ as a function of α for γ fixed at 0, 0.005, 0.15 and 0.2 respectively. Obtained results are reported in Figure 7.

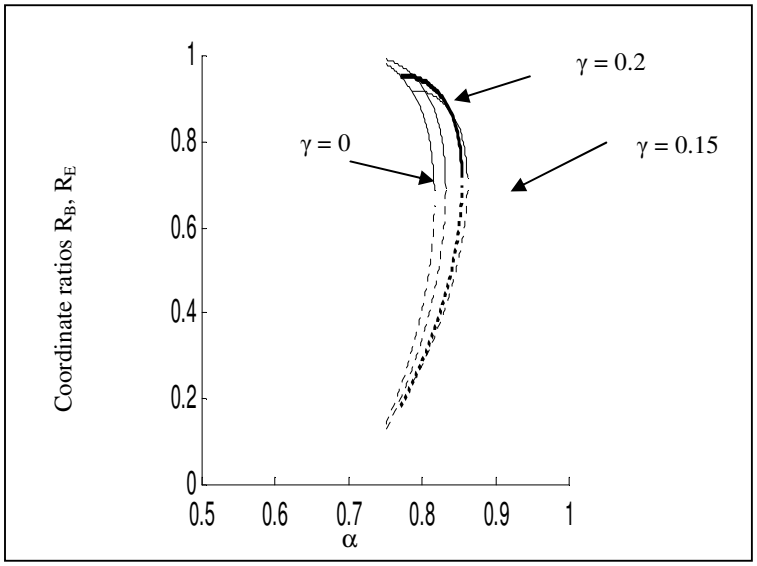
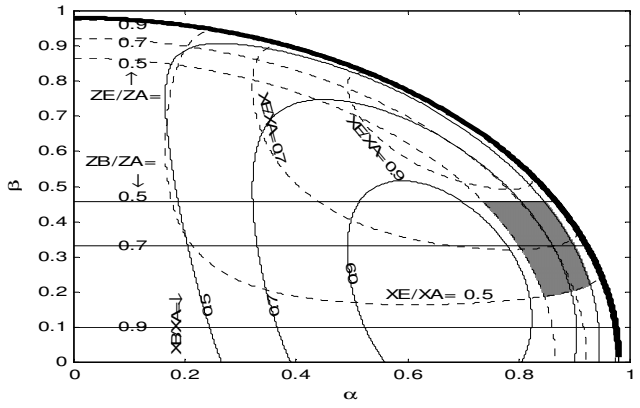


Figure 7. The coordinate ratios R_B and R_E calculated versus α for different values of γ

In evaluating the coordinate ratios, the parameter β is calculated using Eq.17. For γ = 0 that corresponds to the isotropic cloning, the α-dependent ratio is similar to that reported in Ref. [10,11]. In such a case, the maximal intrusion is obtained for $\alpha = \frac{2}{\sqrt{6}}$ and both R_E and R_B reach $\frac{2}{3}$. For $\gamma \neq 0$, however, the intrusion is maximum for α larger than $\frac{2}{\sqrt{6}}$ and the coordinate ratio can exceed $\frac{2}{3}$. This means that, for equatorial qubits, there is a wide range of the intrusion parameters to favor the eavesdropping. To further elucidate the latter feature, we have computed the coordinate ratios as a function of α and β in the ranges $0 \le \alpha \le 1$ and $0 \le \beta \le 1$. We report the contour lines of $\frac{X_B}{X_A}, \frac{Z_B}{Z_A}, \frac{X_E}{X_A}$ and $\frac{Z_E}{Z_A}$ in Figure 8.a. We define $S_{XZ}(\gamma)$ the normalized area in the α-β plane for coordinate ratios upper than an arbitrary threshold. The area S_{XZ} shall be calculated at a fixed γ. Here, calculation of S_{XZ} is made versus γ for a threshold equal to 0.5. The results are depicted in Figure 8.b. As shown, S_{XZ} increases and then decreases, reaching a maximum for γ close to 0.15. Such a value corresponds to the maximum of $R_B = R_E$ as demonstrated above. In the same plot, is also reported the normalized area S_{XYZ} calculated for isotropic cloning. It is seen that, the area S_{XYZ} has its maximum at $\gamma = 0$ and vanishes sharply with the increase of γ. For $\gamma \rangle 0.18$, S_{XYZ} is identically null. In other words, the conditions imposed to the coordinate ratios are no longer satisfied by any couple (α,β) for isotropic cloning. We also note that the area S_{XZ} is greater than S_{XYZ} in the entire range of γ studied. This favors the intrusion by using equatorial qubits.

(a) : S_{xyz}



(b) : S_{xz}

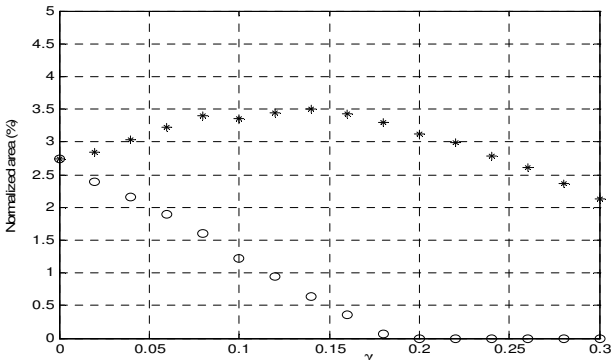


Figure 8. (a) The contour plots of the coordinate ratios calculated versus α and β for equatorial cloning, (b) The areas S_{xz} and S_{xyz} as a function of the parameter γ

5. CONCLUSIONS

The intrusion based on Bužek-Hillery universal quantum copying machine (UQCM) has been investigated using the coordinate ratios. When Alice and Bob use a six-state protocol i.e. the detection is carried out along the x-, y- and z-axis of the Bloch sphere, the isotropic cloning is necessary. In this case, the range of the intrusion parameter α is very narrow ($0.707 \le \alpha \le 0.81$) and for a given value of α, the other parameters β, γ and δ have each a unique value. The maximal intrusion is obtained for $\alpha = 0.816$. For this value, Eve succeeds in making two identical imperfect copies of the original state. Furthermore, she minimizes the perturbation of the qubit received by Bob and at the same time she obtains the maximum of information allowed by the machine for isotropic cloning.

In order to enlarge the useful range of the intrusion parameters, we have extended the study and considered that the parameters α, β and γ are independent. The results reveal that to reach the maximal intrusion in the case of isotropic cloning, the preparation circuit built by the eavesdropper Eve should have the following parameters $\alpha \approx 0.82$, $\beta \approx \delta \approx 0.41$ and $\gamma \approx 0$. If we tolerate some uncertainties on the coordinate ratios, the useful region is extended in the vicinity of this point.

For the equatorial cloning based on Bužek-Hillery 1→2 machine, two main features were revealed:

(i) the coordinate ratios of qubit states sent to Bob and Eve reach $\frac{\sqrt{2}}{2}$ which exceeds the value $\frac{2}{3}$ found for isotropic cloning. (ii) The normalized area Sxz, as defined in the x-z plane, is higher than the area Sxyz which corresponds to the isotropic cloning in the range of the parameters γ studied. As evidenced from this study, there's a strong correlation between the coordinate ratios and the fidelity. Thus, like the fidelity, the coordinate ratios can provide further information on the degree of intrusion. They are also helpful for designing quantum circuits.

REFERENCES

[1] W.K.Wootters and W.H.Zurek, Nature (1982), p.802

[2] V.Buzek and M.Hillery, Phys.Rev.A 54 (1996), p.1844

[3] N.Gisin, S. Massar, Phys. Rev. Lett. 79, (1997), p.2153

[4] D.Bruß, D.P. Di Vincenzo, A. Ekert, C.A. Fuchs, C. Macchiavello, J.A. Smolin, Phys. Rev. A 57, (1998), p.2368

[5] N.Gisin, Phys. Lett. A 242, (1998), p.1

[6] D.Bruß, M. Cinchetti, G.M. D'Ariano, C. Macchiavello, Phys. Rev. A 62, (2000), 012302

[7] H.Fan, H. Imai, K. Matsumoto, X.B. Wang, Phys. Rev. A 67, (2003), 022317

[8] H.Fan, K. Matsumoto, X.B.Wang, M. Wadati, Phys. Rev. A 65, (2001), 012304

[9] V.N.Dumachev, arXiv:quant-ph/0602035v1 (2006)

[10] S.Felloni, G.Strini, Electronic Journal of Theoretical Physics 3, n°11 (2006), p.159

[11] T. Wei, K. Nemoto, P. Goldbart, P. Kwiat, W.J. Munro, F. Verstraete, Phys. Rev. A 67 (2003) 022110

[12] G.Benenti, S.Felloni, G.Strini, European Physical

[13] H. Fan, K. Matsumoto, X.B.Wang and H.Imai, J. Phys. A: Math. Gen. 35 (2002) 7415–7423