Information Geometrical Approximation of Quantum Channel Security

Laszlo Gyongyosi
Department of Telecommunications, Budapest
University of Technology
Magyar tudosok krt. 2., Budapest, H-1117, Hungary
gyongyosi@hit.bme.hu

Sandor Imre
Department of Telecommunications, Budapest
University of Technology
Magyar tudosok krt. 2., Budapest, H-1117, Hungary
imre@hit.bme.hu

Abstract— **The problem of quantum cloning is closely connected to quantum cryptography. While an eavesdropper on a quantum channel cannot copy perfectly the sent quantum states, in many cases a cloning machine is known to be the most powerful eavesdropping strategy with which to counter quantum cryptographic protocols. In this paper, effective computational geometrical methods are used to analyze cloning activity on a quantum channel. A geometric approach is demonstrated which analyzes the security of the quantum channel, based on quantum relative entropy and Delaunay triangulation on the Bloch sphere. In the security analysis, an approximation algorithm derived from classical computational geometry is used to determine the smallest enclosing ball of balls using core-sets. An improved version is presented which is able to obtain a more effective approximation algorithm in quantum space, while the performances of the proposed geometric algorithms are compared.**

Keywords - quantum cryptography; quantum cloning; quantum informational distance

I. INTRODUCTION

In the past few years, quantum key distribution schemes have invited much study [1]. Quantum theory takes advantage of quantum mechanical principles such as the superposition of states and their no-cloning principle, introduced by Wooters and Zurek [2]. According to the no-cloning theorem, an unknown quantum state cannot be copied perfectly. The method of imperfect cloning was first published by Buzek and Hillery in 1996 [3], while Mozyrsky and Privman have subsequently analyzed other possible imperfect quantum copying approaches and their practical realization [4].

The problem of quantum cloning is closely connected to quantum cryptography, a cryptographic method based on the principles of quantum theory. Using current network technology, interfaces able to manage both quantum and classical channels simultaneously must be implemented in order to spread quantum cryptography.

In our fundamentally new security analysis of quantum cryptography, the fidelity of the eavesdropper's cloning machine is derived from Laguerre-type Delaunay diagrams on the Bloch sphere. Voronoi diagrams are the geometric dual of ordinary Delaunay diagrams, and their application in quantum space has been studied by Kato et al. [5]. In computational geometry, many complex high dimensional problems can be expressed with graphs and tessellation diagrams. Using Laguerre diagrams [6][7], the radii of the smallest enclosing balls of mixed states on the Bloch sphere can be calculated efficiently, while the level of eavesdropping activity can also be measured. The geometric interpretation of quantum states investigates informational distances between two different quantum states [8][9]. The fidelity of the quantum cloning transformation is here computed using a classical informational geometric algorithm presented by Badoui and Clarkson [10], and the Laguerre Delaunay triangulation on the Bloch sphere. The geometric interpretation of the smallest ball problem in informational space has been investigated previously by Nielsen and Nock [11].

As classical cryptographic methods used in wired and wireless security have been found to have vulnerabilities, new methods based on quantum mechanical principles have been deployed [12]. Quantum cryptography is an emerging technology that may offer new forms of security protection. However, quantum cloning-based attacks against quantum cryptography protocols will play a crucial role in the future [13][14][15][16].

Our goal is to identify these imperfect quantum cloning-based attacks, and find potential and efficient solutions for their detection in secret quantum communications. Analysis of the fidelity of the eavesdropper's cloning machine indicates how far the eavesdropper preserves the size of the space of quantum states. In the proposed method, quantum informational distance plays an important role in the estimation of this fidelity. Also presented is a fundamentally new method of deriving quantum relative entropy based on Delaunay tessellation on the Bloch ball and the computation of the radius of smallest enclosing quantum informational ball, to detect eavesdropping activity on the quantum channel.

This paper is organized as follows. In Section II, basic facts about computational geometry and quantum information theory are discussed. In Section III, the basic properties of quantum cloners are explained, while in Sections IV and V, the application of the method for the security analysis of eavesdropping detection on the quantum channel is shown. In Section VI, the optimized algorithm is presented, and the performances of the proposed methods compared. In Section VII, an illustrative example is provided which presents the main steps of the proposed quantum informational geometric security analysis. Finally, in Section VIII a conclusion is drawn from the results.

II. Attacker Model and Geometric Background

The map of the quantum cloner compresses the Bloch ball as an affine map. This affine map has to be a completely positive, trace-preserving map which shrinks the Bloch ball along the *x*, *y* and *z* axes. Quantum informational theoretical analysis of the eavesdropper's cloning machine indicates to what extent the size of the space of quantum states is preserved. In the proposed model, due to eavesdropper activity the sent pure quantum states become mixed states. Eve's output is represented by a 2×2 density matrix, her operation being a trace-preserving completely positive (CP) map. Eve's map is denoted by L , which is trace-preserving if $Tr(\mathrm{L}(\rho)) = Tr(\rho)$ for all density matrices ρ , and positive if the eigenvalues of $\mathrm{L}(\rho)$ are non-negative, whenever the eigenvalues of ρ are non-negative. As Eve's map L has to be CP, $\mathrm{I}_n \otimes \mathrm{L}$ is thus a positive map for all *n*, where I_n is the identity map on $n \times n$ matrices [15].

A computational geometric method is used to analyze cloning activity on a quantum channel, using the Bloch ball representation. The activity of an eavesdropper on a single qubit in the Bloch sphere representation can be expressed by an affine map as

$$\mathbf{r}_E = \mathrm{L}(\mathbf{r}) = A\mathbf{r} + \vec{b}, \tag{1}$$

where A is a 3×3 real matrix, $\vec{b}$ is a three-dimensional vector, $\mathbf{r}$ is the initial Bloch vector of the sent pure quantum state, and $\mathbf{r}_E$ is the Bloch vector of the cloned state.

A. *Related Work*

To analyze the informational geometric impacts of cloning activity on the quantum channel, the mathematical results of Aurenhammer and Klein [6], Badoiu and Clarkson [10], Panigrahy [17], Badoiu et al. [18], Kumar et al. [19], Kato et al. [5] and Nielsen and Nock [11] are used. The proposed geometric analysis of this paper is based on the most important studies of the security analysis of QKD protocols. Our approach integrates the results of Cerfand Bourennane [14], D'Ariano and Macchiavello [15], Acín et al. [16], Kraus et al. [20], Hillery et al. [21], Cerf et al. [22], D'Ariano and Macchiavello [23], Gisin et al. [24], Gisin and Popescu [25], Niederberger et al. [26] and Mozyrsky and Privman [4]. The geometric approach of Kato et al. [5] is based on the computation of Voronoi diagrams using a lower envelope technique. However, the current paper shows that an enhanced version of the method presented by Nielsen and Nock [11] can be applied in quantum space, and by the introduction of quantum Delaunay diagrams for convex hull calculation, a more powerful method can be achieved.

In our security analysis, the informational theoretical meaning of quantum cloning activity in the quantum channel is studied. Alice's side is modeled by the random variable $X = \{p_i = P(x_i)\}, i = 1, \ldots N.$, while Bob's side can be modeled by another random variable *Y*. The Shannon entropy for the discrete random variable *X* is denoted by $H(X)$, which can be defined as

$$H(X) = -\sum_{i=1}^{N} p_i \log(p_i). \tag{2}$$

For conditional random variables, the probability of the random variable *X* given *Y* is denoted by $p(X|Y)$. Alice sends a random variable to Bob, who subsequently produces an output signal with a given probability.

The effects of Eve's quantum cloner on Bob's received quantum state are then geometrically analyzed. The presence of Eve's cloner in the quantum channel increases the uncertainty in *X*, given Bob's output of *Y*. The informational theoretical noise of Eve's quantum cloner increases conditional Shannon entropy $H(X|Y)$, where

$$H(X|Y) = \sum_{i=1}^{N_X} \sum_{j=1}^{N_Y} p(x_i, y_j) \log p(x_i|y_j). \tag{3}$$

The general model for the quantum cloner based attack is illustrated in Figure 1.

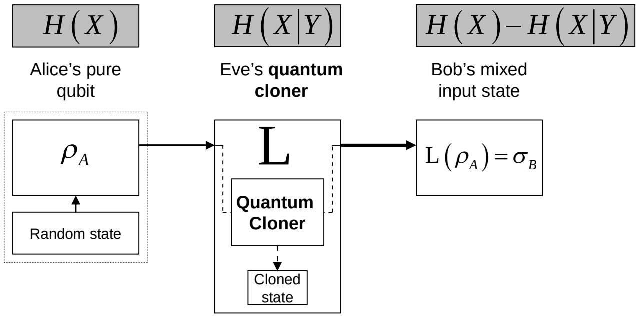


Figure 1. The analyzed attacker model and entropies.

The proposed geometric security analysis focuses on the cloned mixed quantum state, which is received by Bob. The type of quantum cloner machine depends on the actual protocol. For example, in the four-state protocol Eve chooses the phase-covariant cloner, while in the six-state protocol she uses the universal quantum cloner (UCM) machine. Alice's pure state is denoted by ρ_A , Eve's cloner modeled by an affine map L, and Bob's mixed input state denoted by $\mathrm{L}(\rho_A) = \sigma_B$.

Our calculations utilize the fact that for random variables *X* and *Y*, $H(X,Y) = H(X) + H(Y|X)$, where $H(X)$, $H(X,Y)$ and $H(Y|X)$ are defined by probability distributions. Information which can be transmitted in the presence of an eavesdropper on the quantum channel is measured in a geometric representation. In a secret quantum channel, $H(X)$ and $H(X|Y)$ are sought to be maximized and minimized, respectively, in order to maximize the radius r^* of the smallest enclosing ball of Bob, whose radius describes the maximum transmittable information from Alice to Bob in the *attacked* quantum channel:

$$r^* = Max_{\{all\ possible\ x_i\}} H(X) - H(X|Y). \tag{4}$$

To calculate the radius r^* of the smallest informational ball of quantum states and the entropies between the cloned quantum states, von Neumann entropy and quantum relative entropy are used rather than classical Shannon entropy.

Geometrically, the presence of an eavesdropper causes detectable mapping to change from a noiseless one-to-one relationship to a stochastic map. If there is no cloning activity on the channel, then $H(X|Y) = 0$ and the radius of the smallest enclosing quantum informational ball on Bob's side will be maximized.

B. *Properties of Quantum States*

In the quantum space, a quantum state can be described by their density matrix $\rho \in \square_{d\times d}$, which is a $d \times d$ matrix, where *d* is the level of the given quantum system. For an *n* qubit system, the dimension is $d = 2^n$. The two-level quantum states can be given by their density matrices in the following way:

$$\rho = \frac{1}{2}\begin{pmatrix} 1+z & x-iy \\ x+iy & 1-z \end{pmatrix},\ x^2 + y^2 + z^2 \le 1, \tag{5}$$

where *i* denotes the complex imaginary $i^2 = -1$. In quantum cryptography, the encoded pure quantum states are sent through a quantum communication channel. Using the Bloch sphere representation, the quantum state ρ can be given as a three-dimensional point $\rho = (x, y, z)$ in $\square^3$, and it can be represented by spherical coordinates

$$\rho = (r, \theta, \varphi), \tag{6}$$

where *r* is the radius of the quantum state to the origin, while θ and φ represents the latitude and longitude rotation angles. On the Bloch ball B, the *pure* states are on the boundary of the Bloch ball B, while the *mixed* states are inside the Bloch ball.

C. *Measuring Distances between Quantum States*

For two *pure* quantum states ρ and σ, the geometrical distance $d(\rho,\sigma)$ is defined as

$$\cos d_{Pure}(\rho,\sigma) = \sqrt{Tr(\rho\sigma)}, \tag{7}$$

respectively. For the $d_{Pure}(\rho,\sigma)$ geometrical distance between two pure quantum states, an obvious condition can be given in the following way:

$$0 \le d_{Pure}(\rho,\sigma) \le \frac{\pi}{2}. \tag{8}$$

We can define geometrical distances between mixed states and pure states in the following way:

$$d_{P,M}(\rho,\sigma) = \sqrt{1 - Tr\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}}, \tag{9}$$

where the quantum states ρ and σ are arbitrary quantum states. If both ρ and σ are *pure* states, then the distance $d_{P,M}(\rho,\sigma)$ between the quantum states can be given by

$$d_{P,M}(\rho,\sigma) = \sqrt{1 - \mathrm{Tr}(\rho\sigma)}, \tag{10}$$

as we illustrated it in Figure 2.

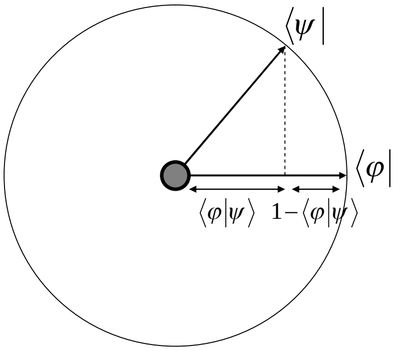


Figure 2. Geometrical representation of distance between pure quantum states.

Hence, for pure quantum states there is a coincidence between distances, since

$$d_{Pure}(\rho,\sigma) = d_{P,M}(\rho,\sigma), \tag{11}$$

thus, the distances $d_{P,M}(\rho,\sigma)$ and $d_{Pure}(\rho,\sigma)$ are the same for pure quantum states.

In our security analysis, the distances between quantum states is defined by the quantum relative entropy. The relative entropy of quantum states measures the informational distance between quantum states.

The classical Shannon-entropy of a discrete *d*-dimensional distribution *p* can be given by

$$H(p)=\sum_{i=1}^{d} p_i \log\frac{1}{p_i}=-\sum_{i=1}^{d} p_i \log p_i \ . \qquad (12)$$

The von Neumann entropy S of quantum states is a generalization of the classical Shannon entropy to density matrices [8][9]. The entropy of quantum states can be given by:

$$\mathrm{S}(\rho)=-Tr(\rho\log\rho). \qquad (13)$$

The quantum entropy $\mathrm{S}(\rho)$ is equal to the Shannon entropy for the eigenvalue distribution:

$$\mathrm{S}(\rho)=\mathrm{S}(\lambda)=-\sum_{i=1}^{d}\lambda_i\log\lambda_i, \qquad (14)$$

where *d* is the level of the quantum system.

The relative entropy in classical systems is a measure, that quantifies how close a probability distribution *p* to a model or candidate probability distribution *q* [8][9]. For *p* and *q* probability distributions the relative entropy can be given by

$$D(p\|q)=\sum_i p_i\log_2\frac{p_i}{q_i}\ . \qquad (15)$$

The relative entropy between quantum states can be measured by

$$D(\rho\|\sigma)=Tr\left[\rho(\log\rho-\log\sigma)\right]. \qquad (16)$$

The quantum relative entropy plays a key role in the description of the quantum state space. The quantum informational distance has some distant-like properties, however it is not commutative [8][9], thus $D(\rho\|\sigma)\neq D(\sigma\|\rho)$, and $D(\rho\|\sigma)\geq 0$ iff $\rho\neq\sigma$, and $D(\rho\|\sigma)=0$ iff $\rho=\sigma$. The quantum information theoretical distance is not symmetric, nor do they satisfy the triangular inequality of metrics.

D. Quantum Informational Distance between Quantum States

The quantum relative entropy reduces to the classical Kullback-Leibler relative entropy for simultaneously diagonal matrices. Using the negative entropy of quantum states, the relative entropy of quantum states can be described by a strictly convex and differentiable generator function $\mathbf{F}$:

$$\mathbf{F}(\rho)=-\mathrm{S}(\rho)=Tr(\rho\log\rho). \qquad (17)$$

The quantum informational distance $D(\rho\|\sigma)$ for density matrices ρ and σ can be given by generator function $\mathbf{F}$ in the following way:

$$D(\rho\|\sigma)=\mathbf{F}(\rho)-\mathbf{F}(\sigma)-\langle\rho-\sigma,\nabla\mathbf{F}(\sigma)\rangle, \quad (18)$$

where $\langle\rho,\sigma\rangle=Tr(\rho\sigma^{*})$ is the inner product of quantum states, and $\nabla\mathbf{F}(\cdot)$ is the gradient. In Figure 3, we have depicted the geometrical interpretation of quantum informational distance between quantum states ρ and σ [1][5][6]. The point of intersection of quantum state ρ on $H(\sigma)$ is denoted by $H_\sigma(\rho)$. The tangent hyperplane to hypersurface $\mathbf{F}(x)$ at quantum state σ is

$$H_\sigma=\mathbf{F}(\sigma)+\langle\nabla\mathbf{F}(\sigma),x-\sigma\rangle. \qquad (19)$$

We have depicted the quantum informational distance, $D(\rho\|\sigma)$, as the vertical distance between the generator function $\mathbf{F}$ and $H(\sigma)$, the hyperplane tangent to $\mathbf{F}$ at σ.

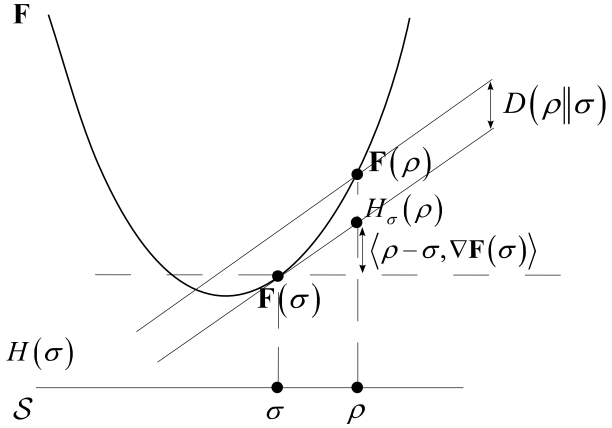


Figure 3. Depiction of generator function as negative von Neumann entropy.

We note, if σ has zero eigenvalues, quantum relative entropy function $D(\rho\|\sigma)$ may diverge, otherwise it is a finite and continuous function.

The quantum relative entropy for general quantum state $\rho=(x,y,z)$ and mixed state $\sigma=(\tilde{x},\tilde{y},\tilde{z})$, with radii $r_\rho=\sqrt{x^2+y^2+z^2}$ and $r_\sigma=\sqrt{\tilde{x}^2+\tilde{y}^2+\tilde{z}^2}$, can be expressed as

$$\begin{aligned}D(\rho\|\sigma)=&\frac{1}{2}\log\frac{1}{4}\left(1-r_\rho{}^2\right)+\frac{1}{2}r_\rho\log\frac{\left(1+r_\rho\right)}{\left(1-r_\rho\right)}\\&-\frac{1}{2}\log\frac{1}{4}\left(1-r_\sigma{}^2\right)-\frac{1}{2r_\sigma}\log\frac{\left(1+r_\sigma\right)}{\left(1-r_\sigma\right)}\langle\rho,\sigma\rangle,\end{aligned}\tag{20}$$

where $\langle\rho,\sigma\rangle=(x\tilde{x}+y\tilde{y}+z\tilde{z})$. For a maximally mixed state $\sigma=(\tilde{x},\tilde{y},\tilde{z})=(0,0,0)$ and $r_\sigma=0$, the quantum divergence can be expressed as

$$D(\rho\|\sigma)=\frac{1}{2}\log\frac{1}{4}\left(1-r_\rho{}^2\right)+\frac{1}{2}r_\rho\log\frac{\left(1+r_\rho\right)}{\left(1-r_\rho\right)}-\frac{1}{2}\log\frac{1}{4}.\tag{21}$$

Using Bloch vector representation $\rho=\frac{1}{2}\left(\mathbf{1}+\vec{r}_\rho\cdot\vec{\sigma}\right)$ and $\sigma=\frac{1}{2}\left(\mathbf{1}+\vec{r}_\sigma\cdot\vec{\sigma}\right)$ of two mixed states ρ and σ, the quantum relative entropy between them can be given by the following formula:

$$\begin{aligned}D(\rho\|\sigma)=&\frac{1}{2}\log\left(\frac{1-r_\rho^2}{1-r_\sigma^2}\right)+\frac{1}{2}r_\rho\log\left(\frac{1+r_\rho}{1-r_\rho}\right)\\&-\frac{1}{2}\left(r_\rho\cos\theta\right)\log\left(\frac{1+r_\sigma}{1-r_\sigma}\right),\end{aligned}\tag{22}$$

where r_ρ and r_σ denote the lengths of Bloch vectors, and θ is the angle between the two mixed quantum states. The quantum informational distance between two mixed quantum states depends on the lengths of their Bloch vectors and the angle θ between them, as illustrated in Figure 4.

The density matrices of quantum states are represented by 3D points in the Bloch ball. The eavesdropper's cloner transformation is modeled by an affine map, which maps quantum states to other quantum states. Geometrically, the eavesdropper maps the Bloch ball to a deformed ball. The cloning activity in the channel can then be analyzed by the radius of the deformed Bloch ball, which can be computed by the proposed geometric methods.

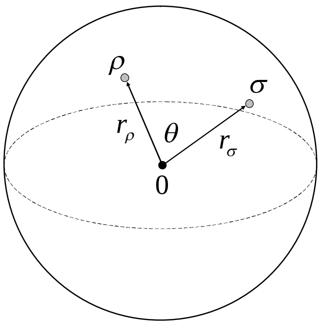


Figure 4. The quantum relative entropy between two mixed quantum states.

In our security analysis a Delaunay tessellation is used, whose diagram is symmetrical only for pure states, and asymmetrical for quantum states if the lengths of the radii differ. To construct a Delaunay triangulation, three-dimensional Laguerre diagrams are used.

E. The Smallest Enclosing Quantum-Information Ball

We would like to compute the radius r of the smallest enclosing ball, thus first we have to seek the center $\mathbf{c}^*$ of the point set S. The set S of quantum states is denoted by $\mathrm{S}=\{\rho_i\}_{i=1}^n$. The distance function $d(\cdot,\cdot)$ between any two quantum states of S is measured by quantum relative entropy, thus the minimax mathematical optimization is applied to quantum informational distance to find the center $\mathbf{c}$ of the set S of quantum states. We denote the quantum informational distance from $\mathbf{c}$ to the furthest point of S by distance function $d(\cdot,\cdot)$ as

$$d(\mathbf{c},\mathrm{S})=\max_i d(\mathbf{c},s_i).\tag{23}$$

Using the minimax optimization, we can minimize the maximal quantum relative entropy from $\mathbf{c}$ to the furthest point of S by

$$\mathbf{c}^*=\arg\min_{\mathrm{c}} d(\mathbf{c},\mathrm{S})\tag{24}$$

In Figure 5, we illustrated the circumcenter $\mathbf{c}^*$ of S, and the smallest enclosing balls for the Euclidean distance and quantum relative entropy [11].

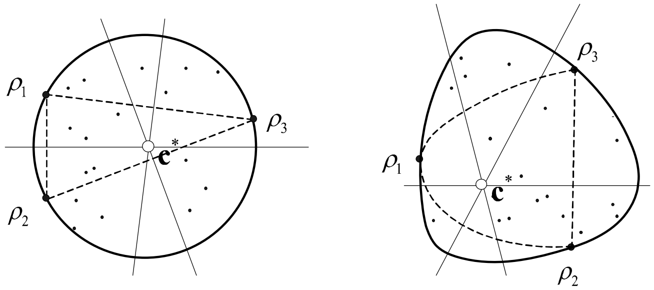


Figure 5. Circumcenter for Euclidean distance ball and quantum relative entropy ball.

In Figure 6, we compare the smallest quantum informational ball and the ordinary Euclidean ball [11]. We can conclude that the quantum states ρ_1, ρ_2 and ρ_3, which determine the Euclidean smallest enclosing ball are different from the states of the quantum informational ball.

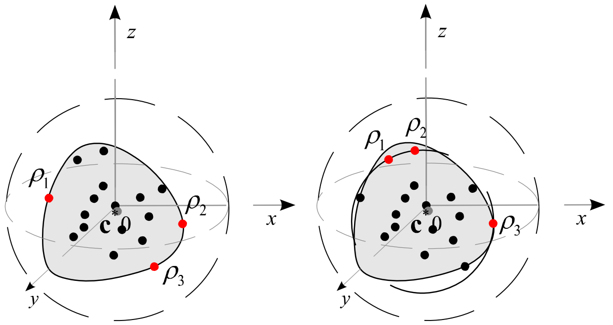


Figure 6. The maximum distance states of the smallest balls differ for the quantum informational distance and Euclidean distance.

The informational theoretical effect of the eavesdropper's cloning machine is described by the *radius* of the smallest enclosing quantum informational ball, denoted by r^*. This quantum informational theoretical radius is equal to the maximum quantum informational distance from the center, and can be expressed as:

$$r^* = \min_{\sigma \in \mathrm{S}(\mathbb{C}^2)} \max_{\rho \in \mathrm{S}(\mathbb{C}^2)} D\left(\mathrm{L}(\rho) \| \mathrm{L}(\sigma)\right). \tag{25}$$

In the proposed procedure of calculating the smallest enclosing information ball, a Delaunay tessellation is used because it is the *fastest* known tool with which to seek the center of a smallest enclosing ball of points.

III. Quantum Cloning in Quantum Cryptography

The quantum cloning machine does a trace-preserving, completely positive map $\{U, |\mathrm{M}\rangle\}$. When apriori information about the input states is given so that input quantum states can be particularly characterized, we call it state-dependent quantum cloning. By the outputs, there are symmetric and asymmetric cloning machines. A cloning machine is called symmetric if at the output all the clones have the same fidelity, and asymmetric if the clones have different fidelities.

The quantum channel's error rate is denoted by D_C^{attack}, and the maximal information theoretic fidelity of the eavesdropper's cloning machine is denoted by F_{Eve}. The parameter F_{Eve} represents the theoretical upper bound on the cloning machine's fidelity. The cloning machine based attack has a critical value for the error rate

$$D_C^{attack} = 1 - F_{Eve}, \tag{26}$$

thus Eve's cloning machine fidelity is

$$F_{Eve} = 1 - D_C^{attack}. \tag{27}$$

For example, if Eve uses universal quantum cloner, then the value of parameter F_{Eve} is independent of input quantum state $|\psi\rangle$, and the fidelity of her optimal quantum cloning machine can be defined by

$$F_{Eve} = \langle\psi|^{(in)} \rho^{(out)} |\psi\rangle^{(in)} = \frac{1}{2}(1+\eta), \tag{28}$$

where η is the reduction factor. The quantum cloning transformation is optimal [14][15], if $\eta = \frac{2}{3}$, hence the maximal fidelity of optimal universal cloning is $F_{Eve} = \frac{5}{6}$, and the maximal radius $r_{Eve}^{universal}$ is

$$r_{Eve}^{universal} = \frac{2}{3}. \tag{29}$$

The quantum informational theoretical radius can be defined as

$$r_{Eve}^{*universal} = 1 - \mathrm{S}\left(r_{Eve}^{universal}\right), \tag{30}$$

where S is the von Neumann entropy of corresponding quantum state with radius length $r_{Eve}^{universal}$.

In general, the universal cloning machine [14][15][16] output state is can be given as

$$\rho^{(out)} = F_{Eve} |\psi\rangle_a \langle\psi| + (1 - F_{Eve}) |\psi_\perp\rangle_a \langle\psi_\perp|. \tag{31}$$

Asymmetric cloning has direct application to eavesdropping strategies in quantum cryptography. The best-known example of state-dependent quantum cloning machine is the phase-covariant cloning machine. Here, the states lie in the equator $(x-y)$ of the Bloch sphere, thus the fidelity of the cloning will be independent of φ.

A. *Optimal Individual Eavesdropping Strategy for QKD*

The phase-covariant cloning machine has a remarkable application in quantum cryptography, namely its use in optimal individual eavesdropping strategies in the BB84 protocol [20][22][23]. Using an individual-type cloning-based attack, Eve applies the same unitary transformation to each sent quantum state. She does not introduce correlation among the copies, measuring her state after she clones it [9]. Alice, Bob and Eve immediately measure their respective quantum states, since the parties have no ability to store qubits.

The results of their measurements can be described by a probability distribution $P(A,B,E)$. Eve's quantum state is denoted by $|E\rangle$, while the unitary operation, which describes the interaction between the sent qubit and Eve's state, is denoted by L, and thus the whole transformation can be expressed as [24][26]:

$$\begin{aligned} |E\rangle \otimes |0\rangle &\xrightarrow{\mathrm{L}} |E_{0,0}\rangle|0\rangle + |E_{0,1}\rangle|1\rangle, \\ |E\rangle \otimes |1\rangle &\xrightarrow{\mathrm{L}} |E_{1,0}\rangle|0\rangle + |E_{1,1}\rangle|1\rangle, \end{aligned} \quad (32)$$

where $|E_{i,j}\rangle$ denotes Eve's cloned quantum state. $|E\rangle$ can be written as a 2×2 matrix, whose elements are Eve's states $|E_{i,j}\rangle$ [9].

Eve's cloning activity can be written in the following form:

$$\begin{aligned} |E\rangle \otimes |0\rangle &\xrightarrow{\mathrm{L}} \sqrt{F}\,|E_{0,0}\rangle|0\rangle + \sqrt{D}\,|E_{0,1}\rangle|1\rangle, \\ |E\rangle \otimes |1\rangle &\xrightarrow{\mathrm{L}} \sqrt{D}\,|E_{1,0}\rangle|0\rangle + \sqrt{F}\,|E_{1,1}\rangle|1\rangle, \end{aligned} \quad (33)$$

where $|E_{i,j}\rangle$ represents Eve's normalized state in case Alice sent an *i*-bit and Bob detected a *j*-bit. F is the fidelity parameter, while D is the disturbance. The fidelity F provides the probability that Bob detected Alice's bit correctly using the same basis, while D provides the probability of an incorrect detection [9].

B. *Different Types of Quantum Cloners*

In quantum cryptography the optimal eavesdropping attack is done by a phase-covariant cloning machine, which clones the *x* equator. The importance of equatorial qubits lies in the fact, that quantum cryptography requires these states, rather than the states that span the whole Bloch sphere [9].

The transformations were restricted for pure input states of the form

$$|\psi_\phi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\phi}|1\rangle\right), \quad (34)$$

where the parameter $\phi \in [0, 2\pi)$ represents the angle between the Bloch vector and the *x*-axis. These qubits are called equatorial qubits, because the *z*-component of their Bloch vector is zero. The phase-covariant quantum cloners [14][15][16] can clone arbitrary equatorial qubits, and they keep the quality of the copies same for all equatorial qubits. The reduced density operator of the copies at the output can be expressed as [9]

$$\rho^{(out)} = \left(\frac{1}{2} + \sqrt{\frac{1}{8}}\right)|\psi_\phi\rangle\langle\psi_\phi| + \left(\frac{1}{2} - \sqrt{\frac{1}{8}}\right)|\psi_{\phi,\perp}\rangle\langle\psi_{\phi,\perp}|, \quad (35)$$

where $|\psi_{\phi,\perp}\rangle$ is orthogonal to state $|\psi_\phi\rangle$. Thereby, the optimal fidelity of 1 to 2 phase-covariant cloning transformation is given by

$$F_{1\to 2}^{phase} = \frac{1}{2} + \sqrt{\frac{1}{8}} \approx 0.8535. \quad (36)$$

If Eve has a phase-covariant quantum cloner, then the maximal value of her *radius* r_{Eve}^{phase} is

$$r_{Eve}^{phase} = 2\sqrt{\frac{1}{8}}. \quad (37)$$

The quantum informational radius r_{Eve}^{*phase} of the phase-covariant cloner can be defined as

$$r_{Eve}^{*phase} = 1 - \mathrm{S}\left(r_{Eve}^{phase}\right), \quad (38)$$

where S is the von Neumann entropy of corresponding quantum state with radius length r_{Eve}^{phase}.

The phase-covariant quantum cloning transformation produces two copies of the equatorial qubit, with optimal fidelity. The phase-covariant cloning transformation without ancilla is a two-qubit unitary transformation, it can be given by $|0\rangle|0\rangle \to |0\rangle|0\rangle$ and $|1\rangle|0\rangle \to \cos\eta|1\rangle|0\rangle + \sin\eta|0\rangle|1\rangle$, where $\eta \in [0, \pi/2]$ is the shrinking parameter, which is related to the fidelity [14][15][16][23].

IV. Computation of Quantum Channel Security

In this section the informational geometric model of the proposed security analysis is defined, fundamentally based on the results of Gyongyosi and Imre [1]. In the computation of the smallest enclosing quantum informational ball, the results of Kato et al. [5] and Nielsen and Nock [11] are also used.

In the proposed model, the fidelity of the eavesdropper's cloning machine is derived from the quantum informational theoretical radius r^* of the smallest enclosing quantum informational ball and the theoretical upper bound of the quantum informational radius of the eavesdropper's cloning machine, denoted by r_{Eve}^*.

Theorem

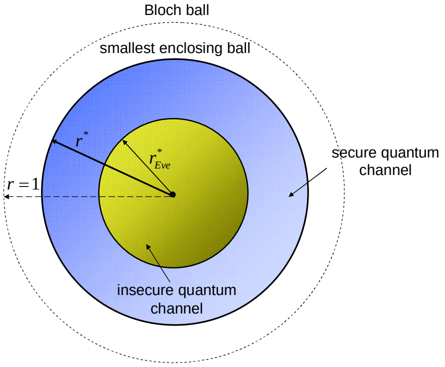
For a secure quantum channel, the radius r^* of the smallest enclosing quantum informational ball of mixed states must be greater than r_{Eve}^*, thus

$$r^* > r^*_{Eve} , \qquad (39)$$

where r^* is the radius of the smallest enclosing informational ball, computed by the proposed method. In terms of the second part, for an insecure quantum channel the radius r^* is smaller than or equal to r^*_{Eve} and thus

$$r^* \le r^*_{Eve} . \qquad (40)$$

Figure 7 shows a geometric interpretation of the proposed model for a secure quantum channel.

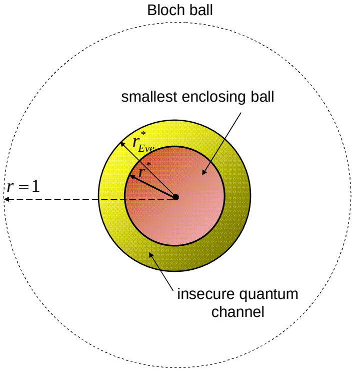


$r^* > r^*_{Eve}$

Figure 7. The radius of the smallest enclosing informational ball for secure quantum communication**.**

In our security analysis, a spherical Delaunay tessellation is used to compute the quantum informational theoretical radius r^*, since it can be simply obtained as an ordinary Euclidean Delaunay triangulation mesh. The quantum relative entropy-based Delaunay tessellation of pure states is identical to conventional spherical Delaunay tessellation [1][6].

Figure 8 shows a geometric interpretation of the proposed model for an insecure quantum channel [1].



$r^* \le r^*_{Eve}$

Figure 8. The radius of the smallest enclosing informational ball for insecure quantum communication.

In this scheme, the radii r_{UCM} and $r_{phasecov}$ of corresponding quantum cloners are derived from the smallest enclosing quantum informational balls.

The informational theoretical radius r^*_{UCM} of a universal quantum cloner can be expressed as

$$r^*_{UCM} = 1 - \mathrm{S}(r_{UCM}) . \qquad (41)$$

For a phase-covariant cloner, the informational theoretical radius $r^*_{phasecov}$ can be defined as

$$r^*_{phasecov} = 1 - \mathrm{S}(r_{phasecov}) , \qquad (42)$$

where S is the von Neumann entropy of the corresponding quantum state. In our numerical calculations, the notations r_{UCM} and $r_{phasecov}$ are used for the maximal radii.

The values of r_{UCM} and $r_{phasecov}$ can be computed from the informational theoretical radii of the smallest enclosing quantum informational balls, denoted by r^*_{UCM} and $r^*_{phasecov}$.

Theorem

For UCM and phase-covariant cloner machines, the connection between informational theoretical radii r^*, r^*_{Eve} and the Bloch vectors r and r_{Eve} can be defined as:

$$r^* = 1 - \mathrm{S}(r), \qquad (43)$$

and

$$r^*_{Eve} = 1 - \mathrm{S}(r_{Eve}), \qquad (44)$$

where S is the von Neumann entropy, and r and r_{Eve} are the Euclidean lengths of the vectors from the Bloch sphere origin.

The smallest quantum informational ball with radius r^* is shown in gray, with the ball of the ideal UCM cloner with radius r^*_{UCM} shown in light gray.

It can be concluded that if $r_{\mathrm{E}} \ge r_{\mathrm{E},UCM}$, then $r^* \le r^*_{UCM}$, and hence the informational theoretical radius will be smaller.

Figure 9 compares ideal and imperfect universal and phase-covariant cloner quantum balls.

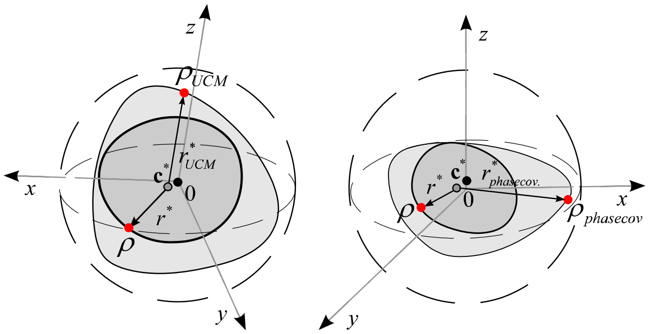


Figure 9. Smallest enclosing quantum informational balls of optimal and imperfect universal and phase-covariant cloners.

It can be concluded that the informational theoretical radii for ideal and imperfect phase-covariant cloning are different.

Figure 10 illustrates the radii r^*_{UCM} and $r^*_{phasecov}$ of the smallest enclosing quantum informational ball for UCM-based and phase-covariant cloner based attacks, in Bloch sphere representation.

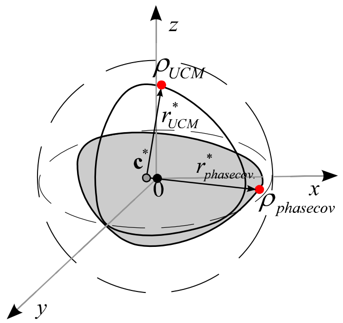


Figure 10. Comparison of smallest enclosing quantum informational ball of UCM-based and phase-covariant cloners.

Geometrically, the smallest quantum informational ball can be computed from the intersection of the contours of the quantum relative entropy ball with the ellipsoid of the secret channel, the latter being generated by the eavesdropper's cloner machine.

A. *Geometrical Calculation of Channel Security*

In the Bloch sphere representation, the smallest value of $D(\rho\|\sigma)$ corresponds to the contour closest to the location of density matrix.

In Figure 11, the smallest quantum informational ball with radius $r^* = D_{\max}(\mathbf{r}_\rho\|\mathbf{r}_\sigma)$, intersects the channel ellipsoid at the magnitude m_ρ of Bloch vector $\mathbf{r}_\rho$. The Euclidean distance between the origin and center $\mathbf{c}^*$ is denoted by m_σ. Similarly, the Euclidean distance between the origin and state ρ is denoted by m_ρ, respectively.

We note, that for a perfect UCM cloner and a perfect phase-covariant cloner, the center of the channel ellipsoid is equal to the Bloch sphere origin. In our next example, we will use an imperfect quantum cloner model, where the center slightly differs from the Bloch sphere origin.

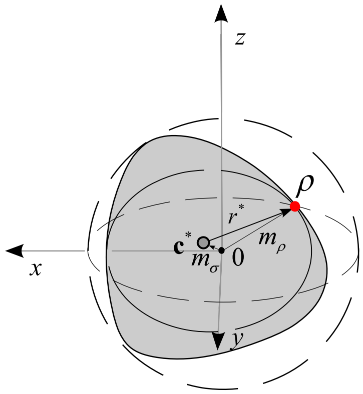


Figure 11. Intersection of radius of smallest enclosing quantum informational ball and channel ellipsoid.

In our geometrical iteration algorithm, we would like to determine the location of vector $\mathbf{r}_\sigma$ inside the channel ellipsoid such that, the largest possible contour value $D_{\max}(\mathbf{r}_\rho\|\mathbf{r}_\sigma)$ touches the channel ellipsoid surface, and the remainder of the $D_{\max}$ contour surface lies entirely outside the channel ellipsoid. The point on the channel ellipsoid surface is defined as the set of channel output ρ. The vector $\mathbf{r}_\sigma$ is defined in the interior of the ellipsoid, as the convex hull of the channel ellipsoid.

To determine the optimal length of the radius, the algorithm moves point σ. As we move vector $\mathbf{r}_\sigma$ from the optimum position, a larger contour corresponding to the larger value of the quantum relative entropy D will intersect the channel ellipsoid surface, thereby $\max_{\mathbf{r}_\rho} D(\mathbf{r}_\rho\|\mathbf{r}_\sigma)$ will increase. We can conclude that vector $\mathbf{r}_\sigma$ should be adjusted to minimize $\max_{\mathbf{r}_\rho} D(\mathbf{r}_\rho\|\mathbf{r}_\sigma)$, as we illustrated it in Figure 12.

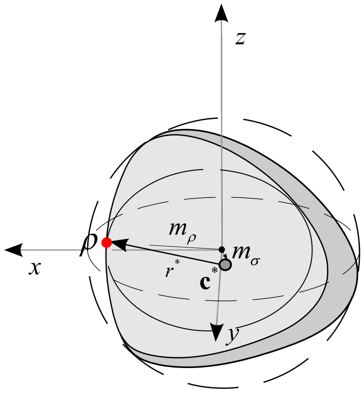


Figure 12. Moving of the vector from the optimum position will increase quantum relative entropy. The optimal ball is shown in light-grey.

The maximum length radius $\mathbf{r}_\rho$ can be determined by an iterative algorithm, suing the quantum relative entropy as distance measure. The computed radius is equal to the radius of the smallest quantum informational ball, hence the quantum informational radius can be used to derive the fidelity of the eavesdropper's quantum cloner machine.

B. Geometrical Representation of the Iteration Process

The vector $\mathbf{r}_\sigma$ should be adjusted to minimize the value of $\max_{\mathbf{r}_\rho} D\left(\mathbf{r}_\rho \| \mathbf{r}_\sigma\right)$. To find the optimal value of vector $\mathbf{r}_\sigma$ in our geometrical analysis, we choose a start point for vector $\mathbf{r}_\sigma$ in the interior of the ellipsoid.

In Figure 13(a), we show the initial start point inside the channel ellipsoid chosen by the algorithm. The vector of state σ is denoted by $\mathbf{r}_\sigma$. In the next step, the algorithm determines the set of points to the vector $\mathbf{r}'_\rho$ on the ellipsoid surface most distant from $\mathbf{r}_\sigma$, using the quantum relative entropy as distance measure. In Figure 13(b), the new state is notated by ρ'.

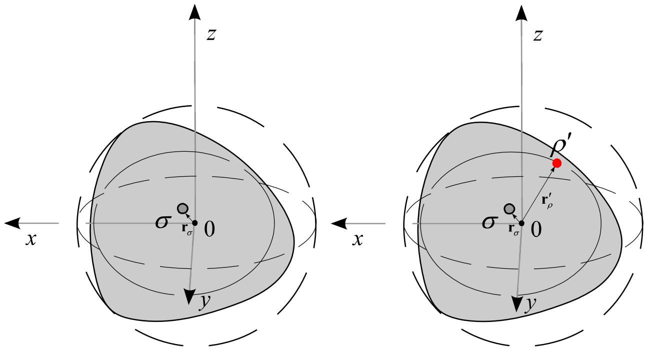


Figure 13. The algorithm determines the points on the ellipsoid surface most distant from the point, using the quantum relative entropy.

The maximum distance between the states can be expressed as

$$\max_{\mathbf{r}_\rho} D\left(\mathbf{r}'_\rho \| \mathbf{r}_\sigma\right). \tag{45}$$

We choose a random Bloch sphere vector from the maximal set of points according to vector $\mathbf{r}'_\rho$. The selected point is denoted by $\mathbf{r}''_\rho$. The algorithm makes a step from $\mathbf{r}_\sigma$ towards the surface point vector $\mathbf{r}''_\rho$ in the Bloch sphere space. In this step, the algorithm updates vector $\mathbf{r}_\sigma$ to

$$\mathbf{r}^*_\sigma = (1-\gamma)\mathbf{r}_\sigma + \gamma \mathbf{r}''_\rho, \tag{46}$$

where γ denotes the size of the step.

In Figure 14(a), the updated state and the vector of the state are denoted by ρ'' and $\mathbf{r}''_\rho$. The center of the quantum informational ball is denoted by $\mathbf{r}^*_\sigma$.

In Figure 14(b), we illustrate the quantum informational distance between the final center point and the maximal distance state ρ, using the notation $\max_{\mathbf{r}_\rho} D\left(\mathbf{r}_\rho \| \mathbf{r}_\sigma\right)$.

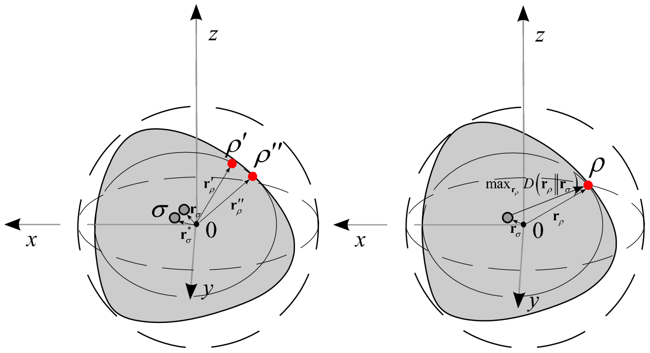


Figure 14. The algorithm makes a step towards the found surface point vector and updates the vector.

Using the updated vector $\mathbf{r}^*_\sigma$, the algorithm continues to loop until $\max_{\mathbf{r}^*_\rho} D\left(\mathbf{r}'_\rho \| \mathbf{r}^*_\sigma\right)$ no longer changes. We conclude that the iteration converges to the optimal $\mathbf{r}_\sigma$, because the algorithm minimizes $\max_{\mathbf{r}_\rho} D\left(\mathbf{r}_\rho \| \mathbf{r}_\sigma\right)$. At the end of the iteration process, the radius of the smallest quantum informational ball can be expressed as

$$\min \max_{\mathbf{r}_\rho} D\left(\mathbf{r}_\rho \| \mathbf{r}_\sigma\right). \tag{47}$$

We would like to compute the radius r^* of the smallest enclosing ball, thus first we have to seek the center $\mathbf{c}^*$ of the point set S.

C. Delaunay Triangulation on the Bloch Sphere

The mesh of the Bloch sphere B can be described as a number of points connected in some way by lines, the points and the lines of the mesh are referred to as *edges* and *vertices*.

The triangle t is said to be Delaunay, when its circumcircle is empty. For an empty circumcircle, the circle passing through the quantum states of a triangle $t \in T$, encloses no other vertex of the set S [6][7].

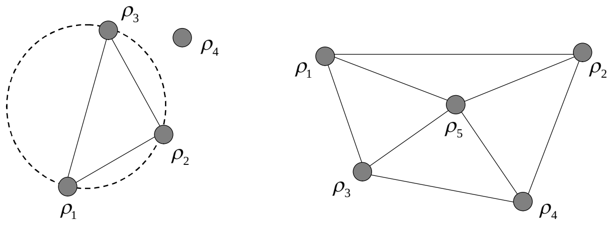


Figure 15. The Delaunay triangulation of a set of quantum states.

The Delaunay triangulation $Del(\mathrm{S})$ of a set of quantum states S is unique, if at most three quantum states $\rho \in \mathrm{S}$ are co-circular. The Delaunay triangulation $Del(\mathrm{S})$ of a set of quantum states $\mathrm{S} = \{\rho_1, \rho_2, \ldots \rho_n\}$ maximizes the minimum angle among all triangulation of a given set of quantum states, and the circle centered at vertex $\mathbf{c}$, gives an empty circumcenter for quantum states $\rho_1\rho_2\rho_3$, as we illustrated it in Figure 16.

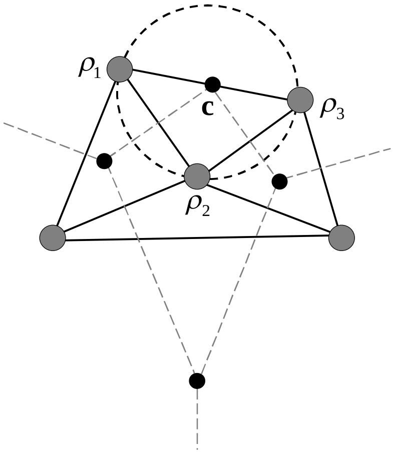


Figure 16. The triangle of quantum states corresponds to the vertex c.

In our paper we use the Laguerre Delaunay diagrams [6][7] to compute the radius of the smallest enclosing ball. In general, the Laguerre distance for generating point x_i with weight r_i^2, is defined by

$$d_L(\rho, x_i) = \|\rho - x_i\|^2 - r_i^2 . \tag{48}$$

The Delaunay diagram for the Laguerre distance is called the Laguerre Delaunay diagram. We illustrated the dual diagram of the Laguerre Delaunay tessellation in Figure 17.

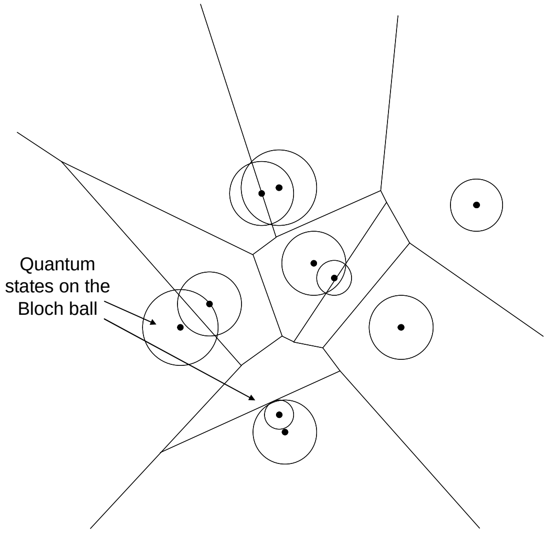


Figure 17. Laguerre diagram for quantum states on the Bloch ball.

We show a fundamentally new method for deriving the quantum relative entropy based Delaunay tessellation on the Bloch ball B, to analyze the informational theoretical impacts of eavesdropping activity on the quantum channel.

V. Geometrical Computation of Smallest Quantum Informational Ball

In our algorithm we present an effective solution to seek the center $\mathbf{c}$ of the set of smallest enclosing quantum information ball, using Laguerre diagrams. Our geometrical-based security analysis has two main steps:

1. *We construct quantum Delaunay triangulation from Laguerre diagrams on the Bloch ball.*
2. *We seek the center of the smallest enclosing ball.*

In our procedure, we use Delaunay tessellation, because it is the *fastest* tool to seek the center of a smallest enclosing ball of points. By the usage of quantum Delaunay triangulation on the Bloch sphere, the convex hull of the quantum states, and the radius of the smallest enclosing quantum informational ball could be determined very efficiently.

A. Delaunay Triangulation from Laguerre Diagrams

The Laguerre distance of a point x to an Euclidean ball $b = b(\rho, r)$ is defined as $d_L(\rho, x) = \|\rho - x\|^2 - r^2$. For n balls, the Laguerre diagram of $b_i = b(\rho_i, r_i)$, where $i = 1, \ldots, n$, b_i can be defined as the minimization diagram of the corresponding n distance functions as [6][7]

$$d_L^i(x) = \|\rho - x\|^2 - r^2 . \tag{49}$$

We use the result of Aurenhammer to construct the quantum relative entropy based dual diagram of the Delaunay tessellation, by the Laguerre diagram of the n Euclidean spheres of equations [6]

$$\langle x-\rho_i', x-\rho_i'\rangle = \langle \rho_i', \rho_i'\rangle + 2\left(\mathbf{F}(\rho_i) - \langle \rho_i, \rho_i'\rangle\right). \quad (50)$$

In Figure 18, we illustrated the Laguerre diagram on the Bloch ball, and the construction of dual Delaunay diagram.

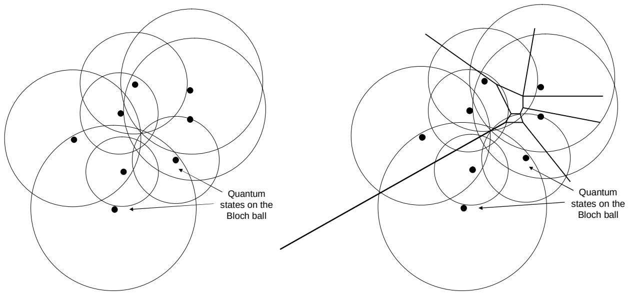

Quantum states on the Bloch ball
Quantum states on the Bloch ball

Figure 18. Tessellation on the Bloch ball, obtained by Laguerre diagram.

The most important result of this equivalence is that we can efficiently construct a quantum relative entropy-based Delaunay triangulation on the Bloch sphere, using fast methods for constructing the classical Euclidean Laguerre diagrams.

In Figure 19, we show the ordinary Delaunay triangulation. The quantum Delaunay triangulation is derived from the Laguerre diagram of Euclidean balls.

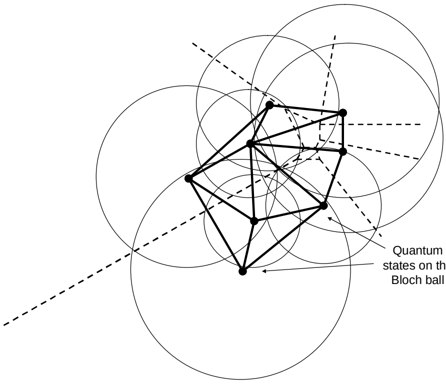


Figure 19. The regular triangulation on the Bloch ball.

We note, the image of quantum relative entropy based Delaunay triangulation by the inverse of gradient ∇_F^{-1}, is a curved triangulation whose vertices are the points of S .

B. Center of the Smallest Quantum Informational Ball

In our security analysis, we apply the approximation algorithm presented by Badoui and Clarkson [10][18], however in our algorithm, the distance measurement between quantum states is based on quantum relative entropy.

The E -core set C is a subset of the set $\mathrm{C} \subseteq \mathrm{S}$, such that for the circumcenter $\mathbf{c}$ of the minimax ball [10][18]

$$d(\mathbf{c}, \mathrm{S}) \le (1+\mathrm{E}) r, \quad (51)$$

where r is the radius of the smallest enclosing quantum information ball of the set of quantum states S [10][18].

The approximating algorithm, for a set of quantum states $\mathrm{S} = \{\rho_1, \ldots, \rho_n\}$ and circumcenter $\mathbf{c}$, first finds the farthest point ρ_m of ball set *B*, and moves $\mathbf{c}$ towards ρ_m in $\mathrm{O}(dn)$ time in every iteration step.

We denote the set of n d-dimensional balls by $B = \{b_1, \ldots, b_n\}$, where $b_i = Ball(S_i, r_i)$, S_i is the center of the ball b_i and r_i is the radius of the *i*-th ball. The smallest enclosing ball of set $B = \{b_1, \ldots, b_n\}$ is the unique ball $b^* = Ball(\mathbf{c}^*, r^*)$ with minimum radius r^* and center $\mathbf{c}^*$ [11].

In Figure 20, we illustrate the smallest enclosing ball of balls in the quantum space.

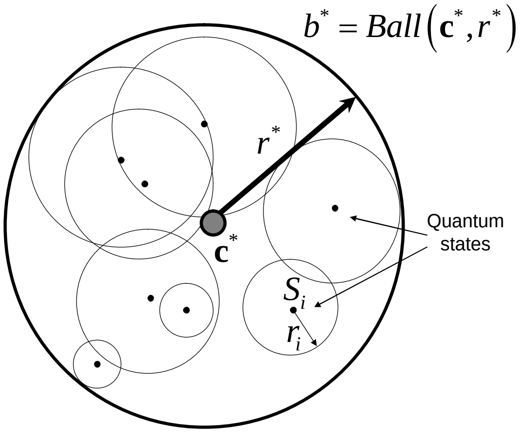


Figure 20. The smallest enclosing ball of a set of balls in the quantum space.

The *main steps* of our algorithm can be summarized as:

Algorithm 1.

```
1. Select a random center $\mathbf{c}_1$ from the set of quantum states S
        $\mathbf{c}_1 = S_1$
    for $\left(i = 1, 2, \ldots, \left\lceil \frac{1}{\mathrm{E}^2} \right\rceil\right)$
    do
2. Find the farthest point $S$ of S
        $S \leftarrow \arg\max_{s' \in \mathrm{S}} D_F(\mathbf{c}_i, S')$
3. Update the circumcircle:
        $\mathbf{c}_{i+1} \leftarrow \nabla_F^{-1}\left(\frac{i}{i+1}\nabla_F(\mathbf{c}_i) + \frac{1}{i+1}\nabla_F(S)\right).$
4. Return $\mathbf{c}_{i+1}$.
```

The smallest enclosing ball of ball set $B=\{b_1,\ldots,b_n\}$, fully enclosing B, thus $B\subseteq Ball\left(\mathbf{c}^*,r^*\right)$. The algorithm does

$$\left\lfloor \frac{1}{\mathrm{E}^2} \right\rfloor \tag{52}$$

iterations to ensure an $\left(1+\mathrm{E}\right)$ approximation, thus the overall cost of the algorithm is $\mathrm{O}\left(\frac{dn}{\mathrm{E}^2}\right)$ [18]. The smallest enclosing ball of a ball set B can be written as

$$\min\nolimits_{\mathbf{c}} \mathbf{F}_B\left(\mathbf{c}\right), \tag{53}$$

where $\mathbf{F}_B\left(X\right)=d\left(X,B\right)=\max_{i\in\{1,\ldots,n\}} d\left(X,B_i\right)$, and the distance function $d\left(\cdot,\cdot\right)$ measures the relative entropy between quantum states [6].

The minimum ball of the set of balls is unique, thus the circumcenter $\mathbf{c}^*$ of the set of quantum states is:

$$\mathbf{c}^*=\arg\min\nolimits_{\mathbf{c}} \mathbf{F}_B\left(\mathbf{c}\right). \tag{54}$$

At the end of our algorithm, the radius r^* of the smallest enclosing ball B^* with respect to the quantum informational distance is equal to $\min\limits_{\sigma\in\mathrm{S}\left(\square^2\right)} \max\limits_{\rho\in\mathrm{S}\left(\square^2\right)} D\left(\mathrm{L}\left(\rho\right)\middle\|\mathrm{L}\left(\sigma\right)\right)$.

The *security* of the quantum channel is determined by our geometrical model, with assumptions

$$r^*>r^*_{Eve}, \tag{55}$$

and

$$r^*\leq r^*_{Eve}, \tag{56}$$

as we have defined it at Eq. (39) and Eq. (40).

Finally, the approximated value of the fidelity parameter F_{Eve}, can be expressed as:

$$F_{Eve}=\left\langle\psi\right|^{(in)}\rho^{(out)}\left|\psi\right\rangle^{(in)}=\frac{1}{2}\left(1+r\right), \tag{57}$$

where r can be derived from the quantum informational theoretical radius r^* by $r^*=1-\mathrm{S}\left(r\right)$, where S is the von Neumann entropy.

C. The Computational Complexity of our Algorithm

The quantum relative entropy-based algorithm at the *i*-th iteration provides an $\mathrm{O}\left(1+\sqrt{i}\right)$-approximation of the real circumcenter, thus to obtain an $\left(1+\mathrm{E}\right)$ approximation, a time

$$\mathrm{O}\left(\frac{dn}{\varepsilon^2}\right)=\mathrm{O}\left(\frac{d}{\varepsilon^2}\frac{1}{\varepsilon}\right)=\mathrm{O}\left(\frac{d}{\varepsilon^3}\right) \tag{58}$$

is required, by first sampling $n=\frac{1}{\varepsilon}$ points [10]. Based on the computational complexity of the smallest enclosing ball, the $\left(1+\varepsilon\right)$ approximation of the fidelity of the eavesdropper cloning machine can be computed in a time

$$\mathrm{O}\left(\frac{d}{\varepsilon^2}\right). \tag{59}$$

VI. Optimized Algorithm

In this section an improved core-set algorithm is shown which determines the smallest quantum informational ball in a more efficient manner [18]. This improved method obtains a

$$\mathrm{O}\left(\frac{d}{\varepsilon}\right) \tag{60}$$

time $\left(1+\varepsilon\right)$ approximation algorithm in quantum space. In comparison with current geometric methods in the literature, this approach has a lower complexity than that presented by Kato et al. [5] or Nielsen and Nock [11].

In Figure 21, we illustrate the improved algorithm on a set of quantum states. The approximate ball has radius r, the enclosing ball has radius $r+\delta$. The approximate center $\mathbf{c}$ is denoted in black, the core-set is denoted by grey circles. The optimal radius between the center $\mathbf{c}$ and the farthest quantum state is denoted by r^* [18].

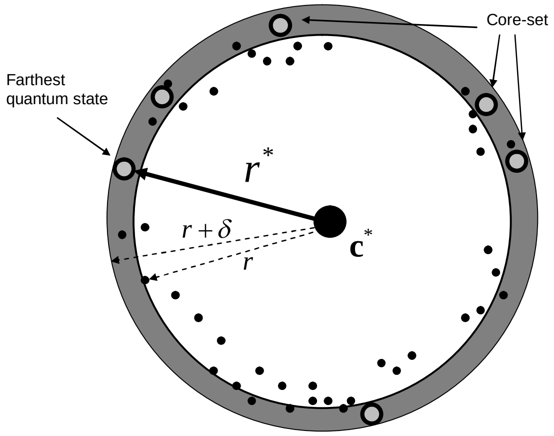


Figure 21. The approximate (light) and enclosing quantum information ball (darker).

The main steps of our improved algorithm can be summarized as:

Algorithm 2.

```
Select a random center $\mathbf{c}_1$ from the set of quantum states S
        $\mathbf{c}_1 \in \mathrm{S}$
$r = \frac{1}{2}\max_i D_F\left(\mathbf{c}_1, \mathrm{S}\right);$
$\delta = \frac{1}{2}\max_i D_F\left(\mathbf{c}_1, \mathrm{S}\right);$
for $\left(i = 1, 2, \ldots, \left(\frac{1}{\delta}\right)\right)$
  do
    $S = \arg\max_i D_F\left(c, \mathrm{S}\right);$
    Move $Ball\left(c, r\right)$ on the geodesic until it touches
    the farthest point $S$;
    $s = \max_i D_F\left(c, S_i\right) - r;$
    if $s \leq \frac{3\delta}{4}$ then
        $\delta = \frac{3\delta}{4}$
    else
        $r = r + \frac{\delta}{4};$
        $\delta = \frac{3\delta}{4};$
until $\delta \leq \varepsilon$.
```

The improved algorithm increments the radius of the quantum information ball from a lower bound r of the optimal radius r^* [18]. In this algorithm, the optimal radius is between $r \leq r^* \leq r + \delta$, and the process is terminates as $\delta \leq \varepsilon$, in at most

$$\mathrm{O}\left(\frac{1}{\varepsilon}\right) \tag{61}$$

iterations.

A. Rate of Converge

We made simulations and numerical analysis on the performances of the proposed algorithms. We have compared the core-set algorithm and the improved core-set algorithm to find the smallest enclosing quantum information ball. We have analyzed the approximation algorithms for 30 center updates.

In the simulation work, the quantum information ball is generated random, and the quantum relative entropy based approximation used uniformly sampled quantum states. In our numerical analysis, we have measured the quality of the approximation with respect to quantum relative entropy. At first we have simulated the algorithm presented in Section V, then we analyzed the improved algorithm presented in Section VI.

The results of our simulation are shown in Figure 22. The *x*-axis represents the number of center updates to find the center of the smallest enclosing quantum informational ball, the *y*-axis represents the quantum informational distance between the found center $\mathbf{c}$ and the optimal center $\mathbf{c}^*$.

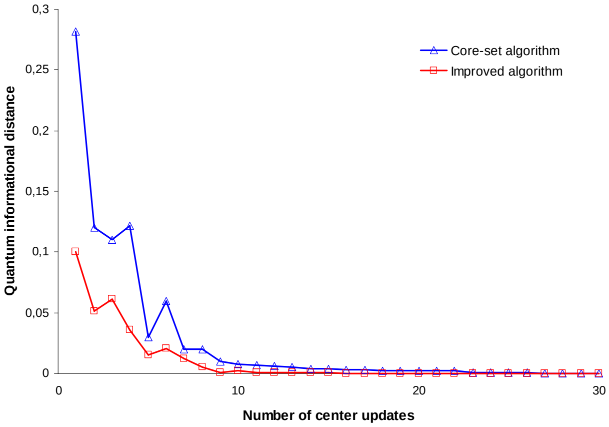


Figure 22. The converge rate of the approximation algorithms.

From the results, it can be seen that each presented algorithm finds the approximate center $\mathbf{c}$ to the optimal center $\mathbf{c}^*$ extremely quickly. The quantum relative entropy-based approximation algorithms have a very accurate convergence of $\mathbf{c}$ towards $\mathbf{c}^*$, but the improved core-set algorithm presented in Section VI converges more rapidly with a smaller number of center updates.

It can be concluded that only a small set of quantum states are required to compute the center of the quantum informational ball, with the proposed algorithms providing very solid approximations of the smallest quantum informational ball.

VII. Illustrative Example

In this section, the steps of the proposed algorithm are summarized. Here the six-state quantum cryptography protocol is used, together with the universal (UCM) quantum cloner-based attacker model. The smallest enclosing quantum informational ball for six mixed quantum states is computed. The proposed example illustrates the theoretical results of Section IV, integrating the mathematical background investigated by Gyongyosi and Imre [1], Kato et al. [5] and Nielsen and Nock [11].

As declared in Section IV, the quantum channel is secure if $r^* > r^*_{UCM}$. In the first step, the convex hull for the cloned states is computed by Delaunay tessellation, with respect to quantum informational distance.

Figure 23 illustrates the Voronoi cells for the cloned states, using the six-state quantum cryptography protocol. The cloned states were generated by Eve's universal quantum cloner machine. Cloned mixed states are denoted by $\rho_1, \rho_2, \rho_3, \rho_4, \rho_5$ and ρ_6.

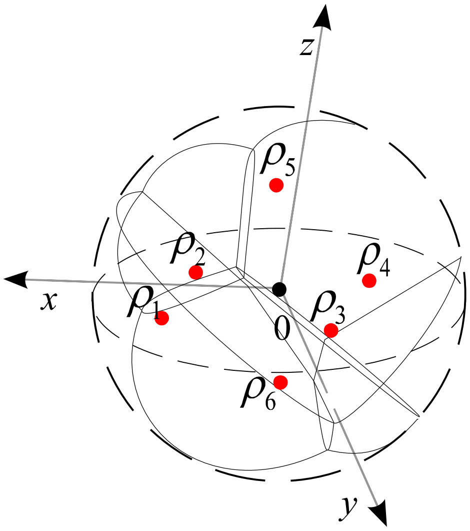


Figure 23. The dual Delaunay diagram in Bloch sphere representation.

In the next step of security analysis, the quantum Delaunay triangulation for the six cloned states is computed. Using quantum relative entropy-based Delaunay tessellation, the three-dimensional convex hull for cloned mixed quantum states $\rho_1, \rho_2, \rho_3, \rho_4, \rho_5$ and ρ_6 can be calculated.

Figure 24 illustrates the three-dimensional *convex hull* (light-gray) of cloned states $\rho_1, \rho_2, \rho_3, \rho_4, \rho_5$ and ρ_6.

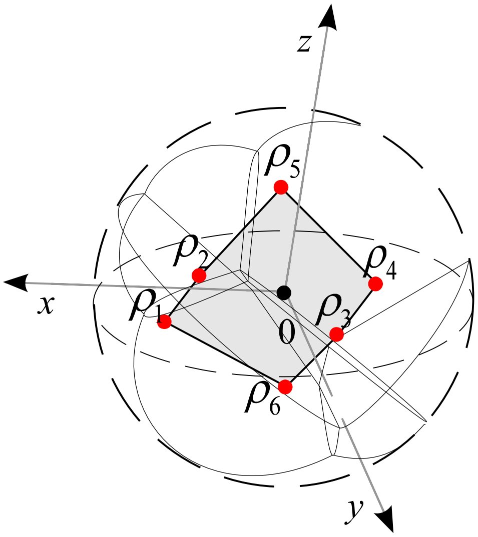


Figure 24. The convex hull computed by quantum Delaunay triangulation.

Finally, the center of the convex hull and radius r^* of the smallest enclosing quantum informational ball are computed.

In Figure 25, the center and informational theoretical radius of the smallest enclosing quantum informational ball are denoted by $\mathbf{c}^*$ and r^*, respectively.

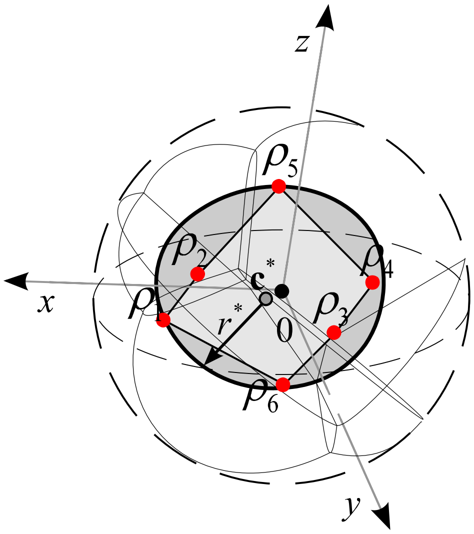


Figure 25. The smallest enclosing quantum informational ball.

Figure 26 shows an example of a two-dimensional smallest enclosing quantum informational ball.

The center point is $\mathbf{c}^* = (0.3287, 0.3274)$, and the radius r^* of the smallest enclosing quantum informational ball is $r^* = 0.4907$.

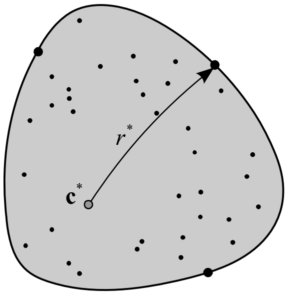


Figure 26. The smallest enclosing quantum informational ball inside the Bloch sphere.

As can be noticed, the center $\mathbf{c}^*$ of the smallest enclosing quantum informational ball differs from the center of an Euclidean ball.

VIII. Conclusion And Future Work

This paper proposes a fundamentally new method of calculating the security of a quantum channel, based on Laguerre diagrams and quantum relative entropy. Using a Delaunay tessellation on the Bloch sphere, the geometric space can be divided and can be calculated extremely efficiently, in a reasonable computational time. A generalization of an effective approximation algorithm of the smallest enclosing quantum information ball of the set of quantum states was presented, equipped with quantum relative entropy as a distance measure. This improved approximation algorithm was demonstrated to obtain a more efficient optimized geometric method. Finally the performances of the proposed methods were compared.

In this paper a new algorithm with which to compute the quantum informational theoretical impacts of an eavesdropper's cloning machine on the quantum channel was also proposed. In this analysis, the fidelity of the eavesdropper's cloning machine is numerically computed by tessellation on the Bloch sphere. A very effective core-set algorithm and an optimized core-set method were also designed. The adaptability of classical computational geometric methods in the quantum space was presented, while the performance of the basic and improved core-set algorithms were analyzed and compared. It was shown that both of the proposed algorithms provide very strong results concerning the approximation of the smallest quantum informational ball.

In terms of future work, it is hoped that the method will be extended to analyze coherent and individual attacks for quantum cryptography, while an in-depth study on the geometric impacts of physically allowed quantum cloning transformations is also intended.

REFERENCES

[1] L. Gyongyosi and S. Imre, Quantum Informational Geometry for Secret Quantum Communication, In: Proceedings of the First International Conference on Future Computational Technologies and Applications, FUTURE COMPUTING 2009, International Academy, Research and Industry Association (IARIA), pp. 580-585, 2009.

[2] W. K. Wootters and W. H. Zurek, 1982, Nature London 299, 802.

[3] V. Bužek and M. Hillery, 1996, Phys. Rev. A 54, 1844.

[4] D. Mozyrsky and V. Privman, Quantum Signal Splitting that Avoids Initialization of the Targets, Modern Phys. Lett. B 11, 1277-1283 (1997); e-print quant-ph/9609010;

[5] K. Kato, M. Oto, H. Imai, and K. Imai, "Voronoi diagrams for pure 1-qubit quantum states,quant-ph/0604101, 2006.

[6] F. Aurenhammer and R. Klein. Voronoi Diagrams. In J. Sack and G. Urrutia (Eds), Handbook of Computational Geometry, Chapter V, pp. 201–290. Elsevier Science Publishing, 2000. 03.

[7] J.-D. Boissonnat, C. Wormser, and M. Yvinec. Curved Voronoi diagrams. In J.-D.Boissonnat and M. Teillaud (Eds) Effective Computational Geometry for Curves and Surfaces, pp. 67–116. Springer-Verlag, Mathematics and Visualization, 2007.

[8] P. W. Lamberti, A. P. Majtey, A. Borras, M. Casas, and A. Plastino. Metric character of the quantum Jensen-Shannon divergence. Physical Review A (Atomic, Molecular, and Optical Physics), 77(5):052311, 2008.

[9] M. A. Nielsen and I. L. Chuang: Quantum Computation and Quantum Information. Cambridge University Press, 2000.

[10] M. Badoiu and K. L. Clarkson. Smaller core-sets for balls. In Proceedings 14th ACM-SIAM Symposium on Discrete Algorithms, pages 801–802, 2003.

[11] F. Nielsen and R. Nock, "On the smallest enclosing information disk," Information Processing Letters, vol. 105, no. 3, pp. 93–97, 2008.

[12] S. Imre and F. Balazs: Quantum Computing and Communications – An Engineering Approach, Published by John Wiley and Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England, 2005, ISBN 0-470-86902-X, 283 pages

[13] L. Gyongyosi and S. Imre: Computational Geometric Analysis of Physically Allowed Quantum Cloning Transformations for Quantum Cryptography, In Proceedings of the 4th WSEAS International Conference on Computer Engineering and Applications (CEA '10). Harvard University, Cambridge, USA. 2010. pp. 121-126. Paper 18.

[14] N.J. Cerf and M. Bourennane, A. Karlsson and N. Gisin, 2002, Phys. Rev. Lett. 88, 127902.

[15] G.M. D'Ariano and C. Macchiavello, 2003, Phys. Rev. A 67, 042306.

[16] A. Acín, N. Gisin, L. Masanes and V. Scarani, 2004, Int. J. Quant. Inf. 2, 23.

[17] R. Panigrahy. Minimum enclosing polytope in high dimensions. CoRR, cs.CG/0407020, 2004.

[18] M. Badoiu, S. Har-Peled, and P. Indyk. Approximate clustering via core-sets. In Proceedings 34th ACM Symposium on Theory of Computing, pages 250–257, 2002.

[19] P. Kumar, J. S. B. Mitchell, and A. Yıldırım. Computing core-sets and approximate smallest enclosing hyperspheres in high dimensions. In Algorithm Engineering and Experimentation, LNCS, pages 45–55. Springer-Verlag, 2003.

[20] B. Kraus, N. Gisin, and R. Renner, 2005, Phys. Rev. Lett. 95, 080501.

[21] M. Hillery, M. Ziman, and V. Bužek, 2004, Phys. Rev. A 69, 042311.

[22] N. J. Cerf, O. Krüger, P. Navez, R. F. Werner, and M. M. Wolf, 2005, Phys. Rev. Lett. 95, 070501.

[23] G. M. D'Ariano and C. Macchiavello, 2003, Phys. Rev. A 67, 042306.

[24] N., G. Gisin, Ribordy, W. Tittel, and H. Zbinden, 2002, Rev. Mod. Phys. 74, 145.

[25] N. Gisin and S. Popescu, 1999, Phys. Rev. Lett. 83, 432.

[26] A. Niederberger, V. Scarani, and N. Gisin, 2005, Phys. Rev. A 71, 042316.