Quantum information theoretical based geometrical representation of eavesdropping activity on the quantum channel

LÁSZLÓ GYÖNGYÖSI, SÁNDOR IMRE

Department of Telecommunications, Budapest University of Technology and Economics
{gyongyosi, imre}@hit.bme.hu

Keywords: quantum cryptography, quantum cloning, quantum informational distance

Quantum cryptography is an emerging technology that may offer new forms of security protection, however the quantum cloning based attacks against the protocol will play a crucial role in the future. According to the no-cloning theorem, an eavesdropper on the quantum channel can not copy perfectly the sent quantum states. The best eavesdropping attacks for quantum cryptography are based on imperfect cloning machines. In our method we use quantum relative entropy as an informational distance between quantum states. We show a geometrical approach to analyze the security of quantum cryptography, based on quantum relative entropy and Laguerre Delaunay triangulation on the Bloch sphere. Using Laguerre diagrams, we can compute efficiently the radius of the smallest enclosing ball of quantum states on the Bloch sphere. We present a basically new method to derive quantum relative entropy based Delaunay tessellation on the Bloch ball and to compute the radius of smallest enclosing ball of balls to detect eavesdropping activity on the quantum channel.

1. Introduction

The security of modern cryptographic methods like asymmetric cryptography, relies heavily on the problem of factoring large integers. In the future, if quantum computers become reality, any information exchange using current classical cryptographic schemes will be immediately insecure. Current classical cryptographic methods are not able to guarantee long-term security. Other cryptographic methods, with absolute security must be applied in the future. Cryptography based on quantum theory principles is known as quantum cryptography. Using current network technology, in order to spread quantum cryptography, interfaces able to manage together the quantum and classical channel must be implemented [2]. Quantum cryptography provides new ways to transmit information securely, using the fundamental principles of quantum-mechanics. As classical cryptography uses and manipulates classical bits, quantum cryptography does the same with qubits to realize provably, absolute secure communication. In quantum cryptographic schemes, the secret information is not encoded directly into the quantum states, the qubits are used only to generate a secret cryptographic key, shared between two legal parties, called Alice and Bob. The main idea behind the quantum cryptographic protocols was the absolute secure key distribution, hence we rather call these cryptographic methods as Quantum Key Distribution (QKD) systems [2,7].

Using computational geometry, many complex high dimensional problems can be expressed with graphs and tessellation diagrams [6]. In our fundamentally new security analysis of quantum cryptography, we derive the fidelity of the eavesdropper's cloning machine from Laguerre-type Delaunay diagrams on the Bloch sphere. Using Laguerre diagrams, we can compute efficiently the radius of the smallest enclosing balls of mixed states on the Bloch sphere, and give the level of eavesdropping activity. The geometric interpretation of quantum states can be used to investigate informational distances between two different quantum states [5,6]. We compute the fidelity of the quantum cloning transformation using the classical algorithm presented by Badoui and Clarkson, and the Laguerre Delaunay triangulation on the Bloch sphere [11,13].

Our paper is organized as follows. First we discuss the basic facts about computational geometry and quantum information theory. Then we explain the main elements of our security analysis, and we show the application of our theory for the security analysis of eavesdropping detection on the quantum channel. Finally, we summarize the results.

2. Preliminaries

The security of QKD schemes relies on the *no-cloning* theorem [2]. Contrary to classical information, in a quantum communication system the quantum information cannot be copied perfectly. If Alice sends a number of photons $|\psi_1\rangle, |\psi_2\rangle, ..., |\psi_N\rangle$ through the quantum channel, an eavesdropper is not interested in copying an arbitrary state, only the possible polarization states of the attacked QKD scheme. To copy the sent quantum state, an eavesdropper has to use a quantum cloner machine, and a known *"blank"* state $|0\rangle$, onto which the eavesdropper would like to copy Alice's quantum state.

If Eve wants to copy the *i*-th sent photon $|\psi_i\rangle$, she has to apply a unitary transformation *U*, which gives the following result:

$$U\left(|\psi_i\rangle \otimes |0\rangle\right) = |\psi_i\rangle \otimes |\psi_i\rangle, \quad (1)$$

for each polarization states of qubit $|\psi_i\rangle$. A photon chosen from a given set of polarization states can be cloned perfectly only, if the polarization angles in the set that are distinct, are all mutually orthogonal [2,7]. The unknown non-orthogonal states cannot be cloned perfectly, the cloning process of the quantum states is possible only if the information being cloned is classical, hence the quantum states are *all orthogonal*. The polarization states in the QKD protocols are not all orthogonal states, which makes no possible to an eavesdropper to copy the sent quantum states [2].

Our goal is to measure the level of quantum cloning activity on the quantum channel, using fast computational geometric methods. The fidelity analysis of the eavesdropper's cloning machine indicates, how much the eavesdropper preserves the quality of the cloned quantum states. In our method, quantum informational distance plays an important role in the estimation of the fidelity of eavesdropper's cloning machine.

2.1 The communication model

In our method we measure the *informational theoretical* impacts of quantum cloning activity in the quantum channel. Alice's side is modeled by random variable $X=\{p_i=P(x_i)\}, i=1,...N$. 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 $H(X)=-\sum_{i=1}^{N} p_i \log(p_i)$, 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 produce an output signal with a given probability.

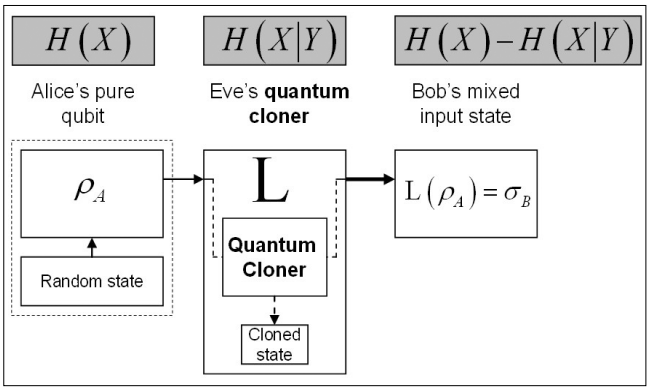
We analyze in a geometrical way the effects of Eve's quantum cloner on Bob's received quantum state. Eve's cloner in the quantum channel increases the uncertainty in X, given Bob's output Y. The informational theoretical noise of Eve's quantum cloner increases conditional Shannon entropy $H(X|Y)$, where

$$H\left(X|Y\right) = -\sum_{i=1}^{N_X}\sum_{j=1}^{N_Y} p\left(x_i, y_j\right)\log p\left(x_i|y_j\right), \quad (2)$$

Our geometrical security analysis is focused on the cloned mixed quantum state, received by Bob. The type of the quantum cloner machine depends on the actual protocol. For the four-sate QKD protocol (BB84), Eve chooses the phase-covariant cloner, while for the Six-state protocol she uses the universal quantum cloner (UCM) machine [7,9,10]. Alice's pure state is denoted by ρ_A, Eve's cloner modeled by an affine map $\mathcal{L}$, and Bob's mixed input state is denoted by $\mathcal{L}(\rho_A)=\sigma_B$. In our calculations, we can use 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 using probability distributions $p(x)$, $p(x,y)$ and $p(y|x)$. We measure in a geometrical representation the information which can be transmitted in presence of an eavesdropper on the quantum channel.

In *Fig. 1* we illustrated Eve's quantum cloner on the quantum channel. Alice's pure state is denoted by ρ_A, the eavesdropper's quantum cloner transformation is denoted by $\mathcal{L}$. The mixed state received by Bob, is represented by σ_B.

Figure 1.
The analyzed attacker model and the entropies



In a private quantum channel, we seek to maximize $H(X)$ and minimize $H(X|Y)$ in order to maximize the radius r^* of the smallest enclosing ball, which describes the maximal transmittable information from Alice to Bob in the *attacked* quantum channel:

$$r^* = Max_{\{all\ possible\ x_i\}} H\left(X\right) - H\left(X|Y\right). \quad (3)$$

To compute the radius r^* of the smallest informational ball of quantum states and the entropies between the cloned quantum states, instead of classical Shannon entropy, we can use von Neumann entropy and quantum *relative entropy*.

Geometrically, the presence of an eavesdropper causes a 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 maximal.

2.2 Geometrical representation of quantum states

A quantum state can be described by its *density matrix* $\rho\in\mathbb{C}^{d\times d}$, which is a $d\times d$ matrix, where d is the level of the given quantum system. For an n qubit system, the level of the quantum system is $d=2^n$. In our model, we use the fact, that particle state distributions can be analyzed probabilistically by means of density matrices.

A *two-level* quantum system can be given by its density matrices in the following way:

$$\rho = \frac{1}{2}\begin{pmatrix} 1+z & x-iy \\ x+iy & 1-z \end{pmatrix},\ x^2+y^2+z^2 \le 1, \quad (4)$$

where i denotes the complex imaginary $i^2=-1$.

The density matrix $\rho=\rho(x,y,z)$ can be identified with a *point* (x,y,z) in the 3-dimensional space, and a ball **B** formed by such points $\mathbf{B}=\{(x,y,z)\,|\,x^2+y^2+z^2\le 1\}$, is called Bloch ball. The eigenvalues λ_1,λ_2 of $\rho(x,y,z)$ are given by

$$\left(1 \pm \sqrt{x^2+y^2+z^2}\right)\Big/2, \quad (5)$$

the eigenvalue decomposition ρ is $\rho=\sum_i \lambda_i E_i$, where $E_i E_j$ is E_i for $i=j$ and 0 for $i\neq j$. For a *mixed* state $\rho(x,y,z)$, $\log\rho$ defined by $\log\rho=\sum_i(\log\lambda_i)E_i$.

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 $\mathbb{R}^3$, 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, θ and φ represents the latitude and longitude rotation angles. Using the spherical coordinates, a three-dimensional point on the Bloch sphere $\mathcal{B}$, can be given by:

$$\begin{aligned} x &= r\sin\theta\cos\varphi,\\ y &= r\sin\varphi,\\ z &= r\cos\theta\cos\varphi. \end{aligned} \tag{7}$$

A mesh of the Bloch sphere $\mathcal{B}$ 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.

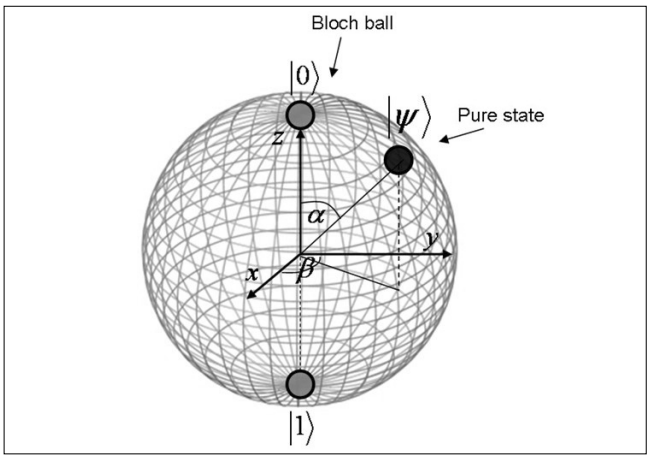
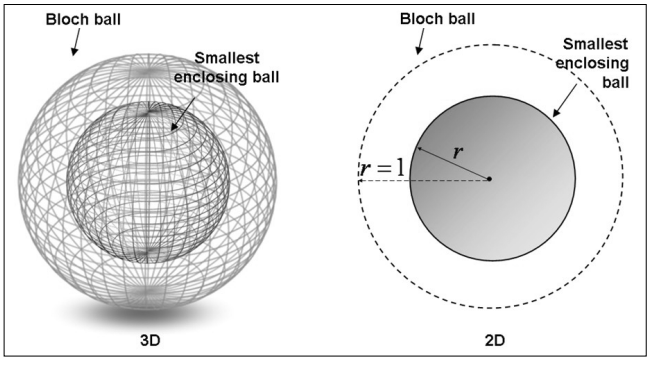


Figure 2. Mesh of Bloch sphere

Geometrically, the *pure* states are on the boundary of the Bloch ball $\mathcal{B}$, while the *mixed* states are inside the Bloch ball. In *Fig. 3* the pure states with unit radius are on the surface of the Bloch-sphere, while the mixed states with radius $r<1$ are contained inside the sphere.

Figure 3.
The effect of the eavesdropper's cloning transformation in geometrical representation



A pure state can be given by $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$ and the projector of the state is

$$|\psi\rangle\langle\psi| = \frac{1}{2}\left(\mathbf{1}+\hat{n}\cdot\vec{\sigma}\right),$$

where $\hat{n}$ is the Bloch vector, and it can be given by $\hat{n}=(2\mathrm{Re}(\alpha\beta^*), 2\mathrm{Im}(\alpha\beta^*), |\alpha|^2-|\beta|^2)$ [4,7].

2.3 Measuring distances between quantum states

In the proposed security analysis, the distance between quantum states is defined by the *quantum relative entropy* of quantum states. The relative entropy of quantum states measures the *informational distance* between quantum states. In our model, the informational distance between quantum states is computed by using their density matrices. The classical Shannon-entropy of a discrete d-dimensional distribution p can be given by

$$H(p)=\sum_{i=1}^{d} p_i \log\frac{1}{p_i} = -\sum_{i=1}^{d} p_i \log p_i\ . \tag{8}$$

The *von Neumann* entropy $S(\rho)$ of quantum states is a generalization of the classical Shannon entropy to density matrices [4,7]. The entropy of quantum states can be given by:

$$\mathrm{S}(\rho) = -Tr(\rho\log\rho). \tag{9}$$

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

$$\mathrm{S}(\rho)=\mathrm{S}(\lambda)=-\sum_{i=1}^{d}\lambda_i\log\lambda_i, \tag{10}$$

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 is to a model or candidate probability distribution q [4,7]. For p and q probability distributions the *relative entropy* can be given by

$$D(p\|q)=\sum_i p_i\log_2\frac{p_i}{q_i}, \tag{11}$$

while the relative entropy between quantum states measured by

$$D(\rho\|\sigma)=Tr\left[\rho\left(\log\rho-\log\sigma\right)\right]. \tag{12}$$

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 [4,7], thus $D(\rho\|\sigma)\neq D(\sigma\|\rho)$ and $D(\rho\|\sigma)\geq 0$ iff $\rho\neq\sigma$, and $D(\rho\|\sigma)=0$ iff $\rho=\sigma$. We note, that if σ has zero eigenvalues $D(\rho\|\sigma)$ may *diverge*, otherwise it is a finite and continuous function. The quantum relative entropy reduces to the classical Kullback-Leibler relative entropy for simultaneously diagonal matrices.

2.4 Quantum relative entropy

The *relative entropy* between *quantum states* can be described by a strictly convex and differentiable generator function **F** as:

$$\mathbf{F}(\rho) = -\mathrm{S}(\rho) = Tr(\rho\log\rho), \tag{13}$$

where –S is the negative von Neumann entropy function.

The *relative quantum entropy* $D(\rho\|\sigma)$ for density matrices ρ and σ can be given by generator function **F** in the following way:

$$D\left(\rho\middle\|\sigma\right)=\mathbf{F}\left(\rho\right)-\mathbf{F}\left(\sigma\right)-\left\langle\rho-\sigma,\nabla\mathbf{F}\left(\sigma\right)\right\rangle, \quad (14)$$

where $\langle\rho,\sigma\rangle=\mathrm{Tr}(\rho\sigma^*)$ is the *inner product* of quantum states, and $\nabla\mathbf{F}(\cdot)$ is the gradient.

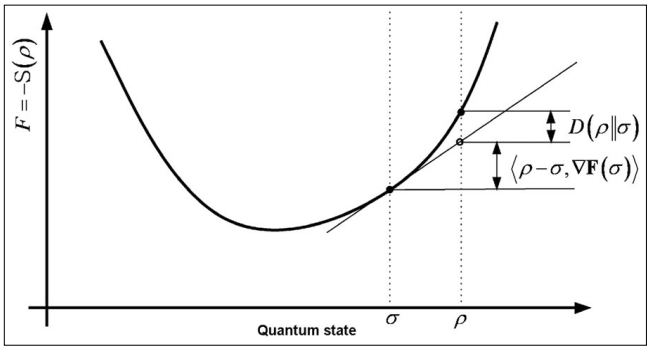


Figure 4.
Visualizing generator function as negative von Neumann entropy

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

$$\begin{aligned}D\left(\rho\middle\|\sigma\right)=&\frac{1}{2}\log\frac{1}{4}\left(1-r_\rho{}^2\right)+\frac{1}{2}r_\rho\log\frac{\left(1+r_\rho\right)}{\left(1-r_\rho\right)}\\&-\frac{1}{2}\log\frac{1}{4}\left(1-r_\sigma{}^2\right)-\frac{1}{2r_\sigma}\log\frac{\left(1+r_\sigma\right)}{\left(1-r_\sigma\right)}\left\langle\rho,\sigma\right\rangle\end{aligned} \quad (15)$$

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 informational distance can be expressed as

$$\begin{aligned}&D\left(\rho\middle\|\sigma\right)=\\&\frac{1}{2}\log\frac{1}{4}\left(1-r_\rho{}^2\right)+\frac{1}{2}r_\rho\log\frac{\left(1+r_\rho\right)}{\left(1-r_\rho\right)}-\frac{1}{2}\log\frac{1}{4}.\end{aligned} \quad (16)$$

The density matrices of quantum bits are represented by 3D points in the Bloch ball. If we compute the distance between two quantum states in the 3D Bloch ball representation, we compute the distance between two Hermitian matrices ρ and σ.

The eavesdropper's cloner transformation is modeled by an affine map, that maps quantum states to quantum states. Geometrically, the effect of the eavesdropper is to map the Bloch ball to a deformed ball. The cloning activity in the channel can be analyzed by the radius of the deformed Bloch ball, which can be computed by geometrical methods.

In our security analysis we use Delaunay tessellation, which is *symmetric* only for pure states, and *asymmetric* for mixed states. It can be proven, that for pure states the Delaunay diagram coincidences with Euclidean Delaunay diagram, but for *mixed* states the Delaunay diagram is asymmetric, hence it is not identical to Euclidean diagrams [16].

3. Eavesdropping activity on the quantum channel

In quantum cryptography the best eavesdropping attacks use the quantum cloning machines [7-9]. However, an eavesdropper can not measure the state $|\psi\rangle$ of a single quantum bit, since the result of her measurement is one of the single quantum system's eigenstates. The measured eigenstate gives only very poor information to the eavesdropper about the original state $|\psi\rangle$ [2,7].

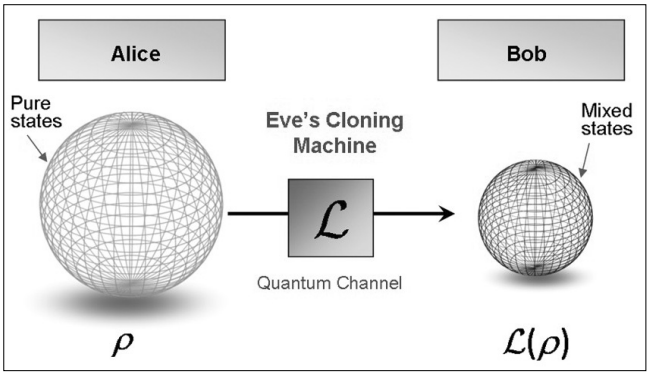


Figure 5.
The effect of quantum cloning attack on the sent pure quantum state

The process of cloning of *pure* states can be generalized as

$$\left|\psi\right\rangle_a\otimes\left|\Sigma\right\rangle_b\otimes\left|Q\right\rangle_x\rightarrow\left|\Psi\right\rangle_{abx}, \quad (17)$$

where $|\psi\rangle$ is the state in the *Hilbert space* to be copied, $|\Sigma\rangle$ is a *reference* state, and $|Q\rangle$ is the *ancilla* state [7]. 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 [8,9].

The no-cloning theorem has important role in quantum cryptography, since it makes no possible to copy a quantum state perfectly. In 1996 Buzek and Hillery published the method of imperfect cloning, while the original no-cloning theorem was applied only to perfect cloning [2]. The asymmetric cloning machines have been discussed for eavesdropping of quantum cryptography in [10,15]. For attacks on some quantum cryptography protocol, it has been proven that the best strategy uses quantum cloning machines [7,9].

3.1 The smallest enclosing quantum-information ball

We would like to compute the radius *r* of the smallest enclosing ball of the cloned mixed quantum states, thus first we have to seek the center **c*** of the point set S. The set S of quantum states is denoted by $S=\{\rho_i\}_{i=1}^n$.

The distance function $d(\cdot,\cdot)$ between any two quantum states of S is measured by quantum relative entropy, thus the *minimax* mathematical optimization can be applied to *quantum relative entropy* based distances to find the center **c** of the set S. We denote the quantum relative entropy from **c** to the furthest point of S by

$$d\left(\mathbf{c},\mathcal{S}\right)=\max_i d\left(\mathbf{c},\rho_i\right). \quad (18)$$

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

$$\mathbf{c}^* = \arg\min_{\mathbf{c}} d(\mathbf{c}, \mathcal{S}). \quad (19)$$

In *Fig. 6* we illustrated the *circumcenter* **c*** of $\mathcal{S}$ for the Euclidean distance and for *quantum relative entropy* [1].

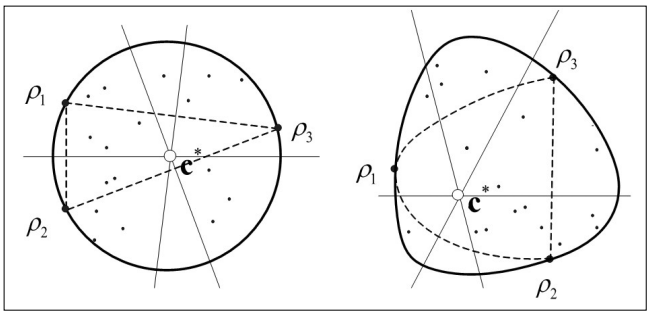


Figure 6.
Circumcenter for Euclidean distance ball and quantum relative entropy ball

In our fidelity analysis we assume, that the eavesdropper's cloning machine does a *linear transform* $\mathcal{L}$ that maps quantum states to quantum states. The eavesdropper's cloning transformation $\mathcal{L}$ is a trace-preserving, i.e. $Tr\mathcal{L}(\rho)=Tr(\rho)$, and completely positive map [1]. The informational theoretical effect of the *eavesdropper's cloning machine* is described the radius of the smallest enclosing quantum informational ball by r^*. The quantum informational theoretical radius equal to the *maximum* quantum informational distance from the center, and it can be expressed as:

$$r^* = \min_{\sigma \in \mathcal{S}(\mathbb{C}^2)} \max_{\rho \in \mathcal{S}(\mathbb{C}^2)} D\left(\mathcal{L}(\rho) \| \mathcal{L}(\sigma)\right). \quad (20)$$

In our procedure of computing smallest enclosing information ball, we use quantum Delaunay diagrams, because it is the *fastest* known tool to seek a center of a smallest enclosing ball of points.

4. Geometrical model of secure quantum communication

4.1 Properties of quantum cloners

The *maximal* 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* [1]. 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 is

$$F_{Eve} = \langle\psi|^{(in)} \rho^{(out)} |\psi\rangle^{(in)} = \frac{1}{2}(1+\eta), \quad (21)$$

where η is the *reduction* factor. The quantum cloning transformation optimal [8,9], if $\eta=2/3$, hence the maximal fidelity of optimal universal cloning is $F_{Eve}=5/6$, and the maximal radius of the cloned state is

$$r_{Eve}^{universal} = \frac{2}{3}. \quad (22)$$

The *quantum informational theoretical* radius can be defined as

$$r_{Eve}^{*universal} = 1 - \mathrm{S}\left(r_{Eve}^{universal}\right), \quad (23)$$

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

In general, the universal cloning machine output state can be expressed by [7-9]

$$\rho^{(out)} = F_{Eve} |\psi\rangle_a \langle\psi| + (1 - F_{Eve}) |\psi_\perp\rangle_a \langle\psi_\perp|. \quad (24)$$

4.2 Asymetric phase-covariant quantum cloner

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. The phase-covariant cloning machine has a remarkable application in quantum cryptography, since it is used in the optimal strategy for eavesdropping [8-10]. 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].

In phase-covariant cloning, the transformations restrict for pure input states

$$|\psi_\phi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\phi}|1\rangle\right), \quad (25)$$

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 [9] 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]

$$\rho^{(out)} = \left(\frac{1}{2} + \sqrt{\frac{1}{8}}\right)|\psi_\phi\rangle\langle\psi_\phi| + \left(\frac{1}{2} - \sqrt{\frac{1}{8}}\right)|\psi_{\phi,\perp}\rangle\langle\psi_{\phi,\perp}|, \quad (26)$$

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

$$F_{1\to2}^{phasecov.} = \frac{1}{2} + \sqrt{\frac{1}{8}} \approx 0.8535. \quad (27)$$

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

$$r_{Eve}^{phasecov.} = 2\sqrt{\frac{1}{8}}. \quad (28)$$

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

$$r_{Eve}^{*phasecov.} = 1 - \mathrm{S}\left(r_{Eve}^{phasecov.}\right), \quad (29)$$

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 $|0\rangle|0\rangle \rightarrow |0\rangle|0\rangle$ and $|1\rangle|0\rangle \rightarrow \cos\eta|1\rangle|0\rangle + \sin\eta|0\rangle|1\rangle$, where $\eta \in [0,\pi/2]$ is the shrinking parameter, which is related to the fidelity.

In *Fig. 7* we compared the information theoretical radiuses r^*_{UCM} and $r^*_{phasecov.}$ of the smallest enclosing quantum informational balls for idealistic UCM based attack and idealistic phase-covariant cloner based attack. The maximal distance states are denoted by ρ_{UCM} and $\rho_{phasecov.}$

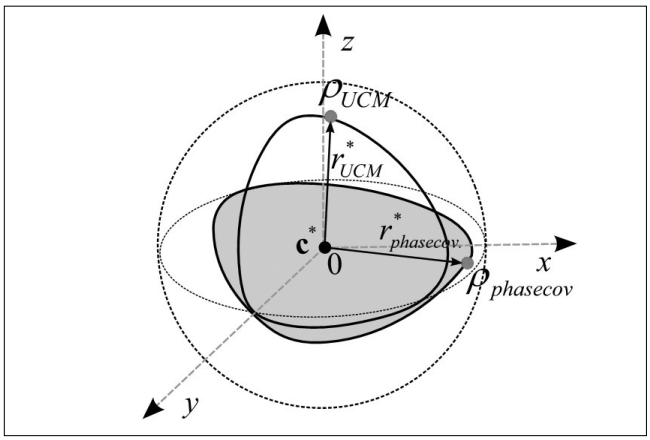


Figure 7.
Comparison of smallest enclosing quantum informational balls of idealistic UCM and phase-covariant based attack

The best quality of the two outputs simultaneously can be realized with an UCM. If an eavesdropper uses a phase-covariant cloner, one of the two outputs should have better fidelity, while the fidelity of second output will be lower.

4.3 Quantum cloning detection

In our model we derive the fidelity of the eavesdropper's cloning machine from the quantum informational theoretical radius r^* of the smallest enclosing quantum informational ball, and the theoretical upper bound on the *quantum informational theoretical* radius of the eavesdropper's cloning machine denoted by r^*_{Eve} [1].

As the first part of our theorem, for a *secure* quantum channel, the radius r^* of the smallest enclosing quantum information ball of *mixed states* has to be greater than r^*_{Eve}, thus

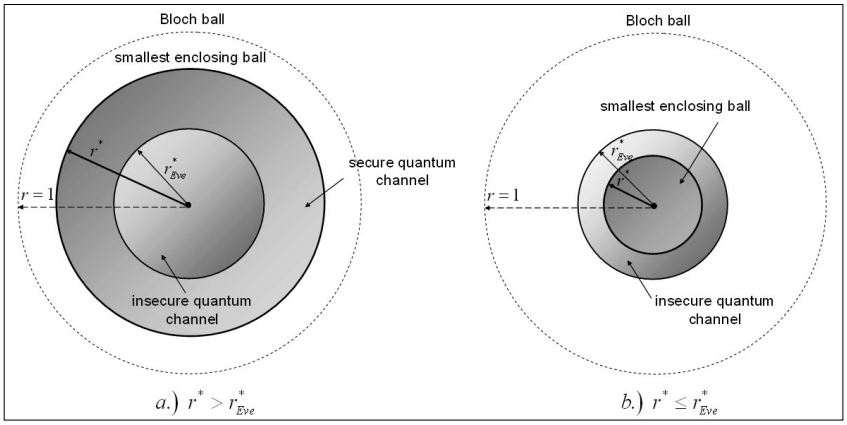
$$r^* > r^*_{Eve}. \tag{30}$$

As the second part, for an *insecure* quantum channel, the radius r^* is smaller than or equal to r^*_{Eve}, thus

$$r^* \leq r^*_{Eve}. \tag{31}$$

In *Fig. 8* we show the geometrical interpretation of our model [1].

Figure 8.
The radius of the smallest enclosing information ball for a secure (a) and insecure (b) quantum communication



In our security analysis, we use the spherical Delaunay tessellation to compute the quantum information 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 the conventional spherical Delaunay tessellation, and it differs between mixed quantum states [6].

5. Tessellation on the Bloch sphere

5.1 Mathematical background

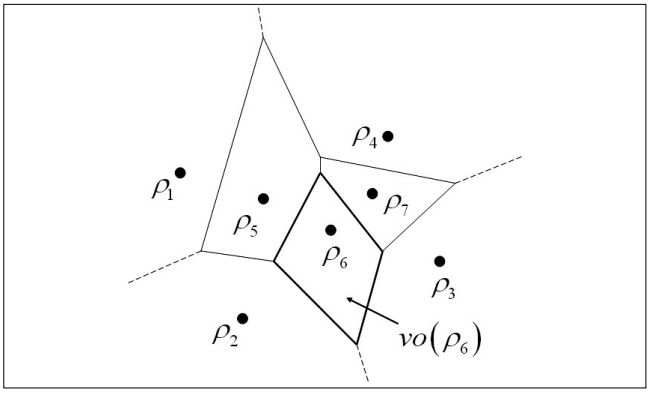
The dual of Delaunay diagram of a set of quantum states on the Bloch ball $\mathcal{B}$, is the division of the space into regions. The regions contain the part of the *quantum space* which is closer to that point than any other. Formally, for a given set of quantum states $\mathcal{S}=\{\rho_1,\rho_2,...\rho_n\}$ in $\mathbb{R}^d$, the Voronoi diagram $V(\mathcal{S})$ is the partition of $\mathbb{R}^d$ into *n polyhedral* regions, one for each quantum states ρ_i. These regions on the Bloch ball $\mathcal{B}$ are the *Voronoi cells*, denoted by $vo(\rho)$, containing the points in $\mathbb{R}^d$ which are closer to quantum state ρ than all other points.

Formally, the Voronoi cell $vo(\rho)$ for quantum state ρ and the set of quantum state $\mathcal{S}$ can be given by

$$vo(\rho) = \left\{ x \in \mathbb{R}^d \middle| d(x,\rho_i) \leq d(x,\rho_j) \in \mathcal{S}\{\rho_i\} \right\}, \tag{32}$$

where $d(\cdot)$ is the *distance* function. The Voronoi vertices are in the intersections of the *bisectors* or *boundaries*, as we illustrated it in *Fig. 9*.

Figure 9. An Euclidean tessellation on the Bloch ball



On the Bloch ball $\mathcal{B}$ every $vo(\rho)$ corresponds to a quantum state ρ, thus we have n Voronoi cells for n quantum states, and there are $O(n)$ vertices and edges [6].

5.2 Delaunay triangulation in the quantum space

We use the *Voronoi vertices* in our security analysis, since these vertices play a crucial role in the computation of Delaunay triangulation on the Bloch ball $\mathcal{B}$. The circumcenter of the given quantum states is the *circle* that passes through the quantum states ρ_1 and ρ_2 of the edge $\rho_1\rho_2$ and endpoints ρ_1, ρ_2 and ρ_3 of the triangle $\rho_1\rho_2\rho_3$.

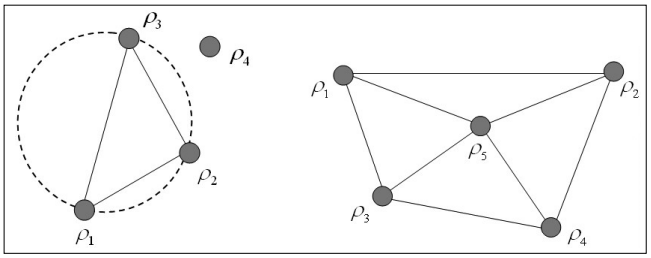


Figure 10.
The Delaunay triangulation of a set of quantum states

The triangle t is said to be *Delaunay*, when its circumcenter is *empty* [6]. The circle centered at a vertex **c**, gives an *empty* circumcenter for quantum states $\{\rho_1, \rho_2, \rho_3\}$. The Delaunay triangulation of a set of quantum states S, denoted by $Del(S)$, is unique, if at most three quantum states $\rho \in S$ are co-circular [5]. The *Delaunay triangulation* $Del(S)$ of a set of quantum states $S=\{\rho_1, \rho_2, ...\rho_n\}$ *maximizes* the *minimum* angle among all triangulation of the given set of quantum states.

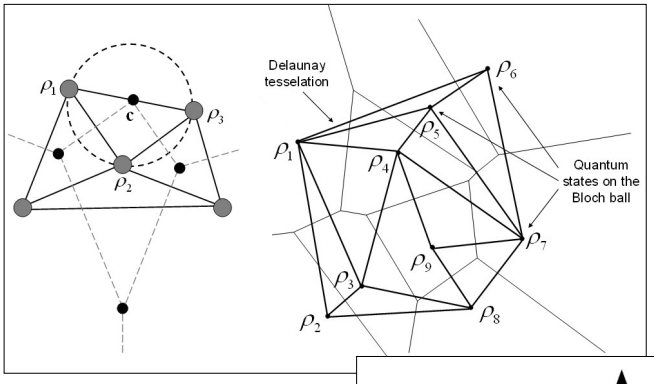


Figure 11.
The triangle of quantum states corresponds to the vertex c, which is the center of its circumcenter (a) and Delaunay tessellation on the Bloch sphere (b)

In our security analysis we use the fact, that the Voronoi diagram $V(S)$ of set of quantum states S, and the Delaunay triangulation $D(S)$ are dual to each other in Euclidean space, and in the quantum space with geodesic edges [6].

Using the Voronoi-Delaunay duality, every triangle $t \in Del(S)$ corresponds to a vertex $v \in V(S)$, and every edge $e(\rho,\sigma) \in Del(S)$ in the *Delaunay triangle* between two quantum states in S corresponds to the boundary edge between the Voronoi cells $vo(\rho)$ and $vo(\sigma)$.

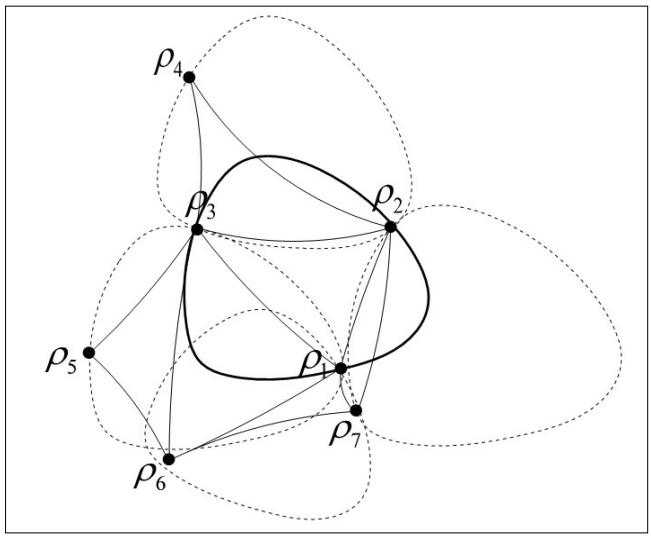


Figure 12. The empty ball property for quantum Delaunay triangulation

The quantum Delaunay diagrams between mixed states differ from Euclidean diagrams, as we have illustrated it in *Fig. 12*.

In *Fig. 13/a* we illustrated the dual-Delaunay diagram for pure quantum states, with unit length radiuses. The quantum diagram for pure states is equivalent to the ordinary Euclidean diagram on the Bloch-sphere.

In *Fig. 13/b* we illustrated the quantum diagrams for mixed states with radiuses $r_{\rho_{1,2,3,4}}<1$, in the Bloch ball representation. Since the quantum informational distance is asymmetric, we can define two types of diagrams. The first-type diagram is illustrated by bold lines, the dashed lines show the dual curved, second-type diagram.

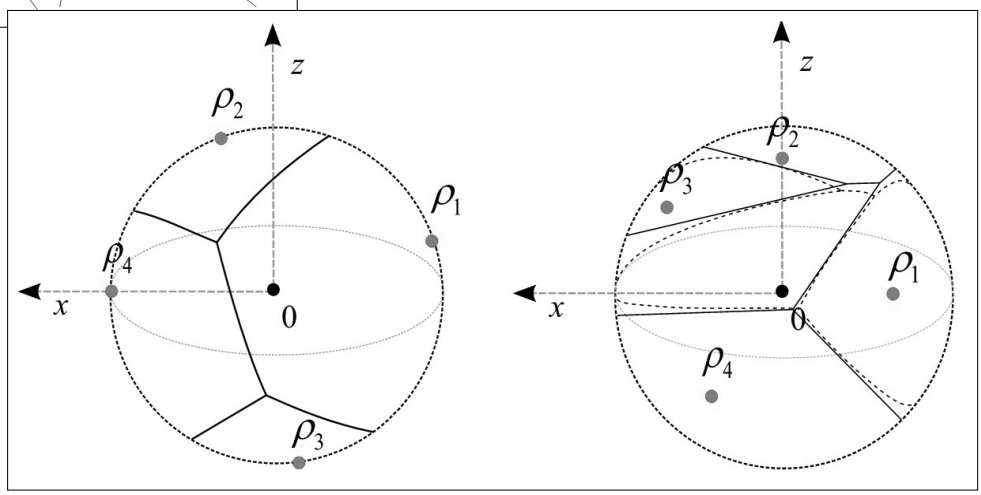


Figure 13.
Dual-Delaunay diagram for pure states (a) and for mixed states (b) on the Bloch ball. For mixed states, the quantum diagrams differ from the Euclidean diagram.

As we can conclude, the quantum diagrams of *pure* quantum states are *equivalent* to ordinary Euclidean diagrams. The quantum diagrams of mixed states with different radiuses are equivalent to quantum informational diagrams.

5.3 Laguerre diagram for quantum states

We use *Laguerre* Delaunay diagram to compute the radius of the smallest enclosing ball [6]. In generally, the *Laguerre* distance for generating quantum state x_i and with weight r_i^2 can be expressed as

$$d_L(\rho, x_i) = \|\rho - x_i\|^2 - r_i^2 . \quad (33)$$

The Delaunay diagram with respect to the *Laguerre* distance is called *Laguerre* Delaunay diagram. For the *Laguerre* bisector of two *three-dimensional* Euclidean balls $B(\rho,r_\rho)$ and $B(\sigma,r_\sigma)$ centered at quantum states ρ and σ, we can write the following equation [6]:

$$2\langle x, \sigma - \rho\rangle + \langle \rho, \rho\rangle - \langle \sigma, \sigma\rangle + r_\sigma^2 - r_\rho^2 = 0. \quad (34)$$

The bisector equation for the ordinary three-dimensional Euclidean Delaunay tessellation can be given by

$$2\langle x, \sigma - \rho\rangle + \langle \rho, \rho\rangle - \langle \sigma, \sigma\rangle = 0, \quad (35)$$

thus for *pure* quantum states, where $r_\sigma^2 = r_\rho^2$, the *quantum relative entropy* based *Delaunay tessellation* on the Bloch ball coincidences with the ordinary Euclidean distance based Delaunay tessellation [6]. On the *Laguerre* diagram, the center of the quantum informational ball can be described by the density matrix χ_i as [6]:

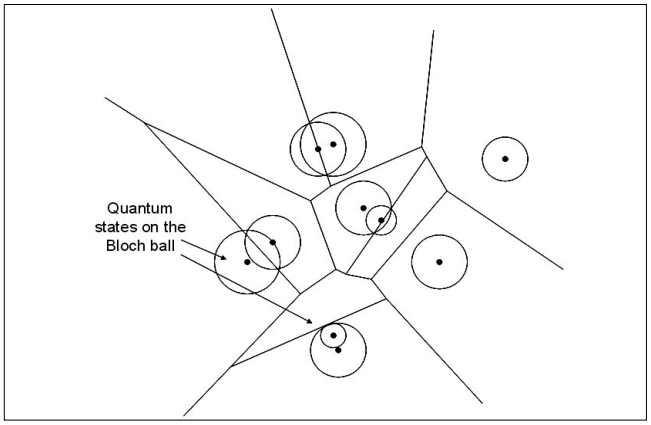
$$\nabla F_{\mathcal{B}}(\chi_i) = \log \chi_i = A_i \begin{pmatrix} \log \lambda_{i,1} & 0 \\ 0 & \log \lambda_{i,2} \end{pmatrix} A_i^*, \quad (36)$$

where (37)

$$A_i = \frac{1}{\sqrt{2}} \begin{pmatrix} \frac{x_i - iy_i}{\sqrt{x_i^2 + y_i^2}} \sqrt{\frac{r_i + z_i}{r_i}} & \frac{x_i - iy_i}{\sqrt{x_i^2 + y_i^2}} \sqrt{\frac{r_i - z_i}{r_i}} \\ \sqrt{\frac{r_i - z_i}{r_i}} & -\sqrt{\frac{r_i + z_i}{r_i}} \end{pmatrix}.$$

We illustrated the dual diagram of the *Laguerre* Delaunay tessellation in the Euclidean space in *Fig. 14*.

Figure 14.
Laguerre diagram for quantum states on the Bloch ball



The squared radius r_i^2 of the quantum state ρ_i on the Bloch sphere can be given by

$$r_i^2 = \quad (38)$$
$$\left\langle \nabla \mathbf{F}_{\mathcal{B}}(\rho_i), \nabla \mathbf{F}_{\mathcal{B}}(\rho_i) \right\rangle + 2\left(\mathbf{F}_{\mathcal{B}}(\rho_i) - \left\langle \rho_i, \nabla \mathbf{F}_{\mathcal{B}}(\rho_i) \right\rangle \right).$$

As we can conclude, for weight r_i^2, the *Laguerre* distance $d_L(\rho,x_i)$ can be interpreted as the square of the length of the line segment starting at ρ and tangent to the circle centered at x_i, with radius $\sqrt{r_i^2}$. Thus, the circle centered at x_i with radius $\sqrt{r_i^2}$ is the circle associated with x_i.

6. The proposed algorithm for quantum cloning detection

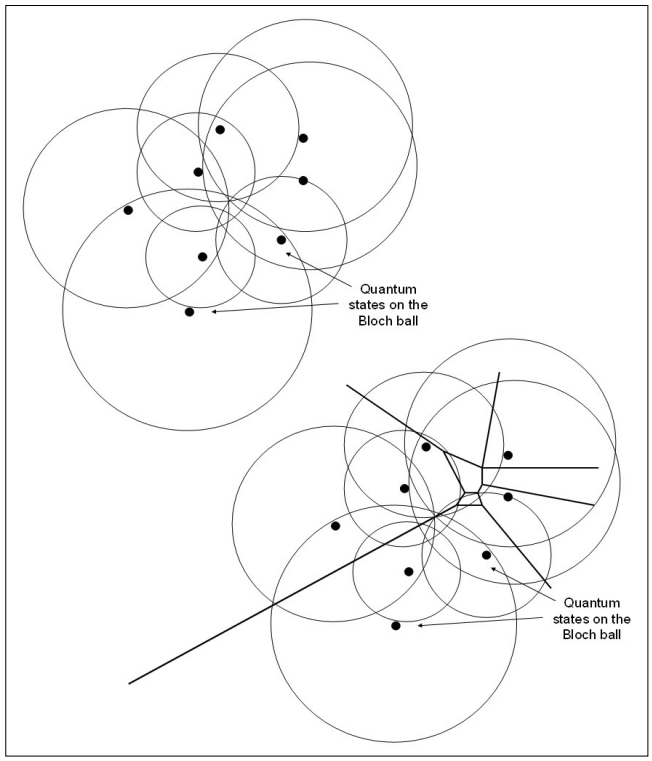
In our algorithm we present an effective solution to seek the *center* **c** of the set of smallest enclosing quantum information ball, using *Laguerre* diagrams.

Our geometrical based algorithm consists of two main steps:

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

A Delaunay triangulation in the *d*-dimensional quantum space can be obtained by other methods, like a *paraboloid* in the *d+1* dimensional space expressed by $x_{d+1}=x_1^2+...+x_d^2$ and *tangent planes* at the points [1]. In this method we can use the fact, that *the lower envelope of the tangent planes* is a Delaunay diagram [3,17]. However, in this paper we show a more effective algorithm to compute Delaunay tessellation on the Bloch sphere $\mathcal{B}$.

Figure 15.
Tessellation on the Bloch ball obtained by Laguerre diagram



6.1 Construction of Delaunay triangulation from Laguerre diagrams

In our algorithm, we use the fact that the Delaunay tessellation can be computed by *Laguerre* diagrams, thus we can give the tessellation from the *Laguerre* diagram of a set of corresponding ball [5].

In *Fig. 15* we illustrated the Laguerre diagram on the Bloch ball, and the construction of Voronoi diagram.

We use the results proposed in [5], to construct the quantum relative entropy based dual diagram of the Delaunay tessellation, using the Laguerre diagram of the n Euclidean spheres of equations

$$\left\langle x-\rho_i', x-\rho_i' \right\rangle = \left\langle \rho_i', \rho_i' \right\rangle + 2\left(\mathbf{F}\left(\rho_i\right) - \left\langle \rho_i, \rho_i' \right\rangle\right),\ \left(i=1,\ldots,n\right), \tag{39}$$

where ρ_i and ρ_i' denote the first-type and second-type diagrams. In *Fig. 16* we show the ordinary triangulation of quantum relative entropy based Voronoi diagram.

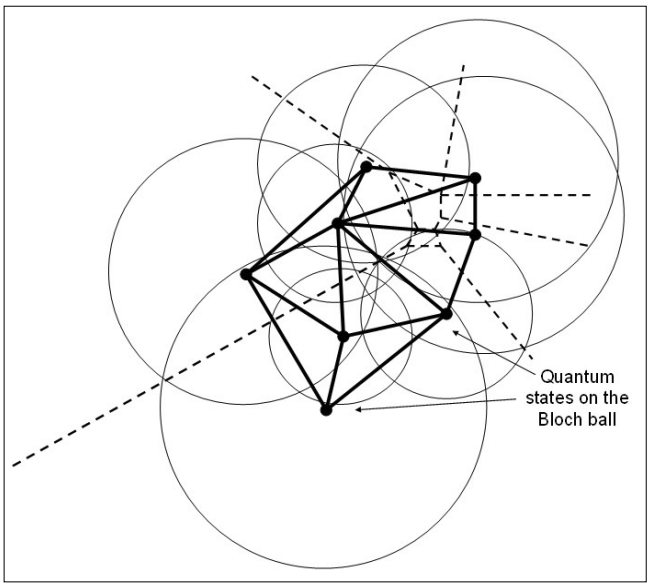


Figure 16. Ordinary Euclidean Delaunay triangulation

The *centers* of the Euclidean spheres are ρ_i, and $\rho_i = \rho_i'$, thus $r_i^2 = 0$. The *generator* function of the quantum relative entropy based diagram is the negative quantum entropy $\mathbf{F}(x) = \sum_i x_i \log x_i$, and the *gradient* $\nabla\mathbf{F}(x) = [\log x_1 \ldots \log x_d]^T$. On the *quantum relative entropy* based diagram, we map quantum state $\rho = [\rho_1 \ldots \rho_d]^T$ to a Euclidean ball of center $\rho' = [\rho_1 \ldots \rho_d]^T$ [5], with radius $r_\rho^2 = \sum_i (\log^2 \rho_i - 2\rho_i)$. The most important result of this equivalence, that we can construct efficiently quantum relative entropy based Delaunay triangulation on the Bloch sphere using Euclidean spheres, which can be calculated efficiently by fast algorithms [5].

6.2 Seek the center of the smallest enclosing quantum informational ball

In our security analysis we use an approximation algorithm from classical *computational geometry* to determine the smallest enclosing ball of balls using *core-sets*. We apply the approximation algorithm presented by *Badoui and Clarkson*, however in our algorithm, the distance measurement between quantum states is based on *quantum informational distance* [11,13]. To apply our approximation algorithm in eavesdropping activity detection, we use the $\mathcal{E}$-core set C for the *minimax* quantum information ball of set of quantum states S [11]. The $\mathcal{E}$-core set C is a subset of the set $C \subseteq S$, such for the *circumcenter* $\mathbf{c}$ of the *minimax* ball

$$d\left(\mathbf{c}, \mathcal{S}\right) \le \left(1+\mathcal{E}\right) r, \tag{40}$$

where r is the radius of the smallest enclosing quantum information ball of set of quantum states S. Our geometrical based eavesdropping detection can be computed very effectively, based on the fact that approximating algorithm can find the *radius* r of the smallest enclosing ball of balls in $O(dn/\mathcal{E}^2)$ time, with an $(1+\mathcal{E})$ approximation [11]. Moreover, in the applied approximation algorithm the *core-set* sizes are bounded by $2/\mathcal{E}$, independently of the dimension [13,14].

Quantum relative entropy based approximation

The approximating algorithm, for a set of quantum states $S = \{s_1,\ldots,s_n\}$ and *circumcenter* $\mathbf{c}$ first finds a farthest point s_m of ball set B, and moves $\mathbf{c}$ towards s_m in $O(dn)$ time in every iteration step. The algorithm does $\lfloor 1/\mathcal{E}^2 \rfloor$ iterations to ensure an $(1+\mathcal{E})$ approximation, thus the overall cost of the algorithm is $O(dn/\mathcal{E}^2)$ [11].

The main steps of our quantum relative entropy based algorithm are:

Algorithm

1. *Select* a random center $\mathbf{c}_1$ from the set of quantum states $\mathcal{S}$

$$\mathbf{c}_1 = s_1$$

for $\left(i = 1,2,\ldots,\left\lceil \frac{1}{\mathcal{E}^2} \right\rceil\right)$ **do**

2. *Find* the farthest point s of $\mathcal{S}$ wrt. *quantum relative entropy*

$$S \leftarrow \arg\max_{s' \in \mathcal{S}} D_F\left(\mathbf{c}_i, s'\right)$$

3. *Update* the circumcircle:

$$\mathbf{c}_{i+1} \leftarrow \nabla_F^{-1}\left(\frac{i}{i+1}\nabla_F\left(\mathbf{c}_i\right) + \frac{1}{i+1}\nabla_F\left(S\right)\right).$$

4. *Return* $\mathbf{c}_{i+1}$

We denote the set of n d-dimensional balls by $B = \{b_1,\ldots,b_n\}$, where $b_i = Ball(s_i, r_i)$, where S_i is the center of the ball b_i, and r_i is the radius of the i-th ball radius. 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 $\mathbf{c}^*$, containing all the set $\{b_1,\ldots,b_n\}$. The smallest enclosing ball of a ball set, can be written as $\min_{\mathbf{c}} F_B(\mathbf{c})$, where $F_B(X) = d(X,B) = \max_{i \in \{1,\ldots,n\}} d(X,B_i)$, and the distance function $d(\cdot,\cdot)$ measures the relative entropy between quantum states [14]. The minimum ball of the set of balls is unique, thus the *circumcenter* $\mathbf{c}^*$ of the set of quantum states is:

$$\mathbf{c}^* = \arg\min_{\mathbf{c}} F_B\left(\mathbf{c}\right). \tag{41}$$

In *Fig. 17* we illustrated the smallest enclosing ball of balls in the quantum space.

At the end of our algorithm, the radius r^* of the smallest enclosing ball $\mathcal{B}^*$ with respect to the quantum informational distance is equal to $\min_{\sigma \in \mathcal{S}(\mathbb{C}^2)} \max_{\rho \in \mathcal{S}(\mathbb{C}^2)} D\left(\mathcal{L}(\rho) \| \mathcal{L}(\sigma)\right)$.

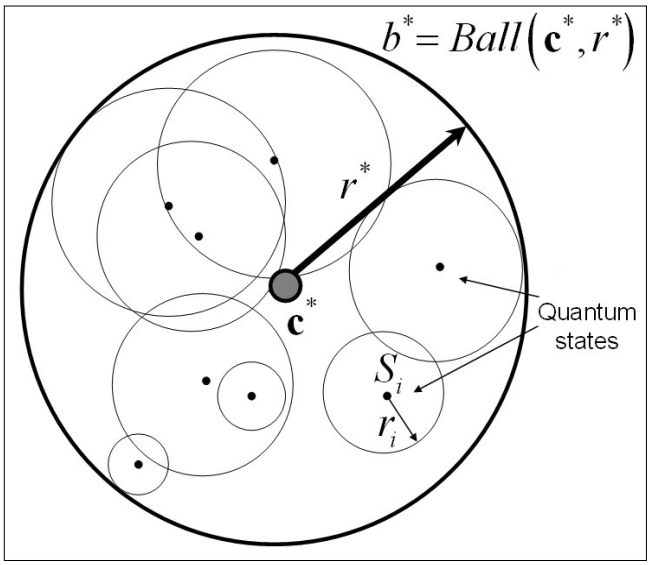


Figure 17.
The smallest enclosing ball of a set of balls in the quantum space

The *security* of the quantum channel is determined by our geometrical model with assumptions $r^* > r^*_{Eve}$, and $r^* \leq r^*_{Eve}$, as we have defined it in Eq. (37) and (38).

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

$$F_{Eve} = \langle \psi |^{(in)} \rho^{(out)} | \psi \rangle^{(in)} = \frac{1}{2}(1+r), \qquad (42)$$

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

In *Fig. 18* we compared the smallest quantum informational ball and the ordinary Euclidean ball (dashed-line) for a random set S of mixed quantum states. As we can conclude, the quantum states ρ_1, ρ_2 and ρ_3, which determine the Euclidean smallest enclosing ball, differ from the states of the quantum informational ball.

Figure 18.
The maximal distance states of the smallest balls are differing for quantum informational distance and Euclidean distance

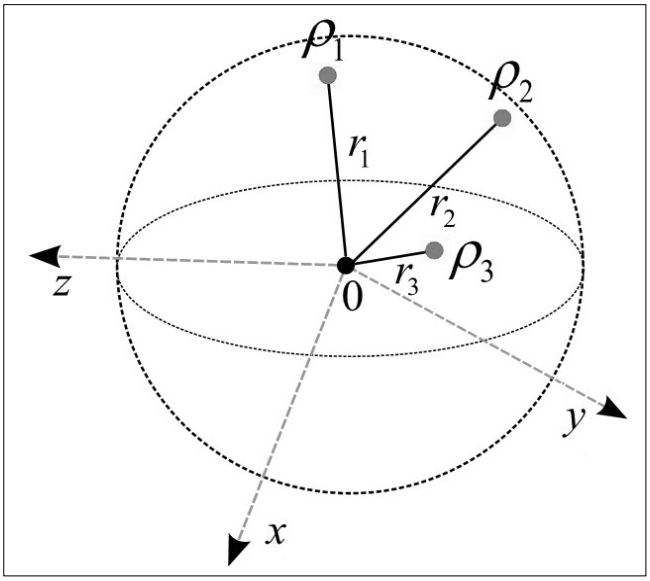
6.3 The computational complexity of the proposed algorithm

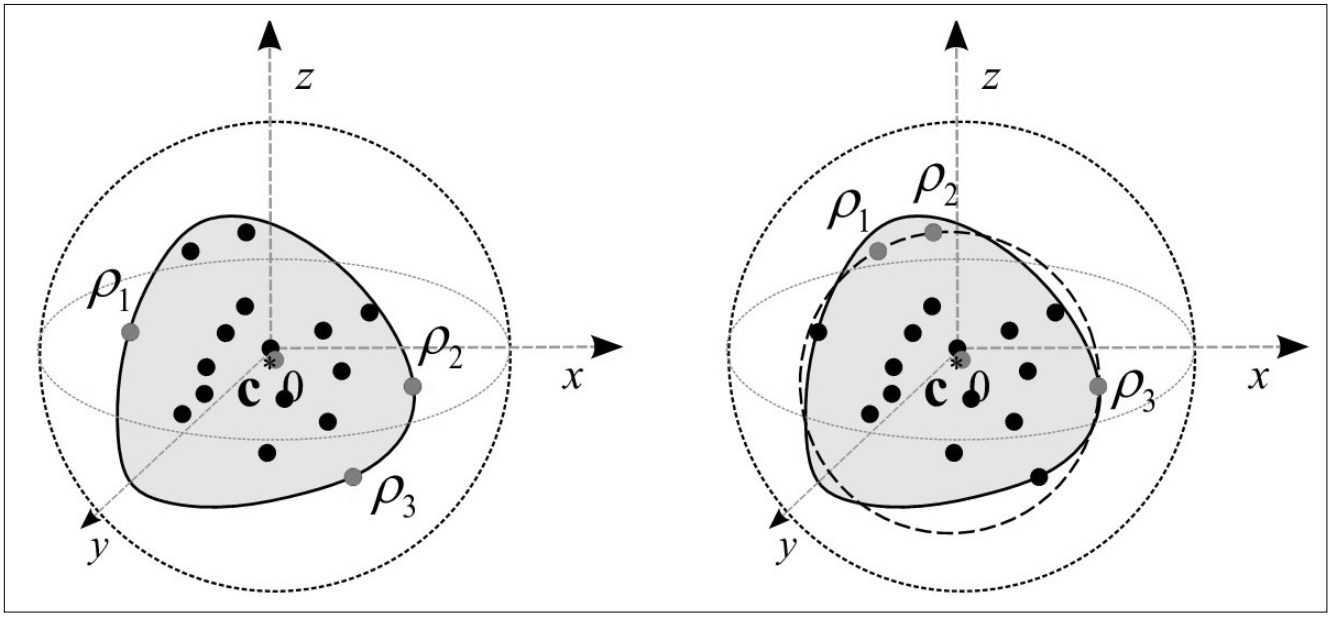
The quantum relative entropy based algorithm at the i-th iteration gives an $O(1+\sqrt{i})$-approximation of the real *circumcenter*, thus to get an $(1+\varepsilon)$ approximation, our algorithm requires

$$\mathcal{O}\left(\frac{dn}{\varepsilon^2}\right) = \mathcal{O}\left(\frac{d}{\varepsilon^2}\frac{1}{\varepsilon}\right) = \mathcal{O}\left(\frac{d}{\varepsilon^3}\right) \qquad (43)$$

time, by first sampling $n = 1/\varepsilon$ points. Based on the computational complexity of the smallest enclosing ball, the $(1+\varepsilon)$ approximation of the fidelity of the eavesdropper cloning machine can be computed in $O(d/\varepsilon^2)$ time. As *future work*, we would like to improve our method to get an $O(d/\varepsilon)$ time $(1+\varepsilon)$-approximation algorithm in quantum space.

Figure 19. Mixed quantum states in the Bloch ball





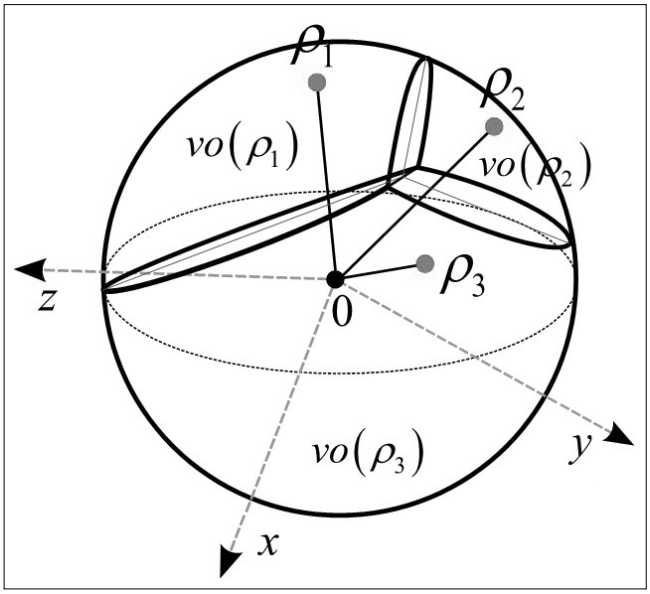


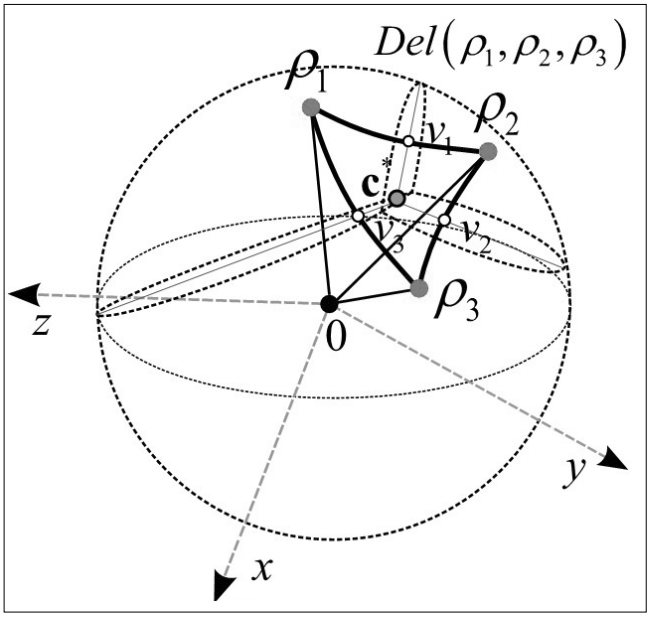
Figure 20.
Voronoi cells of quantum states on the Bloch ball

7. An illustrative example

Finally, we summarize the steps of our quantum relative entropy based cloning machine detecting algorithm. In the next example, we compute the smallest enclosing quantum information ball for three mixed quantum states. In *Fig. 19*, the *mixed* quantum states in the Bloch ball denoted by ρ_1, ρ_2 and ρ_3. The radius of the quantum states are denoted by r_1, r_2 and r_3.

First, we determine the Voronoi cells for the mixed quantum states. The Voronoi cells in the Bloch ball are denoted by $vo(\rho_1)$, $vo(\rho_2)$, and $vo(\rho_3)$. The distance between quantum states calculated with respect to quantum relative entropy.

Figure 21.
Delaunay triangle with respect to quantum informational distance



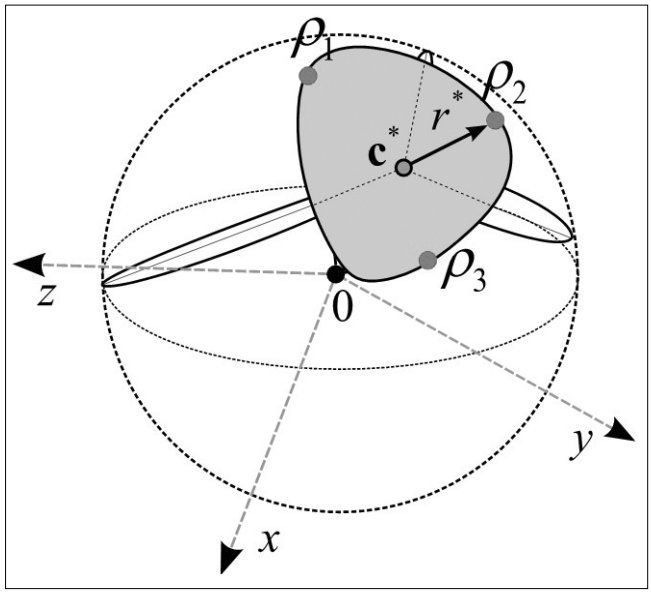
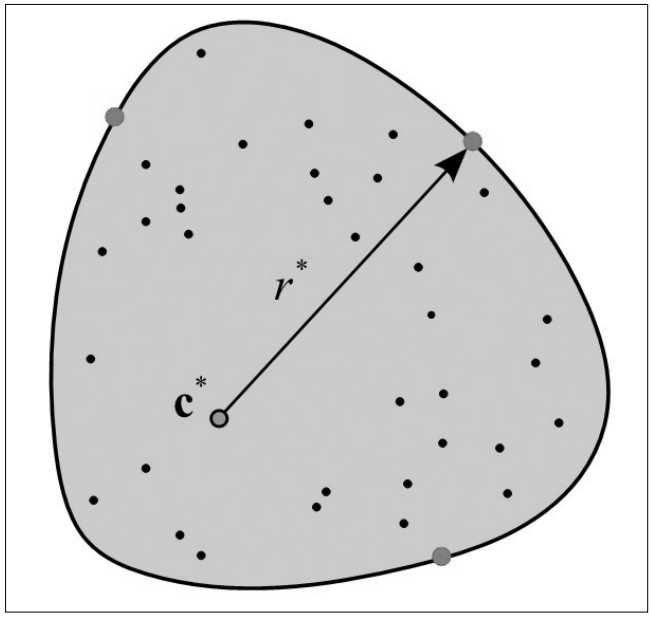


Figure 22.
The smallest enclosing quantum informational ball and its radius

In the next phase we compute the Delaunay triangulation with respect to quantum relative entropy. The quantum informational Delaunay triangle is distorted, according to the distance properties of quantum relative entropy.

In *Fig. 21* the quantum Delaunay triangle is denoted by $Del(\rho_1, \rho_2, \rho_3)$. The bisector points between the quantum states with respect to quantum relative entropy denoted by points v_1, v_2 and v_3. The bisectors intersect the center of the smallest quantum informational ball, denoted by $\mathbf{c}^*$. Finally, we get the radius r^* of the smallest enclosing quantum informational ball, centered at point $\mathbf{c}^*$. The distorted structure of the smallest enclosing quantum relative entropy ball is well observable in *Fig. 22*.

Figure 23.
The smallest enclosing quantum informational ball inside the Bloch sphere



In *Fig. 23* we show an example for a two-dimensional smallest enclosing quantum informational ball. This quantum relative entropy ball is a deformed ball, thus our approximation algorithm is tailored for quantum informational distance.

The center c^* of the smallest enclosing quantum informational ball differs from the center of an Euclidean ball.

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

8. Conclusions

We showed a fundamentally new approach to measure the information theoretical impacts of quantum cloning on the private quantum channel. In our analysis the fidelity of the eavesdropper's cloning machine is numerically computed by tessellation on the Bloch sphere. In classical computational geometry Delaunay triangulations has an important role [4]. Using Delaunay tessellation on the Bloch sphere, the quantum *space* can be divided very efficiently.

We showed, that we can use efficiently *Laguerre* diagrams on the Bloch sphere, since the *Laguerre* diagrams are defined both on mixed and pure quantum states. We presented a novel approach to compute the relative quantum entropy, using an approximation method for the smallest enclosing ball of balls using core-sets. We presented an effective approximation algorithm to compute the informational fidelity using quantum information balls, equipped with quantum relative entropy as a distance measure.

As future work we would like to present a more effective algorithm to compute the eavesdropper's cloning machine, and make a deep study on our algorithm's convergence rate.

Authors

LÁSZLÓ GYÖNGYÖSI, Ph.D Student since 2008, Budapest University of Technology and Economics. He received the M.Sc. degree in Computer Science with Honors from the Technical University of Budapest in 2008. His research interests are in Quantum Computation and Communication, Quantum Cryptography and Quantum Information Theory.

SÁNDOR IMRE was born in Budapest in 1969. He received the M.Sc. degree in Electronic Engineering from the Budapest University of Technology (BME) in 1993. Next he started his Ph. D. studies at BME and obtained dr. univ. degree in 1996, Ph.D. degree in 1999 and DSc degree in 2007. Currently he is carrying his teaching activities as Head of the Dept. of Telecommunications of BME. He was invited to join the Mobile Innovation Centre of BME as R&D director in 2005. His research interest includes mobile and wireless systems, quantum computing and communications. Especially he has contributions on different wireless access technologies, mobility protocols and reconfigutable systems.

Acknowledgments

The authors would like to thank Dr. Katalin Friedl for useful discussions.

References

[1] L. Gyöngyösi, S. Imre,
Computational Geometric Analysis of Physically Allowed Quantum Cloning Transformations for Quantum Cryptography,
4th WSEAS International Conference on Computer Engineering and Applications, Section on Quantum Computing,
University of Harvard, Cambridge (Massachusetts), USA, 2010.

[2] S. Imre, F. Balázs,
Quantum Computing and Communications – An Engineering Approach,
Published by John Wiley and Sons Ltd, The Atrium, England, ISBN 0-470-86902-X (283 pages), 2005.

[3] L. Gyöngyösi, S. Imre,
Geometrical Estimation of Information Theoretical Impacts of Incoherent Attacks for Quantum Cryptography, International Review of PHYSICS, Print ISSN: 1971-680X, 2010.

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

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

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

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

[8] Cerf, N.J., M. Bourennane, A. Karlsson, N. Gisin,
Security of Quantum Key Distribution Using d-Level Systems,
Phys. Rev. Lett. 88, 127902., 2002.

[9] D'Ariano, G.M., C. Macchiavello,
Optimal phase-covariant cloning for qubits and qutrits,
Phys. Rev. A 67, 042306., 2003.

[10] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, V. Scarani,
Device-independent security of quantum cryptography against collective attacks,
Phys. Rev. Lett. 98, 230501., 2007.