Quantum Informational Divergence in Quantum Channel Security Analysis

Laszlo Gyongyosi and Sandor Imre
(Corresponding author: L. Gyongyosi)

Department of Telecommunications, Budapest University of Technology
Magyar tudosok krt. 2., Budapest, H-1117, Hungary (Email: gyongyosi@hit.bme.hu)

(Received May 20, 2009; revised and accepted Mar. 24, 2010)

Abstract

Computational Geometry is the art of designing efficient algorithms for answering geometric questions. Computational Geometry involves efficient and elegant solutions for difficult algorithmic problems and plays a central role in many different areas of computer science. Quantum cloning-based attacks have deep relevance to quantum cryptography. In this paper we use the results of classical Computational Geometry to analyze the security of a quantum channel using current classical computer architectures. To analyze a quantum channel for a large number of input quantum states with classical computer architectures, very fast and effective algorithms are required.

Keywords: Quantum communication, quantum cryptography, quantum informational distance

1 Introduction

In today's communication networks, the widespread use of optical fiber and passive optical elements allows to use quantum cryptography in the current standard optical network infrastructure. In the past few years, quantum key distribution schemes have attracted much study. The security of modern cryptographic methods, like asymmetric cryptography, relies heavily on the problem of factoring large integers [7]. In the future, if quantum computers become reality, any information exchange using current classical cryptographic schemes will be immediately insecure [11, 13]. 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 the principles of quantum theory is known as quantum cryptography. Using current network technology, in order to spread quantum cryptography, interfaces must be implemented that are able to manage together the quantum and classical channels [10].

Many challenging hard algorithmic problems can be studied with computational geometry and, at present, there exist many geometric algorithms that offer an efficient and well implementable solution for hard computational problems. Computational Geometry was originally focused on the construction of efficient algorithms and it provides a very valuable and efficient tool for computing hard tasks [8]. In many cases, the traditional linear programming methods are not very efficient. The computation of the convex hull between quantum states cannot be computed efficiently by linear programming, however the methods of computational geometry are better at solving these kinds of hard problems [18, 3, 8]. Computational Geometry uses the results of classical geometry and the power of computing. In Figure 1, we illustrate the logical structure of the analysis and the cooperation of classical and quantum systems. To this day, the most efficient classical algorithms for this purpose are computational geometric methods. We use these classical computational geometric tools to analyze the security of a quantum channel.

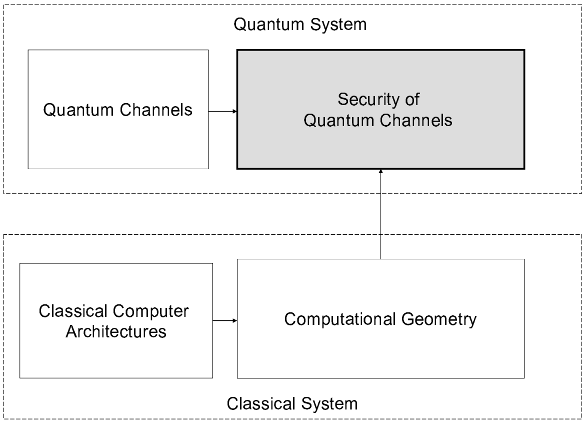


Figure 1: Logical structure of our analysis. We use current classical architectures to analyze the properties of quantum channel.

In this paper, we use the methods of computational geometry to analyze the security of quantum channels, however we use quantum information as a distance measure instead of classical geometric distances. Unlike ordinary geometric distances, a quantum informational distance is not a metric and it is not symmetric, hence this pseudo-distance features as a measure of informational distance. This paper combines the models of information geometry and the fast methods of computational geometry. Using the quantum informational distance as a distance measure, we analyze the privacy of eavesdropped quantum channels [8].

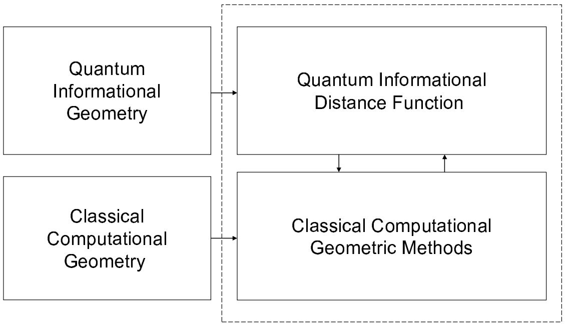

Quantum Informational Geometry
Classical Computational Geometry
Quantum Informational Distance Function
Classical Computational Geometric Methods

Figure 2: Quantum information as distance measure in classical computational geometric methods

From the combination of the quantum informational distance function and classical computational geometric methods, the properties of quantum channels and quantum states in quantum space can be analyzed as geometrical objects in geometrical space.

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

2 Preliminaries

The security of QKD schemes relies on the no-cloning theorem [10]. Contrary to classical information, in a quantum communication system, quantum information cannot be copied perfectly. If Alice sends a number of photons $|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_N\rangle$, through the quantum channel, an eavesdropper is not interested in copying an arbitrary state, only the possible polarization states of the attacked QKD scheme. The unknown states cannot be cloned perfectly, the cloning process of 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 it impossible for an eavesdropper to copy the sent quantum states [10]. Our goal is to measure the level of quantum cloning activity on the quantum channel, using fast computational geometric methods. We measure the *informational theoretical* impacts of quantum cloning activity in the quantum channel. Alice's side is modeled by a random variable $X = \{p_i = P(x_i)\}, i = 1, \ldots, N$. 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 random variable X given Y is denoted by $p(X|Y)$. Alice sends a random variable to Bob, who produces 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 the conditional Shannon entropy $H(X|Y)$, where $H(X|Y) = -\sum_{i=1}^{N_X} \sum_{j=1}^{N_Y} \log p(x_i|y_j)$. Our geometrical security analysis is focused on the cloned mixed quantum state received by Bob. The type of 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 [15, 6, 1]. Alice's pure state is denoted by ρ_A, Eve's cloner is modeled by an affine map L and Bob's mixed input state is denoted by $L(\rho_A) = \sigma_B$. In our calculations, we can use the fact that for random variables X and Y, $H(X,Y) = H(X) + H(Y|X)$, where $H(X)$, and $H(X,Y)$ are defined in terms of probability distributions $p(x), p(x,y)$ and $H(Y|X)$. We measure in a geometrical representation the information which can be transmitted in the presence of an eavesdropper on the quantum channel.

In Figure 3, we illustrate 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 L. The mixed state received by Bob, is represented by σ_R.

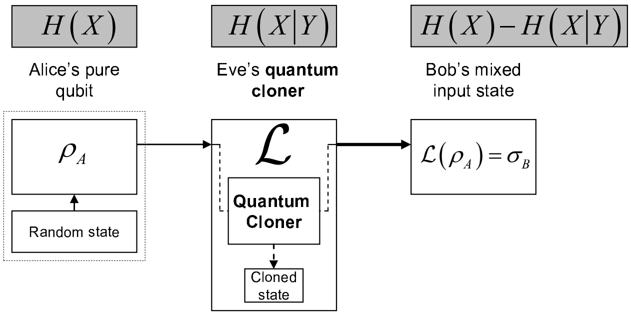


Figure 3: The analyzed attacker model and entropies

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:

$$r^* = MAX_{\{\text{all possible } x\}} H(X) - H(X|Y).$$

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.

2.1 Geometrical Representation of Quantum States

A quantum state can be described by its *density matrix*$\rho \in C^{d\times s}$, 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 $d = 2^n$. We use the fact that particle state distributions can be analyzed probabilistically by means of density matrices. A *two-level* quantum system can be defined by its density matrices in the following way:

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

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 3-dimensional space, and a ball B formed by such points $B = \{(x,y,z)|x^2+y^2+z^2 \leq 1\}$, is called a Bloch ball. The eigenvalues λ_1, λ_2 of $\rho(x,y,z)$ are given by $(1 \pm \sqrt{x^2+y^2+z^2})/2$, the eigenvalue decomposition ρ is $\rho = \Sigma_i \lambda_i E_i$, 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 R^3 and it can be represented in spherical coordinates $\rho = (r,\theta,\varphi)$, where r is the radius of the quantum state to the origin, θ and φ represents the latitude and longitude rotation angles.

2.2 Measuring Quantum Informational Distances between Quantum States

The classical Shannon-entropy of a discrete d-dimensional distribution p is given by $H(p) = \sum_{i=1}^d p_i \log\frac{1}{p_i} = \sum_{i=1}^d p_i \log p_i$. The *von Neumann* entropy $S(\rho)$ of quantum states is a generalization of the classical Shannon entropy to density matrices [12, 15]. The entropy of quantum states is given by $S(\rho) = -Tr(\rho\log\rho)$ The quantum entropy $S(\rho)$ is equal to the Shannon entropy for the eigenvalue distribution $S(\rho) = S(\lambda) = -\sum_{i=1}^d \lambda_i \log\lambda_i$ 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 [12, 15]. For p and q probability distributions, the *relative entropy* is given by $D(p \parallel q) = \sum_i p_i \log_2 \frac{p_i}{q_i}$, while the relative entropy between quantum states is measured by

$$D(\rho \parallel \sigma) \quad = \quad Tr(\rho(\log\rho - \log\sigma)).$$

The quantum informational distance has some distance-like properties, however it is *not* commutative [12, 15], thus $D(\rho \parallel \sigma) \neq D(\sigma \parallel \rho)$, and $D(\rho \parallel \sigma) \geq 0$ iff $\rho \neq \sigma$, and $D(\rho \parallel \sigma) \geq 0$ iff $\rho = \sigma$. 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 $r_\sigma = \sqrt{x^2+y^2+z^2}$ is given by

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

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

$$D(\rho \parallel \sigma) \quad = \quad \frac{1}{2}\log\frac{1}{4}(1-r_\rho^2) + \frac{1}{2}r_\rho\log\frac{(1+r_\rho)}{(1-r_\rho)} - \frac{1}{2}\log\frac{1}{4}$$

The relative entropy of quantum states can be described by a strictly convex and differentiable generator function $\mathbf{F}$:

$$\mathbf{F}(\rho) \quad = \quad -S(\rho) = Tr(\rho\log\rho), \qquad (1)$$

where $-\mathbf{S}$ is the negative entropy of quantum states. The quantum relative entropy $D(\rho\|\sigma)$ for density matrices ρ and σ is given by generator function $\mathbf{F}$ in the following way:

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

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

In Figure 4, we have depicted the quantum informational distance, $D(\rho \parallel \sigma)$, as the vertical distance between the generator function $\mathbf{F}$ and $H(\sigma)$, the hyperplane tangent to $\mathbf{F}$ at σ. The point of intersection of quantum state ρ on $H(\rho)$ is denoted by $H_\sigma(\rho)$.

Before we start to discuss the relation between quantum informational distance and quantum generator function, for simplicity we prove the relation between Euclidean distance and Euclidean generator function. The proof can be extended to quantum informational distances, using the quantum generator function $\mathbf{F}$. If the generator function $\mathbf{F}$ is the squared Euclidean distance, then the strictly convex and differentiable generator function over R^d can be expressed as

$$\mathbf{F}(x) \quad = \quad x^2 = \sum_{i=1}^d x_i^2 = x^T x, \text{with } \nabla F(x) = 2x.$$

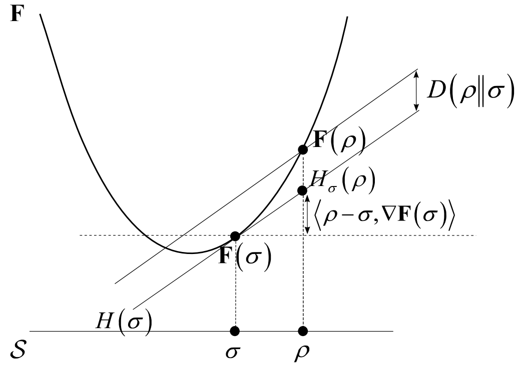


Figure 4: Depiction of generator function as a negative von Neumann entropy

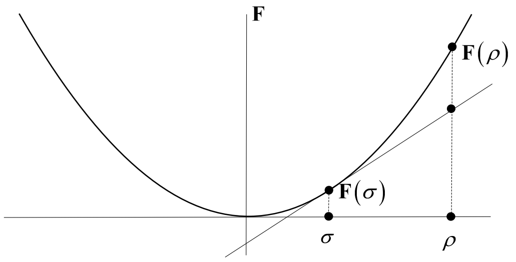


Figure 5: Squared Euclidean generator function

In this case, $D_F(\rho\|\sigma)$ can be expressed as

$$\begin{aligned} D_{\mathbf{F}}(\rho\|\sigma) &= \mathbf{F}(\sigma) - \mathbf{F}(\sigma) - \langle\rho-\sigma, \nabla\mathbf{F}(\sigma)\rangle \\ &= \rho^2 - \sigma^2 - \langle\rho-\sigma, 2\sigma\rangle = \rho^2 + \sigma^2 - 2\rho\sigma \\ &= \rho^T\rho + \sigma^T\sigma - 2\rho^T\sigma = \|\rho-\sigma\|. \end{aligned}$$

In Figure 5, we have illustrated the squared Euclidean distance function $D_{\mathbf{F}}(\rho\|\sigma)$, with Euclidean generator function $\mathbf{F}(x) = x^2 = \sum_{i=1}^{d} x_i^2$.

For the quantum informational distance function, the generator function is the negative von Neumann entropy function $-S$,

$$\mathbf{F}(\rho) \quad = \quad -S(\rho) = Tr(\rho\log\rho),$$

where $F : S(C^d) \rightarrow R$. The quantum informational distance function $D_{\mathbf{F}}(\rho\|\sigma)$ with generator function $\mathbf{F}(\rho) = -S(\rho)$ is illustrated in Figure 6.

The generator function of the quantum informational distance is the negative von Neumann entropy function. The quantum generator function has a classical analogy, because for classical probability distributions p and q, the generator function is the negative Shannon entropy:

$$\mathbf{F}(x) \quad = \quad x\log x = -x\log\frac{1}{x} = \int p(x)\log p(x)dx,$$

and $\nabla\mathbf{F}(x) = 1 + \log x$. Hence, for probability distributions, the informational distance can be expressed as

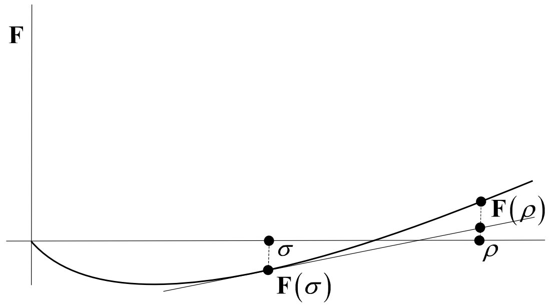


Figure 6: Negative von Neumann generator function

$$\begin{aligned} D(p(x)\|q(x)) &= \int(\mathbf{F}(p) - \mathbf{F}(q) - \langle p-q, \nabla\mathbf{F}(q)\rangle)dx, \\ &= \int(p(x)\log p(x) - q(x)\log q(x) - \langle p(x) \\ &\quad -q(x), \log q(x) + 1\rangle) \\ &= \int p(x)\log\frac{p(x)}{q(x)}dx - \int p(x)dx \\ &\quad - \int q(x)dx) \\ &= \int p(x)\log\frac{p(x)}{q(x)}dx \end{aligned}$$

The quantum informational distance function is a linear operator, thus for convex functions $\forall\mathbf{F}_1 \in Cand\forall\mathbf{F}_2 \in C, D_{\mathbf{F}_1+\lambda\mathbf{F}_2}(\rho\|\sigma) = D_{\mathbf{F}_1}(\sigma\|\sigma) + \lambda D_{\mathbf{F}_2}(\rho\|\sigma)$, for any $\lambda \geq 0$.The density matrices of quantum states can be 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.

3 Security Problem in Quantum Cryptography

In quantum cryptography, the best eavesdropping attacks use quantum cloning machines [4, 6, 15]. However, an eavesdropper cannot measure the state $|\psi\rangle$ of a single quantum bit, since the result of her measurement is one of the single eigenstates of the quantum system. The measured eigenstate gives only very poor information to the eavesdropper about the original state $|\psi\rangle$ [10, 15]. The eavesdropper's cloning transformation is a trace-preserving and completely positive map and it can be described as $\{L, |Q\rangle\}$, where $|Q\rangle$ is the eavesdropper's ancilla state. The process of cloning pure states can be generalized as

$$|\psi\rangle_a \otimes |\Sigma\rangle_b \otimes |Q\rangle_x \rightarrow |\psi\rangle_{abc},$$

where $|\psi\rangle$ is the state in Hilbert space to be copied, $|\Sigma\rangle$ is a reference state and $|Q\rangle$ is the ancilla state [15]. As

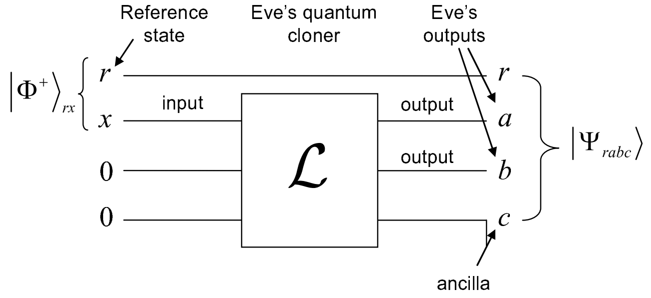


Figure 7: General model of Eve's quantum cloner

Wooters and Zurek have shown, an unknown quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ cannot be cloned perfectly [15], however it was later shown that an unknown quantum state can be cloned approximately [10]. 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 [4, 6]. The effect of the eavesdropper's quantum cloner simply shrinks the Bloch ball B, with given probability p. The general model of Eve's cloning machine is shown in Figure 7 [1, 4, 6, 14].

The input qubit state is denoted by x, which is initially in an entangled state with a reference qubit r, denoted by the Bell state $|\Phi^{+}\rangle_{rx}$. After the cloning transformation, the overall system consists of the three outputs and the reference quantum state, thus the output state $|\Phi^{+}_{rabc}\rangle$ can be written as a superposition of double Bell states [8]:

$$\begin{aligned}|\Psi_{ra,bc}\rangle &= v|\Phi^{+}\rangle\langle\Phi^{+}| + z|\Phi^{-}\rangle\langle\Phi^{-}| + x|\Psi^{+}\rangle\langle\Psi^{+}| \\ &\quad + y|\Psi^{-}\rangle\langle\Psi^{-}|,\end{aligned}$$

where x, y, z and v are complex amplitudes with $|x|^2 + |y|^2 + |z|^2 + |v|^2 = 1$. The qubit pairs ra and bc are Bell mixtures with $|x|^2 = p_x$, $|y|^2 = p_y$, $|z|^2 = p_z$ and $|v|^2 = 1 - p$ Equation $v = x + y + z$ describes a three-dimensional surface in the space, where each point (x, y, z) represents parameters $|x|^2 = p_x$, $|y|^2 = p_y$, and $|z|^2 = p_z$ This surface is an oblate *ellipsoid* E [1, 4, 6, 14] and we denote the coordinates of the ellipsoid E by (x_E, y_E, z_E). The ellipsoid E has polar radius $x_E = \frac{1}{2}$, while the equatorial radius is $z_E = 1$ [4, 8]. In Figure 8, we have illustrated the effects of phase-covariant and universal quantum cloners that have been analyzed.

The radii which describe the shrinking of the cloned state are denoted by $r_{E,phasecov}$ and $r_{E,UCM}$ in the three-dimensional ellipsoidal representation.

3.1 Cloning Machine-based Attacks in Quantum Cryptography

Our security analysis is based on the Four-state (BB84) and Six-state quantum cryptography protocols. In this setting, Alice sends a qubit $|\psi\rangle$ to Bob and Eve clones the sent qubit using her ancilla qubit $|E\rangle$. In the cloning process, Eve's ancilla state $|E\rangle$ interacts with the sent qubit $|\psi\rangle$ and the unknown state is forwarded to Bob who makes his standard measurement. In the *BB84* protocol [15], Eve uses a phase-covariant cloning machine, thus Eve clones only equatorial states $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\varphi}|1\rangle)$. In the *Six-state* protocol [15], Eve uses universal cloning and she clones all the states:

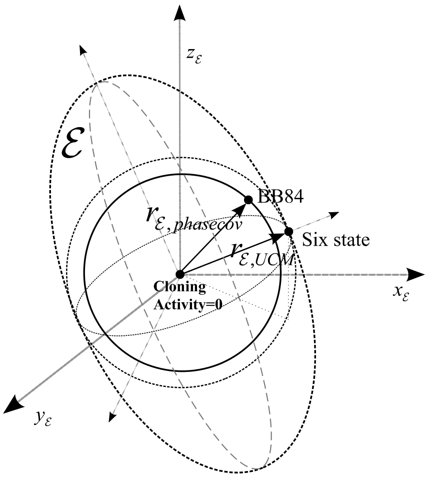


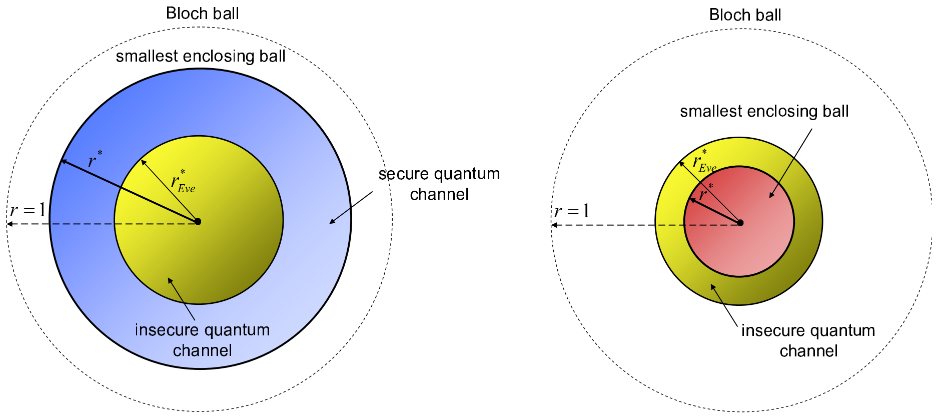
Figure 8: Comparison of UCM and phase-covariant based attack in ellipsoidal representation

$$|\psi\rangle = \{|0\rangle, |0\rangle, \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle, \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)\}$$

If Eve uses the universal quantum cloner, then the value of the parameter F_{Eve} is independent of the input quantum state $|\psi\rangle$. The quantum cloning transformation is optimal [4, 6], if $\eta = \frac{2}{3}$ and hence the maximum fidelity of optimal universal cloning is $F_{Eve} = \frac{5}{6}$, and the maximum radius is $r^{UCM}_{Eve} = \frac{2}{3}$. The *quantum information theoretical* radius can be defined as $r^{*UCM}_{Eve} = 1 - S(r^{*UCM}_{Eve})$, where S is the *von Neumann* entropy of the corresponding quantum state with radius r^{UCM}_{Eve}. In general, the *universal* cloning machine output state can be given as [4, 6, 15]

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

Universal cloning has direct application to eavesdropping strategies in Six-state quantum cryptography. In the Four-state (BB84) quantum cryptography protocol, the optimal eavesdropping attack is performed by a phase-covariant cloning machine, which clones the x equator [1, 4, 6, 14]. The importance of equatorial qubits lies in the fact that Four-state quantum cryptography requires these states rather than the states that span the whole Bloch sphere [6]. The optimal fidelity of 1 to 2 phase-covariant cloning transformation is given by $F^{phasecov.}_{1\to 2} = \frac{1}{2} + \sqrt{\frac{1}{8}} \approx 0.8535$ [1, 4, 6, 14]. If Eve has a phase-covariant quantum cloner, then the maximum value of her radius is $r^{phasecov.}_{Eve} = 2\sqrt{\frac{1}{8}}$. The quantum information theoretical radius $r^{*phasecov.}_{Eve}$ of the phase-covariant



$a.)\ r^* > r^*_{Eve}$ $b.)\ r^* \leq r^*_{Eve}$

Figure 9: Radius of the smallest enclosing information ball for secure and attacked quantum communication

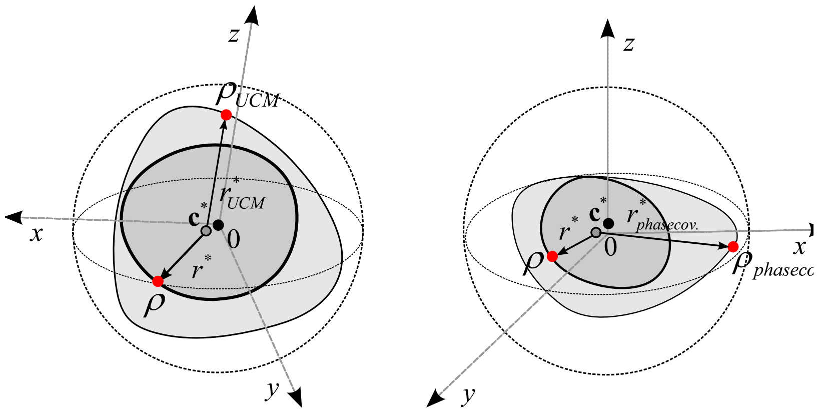


Figure 10: Smallest enclosing quantum informational balls of optimal and imperfect universal and phase-covariant cloners

cloner can be defined as $r^{phasecov.}_{Eve} = 1 - S(r^{phasecov.}_{Eve})$, where S is the von Neumann entropy of the corresponding quantum state with radius $r^{phasecov.}_{Eve}$. The phase-covariant quantum cloning transformation produces two copies of the equatorial qubit with optimal fidelity.

4 Proposed Model for Quantum Cloning-based Eavesdropping Detection

The information theoretical impacts of the eavesdropper's cloning machine are measured by the radius r^* of the smallest enclosing quantum informational ball. We use the Delaunay tessellation, because it is the fastest known tool for seeking the center of the smallest enclosing ball of points. 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 $r^* > r^*_{Eve}$. As the second part, for an insecure quantum channel, the radius r^* is smaller than or equal to r^*_{Eve}, thus $r^* \leq r^*_{Eve}$. In Figure 9, we show a geometrical interpretation of our model for a secure and for an *attacked* quantum channel [9].

In our security analysis, we use the spherical Delaunay tessellation to compute the 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 [3]. The smallest quantum informational ball with radius r^* is shown in grey, the ball of the ideal UCM cloner with radius r^*_{UCM} is shown in light grey. We conclude that, if $r_E \geq r_{E,UCM}$, then $r^* \leq r^*_{UCM}$, hence the informational theoretical radius will be smaller.

In Figure 10, we compare the ideal and imperfect universal and phase-covariant cloner quantum balls.

It can be concluded that the informational theoretical radii for ideal and imperfect phase-covariant cloning are different. In Figure 11, we illustrate the radii r^*_{UCM} and

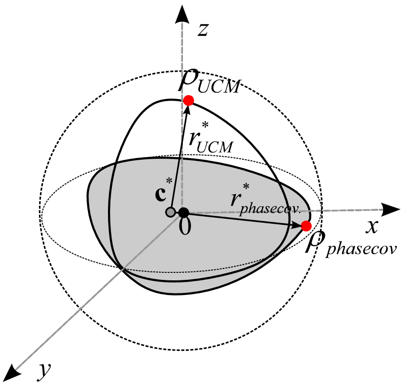


Figure 11: Comparison of smallest enclosing quantum informational ball of UCM-based and phase-covariant cloners

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

We would like to compute the radius r^* of the smallest enclosing ball of the cloned mixed quantum states, thus we must first seek the center c^* of the set of quantum states S. The set S of quantum states is denoted by $S = \{\rho_i\}_{i=1}^n$. The distance $d(.,.)$ between any two quantum states of S is measured by the quantum relative entropy, thus a minimax mathematical optimization is applied to the 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 $d(c, S) = max_i d(c, \rho_i)$. Using a minimax optimization, we can minimize the maximal quantum relative entropy from C to the furthest point S of by $c^* = argmin_c d(c, s)$. In Figure 12, we have illustrated the circumcenter c^* of S for the Euclidean distance and for quantum relative entropy [9].

In Figure 13, we compare the smallest quantum informational ball and the ordinary Euclidean ball.

We conclude that the quantum states ρ_1, ρ_2 and ρ_3 which determine the smallest enclosing ball in a Euclidean geometry differ from the states of the quantum informational ball.

4.1 Computation of Delaunay Triangulation on Bloch Sphere

In classical computational geometry, Voronoi diagrams and Delaunay triangulations play an important role [3, 18]. A Voronoi diagram is a division of space. The dual diagram for a Voronoi diagram is called a Delaunay tessellation [3, 18]. In the graph of a Delaunay triangulation, any circle is empty if it contains no vertex of S in its interior. If two quantum states of set S are denoted by ρ and σ, then edge e is in $Del(S)$ if and only if there exists an empty circle that passes through ρ and σ. An edge satisfying the empty circle property is said to be Delaunay. The Delaunay triangulation is guaranteed to be a triangulation only if the vertices of S are in a general position, thus there are no four quantum states of S lying on the same circle. The circumcircle of a triangle is the unique circle that passes through all three of its vertices, and the triangle is Delaunay if and only if its circumcircle is empty. The quantum Delaunay triangulation of a set of quantum states S, denoted by $Del(S)$, is the geometric dual of quantum Voronoi diagrams $vo(S)$. The quantum Voronoi diagrams can be first-type or right-sided diagrams. Similarly, we can derive two triangulations from quantum Voronoi diagrams. The first-type quantum informational ball circumscribing any simplex of quantum Delaunay triangulation $Del(S)$ is empty. If we choose a subset x of at most $d + 1$ states in $S = \{\rho_1, \ldots, \rho_n\}$, then the convex hull of the associated quantum states $\rho_i, i \in \chi$, is a simplex of the quantum triangulation of S, iff there exists an *empty quantum* informational ball B passing through the $\rho_i, i \in \chi$. The first-type and second-type quantum diagrams *for* quantum states which have non-equal radii *differ.* The quantum diagrams between these states are to the same as the Euclidean diagrams.

In our geometrical approach, we use the fact from computational geometry that the duality transform of a point in the plane can be constructed with a parabola. The dual of any quantum state on the Bloch sphere can be computed without measuring the distances between the quantum states. If we have a quantum state ρ and a paraboloid function $\mathcal{F}$, and we draw two lines that pass through the state ρ and are tangent to $\mathcal{F}$, then the line ρ^* will be the line that passes through the two points where the tangents touch $\mathcal{F}$, and state ρ represents the intersection of the two tangent lines [3, 18]. The dual of ρ must pass through the duals of the tangent points, and these points are where the tangents touch $\mathcal{F}$, as we have illustrated in Figure 15.

4.1.1 The Lifting Algorithm

In the proposed model, we use a three-dimensional Bloch ball and a *four* dimensional *generator surface* $\mathcal{F}$. The four dimensional object is generated by the quantum relative entropy-based *generator function* as defined in Equation (1):

$$\mathbf{F}(\rho) \quad = \quad -S(\rho(x, y, z)) = Tr(\rho \log \rho).$$

Consider the convex surface defined by the generator function $\mathbf{F}$, then the quantum Delaunay diagram can be obtained as a projection of a lower envelope of tangent planes of surface $\mathcal{F}$ at the Voronoi sites. The quantum relative entropy function $D(\rho \| \sigma)$ can be considered to be σ minus the value of tangent surface at σ. For simplicity, we will use a paraboloid surface in the figures to illustrate the quantum relative entropy-based abstract shape. According to the proposed method, we project back the points from the $3 + 1$ dimension *convex hull* to a *three-dimensional* Bloch ball, via the *lower envelope* of tangent planes. The projection gives the *Delaunay triangulation.*

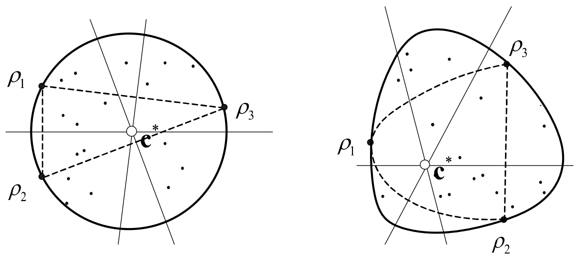


Figure 12: Circumcenter for Euclidean distance and quantum relative entropy

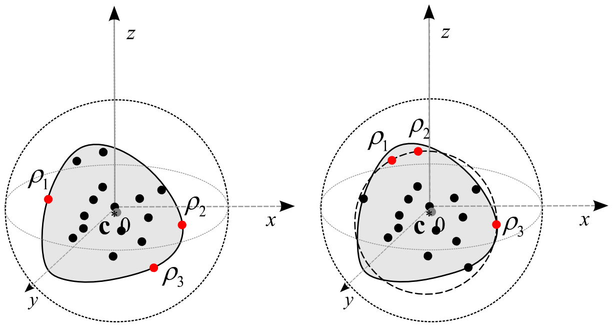


Figure 13: Circumcenter for Euclidean distance and quantum relative entropy

The lower envelope of tangent planes is illustrated in Figure 16.

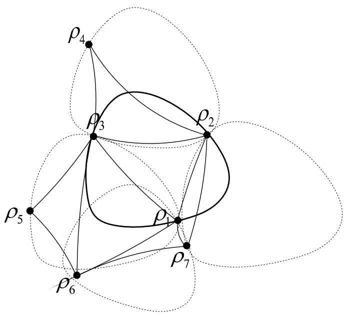


Figure 14: The empty ball property of quantum Delaunay triangulation

The Delaunay triangulation can be determined using tangent planes for any three quantum states $\rho_1, \rho_2, \rho_3 \in S$. If the tangent planes $H(\rho_1), H(\rho_2), H(\rho_3)$ at the lifted quantum states intersect at a point v^* located above v^*, then the corresponding Voronoi cells $vo(\rho_1), vo(\rho_2)$ and $vo(\rho_3)$ share a Voronoi vertex v. The Voronoi vertex point v is the projection of the point of intersection v^* of tangent planes $H(\rho_1), H(\rho_2)$, and $H(\rho_3)$. Since v is the shared vertex between three cells $vo(\rho_1), vo(\rho_2)$ and $vo(\rho_3)$, v is a Voronoi vertex and the circle around v is the circumcircle through the Delaunay triangle $\rho_1\rho_2\rho_3 \in S$. The quantum states ρ_1, ρ_2 and ρ_3 define a unique circle, and the center of this circle is the intersection of tangent planes. According to our method,

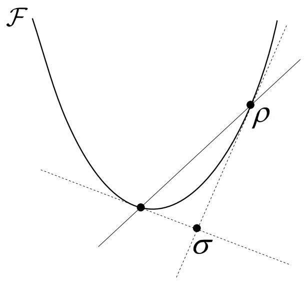


Figure 15: The dual of the quantum state ρ above $\mathcal{F}$ also can be computed without measuring distances

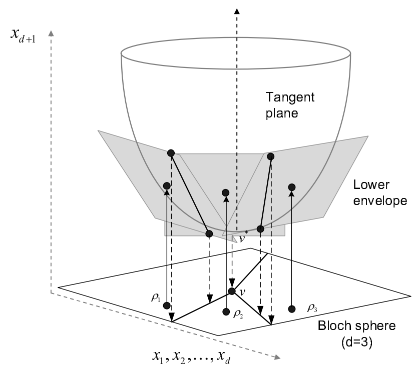


Figure 16: Circumcenter for Euclidean distance and quantum relative entropy

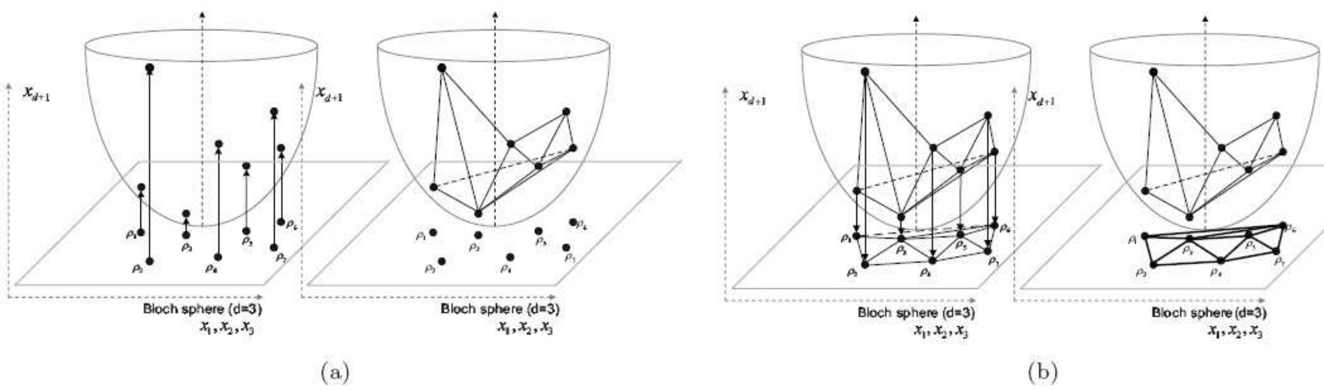


Figure 17: Projection of points in the Bloch sphere to the generator object (a), projection of convex hull edges back onto the Bloch sphere space (b)

we use generator function **F**, hence the intersection of the tangent planes gives the circumcircle of a quantum informational ball.

The steps of the quantum state projection algorithm are:

1) Project the quantum states $\rho = (\rho_x, \rho_y, \rho_z) \in S$ from the Bloch ball to four-dimensional points $\rho = (\rho_x, \rho_y, \rho_z, \mathbf{F}(\rho_x, \rho_y, \rho_z))$, on the quantum relative entropy-based generator surface, centered at the origin.

2) Calculate the *convex hull* of points on the paraboloid.

3) Project the *lowest part* of the convex hull back onto the *three* dimensional Bloch ball, thus compute the Voronoi-diagram via the *lower envelope of the tangent planes. Consider* the tangent planes $H(\rho_1), H(\rho_2)$, and $H(\rho_3)$ at the points ρ_1, ρ_2 and ρ_3. The tangent planes $H(\rho_1), H(\rho_2)$, and $H(\rho_3)$ intersect a Voronoi vertex point v^*, located above $\mathbf{v}$.

4) In the Bloch ball, the *three*-dimensional edges between the vertices form the *Delaunay triangulation of* the set S.

5) Compute the *smallest enclosing information ball.*

In Figure 17(a) and Figure 17(b), we show the main steps of the proposed projection algorithm. In the first phase, we project the quantum states from the Bloch sphere to the generator surface. In the next phase, we project back the intersection points and this projection gives the Delaunay triangulation between the quantum states in the Bloch ball.

The computational complexity of a Voronoi diagram in d-dimensional geometrical space is the same as that of a *convex hull* in $d + 1$ dimensional *geometrical space.* In a d-dimensional geometrical space, the complexity for computation of a *convex hull* has been proven [18] to be , $O(n \log n + n^{\lceil d/2 \rceil})$, thus the complexity of a

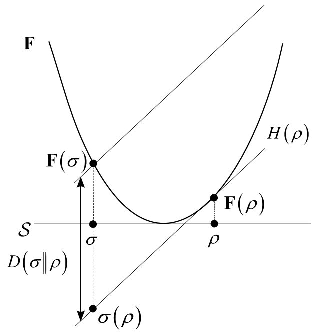


Figure 18: The hyperplane encodes the distance between quantum states

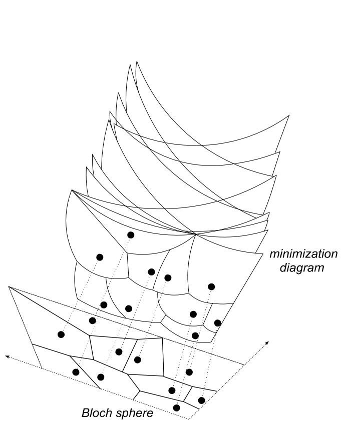


Figure 19: Quantum Delaunay triangulation on the Bloch sphere as a minimization diagram

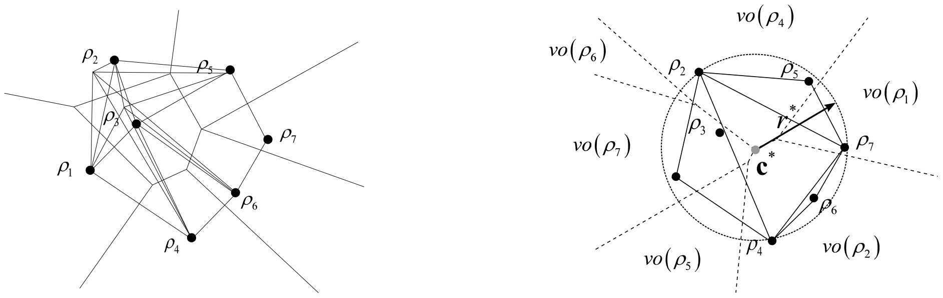


Figure 20: Comparison of ordinary Delaunay triangulation and furthest Delaunay triangulation between quantum states in the Bloch sphere representation

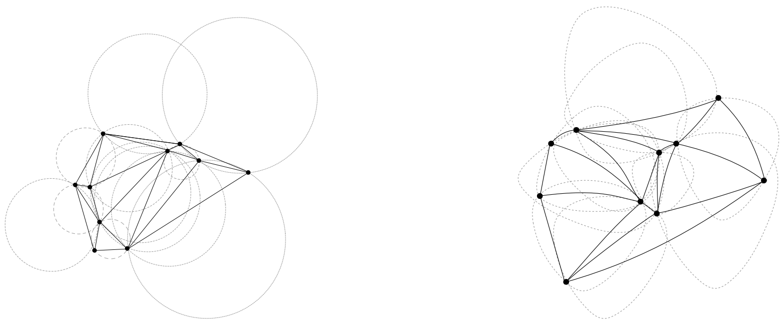


Figure 21: Comparison of first-type and second-type quantum Delaunay triangulations

d-dimensional Voronoi diagram is $O(n \log n + n^{\lceil d/2 \rceil})$. Sharir has shown [12] that a *lower envelope* of algebraic surfaces can be computed in time $O(n^{(d-1)+\varepsilon})$ to a d-dimensional *geometrical* space, and a Voronoi diagram in d-dimensional geometrical space can be computed in time $O(n^{d+\varepsilon})$ [3, 18].

The fact that $H(\rho)$ encodes the distance of quantum states to ρ leads to a correspondence between dual Delaunay diagrams and lower envelopes. Consider the set $H = \{H(\rho)|\rho \in S\}$ of planes, and let $lo(H)$ be the lower envelope of the planes in H.

In this case, the projection of $lo(H)$ onto the plane $z = 0$ is the dual Delaunay diagram of S. Let H be the set of planes $H(\rho)$ for $\rho \in S$. The quantum Delaunay diagram can be computed by a projection of $lo(H)$ onto the plane $z = 0$. The Voronoi cell of a quantum state $\rho \in S$ is the projection of the facet of lower envelope $lo(H)$, that lies on the plane $H(\rho)$. Let σ be a quantum state in the plane $z = 0$ lying in the Voronoi cell of ρ. In this case, $D(\sigma\|\rho) < D(\sigma\|x)$, for all $x \in S$, where $x \neq \rho$. We would like to see that the vertical line through σ intersects the lower envelope $lo(H)$ at a point lying on $H(\rho)$. For quantum state $x \in S$, the plane $H(x)$ is intersected by the vertical line through σ at point $\sigma(x) = (\sigma_x, \sigma_y, \mathcal{F}(\sigma) - D(\sigma\|x))$. The quantum ρ state has the smallest distance to σ, of all states in S, thus $\sigma(\rho)$ is the highest point of intersection. We conclude that the vertical line through σ intersects the lower envelope $lo(H)$ at a point lying on $H(\rho)$. We note that the first-type of dual Delaunay diagram of S is the minimization diagram of n linear functions $H_{\rho_1}(x)$, whose graphs are the hyperplanes H_{ρ_1}. Let $S = \{\rho_1, \ldots, \rho_n\}$ be a finite set of quantum states. To each quantum state ρ_i, a d-variate continuous function D_i can be defined over S. The *lower envelope* of the functions can be expressed as the graph of $min_{1 \leq i \leq n} D_i$. The minimization diagram of the functions is the subdivision of S into cells, where for each cell, $argmin_i f_i$ is fixed.

In Figure 19, we illustrate the method of construction of quantum Delaunay diagram, as a minimization of diagrams for quantum informational distance.

The quantum Delaunay diagram can be obtained as the minimization diagram for $D_i(x) = D(x\|\rho_i)$. In Figure 20, we compare the ordinary Delaunay triangulation and the furthest Delaunay triangulation. The furthest point Delaunay edges do not intersect and the furthest Delaunay triangulation of S determines the convex hull and center of the smallest enclosing ball.

In Figure 21, we illustrate the quantum Delaunay triangulation and its curved edges. We have illustrated the difference between first-type and second-type quantum Delaunay triangulations. The regular Delaunay diagram $reg(B')$ has straight edges, the geodesic Delaunay diagram has curved edges. The second-type Delaunay diagram $Del'(S)$ is the geometric dual of left-sided quantum Voronoi diagrams.

At the end of the proposed algorithm, the radius r^* of the smallest enclosing ball B^* with respect to the quantum informational distance is equal to the fidelity of the

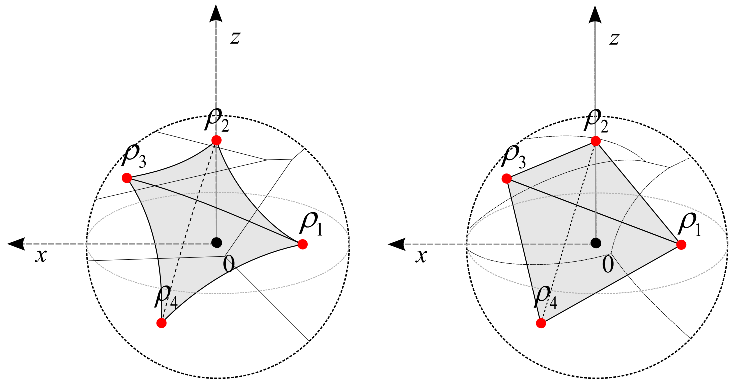


Figure 22: Comparison of first-type and second-type quantum Delaunay triangulations on the Bloch ball

cloning transformation. The approximated value of the information theoretical impacts of the eavesdropper is obtained by r^*, the radius of the smallest information ball. Finally, the *security* of the quantum channel is determined by our geometrical model based on the assumptions $r^* > r^*_{Eve}$ and $r^* \leq r^*_{Eve}$, and the approximate value of the fidelity parameter F_{Eve}, can be expressed as:

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

where r can be derived from the quantum information theoretical radius r^* by $r^* = 1 - S(r)$, where S is the von Neumann entropy. In Figure 22, we compare the *first-type* and *second-type* quantum Delaunay diagrams for mixed quantum states on the Bloch sphere.

The dual of the left-sided quantum Voronoi diagram is a curved diagram, the dual of the right-sided diagram has straight edges. The distorted structure of the smallest enclosing quantum relative entropy ball is easily seen in Figure 23.

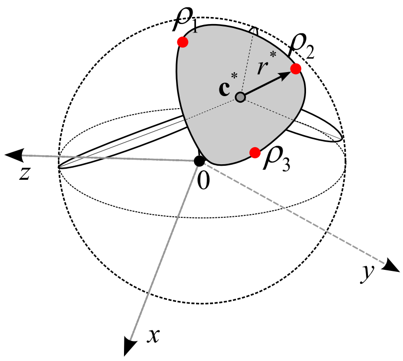


Figure 23: Smallest enclosing quantum informational ball and its radius

In Figure 24, we show an example of 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 a Euclidean ball.

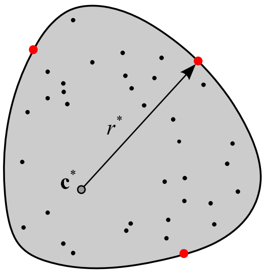


Figure 24: Smallest enclosing quantum informational ball inside the Bloch sphere

5 Conclusion and Future Work

This paper proposes a new algorithm for computing the fidelity of an eavesdropper's cloning machine. The proposed method uses quantum relative entropy to compute the smallest enclosing information ball. We have shown that a Delaunay triangulation based on quantum relative entropy plays an important role in a numerical calculation of the fidelity of quantum cloning machines. According to the proposed method, we compute the smallest enclosing ball based on Delaunay triangulation, which is considered to be a useful and efficient tool. We propose a new algorithm for computing the fidelity of quantum cloning transformation-based attacks in quantum cryptography and for estimating the security of a protocol.

References

[1] A. Acìn, N. Gisin, L. Masanes, and V. Scarani, "Bell's inequalities detect efficient entanglement," *International Journal of Quantum Information*, vol. 2, pp. 23, 2004.

[2] M. Badoiu, and K. L. Clarkson, "Smaller core-sets for balls," *Proceedings 14th ACM-SIAM Symposium on Discrete Algorithms*, pp. 801V802, 2003.

[3] J. D. Boissonnat and M. Teillaud, *Effective Computational Geometry for Curves and Surfaces*, pp. 67-116, Springer-Verlag, Mathematics and Visualization, 2007.

[4] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, "Security of quantum key distribution using d-level systems," *Physical Review Letters*, vol. 88, no. 12, pp. 1-4, 2002.

[5] M. Curty, and N. Lütkenhaus, "Effect of finite detector efficiencies on the security evaluation of quantum key distribution," *Physical Review A (Atomic, Molecular, and Optical Physics)*, vol. 69, 042321, pp. 1-10, 2004.

[6] G. M. D'Ariano, and C. Macchiavello, "Optimal phase-covariant cloning for qubits and qutrits," *Physical Review A (Atomic, Molecular, and Optical Physics)*, vol. 67, 042306, pp.1-9, 2003.

[7] M. R. Doomun, and K. Soyjaudah, "Analytical comparison of cryptographic techniques for resource-constrained wireless security," *International Journal of Network Security*, vol. 9, no. 1, pp. 82-94, 2009.

[8] L. Gyongyosi, and S. Imre, "Geometrical estimation of information theoretical impacts of incoherent attacks for quantum cryptography", *International Review of Physics*, no. 6, pp. 349-362, 2010.

[9] L. Gyongyosi, and S. Imre, "Computational geometric analysis of physically allowed quantum cloning transformations for quantum cryptography," *Proceedings of the 4th WSEAS International Conference on Computer Engineering and Applications*, pp. 121-126, Harvard University, Cambridge, USA, 2010.

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

[11] Y. Kanamori, S. M. Yoo, D. A. Gregory, and F. T. Sheldon, "Authentication protocol using quantum superposition states," *International Journal of Network Security*, vol. 9, no. 2, pp. 101-108, 2009.

[12] 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)*, vol. 77, no. 5, 052311, pp. 1-6, 2008.

[13] I. S. Lee and W. H. Tsai, "Security protection of software programs by information sharing and authentication techniques using invisible ascii control code," *International Journal of Network Security*, vol. 10, no. 1, pp. 1-10, 2010.

[14] A. Niederberger, V. Scarani, and N. Gisin, "Photon-number-splitting versus cloning attacks in practical implementations of the Bennett-Brassard 1984 protocol for quantum cryptography," *Physical Review A (Atomic, Molecular, and Optical Physics)*, vol. 71, 042316, pp. 1-10, 2005.

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

[16] R. Panigrahy, *Minimum Enclosing Polytope in High Dimensions*, CoRR, cs.CG/0407020, 2004.

[17] V. T. Rajan, "Optimality of the Delaunay triangulation in R^d," *Discrete & Computational Geometry*, vol. 12, pp. 189V202, 1994.

[18] J. R. Sack, and G. Urrutia, *Handbook of Computational Geometry*, ch. 5, pp. 201V290, Elsevier Science Publishing, 2000.

Laszlo Gyongyosi, 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. He obtained two Best Paper Awards on international conferences related to future computing and quantum information processing at University of Harvard, USA.

Sandor Imre was born in Budapest in 1969. He received the M.Sc. degree in Electronic Engineering from the Budapest University of Technology (BUTE) in 1993. Next he started his Ph. D. studies at BUTE 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 BUTE. He was invited to join the Mobile Innovation Centre of BUTE 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 reconfigurable systems.