Computational Geometric Analysis of Physically Allowed Quantum Cloning Transformations for Quantum Cryptography

LASZLO GYONGYOSI, SANDOR IMRE
Department of Telecommunications
Budapest University of Technology
Magyar tudósok krt. 2.,
HUNGARY
{gyongyosi, imre}@hit.bme.hu

Abstract: - The safety of quantum cryptography relies on the no-cloning theorem. In secret quantum communications, an eavesdropper cannot clone the sent qubits perfectly, however the best eavesdropping attacks for quantum cryptography are based on imperfect cloning machines. The eavesdropper's physically allowed quantum evolutions on the sent qubit can be described in terms of the quantum state's geometry. We use a fundamentally new computational geometrical method to analyze the informational theoretical impacts of cloning activity on the quantum channel. Our method uses Delaunay tessellation and convex hull calculation, with respect to quantum relative entropy as distance measure. The security analysis is focused on the four state (BB84) and Six state quantum cryptography protocols. The proposed geometrical method can be used to analyze efficiently the informational theoretical impacts of physically allowed quantum cloning transformations.

Key-Words: - Quantum Cryptography, Quantum Cloning, Quantum Informational Distance

1 Introduction

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 [1, 2]. Our goal is to identify the quantum cloning based attacks in the quantum channel, and find potential and efficient solution for their detection in secret quantum communications. The incoherent and coherent attacks against quantum cryptography are based on quantum cloners. The type of used quantum cloner depends on the quantum cryptography protocol. Against the four state (BB84) Eve, the eavesdropper uses the phase-covariant cloner, while for the Six state protocol the optimal results can be achieved by the universal quantum cloner (UCM) [8, 9, 10, 11].

We use a computational geometrical method to analyze the cloning activity on the quantum channel.

1.1. Attacks in Quantum Cryptography

The *incoherent* quantum cloning based attack is the eavesdropper's most general strategy [8, 9], thus in our geometrical based security analysis, we use the incoherent attack based attacker model. In the four state (BB84) and Six state quantum cryptography protocols Alice, the transmitter, sends quantum states from a set of possible quantum states, chosen randomly. On the other side, Bob receives the quantum states in a basis chosen at random between two or three bases. In the *incoherent* attack, Eve clones imperfectly the sent quantum state using her probe quantum state, she sends one copy to Bob, and keeps the other copy. We denote Eve's quantum state by $|E\rangle$, and the unitary operation which describes the interaction between the sent qubit and Eve's state is denoted by U, thus the whole transformation can be given by [6]:

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

where $|E_{i,j}\rangle$ denotes Eve's cloned quantum state, and $|E\rangle$ can be written as 2×2 matrix, whose elements are Eve's states $|E_{i,j}\rangle$. In our method we measure the *informational theoretical* meaning of quantum cloning activity in the quantum channel, where Alice's and Bob's side can be modeled by random variable X and Y. Our geometrical security analysis is focused on the cloned mixed quantum state, received by Bob. 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 $\mathcal{L}(\rho_A) = \sigma_B$. The general model for the quantum cloner based attack in quantum cryptography is illustrated in Figure (1).

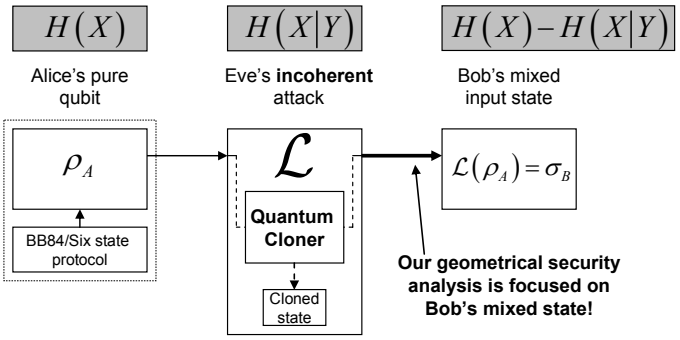

Fig. 1: The analyzed attacker model and the entropies

We measure in a geometrical representation the information, which can be transmitted in a presence of an eavesdropper on the quantum channel. In a secret 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 of Bob, which describes the maximal transmittable information from Alice to Bob in the *attacked* quantum channel:

$$r^* = max_{\{all\ possible\ x_i\}} H(X) - H(X|Y). \quad (2)$$

To compute the radius r^* of the smallest informational ball of 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 [6, 7].

1.2 Attacker Model for BB84 and Six State Protocol

The type of the quantum cloner machine depends on the actual protocol. For BB84, Eve chooses the phase covariant cloner, while for the Six state protocol she uses the universal quantum cloner (UCM) machine [8, 9].

The effect of the eavesdropper's symmetric quantum cloner simply shrinks the Bloch ball $\mathcal{B}$, with given probability *p*. The *UCM* cloning transformation shrinks the vector characterizing the input quantum state by $\eta = 1 - \frac{4p}{3} = \frac{2}{3}$, while the phase covariant cloner shrinks the radius with $\eta = (1 - 3p/2) = 2\sqrt{\frac{1}{8}}$. The fidelity of the UCM cloning transformation can be given by $F = \langle \psi | \rho | \psi \rangle = \frac{1}{2}\left(1 + \frac{2}{3}\right) = \frac{5}{6}$, and the fidelity of phase covariant cloner is $F = \frac{1}{2}\left(1 + 2\sqrt{\frac{1}{8}}\right) = \frac{1}{2} + \sqrt{\frac{1}{8}}$ [8, 9, 11].

2 Geometrical Computation of Quantum Informational Ball

In our 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 [2]. The Shannon entropy $H(p)$ of quantum states can be given by the von-Neumann entropy $\mathrm{S}(\rho)$, which is a generalization of classical entropy to quantum states [2, 3]. The entropy of quantum states can be given by the following way:

$$\mathrm{S}(\rho) = -Tr(\rho \log \rho). \quad (3)$$

The relative entropy of quantum states measures the informational distance between quantum states, using the negative entropy of quantum states [3, 5] as the generator function $\mathbf{F}(\rho)$:

$$\mathbf{F}(\rho) = -\mathrm{S}(\rho) = Tr(\rho \log \rho). \quad (4)$$

The relative quantum entropy between density matrices ρ and σ can be described by the strictly convex and differentiable function $\mathbf{F}$, as:

$$D(\rho \| \sigma) = \mathbf{F}(\rho) - \mathbf{F}(\sigma) - \langle \rho - \sigma, \nabla \mathbf{F}(\sigma) \rangle, \quad (5)$$

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

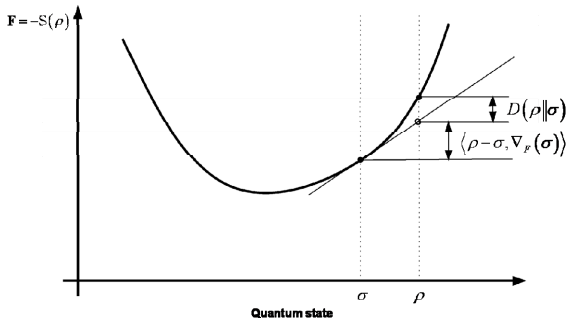

Fig. 2: Visualizing generator function *F* as negative von Neumann entropy and its corresponding relative quantum entropy

2.1. Geometrical background

If the set $\mathcal{S}$ of quantum states is denoted by $S = \{\rho_1, \rho_2, \ldots \rho_n\}$, the Voronoi cell $vo(\rho)$ for quantum state ρ and S the set of point can be given by

$$vo(\rho) = \{x | d(x, \rho_i) \le d(x, \rho_j) \in S\{\rho\}\}, \quad (6)$$

where $d(\cdot)$ is the distance function, which for Euclidean distance can be given by $d(\cdot) = \mathbb{R}^d \times \mathbb{R}^d \to \mathbb{R}$. The circumcircle 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 $\rho_1\rho_2\rho_3$. The triangle *t* is said to be Delaunay, when its circumcircle is empty.

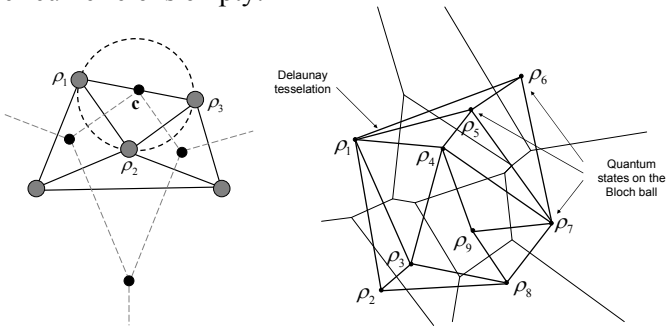

Fig. 3: The triangle of quantum states corresponds to the vertex c (a), and a Delaunay tessellation on the Bloch sphere (b).

For an empty circumcircle, the circle passing through the quantum states of a triangle $t \in T$, encloses no other vertex of the set V [4].
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 [4].

2.2 Connection between Information Theoretical Radius and Bloch Vector

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

$$r^* = \min_{\sigma \in \mathcal{S}(\mathbb{C}^2)} \max_{\rho \in \mathcal{S}(\mathbb{C}^2)} D\big(\mathcal{L}(\rho) \| \mathcal{L}(\sigma)\big). \quad (7)$$

In our geometrical approach, we compute the smallest enclosing information ball by Delaunay tessellation, which is the fastest known tool to seek a center of a smallest enclosing ball of points [4, 5]. For UCM and phase-covariant cloning, the connection between information theoretical radius r^* and the Bloch vector r_{Bloch} can be defined as:

$$r^* = 1 - S(r_{Bloch}), \quad (8)$$

where S is the von Neumann entropy of corresponding quantum state with maximal length vector r_{Bloch}. The informational theoretical radius of UCM and phase-covariant cloners are denoted by r^*_{UCM} and $r^*_{phasecov}$, respectively.

2.3 Laguerre Diagram for Quantum States

In our paper we use Laguerre Delaunay diagram [4] to compute the radius of the smallest enclosing ball. In generally, the Laguerre distance for generating points x_i and with weight r_i^2, in the Euclidean space is defined by

$$d_L(p, x_i) = \|p - x_i\|^2 - r_i^2. \quad (9)$$

The Delaunay diagram with respect to the Laguerre distance is called Laguerre Delaunay diagram. For the Laguerre bisector of two three-dimensional Euclidean balls $B(p, r_P)$ and $B(q, r_Q)$ centered at three dimensional points p and q, we can write equation

$$2\langle x, q - p\rangle + \langle p, p\rangle - \langle q, q\rangle + r_Q^2 - r_P^2 = 0. \quad (10)$$

In the Euclidean space, for weight r_i^2 the Laguerre distance $d_L(p, x_i)$ can be interpreted as the square of the length of the line segment starting at p 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 [4].

We show a basically new method to derive quantum relative entropy based Delaunay tessellation on the Bloch ball $\mathcal{B}$ to detect eavesdropping activity on the quantum channel. 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 security analysis has two main steps:

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

3 Quantum Delaunay Triangulation from Laguerre Diagrams

As we have seen, in the Euclidean space, the Laguerre distance of a point x to an Euclidean ball $b = b(p, r)$ is defined as $d_L(p, x) = \|p - x\|^2 - r^2$, and for n balls $b_i = b(p_i, r_i)$, where $i = 1, \ldots, n$, the Laguerre diagram [4] of b_i is defined as the minimization diagram of the corresponding n distance functions

$$d_L^i(x) = \|p - x\|^2 - r^2. \quad (11)$$

In Figure (4) we show the ordinary triangulation of quantum relative entropy based Voronoi diagram, the image of quantum relative entropy based Delaunay triangulation by the inverse of gradient ∇_F^{-1}, is a curved triangulation whose vertices are the points of $\mathcal{S}$.

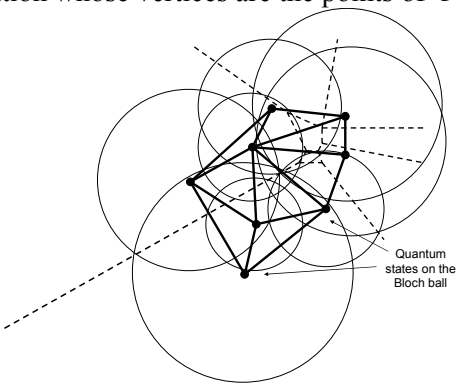

Fig. 4: The regular triangulation on the Bloch ball rooted at gradient vertices

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

$$\langle x - p_i', x - p_i'\rangle = \langle p_i', p_i'\rangle + 2\big(\mathbf{F}(p_i) - \langle p_i, p_i'\rangle\big). \quad (12)$$

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

3.1 Center of the 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*. The core-sets have an important role in our calculation, and approximate method. We apply the approximation algorithm presented by Badoui and

Clarkson, however in our algorithm the distances between quantum states are measured by quantum relative entropy [5, 9]. The $\mathcal{E}$-core set $\mathcal{C}$ is a subset of the set $\mathcal{C}\subseteq\mathcal{S}$, such for the circumcenter $\mathbf{c}$ of the minimax ball [5]

$$d(\mathbf{c},\mathcal{S})\leq(1+\mathcal{E})r, \quad (13)$$

where r is the radius of the smallest enclosing quantum information ball of set of quantum states $\mathcal{S}$ [5, 9]. The approximating algorithm, for a set of quantum states $\mathcal{S}=\{s_1,\ldots,s_n\}$ and circumcenter $\mathbf{c}$ first finds a farthest point s_m of ball set B, and moves $\mathbf{c}$ towards s_m in $\mathcal{O}(dn)$ time in every iteration step. The algorithm seeks the farthest point in the ball set $B=\{b_1=Ball(\mathbf{c}_1,r_1),\ldots,b_n=Ball(\mathbf{c}_n,r_n)\}$ by maximizing the quantum informational distance for a current circumcenter position $\mathbf{c}$ as $\max_{i\in\{1,\ldots,n\}} D_F(\mathbf{c},b_i)$. Using $\max_{x\in b_i} D_F(\mathbf{c},x_i)=D_F(\mathbf{c},S_i)+r_i$, we get

$$\max_{i\in\{1,\ldots,n\}} D_F(\mathbf{c},b_i)=\max_{i\in\{1,\ldots,n\}}\left(D_F(\mathbf{c},S_i)+r_i\right). \quad (14)$$

In Figure (5) we illustrated the smallest enclosing ball of balls in the quantum space.

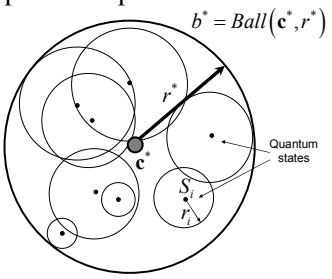

Fig. 5: The smallest enclosing ball of a set of balls in the quantum space

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 $\mathbf{c}^*$ [6]. The smallest enclosing ball of the set of balls $B=\{b_1,\ldots,b_n\}$, fully enclosing B, thus $B\subseteq Ball(\mathbf{c}^*,r^*)$. The algorithm does $\left\lfloor\frac{1}{\mathcal{E}^2}\right\rfloor$ iterations to ensure an $(1+\mathcal{E})$ approximation, thus the overall cost of the algorithm is $\mathcal{O}\left(\frac{dn}{\mathcal{E}^2}\right)$ [5]. The smallest enclosing ball of a ball set B can be written as

$$\min_{\mathbf{c}}\mathbf{F}_B(\mathbf{c}), \quad (15)$$

where $\mathbf{F}_B(X)=d(X,B)=\max_{i\in\{1,\ldots,n\}} d(X,B_i)$, and the distance function $d(\cdot,\cdot)$ measures the relative entropy between quantum states [9]. The minimum ball of the set of balls is unique, thus the circumcenter $\mathbf{c}^*$ of the set of quantum states is $\mathbf{c}^*=\arg\min_{\mathbf{c}}\mathbf{F}_B(\mathbf{c})$. The main steps of our algorithm are:

Algorithm 1.

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*

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

3. *Update* the circumcircle:

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

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

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 the informational theoretical fidelity of the cloning transformation.

Using the information theoretical radius $r^*=\min_{\sigma\in\mathcal{S}(\mathbb{C}^2)}\max_{\rho\in\mathcal{S}(\mathbb{C}^2)} D\left(\mathcal{L}(\rho)\middle\|\mathcal{L}(\sigma)\right)$, the radius of the best cloned state can be expressed as:

$$r^*=1-S(r_{Bloch}), \quad (16)$$

where S is the von Neumann entropy of quantum state with maximal length vector r_{Bloch}.

4 Applying Our Method in Quantum Cryptography

Using the declared statement in Section 2.2., the quantum channel in BB84 and Six state protocols is secure iff $r^*>r^*_{phasecov}$. and $r^*>r^*_{UCM}$. In our geometrical method we compute r^*, the radius of the smallest enclosing quantum informational ball, to determine the security of the quantum communication.

4.1 BB84 Protocol and Phase Covariant Cloning

In Figure (6) we illustrated the dual Delaunay-diagram for cloned equatorial states in BB84 protocol. The sent pure quantum states cloned by Eve's phase-covariant quantum cloner, denoted by ρ_1,ρ_2,ρ_3 and ρ_4.

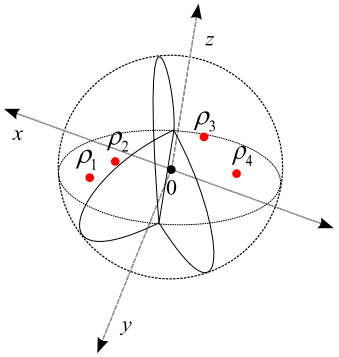

Fig. 6: Dual Delaunay-diagram of cloned equatorial states in BB84 protocol

Using Delaunay tessellation, we compute the *convex-hull* of the cloned equatorial states ρ_1,ρ_2,ρ_3 and ρ_4. In Figure (7) we illustrated the convex-hull of cloned states in two and three dimensional Bloch ball representation.

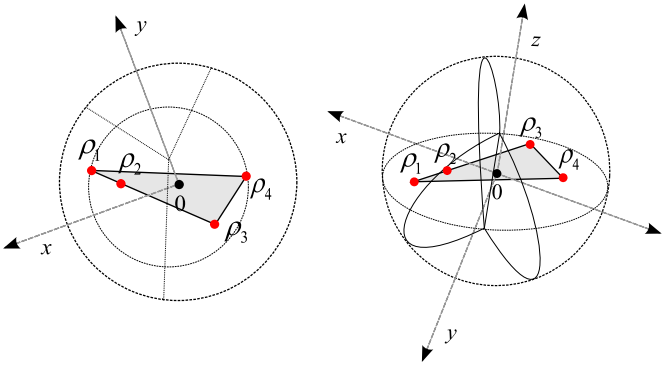

Fig. 7: The convex hull of cloned mixed states. The convex hull computed by Delaunay triangulation

From the convex set, we can compute the smallest enclosing quantum informational ball $\mathcal{B}^*$ and its radius r^*. In Figure (8) we have illustrated the Euclidean smallest enclosing ball by the dashed circle, and the quantum relative entropy ball.

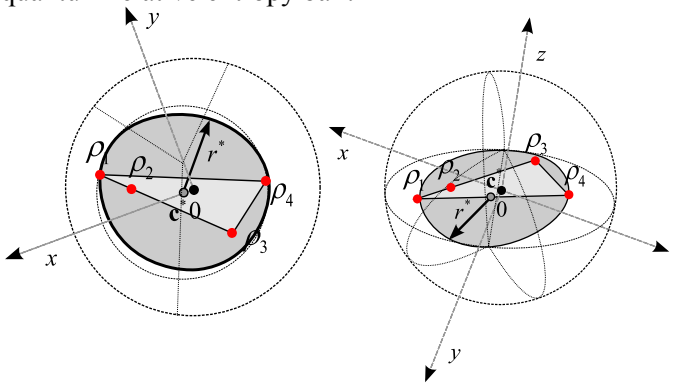

Fig. 8: The smallest enclosing quantum informational ball and its radius

From the smallest enclosing quantum informational ball $\mathcal{B}^*$, we can determine the radius r^*, which describes the informational theoretical impact of the eavesdropper cloning machine. The center of the smallest enclosing quantum informational ball is denoted by $\mathbf{c}^*$.

4.2 Six State Protocol and Universal Cloning

In Figure (9.a) we have illustrated the Voronoi-cells for the cloned states and the three-dimensional *convex hull* (light-grey) of cloned states $\rho_1, \rho_2, \rho_3, \rho_4, \rho_5$ and ρ_6. The cloned states generated by Eve's universal quantum cloner machine, using the Six state quantum cryptography protocol. From the convex hull, we compute the smallest enclosing quantum informational ball $\mathcal{B}^*$. In Figure (9.b) we have illustrated the smallest quantum informational ball and its radius r^*.

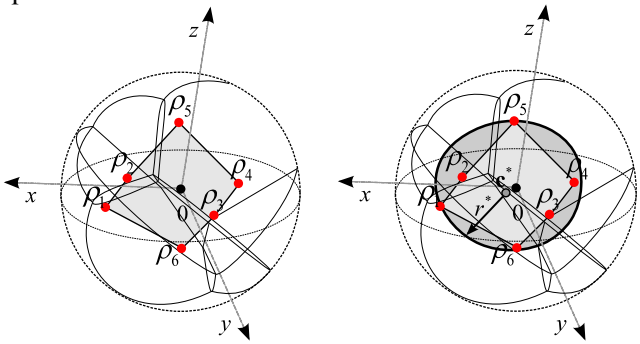

Fig. 9: The convex hull of cloned mixed states in Six state protocol

In Figure (10) we show an example for a two-dimensional smallest enclosing quantum informational ball, and its informational theoretical radius r^*.

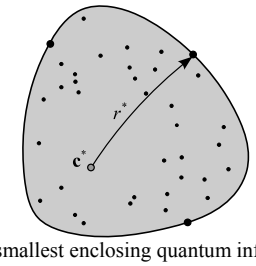

Fig. 10: The smallest enclosing quantum informational ball

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

5 Optimization

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

$$\mathcal{O}\left(\frac{dn}{\varepsilon^2}\right) = \mathcal{O}\left(\frac{d}{\varepsilon^2}\frac{1}{\varepsilon}\right) = \mathcal{O}\left(\frac{d}{\varepsilon^3}\right) \quad (17)$$

time, by first sampling $n = \frac{1}{\varepsilon}$ 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 $\mathcal{O}\left(\frac{d}{\varepsilon^2}\right)$ time. In this section we improve our method to get an $\mathcal{O}\left(\frac{d}{\varepsilon}\right)$ time $(1+\varepsilon)$ approximation algorithm in quantum space. In Figure (11) we illustrated the improved algorithm on a set of quantum states. The approximate ball has radius r, the enclosing ball has radius $r+\delta$. The approximated center $\mathbf{c}$ denoted by black, the core-set are denoted by the grey circles. The optimal radius between the center $\mathbf{c}$ and the farthest quantum state is denoted by r^* [9].

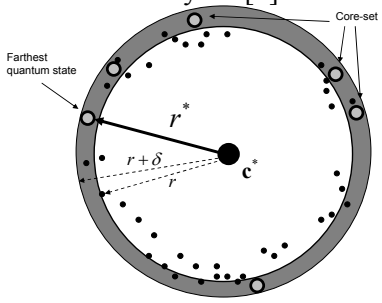

Fig. 11: The approximate (light) and enclosing quantum ball (darker)

In the proposed algorithm the optimal radius is between $r \le r^* \le r+\delta$, and the process is terminates as $\delta \le \varepsilon$, in at most $\mathcal{O}\left(\frac{1}{\varepsilon}\right)$ iterations. The main steps of the improved approximation algorithm are [9]:

Algorithm 2.

1. *Select* a random center $\mathbf{c}_1$ from the set of quantum states $\mathcal{S}$
$$\mathbf{c}_1 \in \mathcal{S}$$
2. $r = \frac{1}{2}\max_i D_F(\mathbf{c}_1, \mathcal{S})$;
3. $\delta = \frac{1}{2}\max_i D_F(\mathbf{c}_1, \mathcal{S})$;
4. **for** $\left(i = 1,2,\ldots,\left(\frac{1}{\delta}\right)\right)$
5. **do**
6. $S = \arg\max_i D_F(c, \mathcal{S})$;
7. Move $Ball(c,r)$ on the geodesic until it touches the *farthest* point S;
8. $s = \max_i D_F(c, S_i) - r$;
9. **if** $s \le \frac{3\delta}{4}$ **then**
10. $\delta = \frac{3\delta}{4}$
11. **else**
12. $r = r + \frac{\delta}{4}$;
13. $\delta = \frac{3\delta}{4}$;
14. **until** $\delta \le \varepsilon$.

5.1 Converge Rate

In our experimental simulation we have compared the core-set algorithm and our improved core-set algorithm to find the smallest enclosing quantum information ball. We have analyzed the approximation algorithms for 30 center updates, and we have measured the quality of the approximation with respect to quantum relative entropy.

The results of our simulation are shown in Figure (12). The *x*-axis represents the number of center updates to find the center of the smallest enclosing quantum informational ball, on the *y*-axis we have illustrated the quantum informational distance between the found center $\mathbf{c}$ and the optimal center $\mathbf{c}^*$.

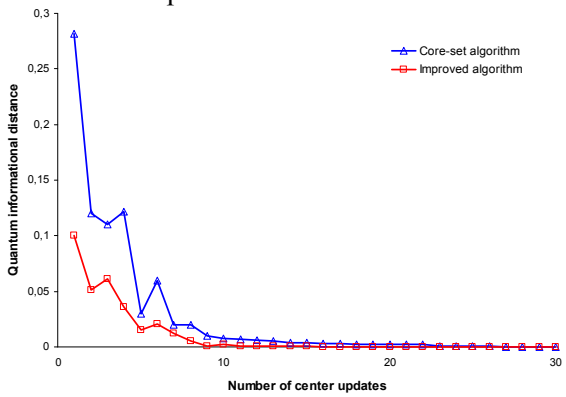

Fig. 12: The converge rate of the approximation algorithms

From the results we can conclude, that each algorithm find the approximate center $\mathbf{c}$ to the optimal center $\mathbf{c}^*$ very fast. The quantum relative entropy based approximation algorithms have a very accurate converge of $\mathbf{c}$ towards $\mathbf{c}^*$, however the improved core-set algorithm converges faster for smaller number of center updates.

6 Conclusions

In quantum cryptography, an eavesdropper cannot clone the sent qubits perfectly, however the best eavesdropping attacks are based on imperfect quantum cloners. We proposed a fundamentally new approach to compute the informational theoretical impacts of an eavesdropper's cloning machine in the quantum channel. The analyzed incoherent attacks are the eavesdropper's most general strategy, however our method can be extended for different types of attacks. The legal parties can detect the disturbance generated by the eavesdropper's cloning activity, and the impacts of her cloning transformation can be measured geometrically. Our method is based on Laguerre diagrams and quantum relative entropy as distance measure. Using Delaunay tessellation on the Bloch sphere, the geometric space can be divided and can be computed very efficiently, in a reasonable computational time.

In the future, we would like to extend our method to other protocols, and to collective and coherent attacks. We would like to make a deep study on the possibility to construct a more effective algorithm to compute the informational theoretical impacts of the eavesdropper's cloning machine.

References:

[1] L. Gyongyosi, S. Imre, Fidelity Analysis of Quantum Cloning Based Attacks in Quantum Cryptography, In: *Proceedings of the 10th International Conference on Telecommunications - ConTEL 2009*. Zagreb, Croatia, 2009.06.08-2009.06.10. 2009. pp. 221-228. Paper 53.

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

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

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

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

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

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

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

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

[10] N. J. Cerf, *Phys. Rev. Lett*. 84, 4497 (2000).

[11] Zhang W.-H., Yu L.-B., Ye L. Optimal asymmetric phase-covariant quantum cloning (2006) *Physics Letters, Section A: General, Atomic and Solid State Physics*, 356 (3), pp. 195-198.