Efficient Computational Information Geometric Analysis of Physically Allowed Quantum Cloning Attacks for Quantum Key Distribution Protocols

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

Abstract: - In secret quantum communications the best eavesdropping attacks on quantum cryptography are based on imperfect cloning machines. The incoherent attack, based on quantum cloning, is the most common eavesdropping strategy. Using a probe, the eavesdropper imperfectly clones the sender's quantum state which keeps one copy and sends the other. The physically allowed transformations of Eve's quantum cloner on Bob's qubit can be described in terms of Completely Positive (CP), trace preserving maps. The map of the quantum cloner compresses the Bloch-ball, as an affine map. This affine map has to be a complete positive, trace preserving map, which shrinks the Bloch ball. The effects of a quantum cloner can be given in tetrahedron representation. In this paper we show a new, quantum information theoretical representation of eavesdropping detection, focused on the Four-state (BB84) and Six-state quantum cryptography protocols. We use a fundamentally new computational geometrical method to analyze the informational theoretical impacts of cloning activity on the quantum channel. The proposed algorithm uses Delaunay tessellation and convex hull calculation on the Bloch sphere, with respect to quantum relative entropy as distance measure. The improved core-set approach can be used to analyze efficiently the informational theoretical impacts of physically allowed quantum cloning attacks.

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

1 Introduction

Quantum cryptography is an emerging technology that offers new forms of security protection, however the quantum cloning based attacks against the protocol will play a crucial role in the future [1, 2]. We identify the quantum cloning based attacks in the quantum channel, and find potential and efficient solutions for their detection in secret quantum communications. The incoherent and coherent attacks against quantum cryptography are based on imperfect quantum cloners. The type of quantum cloner used 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 an efficient computational geometric method to analyze the quantum information theoretical impacts of physically allowed attacks on the quantum channel. Our goal is to measure the level of quantum cloning activity on the quantum channel, using fast computational geometric methods.

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 eavesdropper detection on the quantum channel. Finally, we summarize the results.

1.1 Cloning Attacks in Quantum Cryptography

The *incoherent* quantum cloning based attack is the most common eavesdropping strategy [8, 9], thus in our geometrical based security analysis, we study the incoherent attack based attacker model.

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

$|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_N\rangle$ through the quantum channel, an eavesdropper is not interested in copying an arbitrary state, only the possible polarization states of the attacked QKD scheme. 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:

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

for each polarization states of qubit $|\psi_i\rangle$. A photon chosen from a given set of polarization states can only be perfectly cloned, if the polarization angles in the set are distinct, and 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 it impossible an eavesdropper to copy the sender's quantum states [2].

In the *incoherent-type* attacks, Eve imperfectly clones the sender's quantum state using her quantum state probe, 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 described as [6]:

$$\begin{aligned} |E\rangle \otimes |0\rangle &\xrightarrow{U} |E_{0,0}\rangle|0\rangle + |E_{0,1}\rangle|1\rangle, \\ |E\rangle \otimes |1\rangle &\xrightarrow{U} |E_{1,0}\rangle|0\rangle + |E_{1,1}\rangle|1\rangle, \end{aligned} \qquad (2)$$

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 $|E_{i,j}\rangle$.

We measure the *information theoretical* impact of quantum cloning activity in the quantum channel, where Alice's and Bob's side can be modeled by random variables *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 for quantum cryptography is illustrated in Fig. 1.

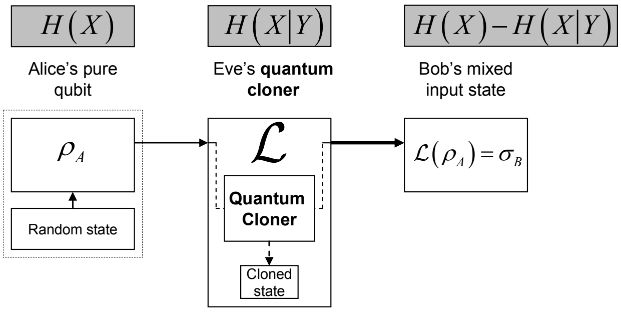

Fig. 1. The analyzed attacker model and the entropies.

We measure in a geometrical representation the information, which can be transmitted in the presence of an eavesdropper on the 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:

$$r^* = max_{\{all\ possible\ x_i\}} H(X) - H(X|Y). \qquad (3)$$

To compute the radius r^* of the smallest informational ball of quantum states, we use the 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].

2 Physically Allowed Transformations

The map of the quantum cloner compresses the Bloch-ball, as an affine map. This affine map must be a complete positive, trace preserving map, which shrinks the Bloch ball along the *x, y* and *z* directions.

The quantum information theoretical analysis of the eavesdropper's cloning machine indicates, how much the eavesdropper clones the sent pure quantum states. In our model, due to eavesdropper activity, the sent pure quantum states become mixed states. Eve's output is represented by a 2×2 density matrix, and her operation is a trace-preserving completely positive (CP) map. We denote Eve's map by $\mathcal{L}$, which is trace preserving if $Tr(\mathcal{L}(\rho)) = Tr(\rho)$ for all density matrices ρ, and positive if the eigenvalues of $\mathcal{L}(\rho)$ are nonnegative, whenever the eigenvalues of ρ are non-negative. Eve's map $\mathcal{L}$ has to be CP, thus $\mathbb{I}_n \otimes \mathcal{L}$ is a positive map for all *n*, where $\mathbb{I}_n$ is the identity map on $n \times n$ matrices [7].

We use a computational geometrical method to analyze the cloning activity on the quantum channel, and we use the Bloch ball representation. The activity of an eavesdropper on a single-qubit in the Bloch sphere representation, can be given by an affine map as

$$\mathbf{r}_E = \mathcal{L}(\mathbf{r}) = A\mathbf{r} + \vec{b}, \tag{4}$$

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

In idealistic UCM and phase-covariant based attacks, the eavesdropper's activity does not change the center of the Bloch ball [11], thus $\vec{b} = 0$, and A is diagonal matrix with entries $\vec{\eta} = (\eta_x, \eta_y, \eta_z)$, which characterizes the tetrahedron $\mathcal{T}$. The entries of matrix A specify the tetrahedron $\mathcal{T}$ in the parameter space of $\{\eta_x, \eta_y, \eta_z\}$, where $\eta \in \mathcal{T}$ if

$$|\eta_x \pm \eta_y| \leq |1 \pm \eta_z|. \tag{5}$$

The tetrahedron $\mathcal{T}$ is the *convex hull* of the points representing $\mathbb{I}$ and the three rotations, thus every transformation corresponding to a point in the tetrahedron $\mathcal{T}$ can be described as a statistical mixture of the $\mathbb{I}, \sigma_x, \sigma_y$ and σ_z extremal transformations [7, 8]. Thus, if all the points in $\mathcal{T}$ can be described by transformations $\mathbb{I}, \sigma_x, \sigma_y$ and σ_z. Fig. 2. illustrates the tetrahedron $\mathcal{T}$.

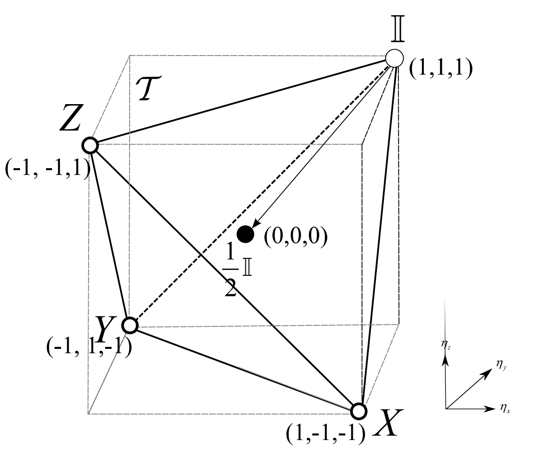

Fig. 2. The tetrahedron representation of physically allowed cloning transformations.

The vertices of tetrahedron $\mathcal{T}$ represent the $\mathbb{I}, \sigma_x, \sigma_y$ and σ_z Pauli-transformations, where $\mathbb{I}$ is the identity transformation, and $\sigma_x, \sigma_y, \sigma_z$ are rotations by π about the *x, y* and *z* axes.

2.1 Geometry of Quantum Cloning Based Eavesdropping

The quantum cloner map compresses the Bloch-ball, as an affine map. This affine map must be a complete positive, trace preserving map, which shrinks the Bloch ball along the *x, y* and *z* directions [2]. The vertices of tetrahedron $\mathcal{T}$ correspond with the four extremal maps which can be described as

$$\rho \to \rho' = \sum_{j=0}^{3} \varepsilon_j A_j \rho A_j^{\dagger}, \tag{6}$$

where A_0 is the identity matrix $\mathbb{I}$, and $j = 1,2,3$ we have $A_j = \sigma_j$ and $\varepsilon_0 + \varepsilon_1 + \varepsilon_2 + \varepsilon_3 = 1$. The general transformation $\mathcal{L}$ of Eve's quantum cloner can be described as a convex sum of these maps as

$$\begin{aligned} &\mathcal{L}(\rho(x,y,z)) \\ &= \varepsilon_1 \sigma_1 \rho \sigma_1 + \varepsilon_2 \sigma_2 \rho \sigma_2 \\ &+ \varepsilon_3 \sigma_3 \rho \sigma_3 + (1 - \varepsilon_1 - \varepsilon_2 - \varepsilon_3)\rho, \end{aligned} \tag{7}$$

where $\varepsilon_1, \varepsilon_2$ and ε_3 are non-negative parameters, $\sigma_x, \sigma_y, \sigma_z$ are the Pauli-transformations, and $\mathbb{I} = (1 - \varepsilon_1 - \varepsilon_2 - \varepsilon_3)$ the identity transformation.

The vertices of $\mathcal{T}$ represent a unitary map for which only one operator is required in the operator sum representation, while the edges of $\mathcal{T}$ represent the two operator maps, and the faces of $\mathcal{T}$ represents the maps with three operators. The points inside $\mathcal{T}$ require all the four operators [17, 18].

2.2 Attacker Model for BB84 and Six State Protocol

In quantum cryptography, the most effective eavesdropping attacks use quantum cloning machines [7, 8, 9]. However, an eavesdropper can not measure the state $|\psi\rangle$ of a single quantum bit, since the result of that 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]. The process of cloning pure states can be generalized as

$$|\psi\rangle_a \otimes |\Sigma\rangle_b \otimes |Q\rangle_x \to |\Psi\rangle_{abc}, \tag{8}$$

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].

As Wooters and Zurek showed, an unknown quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ cannot be cloned perfectly [7], however it has subsequently been shown, that an unknown quantum state can be cloned approximately [2, 8, 9]. 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 effect of the eavesdropper's quantum cloner simply shrinks the Bloch ball $\mathcal{B}$, with given probability *p*. The general model of the eavesdropper's cloning machine is shown in Fig. 3.

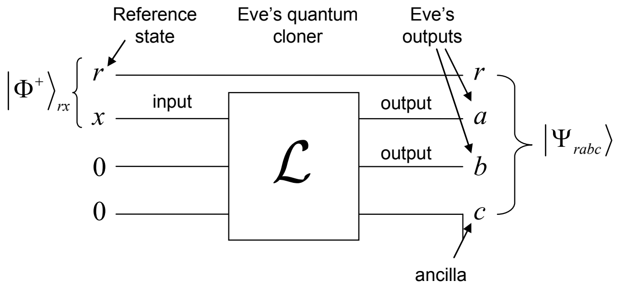

Fig. 3. The general model of Eve's quantum cloner.

The input qubit state is denoted by *x*, which is initially in an entangled state with a reference qubit *r*, denoted by Bell state $|\Phi^{+}\rangle_{rx}$.

After the cloning transformation, the overall system consists of the three outputs and the reference quantum state, thus output state $|\Psi_{rabc}\rangle$ can be written as a superposition of double Bell states [12, 13]:

$$|\Psi_{ra,bc}\rangle = v|\Phi^{+}\rangle\langle\Phi^{+}| + z|\Phi^{-}\rangle\langle\Phi^{-}| + x|\Psi^{+}\rangle\langle\Psi^{+}| + y|\Psi^{-}\rangle\langle\Psi^{-}|, \tag{9}$$

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 $|v|^2 = 1 - p$.

The 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* $\mathcal{E}$, and we denote the coordinates [8] of the ellipsoid $\mathcal{E}$ by $(x_{\mathcal{E}}, y_{\mathcal{E}}, z_{\mathcal{E}})$. As we will see in Section 5, the ellipsoid $\mathcal{E}$ has polar radius $x_{\mathcal{E}} = \frac{1}{2}$, while the equatorial radius is $z_{\mathcal{E}} = 1$ [8, 10].

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].

2.3 Cloning Machine Based Attacks

Eve has a quantum cloner machine, and she interacts with the quantum channel connecting two the legitimate users Alice and Bob. The effect of the eavesdropper's symmetric quantum cloner simply shrinks the Bloch ball $\mathcal{B}$, with given probability *p*.

In the *BB84* protocol [7], Eve uses phase-covariant cloning machine, thus Eve clones only equatorial states:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\varphi}|1\rangle\right). \tag{10}$$

In the *Six-state* protocol Eve considers universal cloning [7], and clones all the states:

$$|\psi\rangle = \left\{|0\rangle, |1\rangle, \frac{1}{\sqrt{2}}\left(|0\rangle \pm |1\rangle\right), \frac{1}{\sqrt{2}}\left(|0\rangle \pm i|1\rangle\right)\right\}. \tag{11}$$

Using the *incoherent*-type cloning based attack, Eve applies the same unitary transformation to each sent quantum state $|\psi(\theta)\rangle$.

Eve does not introduce correlation among the copies, and she measures her state after she cloned it [8]. Alice, Bob and Eve immediately measure their quantum states, since the parties have no ability to store the qubits.

2.3.1 Universal Cloning

If Eve uses a *universal* quantum cloner, then the value of parameter F_{Eve} will be independent of input quantum state $|\psi\rangle$. The quantum cloning transformation optimal [8, 9], if $\eta = \frac{2}{3}$, hence the maximal fidelity of optimal universal cloning is $F_{Eve} = \frac{5}{6}$, and the maximal radius r_{Eve}^{UCM} is

$$r_{Eve}^{UCM} = \frac{2}{3}. \tag{12}$$

The quantum information theoretical radius can be defined as

$$r_{Eve}^{*UCM} = 1 - \mathsf{S}\left(r_{Eve}^{UCM}\right), \tag{13}$$

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

Universal cloning has direct applications to eavesdropping strategies in *Six-state* quantum cryptography. The map $\mathcal{L}$ of UCM cloner based symmetric incoherent attack for the Six-state protocol on pure input state $|\psi\rangle$, can be given by the following completely positive map:

$$\begin{aligned}\mathcal{L} &= \left(1-\left(\frac{4p}{3}\right)\right)|\psi\rangle\langle\psi| + 2\left(\frac{2p}{3}\right)\mathbb{I} \\ &= \left(\frac{2}{3}\right)|\psi\rangle\langle\psi| + \left(\frac{1}{3}\right)\frac{\mathbb{I}}{2},\end{aligned} \tag{14}$$

where $\mathbb{I}$ is the identity transformation. In Fig. 4. we show the quantum cloner based attacker model for the Six-state protocol.

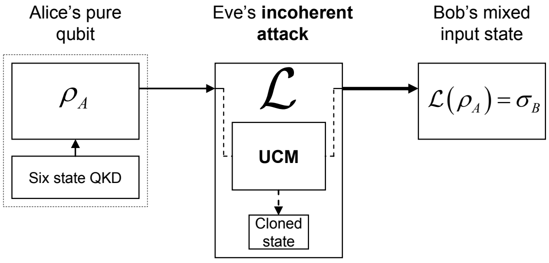

Fig. 4. The UCM cloner based attacker model for the Six-state protocol.

In the UCM based attacker model, Eve has a *state-independent* quantum cloner, where the probabilities are $p_x = p_y = p_z = \frac{p}{3}$, thus $p_x = p_y = p_z = \frac{1}{12}$.

2.3.2 Phase-covariant Cloning

The best-known example of a state-dependent quantum cloning machine is the *phase-covariant* cloning machine [8, 11]. The phase-covariant cloning machines have a remarkable application in quantum cryptography, since they are used in the optimal strategy for eavesdropping [8, 9, 10].

In the Four-state (BB84) quantum cryptography protocol, the optimal eavesdropping attack is done by a phase-covariant cloning machine, which clones the *x* equator. The importance of equatorial qubits lies in the fact that Four-state quantum cryptography requires these states rather than the states that span the whole Bloch sphere [9].

In phase-covariant cloning, the cloning transformations were restricted for pure input states of $|\psi_\phi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\phi}|1\rangle\right)$ form, 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 cloner [9] can clone arbitrary equatorial qubits, and the cloner maintains the quality of the copies for all equatorial qubits [16, 17].

The reduced density operator of the copies at the output can be expressed as [9]

$$\begin{aligned}\rho^{(out)} &= \left(\frac{1}{2}+\sqrt{\frac{1}{8}}\right)|\psi_\phi\rangle\langle\psi_\phi| \\ &+ \left(\frac{1}{2}-\sqrt{\frac{1}{8}}\right)|\psi_{\phi,\perp}\rangle\langle\psi_{\phi,\perp}|,\end{aligned} \tag{15}$$

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

$$F_{1\to 2}^{phasecov.} = \frac{1}{2} + \sqrt{\frac{1}{8}} \approx 0.8535. \tag{16}$$

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

$$r_{Eve}^{phasecov.} = 2\sqrt{\frac{1}{8}}. \tag{17}$$

The quantum information theoretical radius $r_{Eve}^{*\,phasecov.}$ of the phase-covariant cloner can be defined as

$$r_{Eve}^{*\,phasecov.} = 1 - \mathsf{S}\left(r_{Eve}^{phasecov.}\right), \tag{18}$$

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

The map $\mathcal{L}$ of the phase-covariant cloner based attack for BB84 protocol on input state $|\psi\rangle$, can be given by the following completely positive map:

$$\begin{aligned}&\mathcal{L} = (1-3p/2)|\psi\rangle\langle\psi| \\ &+ (p/2)\sigma_y|\psi_\perp\rangle\langle\psi_\perp|\sigma_y + p\frac{\mathbb{I}}{2} = \\ &2\sqrt{\frac{1}{8}}|\psi\rangle\langle\psi| + \frac{1}{2}\left(\frac{2}{3}-\frac{4}{3\sqrt{8}}\right)\sigma_y|\psi_\perp\rangle\langle\psi_\perp|\sigma_y \\ &+ \left(\frac{2}{3}-\frac{4}{3\sqrt{8}}\right)\frac{\mathbb{I}}{2},\end{aligned} \tag{19}$$

with $p_x = p_z = \frac{p}{2}$, $p_y = 0$, where $p = \frac{2}{3} - \frac{4}{3\sqrt{8}}$.

In Fig. 5. we illustrated the quantum cloner based attacker model for the BB84 protocol.

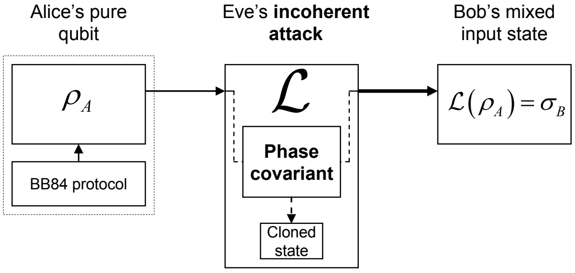

Fig. 5. The phase-covariant cloner based attacker model for the BB84 protocol.

The optimal cloning transformation for the BB84 states can be written as follows [8, 9]:

$$\begin{aligned} U|0\rangle|0\rangle|X\rangle &= \left(\frac{1}{2}+\sqrt{\frac{1}{8}}\right)|00\rangle|0\rangle \\ &+\sqrt{\frac{1}{8}}\left(|01\rangle+|10\rangle\right)|1\rangle+\left(\frac{1}{2}-\sqrt{\frac{1}{8}}\right)|11\rangle|0\rangle, \\ U|1\rangle|0\rangle|X\rangle &= \left(\frac{1}{2}+\sqrt{\frac{1}{8}}\right)|11\rangle|1\rangle \\ &+\sqrt{\frac{1}{8}}\left(|10\rangle+|01\rangle\right)|0\rangle+\left(\frac{1}{2}-\sqrt{\frac{1}{8}}\right)|00\rangle|1\rangle. \end{aligned} \tag{20}$$

The phase-covariant quantum cloning transformation produces *two copies* of the *equatorial* qubit with optimal fidelity.

3 Geometrical Description of Cloning Attacks

Using the radius vector $\mathbf{r}=(x,y,z)$ of the sent pure qubit, the radius vector $\mathbf{r}_E=(x^*,y^*,z^*)$ of the cloned quantum state is given by $\mathbf{r}\to\mathbf{r}_E$ as

$$r^i \to r_E^i = \sum_{j=x,y,z} M_{ij}r^j + C_j, \tag{21}$$

where M_{ij} denotes the components of a 3×3 matrix *M*, and C_j are the three components of a constant real column vector *C*. Eve's cloning transformation operator $\mathcal{L}$ on the sent pure quantum state ρ_A, in the symmetric incoherent attack with BB84 and with a Six-state protocol, can be described as

$$\mathcal{L}(\rho_A)=\sigma_B. \tag{22}$$

The effect of cloning transformation $\mathcal{L}(\rho_A)$ can be given by the affine map $r_E^i = \sum_{j=x,y,z} M_{ij}r^j + C_j$, where r^j is the *j*-th component of Alice's radius vector $\mathbf{r}=(x,y,z)$, and M_{ij} are the nine components of the 3×3 real matrix *M*, while C_j is the *j*-th element of column vector $\vec{C}=0$, which is given by

$$\vec{C}=-\lambda\begin{pmatrix}\sin\zeta\cos\mu\sin\beta\sin\delta \\ \sin\zeta\sin\mu\sin\alpha\sin\beta \\ \cos\zeta\sin\alpha\sin\delta\end{pmatrix}=\begin{pmatrix}0\\0\\0\end{pmatrix}. \tag{23}$$

According to matrix *M*, Eve's quantum cloner maps the cloned state onto a *maximally mixed* state, if any parameter in (α,β,δ) takes the value $\frac{\pi}{2}$. Thus, the effect of Eve's cloning transformation can be described by the affine map [7, 8]:

$$r_E^i = \sum_{j=x,y,z} M_{ij}^* r^j. \tag{24}$$

In a geometrical representation, Eve's quantum cloning transformation $\mathcal{L}$ maps the Bloch ball onto a compressed Bloch ball [7, 8], with radius $r_E<1$. The matrix *M* contains a combination of rotations and contractions of the vectors on the Bloch sphere, while the vector *C* corresponds to a *shift* in the origin of the Bloch sphere.

Eve's UCM-based attack cloning transformation in the Six-state protocol can be described by the radius vector r_E^i, where matrix $M=M_{UCM}^*$ can be expressed as:

$$M_{UCM}^* = \begin{pmatrix}\cos\beta\cos\delta & 0 & 0 \\ 0 & \cos\alpha\cos\beta & 0 \\ 0 & 0 & \cos\alpha\cos\delta\end{pmatrix}, \tag{25}$$

where the parameters (α,β,δ) are the free parameters of the quantum cloning transformation [8, 10, 11].

In the BB84 protocol, the phase-covariant cloning-based attack can be described with parameters $\varepsilon_0=\kappa, \varepsilon_1=\varepsilon_3=\frac{(1-\kappa)}{2}$, $\varepsilon_3=0$ and by matrix $M_{phasecov.}^*$ as:

$$M_{phasecov.}^* = \begin{pmatrix}\varepsilon_0+\varepsilon_1-\varepsilon_2-\varepsilon_3 & 0 & 0 \\ 0 & \varepsilon_0-\varepsilon_1+\varepsilon_2-\varepsilon_3 & 0 \\ 0 & 0 & \varepsilon_0-\varepsilon_1-\varepsilon_2+\varepsilon_3\end{pmatrix} = \begin{pmatrix}\kappa & 0 & 0 \\ 0 & 2\kappa-1 & 0 \\ 0 & 0 & \kappa\end{pmatrix},$$

where $0\le\kappa\le 1$. The affine transformation of this map can be described by matrix $M_{\mathcal{T}}$, where $\mathcal{T}$ represents the tetrahedron $\mathcal{T}$:

$$M_{\mathcal{T}} = \begin{pmatrix}\varepsilon_0+\varepsilon_1-\varepsilon_2-\varepsilon_3 & 0 & 0 \\ 0 & \varepsilon_0-\varepsilon_1+\varepsilon_2-\varepsilon_3 & 0 \\ 0 & 0 & \varepsilon_0-\varepsilon_1-\varepsilon_2+\varepsilon_3\end{pmatrix} = \begin{pmatrix}\eta_x & 0 & 0 \\ 0 & \eta_y & 0 \\ 0 & 0 & \eta_z\end{pmatrix}.$$

The diagonal entries of the matrix take values such that the effect of Eve's quantum cloning transformation can be represented geometrically by a tetrahedron, as we have defined it. In this geometrical representation, each point of (η_x, η_y, η_z) which lies *inside* $\mathcal{T}$ is an allowed set of diagonal elements for the affine transformation of the quantum cloner defined by matrix *M*.

3.1 Geometrical Representation of Incoherent Attacks in QKD Protocols

Using the tetrahedron approach, Eve's cloning activity can be described by $\vec{\eta} = (\eta_x, \eta_y, \eta_z)$. In the BB84 protocol with a phase-covariant cloner, Eve has to minimize η_y, with

$$(\eta_x = \eta_z) = \eta . \tag{26}$$

In the Six-state protocol, Eve uses the UCM transformation which can be described by

$$(\eta_x = \eta_y = \eta_z) = \eta . \tag{27}$$

The probability that Alice and Bob choose the same basis but get a different bit is *D*, while the probability that they get the same bit in the same basis is *F*. The disturbance *D* can be given for any basis *b* by

$${}_b\langle E_{01} | E_{01} \rangle_b = {}_b \langle E_{10} | E_{10} \rangle_b = \frac{1-\eta}{2} = D . \tag{28}$$

The fidelity *F* of the cloner is [10]

$${}_b\langle E_{00} | E_{00} \rangle_b = {}_b \langle E_{11} | E_{11} \rangle_b = \frac{1+\eta}{2} = F = 1 - D . \tag{29}$$

In the BB84 protocol with a phase-covariant cloner, the fidelity of the cloning transformation is

$${}_b\langle E_{00} | E_{11} \rangle_b = {}_b \langle E_{11} | E_{00} \rangle_b = \frac{\eta + \eta_y}{2}, \tag{30}$$

while in the Six-state protocol with UCM, we have

$${}_b\langle E_{00} | E_{11} \rangle_b = {}_b \langle E_{11} | E_{00} \rangle_b = \eta. \tag{31}$$

If Alice and Bob share the same basis and same bit, and Eve guesses correctly the value of the shared bit, Eve has to guess whether her probe is in state $\frac{1}{F} | E_{00} \rangle_{b\,b} \langle E_{00} |$ or $\frac{1}{F} | E_{11} \rangle_{b\,b} \langle E_{11} |$. If Eve uses an optimal measurement to guess this bit value, her success probability [11] p_c is

$$p_c = \frac{1}{2} + \frac{1}{2}\sqrt{1 - \frac{1}{F} \left| {}_b\langle E_{00} | E_{11} \rangle_b \right|^2} . \tag{32}$$

Eve has to maximize p_c given an allowed disturbance level with $\eta \geq \eta_{\min}$ and a maximum allowed disturbance given by $\frac{1-\eta_{\min}}{2} = D_{\max}$. To reduce $\frac{1}{F} \left| {}_b\langle E_{00} | E_{11} \rangle_b \right|^2$, Eve has to minimize $\left| {}_b\langle E_{00} | E_{11} \rangle_b \right|$, and in the phase-covariant cloner-based attack, this minimum can be reached for

$$\vec{\eta} = (\eta_{\min}, 2\eta_{\min} - 1, \eta_{\min}) . \tag{33}$$

In the Six-state protocol, this minimum can be reached for

$$\vec{\eta} = (\eta_{\min}, \eta_{\min}, \eta_{\min}) . \tag{34}$$

In the next sections we will show the tetrahedron interpretation of cloning-based attacks and their physically allowed effects in the BB84 and Six-state protocols.

3.1.1 Modeling Physically Allowed Attacks - Six-State Protocol

The optimal universal quantum cloning machine-based symmetric incoherent attack in the Six-state quantum cryptography protocol can be represented as a *reduced* tetrahedron $\mathcal{T}^*$ formed by matrix M^*_{UCM}.

The vertices of the original tetrahedron $\mathcal{T}$ correspond to a single operator map, the edges are two operator maps, while the four faces represent all three operator maps [8, 9]. The points in the interior of the tetrahedron $\mathcal{T}$ are all four operator maps of

$$\rho \to \rho' = \sum_{j=0}^{3} \varepsilon_j A_j \rho A_j^{\dagger}. \tag{35}$$

In Fig. 6, we show the tetrahedron representation of the optimal universal quantum cloning machine-based attack in the *Six-state* quantum cryptography protocol.

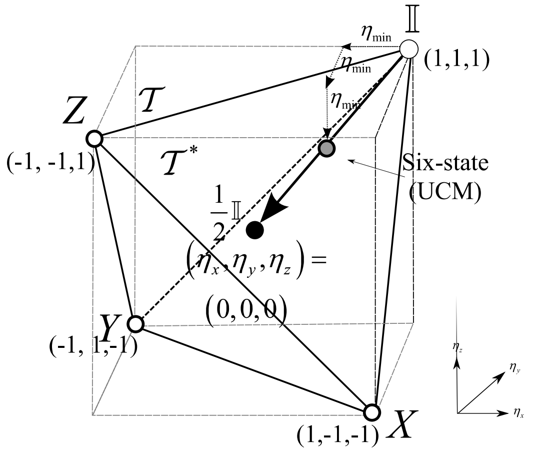

Fig. 6. The optimal universal quantum cloning machine-based attack in the Six-state quantum cryptography protocol.

The cloning transformation can be represented in the reduced tetrahedron $\mathcal{T}^*$ formed by M^*_{UCM}, on

the line between the identity transformation and the maximally mixed state map [15, 16].
Using this result, the affine transformation of Eve's quantum cloning transformation is given by $M_{\mathcal{T}}$, with conditions $\eta_x \geq \eta_y \eta_z$, $\eta_y \geq \eta_z \eta_x$, and $\eta_z \geq \eta_x \eta_y$, where $\eta_x = \cos\delta \cos\beta$, $\eta_y = \cos\beta \cos\alpha$ and $\eta_z = \cos\alpha \cos\delta$. The three diagonal entries of $M_{\mathcal{T}}$ have to ensure the complete positivity of the map, thus the allowed region in the space of η_x, η_y and η_z forms a tetrahedron $\mathcal{T}$ with vertices at $(1,1,1)$, $(1,-1,-1)$, $(-1,1,-1)$ and $(-1,-1,-1)$.

Using tetrahedron $\mathcal{T}$ to represent matrix $M_{\mathcal{T}}$, only the vertices and *edges* of the tetrahedron are touched, and each point (η_x, η_y, η_z) which lies *inside* $\mathcal{T}$ is an allowed set, while no point on the face or any face is contained.

The reduced tetrahedron $\mathcal{T}^*$ can be visualized as the tetrahedron $\mathcal{T}$ with each face of the tetrahedron scooped out and of depth extending all the way to the centroid. In a graphical representation of $\mathcal{T}^*$, all the vertices and edges of $\mathcal{T}$ are contained, while no other point on any face is contained.

3.1.2 BB84 Protocol

The *phase-covariant* quantum cloning-based attack against BB84 cannot be modeled by the reduced tetrahedron $\mathcal{T}^*$, formed by matrix M^*_{UCM}. In the tetrahedron representation, the phase-covariant cloner-based symmetric incoherent attack on BB84 can be represented on the face of the tetrahedron $\mathcal{T}$ formed by $M^*_{phasecov.}$.

The phase-covariant based attack on BB84 can be modeled geometrically on the line between the identity transformation and the mid-point of the edge lying between points from the *Z* and *X*-transformations.

We cannot use tetrahedron $\mathcal{T}^*$ to describe the eavesdropper cloning transformation $M^*_{phasecov}$ in BB84, because the quantum operators removed from $\mathcal{T}$ lie on the faces of $\mathcal{T}$.

The phase-covariant quantum cloning-based attack against BB84 in the tetrahedron representation is illustrated in Fig. 7.

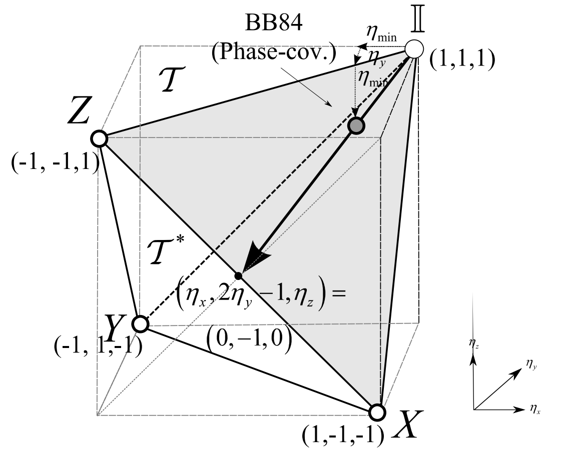

Fig. 7. The phase-covariant quantum cloning-based attack against BB84 in the tetrahedron representation.

The points removed from $\mathcal{T}$ are required to describe the cloning transformation $M^*_{phasecov.}$, thus the reduced tetrahedron $\mathcal{T}^*$ formed by M^*_{UCM} cannot describe all possible outcomes.

4 Proposed Information Theoretical Model for Quantum Cloning Detection

In our security analysis, the distances between quantum states are 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 is given by the von Neumann entropy $\mathsf{S}(\rho)$, which is a generalization of classical entropy to quantum states [2, 3]. The entropy of quantum states can be given in the following way:

$$\mathsf{S}(\rho) = -Tr(\rho \log \rho). \tag{36}$$

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 $\mathbf{F}(\rho)$:

$$\mathbf{F}(\rho) = -\mathsf{S}(\rho) = Tr(\rho \log \rho). \tag{37}$$

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

$$D(\rho \| \sigma) = \mathbf{F}(\rho) - \mathbf{F}(\sigma) - \langle \rho - \sigma, \nabla \mathbf{F}(\sigma) \rangle, \tag{38}$$

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

In Fig. 8, we visualize the quantum informational distance, $D(\rho \| \sigma)$, as the vertical distance between the generator function $\mathbf{F}$ and $H(\sigma)$, the hyperplane tangent to $\mathbf{F}$ at σ. The intersection point at quantum state ρ on $H(\sigma)$ is denoted by $H_\sigma(\rho)$.

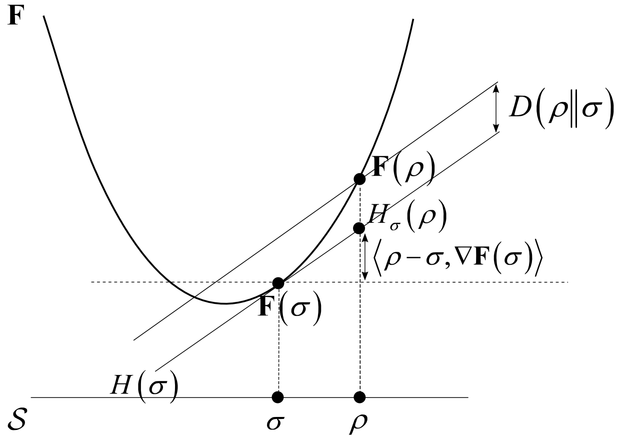

Fig. 8. Visualizing the generator function as negative von Neumann entropy.

The quantum informational distance is not symmetric, nor does it satisfy the triangular inequality of metrics.

The spherical Delaunay triangulation between *pure* states and between pure and mixed states can be simply obtained as the 3D Euclidean Delaunay tessellation restricted to the Bloch sphere [12, 13].

4.1 Quantum Relative Entropy Between Mixed Quantum States

The quantum relative entropy of a 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

$$D(\rho\|\sigma)=\frac{1}{2}\log\frac{1}{4}\left(1-r_\rho{}^2\right)+\frac{1}{2}r_\rho\log\frac{(1+r_\rho)}{(1-r_\rho)}$$
$$-\frac{1}{2}\log\frac{1}{4}\left(1-r_\sigma{}^2\right)-\frac{1}{2r_\sigma}\log\frac{(1+r_\sigma)}{(1-r_\sigma)}\langle\rho,\sigma\rangle, \quad (39)$$

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 relative entropy can be expressed as

$$D(\rho\|\sigma)=\frac{1}{2}\log\frac{1}{4}\left(1-r_\rho{}^2\right)$$
$$+\frac{1}{2}r_\rho\log\frac{(1+r_\rho)}{(1-r_\rho)}-\frac{1}{2}\log\frac{1}{4}. \quad (40)$$

The quantum relative entropy between two mixed quantum states depends on the lengths of their Bloch vectors and the angle θ between them, as illustrated in Fig. 9.

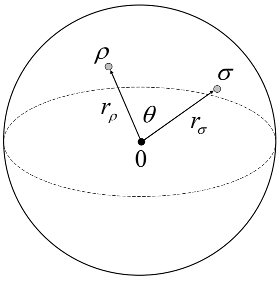

Fig. 9. The quantum relative entropy depends on the lengths of the vectors and the angle between them.

In the proposed Delaunay triangulation method, we apply quantum relative entropy as a distance measure only for mixed states, since the Delaunay triangulation of pure states is identical to the conventional spherical Delaunay diagram [1].

4.2 Geometrical Background

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

$$vo(\rho)=\left\{x\middle|d(x,\rho_i)\leq d(x,\rho_j)\in\mathcal{S}\{\rho\}\right\}, \quad (41)$$

where $d(\cdot)$ is the distance function. 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. The triangle *t* is said to be Delaunay, when its circumcircle is empty.

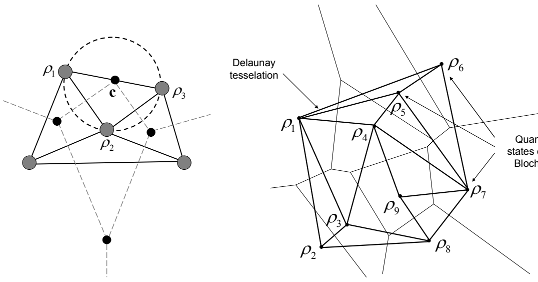

Fig. 10. The triangle of quantum states corresponds to the vertex c (a), and Delaunay tessellation on the Bloch sphere (b).

For an empty circumcircle, the circle passing through the quantum states of a triangle $t\in T$, encloses no other vertex of the set $\mathcal{S}$.

In our security analysis, we use the fact that the Voronoi diagram $vo(\mathcal{S})$ of a set of quantum states

$\mathcal{S}$ and the Delaunay triangulation $Del(\mathcal{S})$ are dual to each other [4].

The quantum Delaunay triangulation of a set of quantum states $\mathcal{S}$ denoted by $Del(\mathcal{S})$ is the geometric dual of quantum Voronoi diagrams $vo(\mathcal{S})$. 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 $Del(\mathcal{S})$, is empty.

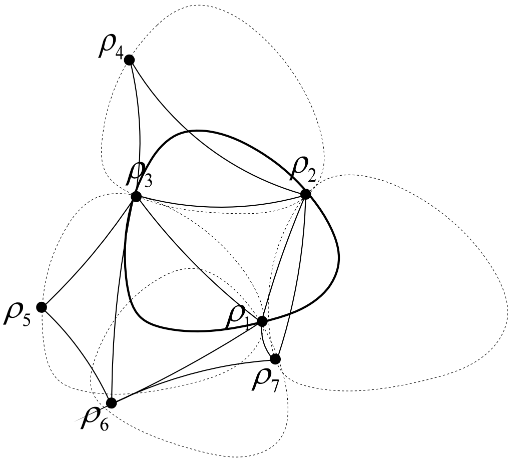

Fig. 11. The empty ball property for quantum Delaunay triangulation.

If we choose a subset χ of at most $d+1$ states in $\mathcal{S}=\{\rho_1,\ldots,\rho_n\}$, then the convex hull of the associated quantum states $\rho_i, i\in\chi$, is a simplex of the quantum triangulation of $\mathcal{S}$, if there exists an empty quantum informational ball passing through the ρ_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 not equal to Euclidean diagrams.

In Fig. 12(a), we illustrate the dual-Delaunay diagram for pure states, with $r_{\rho_1}=r_{\rho_2}=r_{\rho_3}=r_{\rho_4}=1$. The quantum diagram for pure states is equivalent to the ordinary Euclidean diagram.

In Fig. 12(b), we illustrate the first-type and second-type diagrams for mixed states with radii $r_{\rho_{1,2,3,4}}<1$, in Bloch ball representation. The first-type quantum diagram is illustrated by bold lines, the dashed lines show the dual curved second-type diagram.

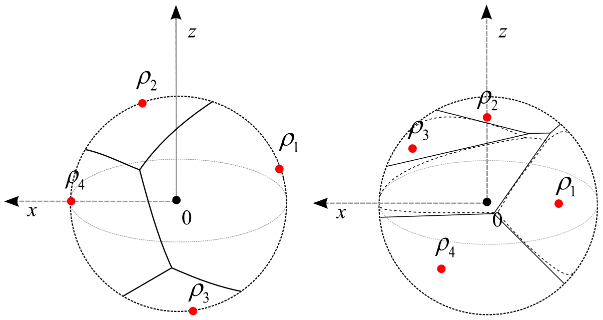

Fig. 12. Dual-Delaunay diagram for pure states (a) and for mixed states (b).

The ordinary quantum Voronoi diagram gives the regions that are nearest to a set of given states. The furthest Voronoi diagrams are the opposite of ordinary Voronoi diagrams. The furthest quantum Voronoi diagrams identify the regions which have the greatest distance from given points.

If we have a classical Voronoi diagram of a set of quantum states $\mathcal{S}=\{\rho_1,\rho_2,\ldots\rho_n\}$, then the cells determine the regions that contain the closest points to the sites. We can define a similar structure for furthest points and such a diagram is called the furthest-point Voronoi diagram [18].

In Fig. 13, we illustrate the difference between classical quantum Voronoi diagrams and furthest quantum Voronoi diagrams for a set of quantum states $\mathcal{S}=\{\rho_1,\rho_2,\rho_3\}$ in the Bloch ball representation. We can conclude that the furthest quantum dual-Delaunay diagram differs from the ordinary Voronoi diagram and has an empty cell.

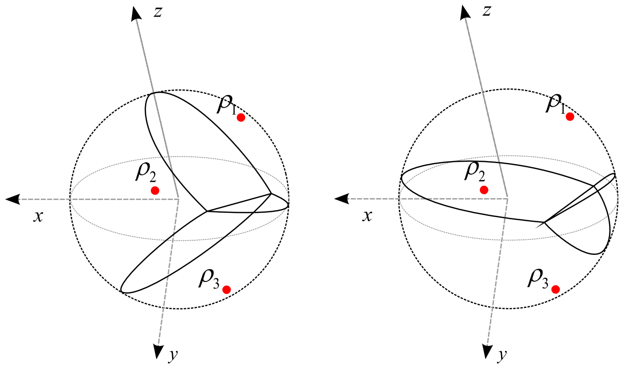

Fig. 13. Comparison of classical quantum Voronoi diagrams and furthest quantum Voronoi diagrams for a set of quantum states in the Bloch ball representation.

In Fig. 14, 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 $\mathcal{S}$ determines the convex hull and the center of the smallest enclosing ball.

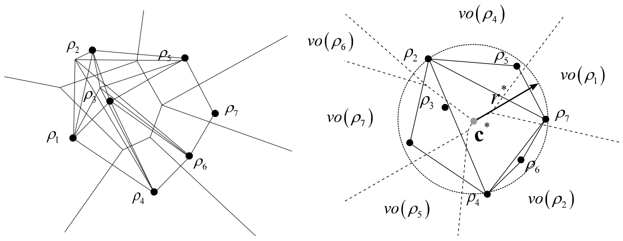

Fig. 14. Comparison of ordinary Delaunay triangulation and furthest Delaunay triangulation.

The quantum diagrams of pure quantum states and of mixed quantum states with equal radii are equivalent to ordinary Euclidean diagrams. The quantum diagrams of mixed states with different radii are equivalent to quantum informational diagrams.

4.3 Computational Geometry in Cloning Detection

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 $\mathbf{c}^*$ of the set $\mathcal{S}$ of quantum states. The set $\mathcal{S}$ of quantum states is denoted by $\mathcal{S}=\{\rho_i\}_{i=1}^{n}$. The distance $d(\cdot,\cdot)$ between any two quantum states of $\mathcal{S}$ is measured by the quantum relative entropy, thus the *minimax* mathematical optimization is applied to quantum relative entropy-based distances to find the center $\mathbf{c}$ of the set $\mathcal{S}$. We denote the quantum relative entropy from $\mathbf{c}$ to the furthest point of $\mathcal{S}$ by

$$d(\mathbf{c},\mathcal{S})=\max_i d(\mathbf{c},\rho_i). \qquad (42)$$

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

$$\mathbf{c}^*=\arg\min_{\mathbf{c}} d(\mathbf{c},\mathcal{S}). \qquad (43)$$

In Fig. 15, we illustrate the circumcenter $\mathbf{c}^*$ of $\mathcal{S}$ for the Euclidean distance and for *quantum relative entropy* [3].

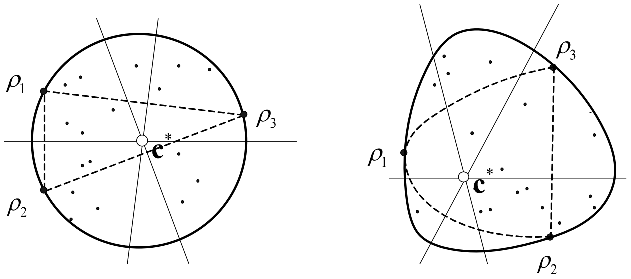

Fig. 15. Circumcenter for Euclidean distance and quantum relative entropy balls.

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^* is equal to the maximum quantum informational distance from the center and can be expressed as:

$$r^*=\min_{\sigma\in\mathcal{S}(\mathbb{C}^2)}\max_{\rho\in\mathcal{S}(\mathbb{C}^2)} D\left(\mathcal{L}(\rho)\middle\|\mathcal{L}(\sigma)\right). \qquad (44)$$

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

$$r^*=1-\mathsf{S}(r_{Bloch}), \qquad (45)$$

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

4.3.1 Laguerre Diagram for Quantum States

We use the Laguerre Delaunay diagram [4, 14, 15] to compute the radius of the smallest enclosing ball. In general, the Laguerre distance for generating points x_i with weight r_i^2, in a Euclidean space is defined by

$$d_L(\rho,x_i)=\left\|\rho-x_i\right\|^2-r_i^2. \qquad (46)$$

The Delaunay diagram for the Laguerre distance is called the Laguerre-Delaunay diagram. For the Laguerre bisector of two three-dimensional Euclidean balls $B(\rho,r_P)$ and $B(\sigma,r_Q)$ centered at quantum states ρ and σ, we can write the equation

$$2\langle x,\sigma-\rho\rangle+\langle\rho,\rho\rangle-\langle\sigma,\sigma\rangle+r_Q^2-r_P^2=0. \qquad (47)$$

In a Euclidean space, the Laguerre distance $d_L(\rho,x_i)$ with weight r_i^2 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 [4].

We show a new method for deriving the 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 $\mathbf{c}$ of the set of smallest enclosing quantum information ball, using *Laguerre* diagrams [5].

Our geometrical-based security analysis has two main steps:

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

4.3.2 Quantum Delaunay Triangulation from Laguerre Diagrams

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

$$d_L^i(x) = \|\rho - x\|^2 - r^2. \quad (48)$$

In Fig. 16, we show the ordinary triangulation of quantum relative entropy-based Voronoi diagram.

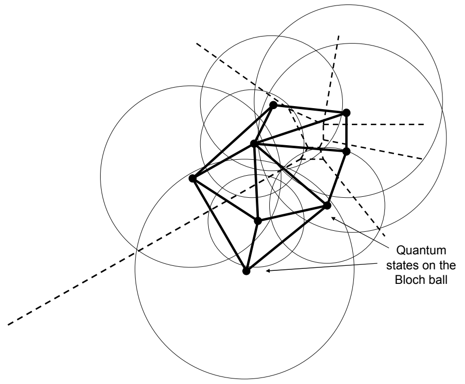

Fig. 16. Regular triangulation on the Bloch ball.

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]

$$\langle x - \rho_i', x - \rho_i' \rangle = \langle \rho_i', \rho_i' \rangle + 2\left(\mathbf{F}(\rho_i') - \langle \rho_i, \rho_i' \rangle\right). \quad (49)$$

The most important result of this equivalence is that we can efficiently construct a quantum relative entropy-based Delaunay triangulation on the Bloch sphere, using fast methods for constructing classical Euclidean Laguerre diagrams [15, 16].

4.4 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 that for the circumcenter $\mathbf{c}$ of the minimax ball [5]

$$d(\mathbf{c}, \mathcal{S}) \leq (1 + \mathcal{E})r, \quad (50)$$

where r is the radius of the smallest enclosing quantum information ball of the set of quantum states $\mathcal{S}$ [5, 9]. The approximating algorithm, for a set of quantum states $S = \{s_1, \ldots, s_n\}$ and circumcenter $\mathbf{c}$, first finds the 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 equation $\max_{x \in b_i} D_F(\mathbf{c}, x_i) = D_F(\mathbf{c}, S_i) + r_i$, we get

$$\begin{aligned} &\max_{i \in \{1,\ldots,n\}} D_F(\mathbf{c}, b_i) \\ &= \max_{i \in \{1,\ldots,n\}} \left(D_F(\mathbf{c}, S_i) + r_i\right). \end{aligned} \quad (51)$$

In Fig. 17, we illustrate the smallest enclosing ball of balls in the quantum space.

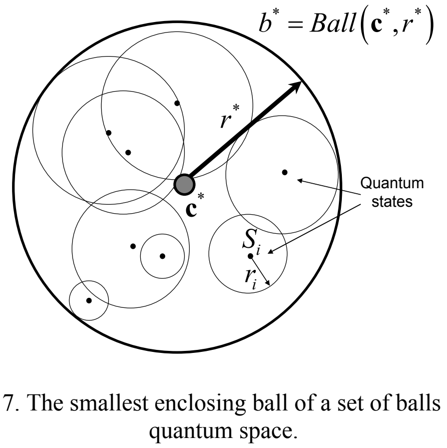

Fig. 17. The smallest enclosing ball of a set of balls in the quantum space.

We denote the set of *n* *d*-dimensional balls by $B = \{b_1, \ldots, b_n\}$, where $b_i = Ball(S_i, r_i)$, S_i is the center of ball b_i and r_i is the radius of the *i*-th ball. The smallest enclosing ball of set $B = \{b_1, \ldots, b_n\}$ is the unique ball $b^* = Ball(\mathbf{c}^*, r^*)$ with minimum radius r^* and center $\mathbf{c}^*$ [6].

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 ball set B can be written as

$$\min_{\mathbf{c}} \mathbf{F}_B(\mathbf{c}), \tag{52}$$

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 can be summarized as:

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

$$r^* = 1 - \mathsf{S}(r_{Bloch}), \tag{53}$$

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

5 Fitting the Smallest Quantum Ball

Geometrically, the smallest quantum informational ball can be computed from the intersection of contours of the quantum relative entropy ball with the ellipsoid of the secret channel, which ellipsoid is generated by the eavesdropper's cloner machine. The maximum length radius $\mathbf{r}_\rho$ can be determined by an iterative algorithm, using the quantum relative entropy as a distance measure.

In Fig. 18(a), the smallest quantum informational ball with radius $r^* = D_{\max}(\mathbf{r}_\rho\|\mathbf{r}_\sigma)$ intersects the channel ellipsoid at magnitude m_ρ of the Bloch vector $\mathbf{r}_\rho$. The Euclidean distance between the origin and center $\mathbf{c}^*$ is denoted by m_σ. Similarly, the Euclidean distance between the origin and state ρ is denoted by m_ρ. In our geometrical iteration algorithm, we would like to determine the location of vector $\mathbf{r}_\sigma$ inside the channel ellipsoid such that, the largest possible contour value $D_{\max}(\mathbf{r}_\rho\|\mathbf{r}_\sigma)$ touches the channel ellipsoid surface and the remainder of the $D_{\max}$ contour surface lies entirely outside the channel ellipsoid. The point on the channel ellipsoid surface is defined as the set of channel output ρ. The vector $\mathbf{r}_\sigma$ is defined in the interior of the ellipsoid, as the convex hull of the channel ellipsoid. To determine the optimal length of the radius, the algorithm moves point σ.

As we move vector $\mathbf{r}_\sigma$ from the optimum position, a larger contour corresponding to the larger value of the quantum relative entropy D will intersect the channel ellipsoid surface, thereby $\max_{\mathbf{r}_\rho} D(\mathbf{r}_\rho\|\mathbf{r}_\sigma)$ will increase. We can conclude that vector $\mathbf{r}_\sigma$ should be adjusted to minimize $\max_{\mathbf{r}_\rho} D(\mathbf{r}_\rho\|\mathbf{r}_\sigma)$, as illustrated in Fig. 18(b).

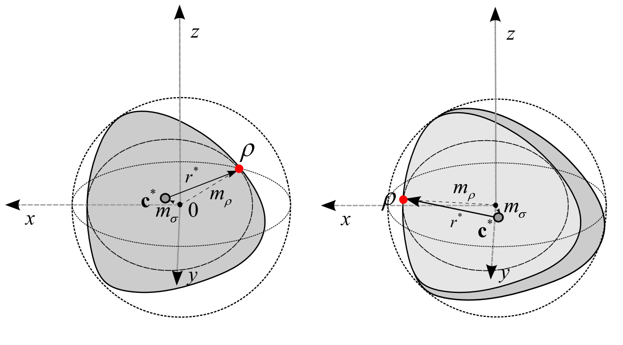

Fig. 18. Intersection of radius of smallest enclosing quantum informational ball and channel ellipsoid (a). The optimal ball is shown in light-grey (b).

The computed radius is equal to the radius of the smallest quantum informational ball, hence the quantum informational radius can be used to derive the fidelity of the eavesdropper's quantum cloner machine. The vector $\mathbf{r}_\sigma$ should be adjusted to minimize the value of $\max_{\mathbf{r}_\rho} D\left(\mathbf{r}_\rho \| \mathbf{r}_\sigma\right)$. To find the optimal value of vector $\mathbf{r}_\sigma$ in our geometrical analysis, we choose a start point for vector $\mathbf{r}_\sigma$ in the interior of the ellipsoid.

In Figure 19(a), we show the initial start point inside the channel ellipsoid chosen by the algorithm. The vector of state σ is denoted by $\mathbf{r}_\sigma$. In the next step, the algorithm determines the set of points to the vector $\mathbf{r}'_\rho$ on the ellipsoid surface most distant from $\mathbf{r}_\sigma$, using the quantum relative entropy as distance measure.

In Figure 19(b), the new state is notated by ρ'.

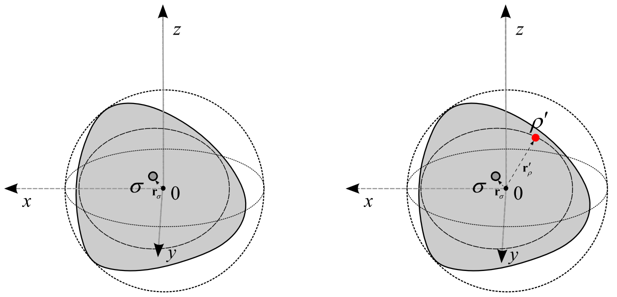

Fig. 19. The algorithm determines the points on the ellipsoid surface most distant from the point, using the quantum relative entropy as distance measure.

The maximum distance between the states can be expressed as $\max_{\mathbf{r}_\rho} D\left(\mathbf{r}'_\rho \| \mathbf{r}_\sigma\right)$. We choose a random Bloch sphere vector from the maximal set of points according to vector $\mathbf{r}'_\rho$. The selected point is denoted by $\mathbf{r}''_\rho$. The algorithm makes a step from $\mathbf{r}_\sigma$ towards the surface point vector $\mathbf{r}''_\rho$ in the Bloch sphere space. In this step, the algorithm updates vector $\mathbf{r}_\sigma$ to

$$\mathbf{r}^*_\sigma = (1-\gamma)\mathbf{r}_\sigma + \gamma\mathbf{r}''_\rho, \tag{54}$$

where γ denotes the size of the step. In Fig. 20(a), the updated state and the vector of the state are denoted by ρ'' and $\mathbf{r}''_\rho$. The center of the quantum informational ball is denoted by $\mathbf{r}^*_\sigma$.

In Fig. 20(b), we illustrate the quantum informational distance between the final center point and the maximal distance state ρ, using the notation $\max_{\mathbf{r}_\rho} D\left(\mathbf{r}_\rho \| \mathbf{r}_\sigma\right)$. Using the updated vector $\mathbf{r}^*_\sigma$, the algorithm continues to loop until $\max_{\mathbf{r}^*_\rho} D\left(\mathbf{r}'_\rho \| \mathbf{r}^*_\sigma\right)$ no longer changes. We conclude that the iteration converges to the optimal $\mathbf{r}_\sigma$, because the algorithm minimizes $\max_{\mathbf{r}_\rho} D\left(\mathbf{r}_\rho \| \mathbf{r}_\sigma\right)$.

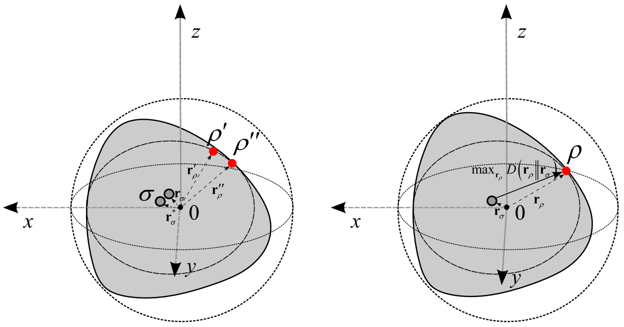

Fig. 20. The algorithm makes a step towards the found surface point vector and updates the vector.

At the end of the iteration process, the radius of the smallest quantum informational ball can be expressed as

$$\min\max_{\mathbf{r}_\rho} D\left(\mathbf{r}_\rho \| \mathbf{r}_\sigma\right). \tag{55}$$

In Fig. 21, we compare the smallest quantum informational ball and the ordinary Euclidean ball.

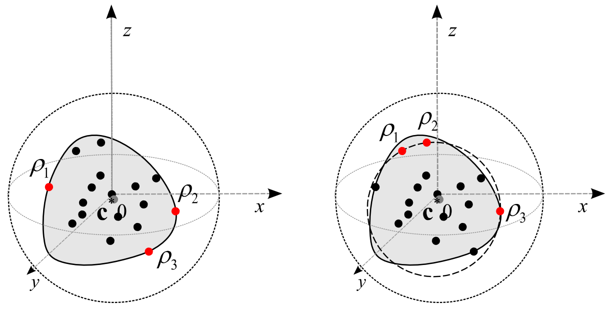

Fig. 21. The maximum distance states of the smallest balls differ for the quantum informational distance and Euclidean distance.

We can conclude that the quantum states ρ_1, ρ_2 and ρ_3, which determine the Euclidean smallest enclosing ball are different from the states of the quantum informational ball.

5.1 Smallest Quantum Informational Ball for UCM-Based Cloning

The UCM cloner-based incoherent attack in the Six-state protocol can be detected if the radius $r_\mathcal{E}$ of imperfect UCM cloning is equal or greater than the radius $r_{\mathcal{E},UCM}$ of the idealistic UCM ball in ellipsoid $\mathcal{E}$ representation, thus

$$r_\mathcal{E} \geq r_{\mathcal{E},UCM} = \sqrt{x_\mathcal{E}{}^2 + y_\mathcal{E}{}^2 + z_\mathcal{E}{}^2} = \sqrt{3\frac{1}{12}} = \frac{1}{2}. \tag{56}$$

This surface is an oblate ellipsoid $\mathcal{E}$ and can be expressed by $\mathcal{E}= x^2+y^2+z^2+xy+xz+yz=\frac{1}{2}$. The ellipsoid $\mathcal{E}\left(x_{\mathcal{E}},y_{\mathcal{E}},z_{\mathcal{E}}\right)$ has polar radius $x_{\mathcal{E}}=\frac{1}{2}$, while the equatorial radius is $z_{\mathcal{E}}=1$. The distance to the origin is $x_{\mathcal{E}}{}^2+y_{\mathcal{E}}{}^2+z_{\mathcal{E}}{}^2=p_x+p_y+p_z$, thus the closest point to the origin is at the pole of the ellipsoid $\mathcal{E}$ and can be expressed as

$$\left(\frac{1}{\sqrt{12}},\frac{1}{\sqrt{12}},\frac{1}{\sqrt{12}}\right). \quad (57)$$

Using the ellipsoid $\mathcal{E}$ representation, we can model the effects of Eve's quantum cloner. The cloning transformation will be detected by Bob, if the point $\left(x_{\mathcal{E}},y_{\mathcal{E}},z_{\mathcal{E}}\right)$ representing the quality of the cloning transformation, lies on or outside the *optimal UCM* ball, represented by ellipsoidal radius $r_{\mathcal{E},UCM}$.

In Fig. 22, we illustrate the radius $r_{\mathcal{E},UCM}$ of the UCM ball and the radius $r_{\mathcal{E}}$ of the corresponding imperfect UCM cloning transformation in the Six-state protocol. The origin of $\mathcal{E}$ represents zero cloning activity in the channel.

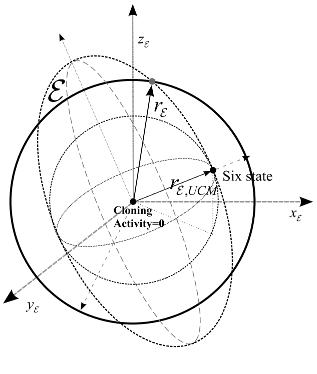

Fig. 22. Comparison of optimal UCM and imperfect universal cloning in Six-state protocol.

In our quantum informational distance-based geometrical security analysis, Bob will detect the quantum cloner, if $r_{\mathcal{E}}\geq r_{\mathcal{E},UCM}$, because in this case we can give the following condition for the radius r^* of his smallest enclosing quantum informational ball:

$$r^*\leq 1-\mathsf{S}\left(1-\frac{4\left(r_{\mathcal{E}}\right)^2}{3}\right)\leq 1-\mathsf{S}\left(1-\frac{4\left(r_{\mathcal{E},UCM}\right)^2}{3}\right), \quad (58)$$

where S is the von Neumann entropy.

In this geometrical representation - if there is no quantum cloner on the quantum channel - then $r_{\mathcal{E}}=0$, thus in this case Bob has a quantum informational ball with radius $r^*=1$.

In Fig. 23, we show the information theoretical radii r^* and r^*_{UCM}. The smallest enclosing quantum ball of the imperfect UCM cloner has radius

$$r^*=1-\mathsf{S}\left(1-\frac{4\left(r_{\mathcal{E}}\right)^2}{3}\right), \quad (59)$$

while the radius of the idealistic UCM-based cloning attack in the Six-state protocol can be expressed as

$$r^*_{UCM}=1-\mathsf{S}\left(1-\frac{4\left(r_{\mathcal{E},UCM}\right)^2}{3}\right). \quad (60)$$

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

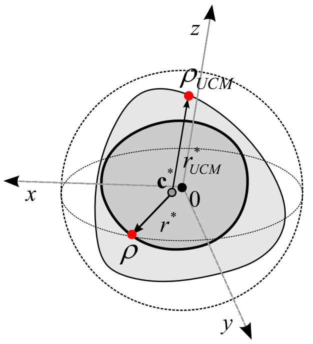

Fig. 23. The smallest enclosing quantum informational ball of optimal and imperfect universal cloner.

We can conclude that, if $r_{\mathcal{E}}\geq r_{\mathcal{E},UCM}$, then $r^*\leq r^*_{UCM}$, hence the informational theoretical radius will be smaller.

5.2 Smallest Quantum Informational Ball for Phase-covariant Based Attack

In the phase-covariant based symmetric incoherent attack in the BB84 quantum cryptography protocol, the cloning activity can be detected by Bob, if the radius $r_{\mathcal{E}}$ of the *imperfect* phase-covariant cloner is equal or greater than the radius $r_{\mathcal{E},phasecov}$ of the phase-covariant ball in the ellipsoid $\mathcal{E}$ representation, $r_{\mathcal{E}}\geq r_{\mathcal{E},phasecov}$.

Using the ellipsoid $\mathcal{E}$ representation, we can model the effects of Eve's phase-covariant quantum cloner-based attack. The imperfect cloning transformation is denoted by point $\left(x_{\mathcal{E}},0,z_{\mathcal{E}}\right)$, which lies on or outside the optimal phase-covariant ball.

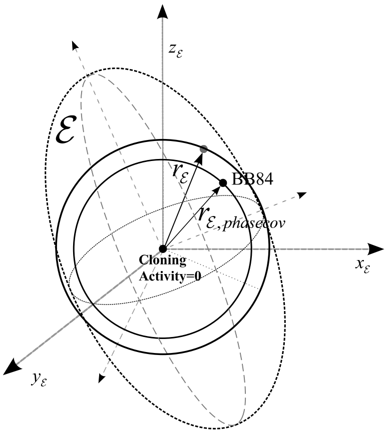

Fig. 24. The ellipsoidal radii for optimal phase-covariant cloning and imperfect cloning activity.

The local coordinate system $\left(x_{\mathcal{E}},0,z_{\mathcal{E}}\right)$ represents the quality of the cloning transformation, and the eavesdropping activity will be detected by Bob, if

$$r_{\mathcal{E}}=\sqrt{x_{\mathcal{E}}{}^{2}+0+z_{\mathcal{E}}{}^{2}}\geq\left(\frac{2}{3}-\frac{4}{3\sqrt{8}}\right). \tag{61}$$

In the quantum cloner-based attack in BB84, Bob will detect the quantum cloner if $r_{\mathcal{E}}\geq r_{\mathcal{E},phasecov}$, where $r_{\mathcal{E}}$ is the radius representing the imperfect phase-covariant cloning attack. In this case, we can give the following condition for the information theoretical radius r^{*} of his smallest quantum informational ball

$$\begin{aligned} r^{*} &\leq 1-\mathsf{S}\left(1-\frac{3\left(r_{\mathcal{E}}\right)^{2}}{2}\right)\\ &\leq 1-\mathsf{S}\left(1-\frac{3\left(r_{\mathcal{E},phasecov}\right)^{2}}{2}\right)=1-\mathsf{S}\left(\frac{1}{2}+\sqrt{\frac{1}{8}}\right), \end{aligned} \tag{62}$$

where S is the von Neumann entropy.

The smallest quantum informational ball with radius r^{*} is shown in grey, the maximal ball of the phase-covariant cloner is shown in light grey. In the figures the information theoretical radius is denoted by r^{*}. The quantum ball of the imperfect phase-covariant cloner is illustrated with radius

$$r^{*}=1-\mathsf{S}\left(1-\frac{3\left(r_{\mathcal{E}}\right)^{2}}{2}\right), \tag{63}$$

the idealistic phase-covariant cloner is denoted by radius

$$r_{phasecov}^{*}=1-\mathsf{S}\left(1-\frac{3\left(r_{\mathcal{E},phasecov}\right)^{2}}{2}\right). \tag{64}$$

In Fig. 25, we compare an idealistic phase-covariant cloner quantum ball and an imperfect phase-covariant cloner quantum ball.

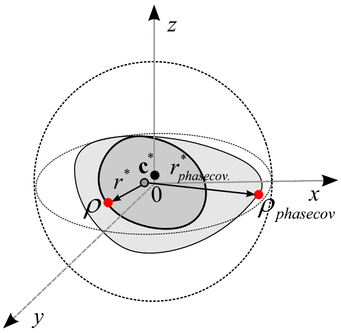

Fig. 25. The smallest enclosing quantum informational ball of optimal and imperfect phase-covariant cloner.

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

5.3 Comparison of UCM and Phase-covariant Based Attacks

In the three-dimensional $\mathcal{E}$ ellipsoid representation, the radius $r_{\mathcal{E},phasecov}$ of the phase-covariant cloner-based attack is smaller than radius $r_{\mathcal{E},UCM}$. For the radius of the UCM and phase-covariant ball in the ellipsoidal $\mathcal{E}$ representation

$$r_{\mathcal{E},phasecov}<r_{\mathcal{E},UCM}, \tag{65}$$

where $r_{\mathcal{E},phasecov}=\sqrt{x_{\mathcal{E}}{}^{2}+y_{\mathcal{E}}{}^{2}+z_{\mathcal{E}}{}^{2}}=\sqrt{\frac{2}{3}-\frac{4}{3\sqrt{8}}}$.

In Fig. 26, we illustrate $r_{\mathcal{E},phasecov}$ and $r_{\mathcal{E},UCM}$ in the three-dimensional ellipsoidal representation.

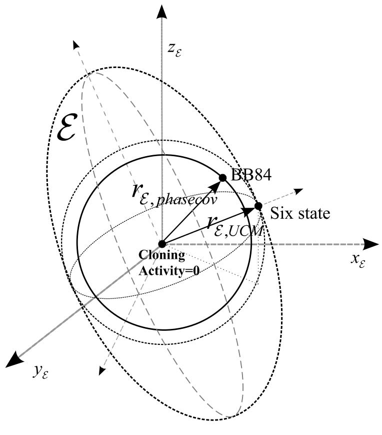

Fig. 26. Comparison of UCM and phase-covariant based attack in ellipsoidal representation.

Using the results derived in Section 3.1, the following connection holds between radii r^*_{UCM} and $r^*_{phasecov}$ of the smallest enclosing quantum informational balls of UCM and phase-covariant cloning-based attack:

$$r^*_{UCM} = 1 - \mathsf{S}\left(1 - \frac{4\left(r_{\mathcal{E},UCM}\right)^2}{3}\right) \leq \qquad (66)$$
$$r^*_{phasecov} = 1 - \mathsf{S}\left(1 - \frac{3\left(r_{\mathcal{E},phasecov}\right)^2}{2}\right).$$

In Fig. 27, we illustrate the radii r^*_{UCM} and $r^*_{phasecov}$ of the smallest enclosing quantum informational ball for a UCM-based attack and for BB84, in the Bloch sphere representation.

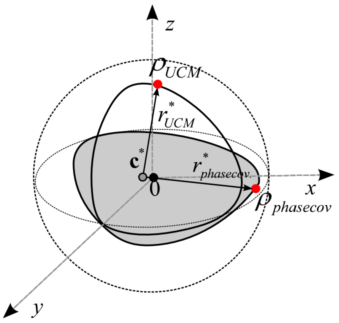

Fig. 27. Comparison of smallest enclosing quantum informational ball of UCM and phase-covariant cloners.

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

6 Applying Our Method to Quantum Cryptography

Using the results derived in Sections 5.1 and 5.2, the quantum channel in the BB84 and Six-state protocols is secure if $r^* > r^*_{phasecov}$. 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.

6.1 BB84 and Phase-covariant Cloning

In this section we illustrate the quantum informational balls for the analyzed quantum cloners. In Fig. 28, we illustrate the dual Delaunay diagram for cloned equatorial states in the BB84 protocol. The sent pure quantum states cloned by Eve's phase-covariant quantum cloner are denoted by ρ_1, ρ_2, ρ_3 and ρ_4.

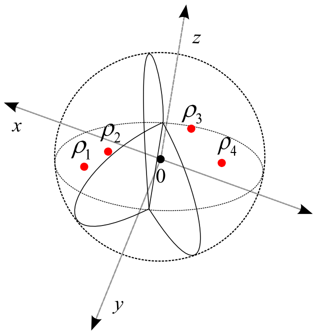

Fig. 28. Dual Delaunay diagram of cloned equatorial states in the BB84 protocol.

Using Delaunay tessellation, we compute the *convex-hull* of the cloned equatorial states ρ_1, ρ_2, ρ_3 and ρ_4. In Fig. 29, we illustrate the convex-hull of cloned states in two- and three-dimensional Bloch ball representations.

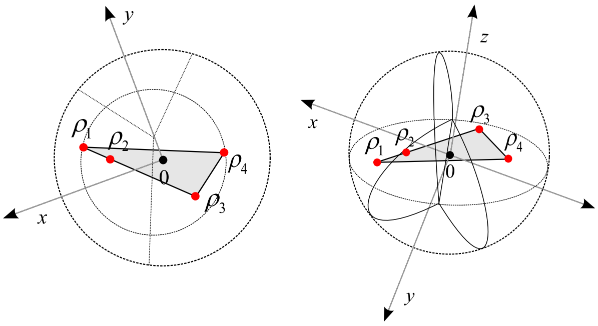

Fig. 29. The convex hull of cloned mixed states. The convex hull computed by Delaunay triangulation.

From the convex set, we can compute the smallest enclosing quantum informational ball $\mathcal{B}^*$ and its radius r^*. In Fig. 30, we have illustrated the Euclidean smallest enclosing ball by the dashed circle, and the quantum relative entropy ball.

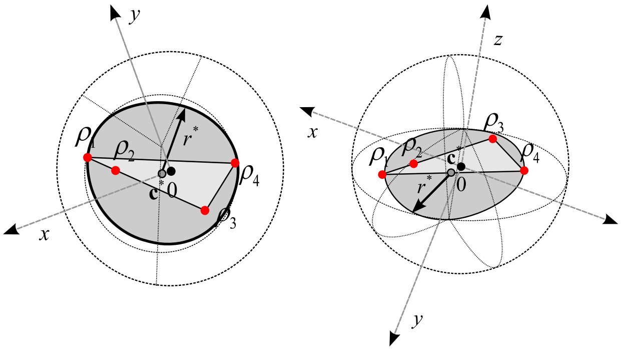

Fig. 30. The smallest enclosing quantum informational balls.

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 $\mathbf{c}^*$.

6.2 Six State Protocol and Universal Cloning

In Fig. 31(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 Fig. 31(b), we have illustrated the smallest quantum informational ball and its radius r^*.

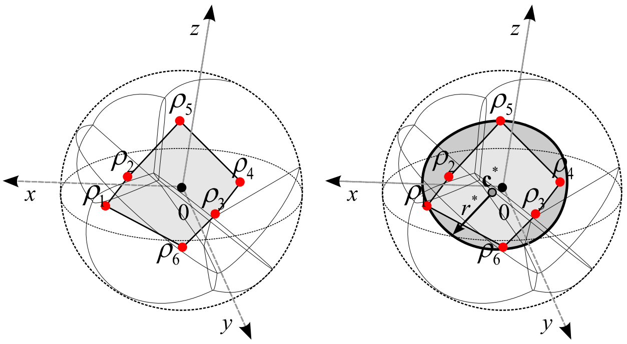

Fig. 31. The convex hull (a) and the smallest quantum ball (b) of cloned mixed states in Six-state protocol.

In Fig. 32, we show an example of a two-dimensional smallest enclosing quantum informational ball, and its informational theoretical radius r^*.

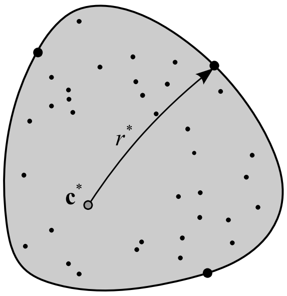

Fig. 32. The smallest enclosing quantum informational ball.

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

7 Optimization

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

$$\mathcal{O}\left(\frac{dn}{\varepsilon^2}\right) = \mathcal{O}\left(\frac{d}{\varepsilon^2}\frac{1}{\varepsilon}\right) = \mathcal{O}\left(\frac{d}{\varepsilon^3}\right), \tag{67}$$

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 a time

$$\mathcal{O}\left(\frac{d}{\varepsilon^2}\right). \tag{68}$$

In this section we improve our method to get a

$$\mathcal{O}\left(\frac{d}{\varepsilon}\right) \tag{69}$$

time, $(1+\varepsilon)$-approximation algorithm in quantum space.

In Fig. 33, we illustrate the improved algorithm on a set of quantum states. The approximate ball has radius r, the enclosing ball has radius $r+\delta$. The approximate center $\mathbf{c}$ is denoted in black, the core-set are denoted by grey circles. The optimal radius between the center $\mathbf{c}$ and the farthest quantum state is denoted by r^* [9].

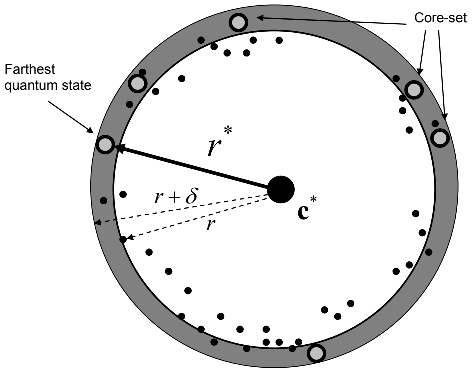

Fig. 33. The approximate (light) and enclosing quantum ball (darker).

In the proposed algorithm, the optimal radius is between $r \le r^* \le r+\delta$, and the process 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.

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

7.1 Rate of Convergence

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 Fig. 34. The x-axis represents the number of center updates to find the center of the smallest enclosing quantum informational ball, the y-axis represents the quantum informational distance between the found center $\mathbf{c}$ and the optimal center $\mathbf{c}^*$.

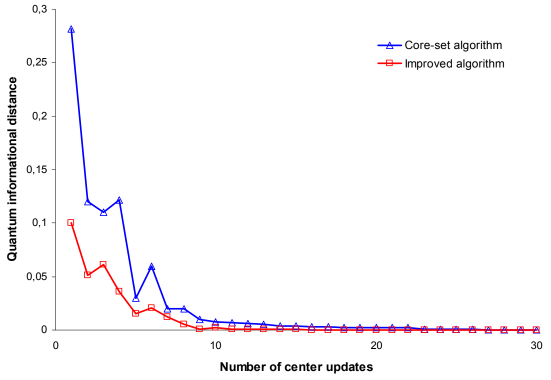

Fig. 34. The rate of converge of approximation algorithms.

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

8 Conclusions

In quantum cryptography, an eavesdropper cannot clone the sent qubits perfectly, however the best eavesdropping attacks are based on imperfect quantum cloners. We have proposed a fundamentally new approach to computing 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 eavesdropper's cloning activity, and the impacts of her cloning transformation can be measured geometrically. Our method is based on Laguerre diagrams with quantum relative entropy used as distance measure We showed, that the geometric space can be divided and can be computed very efficiently by using Delaunay tessellation on the Bloch sphere, in a reasonable computational time.

As future work, we would like to extend our method to other protocols, and to collective and coherent attacks. We would like to construct a more effective algorithm to compute the informational theoretical impacts of the eavesdropper's cloning machine on a private quantum channel.

References:

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

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

[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), 2008, 77(5):052311,.

[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*, 2007, pp. 67–116. Springer-Verlag, Mathematics and Visualization,.

[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, *Physics Letters, Section A: General, Atomic and Solid State Physics*, 356 (3), 2006, pp. 195-198.

[12] Satoshi Iriyama, Masanori Ohya, Mathematical Characterization of Quantum Algorithm, *Proceedings of the 14th WSEAS International Conference on Applied Mathematics (MATH '09)*, 2009. pp. 184-190.

[13] Masanari Asano, Masanori Ohya, Quantum, Teleportation with Non-Maximal Entangled State, *Proceedings of the 14th WSEAS International Conference on Applied Mathematics (MATH '09),* 2009. pp. 191-195.

[14] Yuji Hirota, A Categorical Approach to Quantum Algorithm, *Proceedings of the 14th WSEAS International Conference on Applied Mathematics (MATH '09)*, 2009. pp. 268-270.

[15] Ron Goldman, Four Open Mathematical Problems Related to Computer Graphics and Geometric Modeling, *Proceedings of the International Conference on Computational and Information Science 2009,* pp. 249-255.

[16] Stanislaw P. Kasperczuk, Quantum Deformations of Algebras Associated with Integrable Hamiltonian Systems, *Proceedings of the 15th American Conference on Applied Mathematics, 2009,* pp. 69-73.

[17] Miroslav Svitek, Physics of Information Representation, Transmission and Processing, Recent Advances On Data Networks, Communications, Computers, *Proceedings of the 8th WSEAS International Conference on Data Networks, Communications, Computers, (DNCOCO '09),* 2009. pp. 205-212

[18] Mark Burgin, Mathematical Theory of Information Technology, *Proceedings of the 8th WSEAS International Conference on Data Networks, Communications, Computers,* (DNCOCO '09), 2009. pp. 42-48