Entanglement and Geometrical Distances in Quantum Information and Quantum Cryptography

Rotem Liss

Entanglement and Geometrical Distances in Quantum Information and Quantum Cryptography

Research Thesis

In partial fulfillment of the requirements
for the degree of Master of Science in Computer Science

Rotem Liss

Submitted to the Senate
of the Technion — Israel Institute of Technology
Iyar 5777 Haifa May 2017

The research thesis was done under the supervision of Assoc. Prof. Tal Mor in the Faculty of Computer Science.

Most of the results in this thesis have been published as articles by the author and research collaborators in conferences and journals:

Michel Boyer, Rotem Liss, and Tal Mor. Geometry of entanglement in the Bloch sphere. *Physical Review A*, 95:032308, March 2017.

Michel Boyer, Rotem Liss, and Tal Mor. Security against collective attacks of a modified BB84 QKD protocol with information only in one basis. In *Proceedings of the 2nd International Conference on Complexity, Future Information Systems and Risk – COMPLEXIS, 24-26 April, 2017, Porto, Portugal*, pages 23–29, April 2017.

Acknowledgements

I would like to thank my advisor, Assoc. Prof. Tal Mor, for his very helpful guidance, discussions, ideas, and help during this research. I would also like to thank Assoc. Prof. Michel Boyer for a fruitful research collaboration, discussions, help, and technical help with creating the figures appearing in this thesis.

I would also like to thank Gilles Brassard, John Smolin, Louis Salvail, Yossi Weinstein, Yair Rezek, Yuval Elias, and Itay Fayerverker.

My family deserves special thanks.

The generous financial help of the Technion is gratefully acknowledged.

Contents

List of Figures

Abstract

The counter-intuitive features of Quantum Mechanics make it possible to solve problems and perform tasks that are beyond the abilities of classical computers and classical communication devices. The area of *quantum information processing* studies how representing information by quantum states can help achieving such improvements.

In this research, we use basic notions of quantum information (mainly *entanglement*, *Bloch sphere*, and *geometrical distances between quantum states*) for analyzing relations of quantum states to each other and quantum cryptographic protocols.

Entanglement is an important feature of quantum states. Intuitively (and, partly, inaccurately), entanglement represents *quantum* (non-classical) correlations between several different quantum systems. Entanglement is one of the most important quantum phenomena, and it has many uses in quantum information, quantum communication, and quantum computing.

Some quantum states can be geometrically represented by the *Bloch sphere*: the unit sphere in the three-dimensional Euclidean space. The "standard" quantum states, to which the laws of Quantum Mechanics directly apply, are called *pure states*. Other states are the *mixed states*: probability distributions ("mixtures") of several pure states. The points *on* the Bloch sphere are the pure states, and those *inside* the Bloch sphere are the mixed states. This geometrical representation is useful and intuitive for many purposes.

We provide a geometrical analysis of entanglement for all the quantum mixed states of rank 2 (all the mixtures of exactly *two* pure states): for any such state (in any dimension), we define a *generalized Bloch sphere* by using the two pure states, and we analyze this state and its neighbor states inside this Bloch sphere. We look at the set of *non-entangled states* ("separable states") in the Bloch sphere and characterize it into exactly *five possible classes*. We give examples for each class and prove that there are no other classes. In addition, we suggest possible definitions of "entanglement measures" by using the "trace distance" from the nearest separable state.

Many types of *distances* between quantum states can be defined. One of the most useful distances is the *trace distance*, which bounds the "distinguishability" between the states. The trace distance is very useful in quantum information and quantum cryptography, and it also has a simple geometrical interpretation: it is half of the *Euclidean distance* between the states in the Bloch sphere.

Quantum key distribution (QKD) protocols make it possible for two participators to achieve the classically-impossible task of generating a secret random shared key even if their adversary is computationally unlimited. Several important QKD protocols, including the first protocol of Bennett and Brassard (BB84), have their unconditional security proved against adversaries performing the most general attacks in a theoretical (idealized) setting. We discuss a slightly different protocol, named "BB84-INFO-z", and prove it secure against a broad class of attacks (the collective attacks). Moreover, we make use of the "trace distance" for making our security proof more "composable" than similar security proofs for BB84: namely, for making a step towards proving that the secret key remains secret even when the two participators actually use it for cryptographic purposes.

Chapter 1

Introduction

The area of *quantum information processing* (QIP) uses the laws of quantum physics to perform tasks that are classically impossible (or hard).

In this chapter we discuss some of the basic notions of quantum information, that are needed for the later chapters. See [NC00, Gru99, RP00, GMD02] for more background and explanations regarding QIP.

1.1 Quantum States

In QIP, information is represented by *quantum states*. A quantum state is the state of a specific physical system.

A *Hilbert space* is a vector space over the field $\mathbb{C}$ (the complex numbers) with an inner product, that satisfies the "completeness" property (whose exact definition can be found in standard textbooks, and that is satisfied by all finite-dimensional inner product spaces). A *quantum pure state* is represented by $|\psi\rangle$, that is a normalized column vector (namely, a column vector of norm 1) in the Hilbert space. In other words, the Hilbert space is the set of *all* the possible quantum pure states of a system (including the non-normalized states).

As an important example, the *qubit* Hilbert space is $\mathcal{H}_2 \triangleq \text{Span}\{|0\rangle, |1\rangle\}$, with $|0\rangle$ and $|1\rangle$ being two orthonormal vectors (namely, they are normalized and their inner product is 0). Two other important states in $\mathcal{H}_2$ are $|+\rangle \triangleq \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|-\rangle \triangleq \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. The most general qubit pure state is $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, with $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$ (normalization condition). The qubit states are sometimes denoted by their vector representations in the $\{|0\rangle, |1\rangle\}$ basis: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $|+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, $|-\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$, and $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$.

Note that multiplying a pure state $|\psi\rangle$ by any global phase $e^{i\phi}$ has no physical significance. In other words, two pure states that differ only by a global multiplicative phase $e^{i\phi}$ are the same for all intents and purposes.

The notation $|\psi\rangle$ (the column vector) is called *ket*. A related notation, $\langle\psi|$, is called *bra*, and is a row vector. It is defined by $\langle\psi| \triangleq [|\psi\rangle]^\dagger$ (namely, the bra is the *conjugate transpose* of the ket). For example, if $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, then $\langle\psi| = \alpha^\star\langle 0| + \beta^\star\langle 1|$ (where $\alpha^\star$ is the complex conjugate of α); and, in vector notations, $\langle\psi| = \begin{pmatrix} \alpha^\star & \beta^\star \end{pmatrix}$.

Given an orthonormal basis $\{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle\}$, the *inner product* of two pure states $|\psi\rangle = \sum_{j=1}^n \alpha_j|\psi_j\rangle$ and $|\phi\rangle = \sum_{j=1}^n \beta_j|\psi_j\rangle$ is $\langle\psi|\phi\rangle = \sum_{j=1}^n \alpha_j^\star\beta_j$. The *norm* of $|\psi\rangle$ is $|||\psi\rangle|| \triangleq \sqrt{\langle\psi|\psi\rangle} = \sqrt{\sum_{j=1}^n |\alpha_j|^2}$.

1.1.1 Quantum Measurements

Quantum physics allows us to *measure* a quantum state $|\psi\rangle$ with respect to any orthonormal basis $\{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle\}$. The possible measurement outcomes are all the states "ψ_k" of this orthonormal basis; the probability of getting the outcome "ψ_k" (corresponding to the quantum state $|\psi_k\rangle$) is $p_k = |\langle\psi_k|\psi\rangle|^2$. Note that $\sum_{k=1}^n p_k = \langle\psi|\psi\rangle = 1$. Also note that the result "ψ_k" is a classical indicator that can be read and used; we have not discussed the resulting *quantum state* after the measurement, but we should note that the quantum state may be ruined (or change its state) by the measurement operation itself.

For example, if the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is measured with respect to the orthonormal basis $\{|0\rangle, |1\rangle\}$, then the result "0" is obtained with probability $|\langle 0|\psi\rangle|^2 = |\alpha|^2$, and the result "1" is obtained with probability $|\langle 1|\psi\rangle|^2 = |\beta|^2$.

More general types of measurements exist (see, e.g., in [NC00]), but they can all be reduced to the set of quantum operations described in Section 1.5.

1.1.2 Unitary Operators

Quantum physics allows us to apply any *unitary operator* $U : \mathcal{H} \to \mathcal{H}$ on a quantum state in the Hilbert space $\mathcal{H}$.

Unitary operators are linear operators (namely, $U[\alpha|\psi\rangle + \beta|\phi\rangle] = \alpha U|\psi\rangle + \beta U|\phi\rangle$) that satisfy $U^\dagger = U^{-1}$. They preserve inner products and norms.

As an important example, the *Hadamard operator* on the qubit space is defined by $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$: namely, $H|0\rangle = |+\rangle$ and $H|1\rangle = |-\rangle$. It also satisfies $H|+\rangle = |0\rangle$ and $H|-\rangle = |1\rangle$.

1.2 Bipartite and Multipartite Hilbert Spaces

1.2.1 Tensor Products of Hilbert Spaces

Suppose that we are given two physical systems, A and B, and that we want to represent the compound system AB (that is comprised of the two subsystems A and B) as a physical system. Suppose that the quantum state of subsystem A is represented by a

vector in the Hilbert space $\mathcal{H}_A$ and that the quantum state of subsystem B is represented by a vector in the Hilbert space $\mathcal{H}_B$.

In this case, the quantum state of the compound (*bipartite*) system AB is represented by a vector in the *tensor product* Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. An orthonormal basis for this Hilbert space can be obtained by taking the product of two orthonormal bases (of $\mathcal{H}_A$ and of $\mathcal{H}_B$): namely, if $\{|\psi_1\rangle_A, |\psi_2\rangle_A, \ldots, |\psi_k\rangle_A\}$ is an orthonormal basis of $\mathcal{H}_A$ and $\{|\phi_1\rangle_B, |\phi_2\rangle_B, \ldots, |\phi_n\rangle_B\}$ is an orthonormal basis of $\mathcal{H}_B$, then an orthonormal basis of $\mathcal{H}_A \otimes \mathcal{H}_B$ is $\{|\psi_i\rangle_A \otimes |\phi_j\rangle_B \mid 1 \leq i \leq k, 1 \leq j \leq n\}$.

As an important example, if A and B are both qubit systems (namely, $\mathcal{H}_A$ and $\mathcal{H}_B$ are both $\mathcal{H}_2 = \text{Span}\{|0\rangle, |1\rangle\}$), then the compound *two-qubit system* is represented by $\mathcal{H}_2 \otimes \mathcal{H}_2 = \text{Span}\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\}$. A shorter notation is $\mathcal{H}_2 \otimes \mathcal{H}_2 = \text{Span}\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

The tensor product of three or more Hilbert spaces (giving a *multipartite* Hilbert space) is defined in a similar way. For example, $\mathcal{H}_2 \otimes \mathcal{H}_2 \otimes \mathcal{H}_2$ (a tripartite Hilbert space that is the *three-qubit* space) is $\text{Span}\{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}$.

1.2.2 Tensor Products of Vectors

Given two Hilbert spaces, $\mathcal{H}_A$ with orthonormal basis $\{|\psi_1\rangle_A, |\psi_2\rangle_A, \ldots, |\psi_k\rangle_A\}$ and $\mathcal{H}_B$ with orthonormal basis $\{|\phi_1\rangle_B, |\phi_2\rangle_B, \ldots, |\phi_n\rangle_B\}$, and given two vectors $|\psi\rangle_A \triangleq \sum_{j=1}^{k} \alpha_j |\psi_j\rangle_A \in \mathcal{H}_A$ and $|\phi\rangle_B \triangleq \sum_{j=1}^{n} \beta_j |\phi_j\rangle_B \in \mathcal{H}_B$, the *tensor product* vector $|\psi\rangle_A \otimes |\phi\rangle_B \in \mathcal{H}_A \otimes \mathcal{H}_B$ (or, using a short notation, $|\psi\rangle_A |\phi\rangle_B$) is defined as

$$|\psi\rangle_A |\phi\rangle_B \triangleq \sum_{i=1}^{k} \sum_{j=1}^{n} \alpha_i \beta_j |\psi_i\rangle_A |\phi_j\rangle_B. \tag{1.1}$$

For example, given $|\psi\rangle_A = \alpha|0\rangle_A + \beta|1\rangle_A \in \mathcal{H}_2$ and $|\phi\rangle_B = \gamma|0\rangle_B + \delta|1\rangle_B \in \mathcal{H}_2$, the tensor product vector $|\psi\rangle_A |\phi\rangle_B \in \mathcal{H}_2 \otimes \mathcal{H}_2$ is

$$|\psi\rangle_A |\phi\rangle_B = \alpha\gamma|00\rangle_{AB} + \alpha\delta|01\rangle_{AB} + \beta\gamma|10\rangle_{AB} + \beta\delta|11\rangle_{AB}. \tag{1.2}$$

An example is

$$|+-\rangle_{AB} = \left[\frac{|0\rangle_A + |1\rangle_A}{\sqrt{2}}\right] \otimes \left[\frac{|0\rangle_B - |1\rangle_B}{\sqrt{2}}\right] = \frac{1}{2}[|00\rangle_{AB} - |01\rangle_{AB} + |10\rangle_{AB} - |11\rangle_{AB}]. \tag{1.3}$$

This definition is easily generalized to tensor products of three (or more) vectors: for example,

$$\begin{aligned} |+0-\rangle_{ABC} &= \left[\frac{|0\rangle_A + |1\rangle_A}{\sqrt{2}}\right] \otimes |0\rangle_B \otimes \left[\frac{|0\rangle_C - |1\rangle_C}{\sqrt{2}}\right] \\ &= \frac{1}{2}[|000\rangle_{ABC} - |001\rangle_{ABC} + |100\rangle_{ABC} - |101\rangle_{ABC}]. \end{aligned} \tag{1.4}$$

1.2.3 Tensor Products of Operators

Given two linear operators, U operating on the Hilbert space $\mathcal{H}_A$ and V operating on the Hilbert space $\mathcal{H}_B$, the linear operator $U \otimes V$ operates on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ and is defined as follows:

$$(U \otimes V)(|\psi\rangle_A \otimes |\phi\rangle_B) = (U|\psi_A\rangle) \otimes (V|\phi_B\rangle) \tag{1.5}$$

(It extends by linearity to vectors that are not tensor products, such as $\frac{|00\rangle_{AB}+|11\rangle_{AB}}{\sqrt{2}}$.)

For example, the tensor product of the Hadamard operator H with itself, denoted $H \otimes H$ or $H^{\otimes 2}$, operates as follows:

$$H^{\otimes 2}|00\rangle_{AB} = |{+}{+}\rangle_{AB} \tag{1.6}$$
$$H^{\otimes 2}|01\rangle_{AB} = |{+}{-}\rangle_{AB} \tag{1.7}$$
$$H^{\otimes 2}|10\rangle_{AB} = |{-}{+}\rangle_{AB} \tag{1.8}$$
$$H^{\otimes 2}|11\rangle_{AB} = |{-}{-}\rangle_{AB} \tag{1.9}$$

This definition is easily generalized to tensor products of three (or more) operators.

1.3 Quantum Entanglement of Pure States

A *tensor product* pure state (or *separable* pure state) in a bipartite Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ is a tensor product of two states: in other words, it is of the form $|\psi\rangle_A \otimes |\phi\rangle_B$ with $|\psi\rangle_A \in \mathcal{H}_A$ and $|\phi\rangle_B \in \mathcal{H}_B$.

Any other state in $\mathcal{H}_A \otimes \mathcal{H}_B$ (namely, any state that cannot be presented as $|\psi\rangle_A \otimes |\phi\rangle_B$) is called *entangled*.

For example (two-qubit states): $|{+}{-}\rangle_{AB}$ is a product state, while $\frac{|01\rangle_{AB}-|10\rangle_{AB}}{\sqrt{2}}$ is an entangled state.

Four important entangled two-qubit states (that form together an orthonormal basis of $\mathcal{H}_2 \otimes \mathcal{H}_2$, called *Bell basis* or *BMR basis*) are:

$$|\Phi_\pm\rangle_{AB} = \frac{|00\rangle_{AB} \pm |11\rangle_{AB}}{\sqrt{2}} \tag{1.10}$$
$$|\Psi_\pm\rangle_{AB} = \frac{|01\rangle_{AB} \pm |10\rangle_{AB}}{\sqrt{2}} \tag{1.11}$$

1.4 Quantum Mixed States

A *quantum mixed state* is a probability distribution over several pure states: namely, it is a set $\{(|\psi_j\rangle, q_j)\}_j$ of pairs, each pair consisting of a pure state $|\psi_j\rangle$ and of a probability q_j (with $0 < q_j \leq 1$ and $\sum_j q_j = 1$), such that the pure state $|\psi_j\rangle$ has a probability q_j.

Unlike a pure state, a mixed state is not represented by a vector in Hilbert space. It is represented by a density matrix: $\rho = \sum_j q_j |\psi_j\rangle\langle\psi_j|$, where q_j is the probability

that the system is in the state $|\psi_j\rangle$. (This definition should not be confused with the probabilities of measurement results.) In particular, the pure state $|\psi\rangle$ is represented by the density matrix $\rho = |\psi\rangle\langle\psi|$.

For example, if the system is prepared in the $|0\rangle$ state with probability $\frac{1}{3}$ or in the $|+\rangle$ state with probability $\frac{2}{3}$, then the quantum state of this mixing is the mixed state $\rho = \frac{1}{3}|0\rangle\langle 0| + \frac{2}{3}|+\rangle\langle +|$. It should be emphasized that those probabilities are of the *preparation*, not of any *measurement*. For example, if the state is measured in the $\{|0\rangle, |1\rangle\}$ orthonormal basis, the probability of measuring "0" is $\frac{2}{3}$, and the probability of measuring "1" is $\frac{1}{3}$; if it is measured in the $\{|+\rangle, |-\rangle\}$ basis, the probability of measuring "+" is $\frac{5}{6}$, and the probability of measuring "−" is $\frac{1}{6}$. Notice that the probability of measuring "0" is *not* $\frac{1}{3}$ and that the probability of measuring "+" is *not* $\frac{2}{3}$.

Note that several *different* probability distributions may represent the *same* mixed state: namely, the states they represent are physically the same (e.g., giving exactly the same measurement results in all orthonormal bases). This happens if and only if they are represented by *equal* density matrices. (A similar observation is that a global phase $e^{i\phi}$ for *pure states* has no physical significance; and, indeed, the two pure states $|\psi\rangle$ and $e^{i\phi}|\psi\rangle$ are represented by equal density matrices, $\rho = |\psi\rangle\langle\psi|$.) For example, the *completely mixed state* $\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$ is the same as $\rho = \frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -|$, and those two density matrices are equal.

A (normalized) density matrix satisfies three conditions: it is a *Hermitian* operator; it is *positive semidefinite*; and it is *normalized* (that is, its trace equals 1). Those three conditions are also sufficient: any matrix ρ satisfying them is a (normalized) density matrix. The set of (normalized) density matrices corresponding to the Hilbert space $\mathcal{H}$ is denoted by $\mathcal{L}(\mathcal{H})$ (this is also the *set of mixed states* that are mixtures of pure states from the Hilbert space $\mathcal{H}$). From those three conditions it follows that every (normalized) density matrix ρ can be presented as $\rho = \sum_j \lambda_j |\psi_j\rangle\langle\psi_j|$ (the spectral decomposition), where $\lambda_j \geq 0$, $\sum_j \lambda_j = 1$, and $\{|\psi_j\rangle\}_j$ is an orthonormal set (of eigenvectors). In other words, for any mixed state we can choose a corresponding probability distribution over a set of *orthonormal* states. For example, for $\rho = \frac{1}{3}|0\rangle\langle 0| + \frac{2}{3}|+\rangle\langle +|$, the spectral decomposition is $\rho = \frac{3+\sqrt{5}}{6}\left[\frac{2|0\rangle+(\sqrt{5}-1)|1\rangle}{\sqrt{10-2\sqrt{5}}}\right]\left[\frac{2\langle 0|+(\sqrt{5}-1)\langle 1|}{\sqrt{10-2\sqrt{5}}}\right] + \frac{3-\sqrt{5}}{6}\left[\frac{2|0\rangle-(\sqrt{5}+1)|1\rangle}{\sqrt{10+2\sqrt{5}}}\right]\left[\frac{2\langle 0|-(\sqrt{5}+1)\langle 1|}{\sqrt{10+2\sqrt{5}}}\right]$, and it is the *unique* decomposition of ρ as a mixture of *orthonormal* pure states; on the other hand, the completely mixed state $\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -|$ has an infinite number of decompositions as a mixture of orthonormal pure states, because its eigenvalue $(\frac{1}{2})$ is degenerate – namely, it has two orthonormal eigenvectors corresponding to the same eigenvalue.

The probability distribution in the definition of the mixed state represents the "standard" ("classical") notion of *uncertainty*, and not a quantum phenomenon; it simply represents lack of knowledge. Nonetheless, mixed states naturally arise in many areas of quantum information. Most notably, if a compound system AB is in an *entangled* pure state, then the quantum state of each of the subsystems A and B is mixed. For example,

if the state of the system AB is the entangled pure state $\frac{1}{\sqrt{3}}|0\rangle_A|0\rangle_B + \sqrt{\frac{2}{3}}|1\rangle_A|+\rangle_B$, the quantum state of the subsystem B is the mixed state $\rho = \frac{1}{3}|0\rangle_B\langle 0|_B + \frac{2}{3}|+\rangle_B\langle +|_B$ that we have seen before. Moreover, we note that the state of the system AB can also be represented as $\sqrt{\frac{5}{6}}|+\rangle_A \frac{2|0\rangle_B+|1\rangle_B}{\sqrt{5}} - \frac{1}{\sqrt{6}}|-\rangle_A|1\rangle_B$; thus, the state of the subsystem B can also be represented as $\rho = \frac{5}{6}\left[\frac{2|0\rangle_B+|1\rangle_B}{\sqrt{5}}\right]\left[\frac{2\langle 0|_B+\langle 1|_B}{\sqrt{5}}\right] + \frac{1}{6}|1\rangle_B\langle 1|_B$. This is another example of multiple probability distributions corresponding to the same mixed state.

An important difference between a pure state and a mixed state should be noted: for a pure state $|\psi\rangle$, there is an orthonormal basis (consisting of $|\psi\rangle$ and of states orthonormal to it) such that if $|\psi\rangle$ is measured with respect to it, there is a specific measurement result ($|\psi\rangle$) obtained *for certain*. This is never true for a mixed state ρ: its measurement result is uncertain if measured with respect to any orthonormal basis.

If a mixed state ρ is measured with respect to an orthonormal basis $\{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle\}$, we get the result "$\psi_k$" with probability $p_k = \langle\psi_k|\,\rho\,|\psi_k\rangle$. If we apply a unitary operator U to a mixed state ρ, the resulting state is the mixed state $U\rho U^\dagger$.

1.5 Allowed Quantum Operations

The most general operations allowed by quantum physics for the Hilbert space $\mathcal{H}$ are:

1. applying any unitary operator $U : \mathcal{H} \to \mathcal{H}$ (see Subsection 1.1.2);
2. measuring the state with respect to some orthonormal basis (see Subsection 1.1.1);
3. adding a new (ancillary) subsystem; and
4. removing (ignoring and forgetting) a subsystem.

1.6 Quantum Key Distribution

Quantum Key Distribution (QKD) makes it possible for two legitimate parties, Alice and Bob, to generate an information-theoretically secure key [BB84], that is secure against any possible attack allowed by the laws of quantum physics. Alice and Bob use an insecure quantum channel and an unjammable classical channel. The adversary Eve may interfere with the quantum channel and is limited only by the laws of nature; she may not, however, modify the data sent in the unjammable classical channel (she can only listen to it).

QKD protocols achieve the classically-impossible goal of distributing a secret key to two parties (Alice and Bob), in a way that is secure against all the possible attacks. Moreover, the key shared by Alice and Bob remains secret even if weaknesses in the devices (currently unknown to anyone, *including* the adversary) are discovered in the future: namely, for the adversary Eve to find the key, she must attack when Alice and Bob apply the protocol, and not later (while for encryption methods such as RSA, Eve

may keep the ciphertext until she is able to find the private key, e.g., by factorizing a large number).

The first QKD protocol was BB84 [BB84]. The BB84 protocol, operated by the two parties Alice and Bob, consists of the following steps:

1. Alice sends to Bob N quantum states, all of them randomly chosen from the following set: $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$

2. Bob measures all the received states; for each of the states, he chooses randomly whether to measure it in the z basis $\{|0\rangle, |1\rangle\}$ or in the x basis $\{|+\rangle, |-\rangle\}$. If Bob measures in the z basis, he identifies $|0\rangle$ and $|1\rangle$ with certainty, but gets a random result if $|+\rangle$ or $|-\rangle$ is sent; the converse is true for the x basis.

3. Now Alice and Bob each holds a (classical) bit string: Alice holds the list of bits she sent (bit 0 corresponding to the states $|0\rangle$ and $|+\rangle$, and bit 1 corresponding to the states $|1\rangle$ and $|-\rangle$), and Bob holds the list of bits he measured (with similar interpretations as Alice). In addition, Alice knows the basis she used to send each state, and Bob knows the basis he used to measure each state.

4. Alice and Bob reveal (by using the classical channel) their basis choices, and they discard all the states that Bob measured in a basis different from the one sent by Alice.

5. Alice and Bob reveal some random subset of their bit string ("TEST bits"), compare the bits, and estimate the error rate. They abort the protocol if the error rate is above a specified threshold (in BB84, the asymptotic threshold (for infinite key-length) is 11% [RGK05, SP00]). They discard the revealed bits.

6. Now Alice and Bob keep only the string of bits that were measured by Bob in the same basis they were sent by Alice (and that were not discarded): they are called "INFO bits". If there is no noise or eavesdropping, the INFO bits should be the same for Alice and Bob.

7. Alice sends to Bob error correction information, and Bob corrects the errors in his bit string, so that it is the same as Alice's.

8. Alice and Bob perform a privacy amplification process, yielding a final key that is identical for Alice and Bob and is fully secure against any eavesdropper.

Many QKD protocols have been proven fully (and unconditionally) secure in the theoretical sense; see Section 2.4 for more details about the security of QKD.

However, practical implementations deviate from the theoretical descriptions, and they may thus be insecure. Two important attacks that take advantage of this fact are the "Photon Number Splitting" attack [BLMS00b, BLMS00a] and the "Bright Illumination" attack [LWW$^+$10]. The "Photon Number Splitting" attack takes advantage of the

fact that in most practical implementations, Alice cannot generate only one-photon pulses, but sometimes generates pulses of two (or more) photons: Eve can, under certain conditions, get full information on the secret key without inducing errors. The "Bright Illumination" attack uses a weakness of Bob's detectors, existing in most practical implementations, to get full information on the secret key without inducing errors.

Other QKD protocols, either similar to BB84 or ones that use different approaches, have also been suggested, and in some cases have also been proven fully secure. In particular, the "three-state protocol" [Mor98] uses only the three states $\{|0\rangle, |1\rangle, |+\rangle\}$ (with $|+\rangle$ being used only for testing, while $|0\rangle$ and $|1\rangle$ being used both for key-generation and for testing), and it has been proven secure [FL06, BGLS07, Kra16]; the "classical Bob" protocol [BKM07] is a two-way protocol such that only Alice has quantum capabilities and Bob has only classical capabilities, and it has been proven robust [BKM07] (see Section 2.4 for the definition of robustness) and secure [Kra15]; and the "classical Alice" protocol [ZQL$^+$09] is similar to "classical Bob" with Alice being the classical participant instead of Bob, and it has been proven robust [BM11].

1.7 Structure of this Thesis

In Chapter 2, we present the definitions of several important notions in quantum information, that are useful for this thesis: quantum entanglement of mixed states, Bloch sphere, trace distance, and security of quantum key distribution (QKD).

In Chapter 3, we discuss the geometry of entanglement in the Bloch sphere: we define a generalized notion of a Bloch sphere (corresponding to each 2-dimensional Hilbert subspace, and to each rank-2 quantum mixed state), and we see that the pattern of entanglement in each Bloch sphere always belongs to one of five classes.

In Chapter 4, we discuss a variant of the quantum key distribution (QKD) protocol BB84 that we name BB84-INFO-z, and we prove that BB84-INFO-z is secure against collective attacks. We use the notion of the trace distance for making the proof more composable than similar proofs.

Chapter 2

Preliminaries

In this chapter, we introduce several basic important notions of quantum information, that are useful in later parts of this thesis.

2.1 Quantum Entanglement of Mixed States

We remember that $\mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is the set of *mixed states* that are mixtures of pure states from the bipartite Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$.

A *separable* mixed state in $\mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is a *mixture* of tensor product pure states: in other words, it can be represented as $\rho = \sum_j q_j |\psi_j\rangle_A |\phi_j\rangle_B \langle\psi_j|_A \langle\phi_j|_B$, with $|\psi_j\rangle_A \in \mathcal{H}_A$ and $|\phi_j\rangle_B \in \mathcal{H}_B$.

Any other state in $\mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$ (namely, any state that cannot be presented as a *mixture* of tensor product pure states) is called *entangled*.

For example: $\rho = \frac{1}{2}|00\rangle_{AB}\langle 00|_{AB} + \frac{1}{2}|11\rangle_{AB}\langle 11|_{AB}$ is a separable two-qubit state.

Notice that entanglement is not the same as *correlation*: the state $\rho = \frac{1}{2}|00\rangle_{AB}\langle 00|_{AB} + \frac{1}{2}|11\rangle_{AB}\langle 11|_{AB}$ above has the states of its two subsystems (A and B) correlated, but it is not entangled, because this is only a *classical correlation*. Entanglement, on the other hand, is a quantum phenomenon, representing only *quantum correlations* that have no classical explanation.

Extensions of those definitions to the multipartite case are given in Section 3.9.

2.2 Bloch Sphere

The *Bloch sphere*, also known as the *Poincaré sphere*, is a geometrical representation of the pure and mixed qubit states (namely, of the pure states in $\mathcal{H}_2$ and of their mixtures in $\mathcal{L}(\mathcal{H}_2)$). It is drawn in Figure 2.1.

The Bloch sphere is the *unit sphere* in the *three-dimensional* Euclidean space $\mathbb{R}^3$.

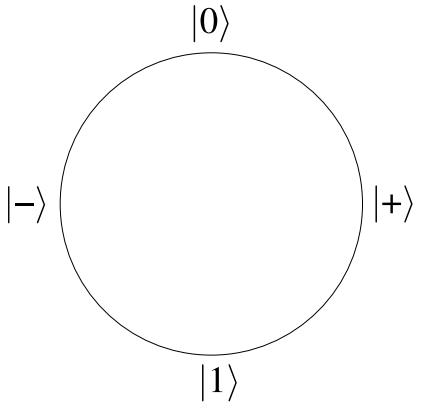

Figure 2.1: **Bloch sphere corresponding to the qubit Hilbert space $\mathcal{H}_2$**

2.2.1 Representation of Pure States on the Bloch Sphere

There is a one-to-one correspondence between the normalized pure states in $\mathcal{H}_2$ and the points *on* the Bloch sphere. Each point on the sphere is represented by the vector $\vec{r}$ in spherical coordinates: (r, θ, ϕ), with $r = 1$. (We note that, as is standard in physics, the angle θ is the angle between the vector $\vec{r}$ and the positive z axis, while the angle ϕ is the angle between the projection of the vector $\vec{r}$ on the $x - y$ plane and the positive x axis.)

The most general normalized pure state in $\mathcal{H}_2$ is:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle \tag{2.1}$$

(The global phase does not matter, so we can assume that the coefficient of $|0\rangle$ is real.)

This state (and any multiple by a global phase) corresponds to the point $(1, \theta, \phi)$ in spherical coordinates – namely, to the point $\vec{r} = (x, y, z) = (\sin\theta\cos\phi, \sin\theta\sin\phi, \cos\theta)$ in Cartesian coordinates.

We can find the density matrix corresponding to $|\psi\rangle$:

$$\begin{aligned}
\rho &= |\psi\rangle\langle\psi| = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) \\ e^{i\phi}\sin\left(\frac{\theta}{2}\right) \end{pmatrix} \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & e^{-i\phi}\sin\left(\frac{\theta}{2}\right) \end{pmatrix} \\
&= \begin{pmatrix} \cos^2\left(\frac{\theta}{2}\right) & e^{-i\phi}\cos\left(\frac{\theta}{2}\right)\sin\left(\frac{\theta}{2}\right) \\ e^{i\phi}\cos\left(\frac{\theta}{2}\right)\sin\left(\frac{\theta}{2}\right) & \sin^2\left(\frac{\theta}{2}\right) \end{pmatrix} \\
&= \begin{pmatrix} \frac{1+\cos\theta}{2} & \frac{(\cos\phi - i\sin\phi)\sin\theta}{2} \\ \frac{(\cos\phi + i\sin\phi)\sin\theta}{2} & \frac{1-\cos\theta}{2} \end{pmatrix} \\
&= \frac{1}{2}\begin{pmatrix} 1+\cos\theta & \sin\theta\cos\phi - i\sin\theta\sin\phi \\ \sin\theta\cos\phi + i\sin\theta\sin\phi & 1-\cos\theta \end{pmatrix} \\
&= \frac{1}{2}\begin{pmatrix} 1+z & x - iy \\ x + iy & 1-z \end{pmatrix}
\end{aligned} \tag{2.2}$$

We thus see that the density matrix ρ of a pure state is directly determined by the corresponding point (x, y, z) on the Bloch sphere. We will soon see that a similar correspondence (by using the same equation) is obtained for the mixed states.

Examples

- For $\theta = 0$, the obtained state is $|0\rangle$, corresponding to the $+\hat{z}$ point on the Bloch sphere.
- For $\theta = \pi$, the obtained state is $e^{i\phi}|1\rangle$ (this is the same state for all ϕ, because a global phase does not matter), corresponding to the $-\hat{z}$ point on the Bloch sphere.
- For $\theta = \frac{\pi}{2}$, the obtained states are $\frac{|0\rangle+e^{i\phi}|1\rangle}{\sqrt{2}}$, corresponding to the points on the Bloch sphere that are on the $x-y$ plane. Examples of such states are $|+\rangle$ (obtained for $\phi = 0$) and $|-\rangle$ (obtained for $\phi = \pi$).

Useful Property An important property satisfied by the Bloch sphere: two pure states $|\psi\rangle$ and $|\phi\rangle$ are orthogonal *if and only if* $|\psi\rangle$ and $|\phi\rangle$ are connected by a diameter in the Bloch sphere. See, for example, Figure 2.2.

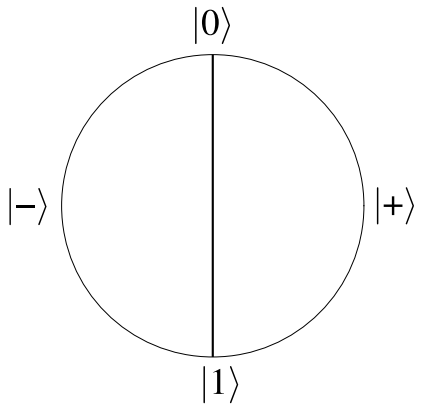

Figure 2.2: **A diameter connects any two orthogonal pure states on the Bloch sphere.**

2.2.2 Representation of Mixed States inside the Bloch Sphere

There is a one-to-one correspondence between the mixtures of states in $\mathcal{H}_2$ (namely, the mixed qubit states in $\mathcal{L}(\mathcal{H}_2)$) and the points *inside* the Bloch sphere.

We analyze a mixture of two pure states, $\rho_1 = q|\psi\rangle\langle\psi| + (1-q)|\phi\rangle\langle\phi|$, such that $|\psi\rangle$ is represented by the point $\vec{r}_\psi \triangleq (x_\psi, y_\psi, z_\psi)$ on the sphere and $|\phi\rangle$ is represented by the point $\vec{r}_\phi \triangleq (x_\phi, y_\phi, z_\phi)$ on the sphere. We represent this mixture ρ_1 by the point $\vec{r}_{\rho_1} = q\vec{r}_\psi + (1-q)\vec{r}_\phi$ inside the Bloch sphere: namely, by a point that is a *convex combination* of the two points $\vec{r}_\psi$ and $\vec{r}_\phi$ (and, thus, that is on the line between them). See Figure 2.3 for an illustration of this representation.

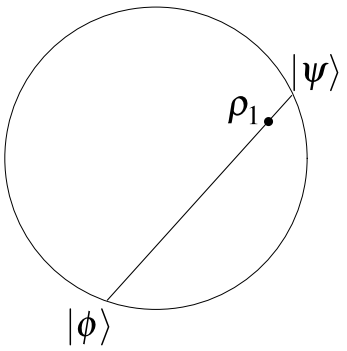

Figure 2.3: **A mixture of two states is represented by their convex combination inside the Bloch sphere** – namely, it is on the line between them.

We now show that, given the above representation, equation (2.2) holds also for mixed states:

$$\begin{aligned}
\rho_1 &= q|\psi\rangle\langle\psi| + (1-q)|\phi\rangle\langle\phi| \\
&= \frac{q}{2}\begin{pmatrix} 1+z_\psi & x_\psi - iy_\psi \\ x_\psi + iy_\psi & 1-z_\psi \end{pmatrix} + \frac{1-q}{2}\begin{pmatrix} 1+z_\phi & x_\phi - iy_\phi \\ x_\phi + iy_\phi & 1-z_\phi \end{pmatrix} \\
&= \frac{1}{2}\begin{pmatrix} 1+[qz_\psi + (1-q)z_\phi] & [qx_\psi + (1-q)x_\phi] - i\,[qy_\psi + (1-q)y_\phi] \\ [qx_\psi + (1-q)x_\phi] + i\,[qy_\psi + (1-q)y_\phi] & 1-[qz_\psi + (1-q)z_\phi] \end{pmatrix} \\
&= \frac{1}{2}\begin{pmatrix} 1+z_{\rho_1} & x_{\rho_1} - iy_{\rho_1} \\ x_{\rho_1} + iy_{\rho_1} & 1-z_{\rho_1} \end{pmatrix}
\end{aligned} \tag{2.3}$$

Equation (2.3) can be easily generalized to *any* mixture of states of any type (pure or mixed): namely, the mixed state $\rho = \sum_j q_j \rho_j$ is represented by the convex combination point $\vec{r}_\rho = \sum_j q_j \vec{r}_{\rho_j}$.

We note that each density matrix corresponds to a unique point inside the Bloch sphere. In particular, different probability distributions that correspond to the same mixed state (and that are thus represented by the same density matrix) correspond to a *single point* inside the Bloch sphere. For example, the completely mixed state correponds to the origin $(0,0,0)$, and it is an equal mixture of the states in any *any* orthonormal basis: $\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -|$, etc.

2.3 Trace Distance

The *trace distance* between two quantum states is, informally, a measure of their *distinguishability*.

2.3.1 Mathematical Definition and Interpretation

The trace distance of two states ρ and σ is defined as follows:

$$D(\rho,\sigma) \triangleq \frac{1}{2}\operatorname{tr}|\rho-\sigma| = \frac{1}{2}\operatorname{tr}\sqrt{(\rho-\sigma)^\dagger(\rho-\sigma)} \tag{2.4}$$

(Because $|A|$ is defined as $\sqrt{A^\dagger A}$.)

This definition can be interpreted as follows [FvdG99]: since $\rho-\sigma$ is a Hermitian operator, it has a spectral decomposition $\rho-\sigma=\sum_j \lambda_j|\psi_j\rangle\langle\psi_j|$, where $\lambda_j\in\mathbb{R}$ and $\{|\psi_j\rangle\}_j$ is an orthonormal set. It also holds that $(\rho-\sigma)^\dagger=\rho-\sigma$. Therefore,

$$|\rho-\sigma| = \sqrt{(\rho-\sigma)^2} = \sqrt{\left(\sum_j \lambda_j|\psi_j\rangle\langle\psi_j|\right)^2} = \sqrt{\sum_j \lambda_j^2|\psi_j\rangle\langle\psi_j|} = \sum_j |\lambda_j||\psi_j\rangle\langle\psi_j|, \tag{2.5}$$

and we find that

$$D(\rho,\sigma) \triangleq \frac{1}{2}\operatorname{tr}|\rho-\sigma| = \frac{1}{2}\sum_j |\lambda_j|. \tag{2.6}$$

We conclude that the trace distance $D(\rho,\sigma)$ is one half of the *sum of absolute values* of the eigenvalues of $\rho-\sigma$.

2.3.2 Geometrical Interpretation for Qubits

In the case of qubit states (pure or mixed), there is a simple geometrical interpretation for the trace distance: the trace distance between ρ and σ is one half of the *Euclidean distance* between the points representing ρ and σ inside the Bloch sphere.

Following [NC00, page 404], we can prove this result as follows: according to equation (2.3), if ρ and σ are represented by the points $\vec{r}_\rho=(x_\rho,y_\rho,z_\rho)$ and $\vec{r}_\sigma=(x_\sigma,y_\sigma,z_\sigma)$ in the Bloch sphere, respectively, then $\rho=\frac{1}{2}\begin{pmatrix}1+z_\rho & x_\rho-iy_\rho\\ x_\rho+iy_\rho & 1-z_\rho\end{pmatrix}$ and $\sigma=\frac{1}{2}\begin{pmatrix}1+z_\sigma & x_\sigma-iy_\sigma\\ x_\sigma+iy_\sigma & 1-z_\sigma\end{pmatrix}$. Let us denote $\Delta\vec{r}=\vec{r}_\rho-\vec{r}_\sigma$. Therefore,

$$\rho-\sigma = \frac{1}{2}\begin{pmatrix}\Delta z & \Delta x-i\Delta y\\ \Delta x+i\Delta y & -\Delta z\end{pmatrix}. \tag{2.7}$$

It can easily be verified that the eigenvalues of $\rho-\sigma$ are $\lambda_\pm=\pm\frac{1}{2}\sqrt{\Delta x^2+\Delta y^2+\Delta z^2}$. Thus, according to equation (2.6),

$$D(\rho,\sigma) = \frac{1}{2}\left[2\cdot\frac{1}{2}\sqrt{\Delta x^2+\Delta y^2+\Delta z^2}\right] = \frac{1}{2}\left|\vec{r}_\rho-\vec{r}_\sigma\right|. \tag{2.8}$$

This idea is demonstrated in Figure 2.4.

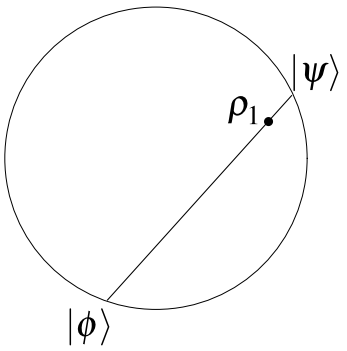

Figure 2.4: **The trace distance between two qubit states is one half of their geometrical distance in the Bloch sphere.**

2.3.3 The Information-Theoretical Meaning of the Trace Distance

It can be proved [FvdG99, BBB$^+$02] that the trace distance $D(\rho, \sigma)$ between the two quantum states ρ and σ upper-bounds the *Shannon Distinguishability* between ρ and σ, that is defined as the classical mutual information between the random variable $T \triangleq \begin{cases} 0 & \text{The quantum state is } \rho \\ 1 & \text{The quantum state is } \sigma \end{cases}$ and the random variable X (the result of a measurement), maximized over *all the possible quantum measurements* (including the ones consisting of adding an ancillary state, performing a general unitary transformation, and then measuring).

In other words, the trace distance upper-bounds the information that some party, who holds some quantum state and *does not know* whether it is ρ or σ (it can be either ρ or σ, with equal probabilities), can find by using a measurement.

For example: $D(|0\rangle\langle 0|, |1\rangle\langle 1|) = 1$, because the quantum states $|0\rangle$ and $|1\rangle$ can be distinguished *for certain* by measuring in the $\{|0\rangle, |1\rangle\}$ basis; and $D(|0\rangle\langle 0|, |0\rangle\langle 0|) = 0$, because the quantum state $|0\rangle$ is equal to $|0\rangle$, so they cannot be distinguished from each other at all.

2.4 Security Definitions of Quantum Key Distribution

Originally, a quantum key distribution (QKD) protocol, as defined in Section 1.6, was defined to be secure if the (classical) *mutual information* between Eve's information and the final key, maximized over all the possible attack strategies and measurements by Eve, is exponentially small in the number of qubits, N. Examples of security proofs of BB84 that use this security definition are [May01, BBB$^+$06, SP00]. Those security proofs used the observation that one cannot analyze the *classical* data held by Eve before privacy amplification (as done in [BBCM95]), but must analyze the *quantum* state held by Eve [BMS96]. In other words, they assumed that Eve could keep her quantum state until the end of the protocol, and only *then* choose the optimal measurement (based on

all the data she observed) and perform the measurement.

Later, it was noticed that this security definition may not be "composable". In other words, the final key is secure if Eve measures the quantum state she holds at the end of the QKD protocol, but the proof does not apply to *cryptographic applications* (e.g., encryption) of the final key: Eve might gain non-negligible information after the key is used, even though her information on the key itself was negligible. This means that the proof is not sufficient for practical purposes. In particular, those applications may be insecure if Eve keeps her quantum state until Alice and Bob use the key (thus giving Eve some new information) and only *then* measures.

Therefore, a new notion of "(composable) full security" was defined [BOHL$^+$05, RGK05, Ren08] by using the trace distance (see Section 2.3), following universal composability definitions for non-quantum cryptography [Can01, PW00]. Intuitively, this notion means that the final joint quantum state of Alice, Bob, and Eve at the end of the protocol is *very close* (namely, the trace distance is exponentially small in N) to their final state at the end of an *ideal* key distribution protocol, that distributes a *completely random* and *secret* final key to both Alice and Bob. In other words, if a QKD protocol is secure, then except with an exponentially small probability, one of the two following events happens: the protocol is aborted, *or* the secret key generated by the protocol is the same as a perfect key that is uniformly distributed (i.e., each possible key having the same probability), is the same for both parties, and is independent of the adversary's information.

Formally, ρ_{ABE} is defined as the final quantum state of Alice, Bob, and Eve at the end of the protocol (with Alice's and Bob's states being simply the "classical" states $|k_A\rangle_A$ and $|k_B\rangle_B$, where k_A and k_B are bit strings that are the final keys held by Alice and Bob, respectively; note that usually $k_A = k_B$); ρ_U is defined as the complete mixture of all the possible keys that are the same for Alice and Bob (namely, if the set of possible final keys is K, then $\rho_U = \frac{1}{|K|}\sum_{k\in K} |k\rangle_A|k\rangle_B\langle k|_A\langle k|_B$); and ρ_E is defined as some state of Eve. For the QKD protocol to be fully (and composably) secure, it is required that

$$\frac{1}{2}\operatorname{tr}|\rho_{ABE} - \rho_U \otimes \rho_E| \leq \epsilon, \tag{2.9}$$

where ϵ is exponentially small in N. Intuitively, ρ_{ABE} is the *actual* joint state of Alice, Bob, and Eve at the end of the QKD protocol; ρ_U is the *ideal* final state of Alice and Bob (an equal mixture of all the possible final keys, that is completely uncorrelated with Eve and is the same for Alice and Bob); and ρ_E is a state of Eve, uncorrelated with the states of Alice and Bob.

Composable security of many QKD protocols, including BB84, has been proved [BOHL$^+$05, RGK05, Ren08].

A much weaker notion is the *robustness* of a QKD protocol [BKM07]. A QKD protocol is completely robust if any nonzero information obtained by Eve on the INFO string implies a nonzero probability that Alice and Bob find errors in the TEST bits.

In other words, if a protocol is completely robust, then Eve cannot find any useful information without causing errors that may be noticed by Alice and Bob. Robustness does not imply full security (because one should prove that Alice and Bob can generate a completely secret final key, by using error correction and privacy amplification, as described in Section 1.6), but it is an important step towards proving security.

Chapter 3

Geometry of Entanglement in the Bloch Sphere

In this chapter, we classify all the possible Bloch spheres (and rank-2 states) into exactly five classes, according to the set of separable states in the Bloch sphere.

This chapter is based on the published journal paper [BLM17a].

3.1 Introduction

Entanglement is a very important property of quantum states, relevant to the foundations of quantum mechanics (e.g., the Einstein-Podolsky-Rosen paradox and Bell's inequality), as well as to quantum information, quantum communication (including quantum teleportation and quantum cryptography), quantum computers and simulators, and quantum many-body systems.

The relations between entanglement, partial transpose (defined in Section 3.2), and non-classical correlations between the subsystems, are well-understood for pure quantum bipartite states. However, for mixed quantum states there are still many open questions. Even bipartite mixed states of rank 2 (namely, states that can be written as $\rho = q|\psi_0\rangle\langle\psi_0| + (1-q)|\psi_1\rangle\langle\psi_1|$, where $0 < q < 1$, and $|\psi_0\rangle, |\psi_1\rangle$ are bipartite orthonormal states and are the eigenstates of ρ), that are discussed in this chapter, are not well-understood. Studying such states is thus a major challenge in the field of mixed-state quantum entanglement.

It is known that if a mixed state does not have a positive partial transpose then it is entangled and presents a nonlocal behavior [Per96]. However, one can find separable states presenting a nonlocal behavior (e.g., [BDF$^+$99]), and one can find entangled states that have a positive partial transpose [HHH96, Hor97]; those states are bound entangled, namely, their entanglement cannot be distilled [HHH98]. It was later proved that bound entangled states cannot have rank 3 or less [HSTT03, CC08]. Therefore, checking whether a *specific* rank-2 state is entangled is trivial: it is entangled if and only if it does not have a positive partial transpose; however, in this chapter we discuss

the problem of classifying each rank-2 state by checking which states in its *Bloch-sphere neighborhood* (namely, in its corresponding Bloch sphere) are entangled.

Entanglement distillation (for pure states) [BBPS96] and entanglement purification (for mixed states) [BBP$^+$96] are processes of distilling Bell states (or other maximally entangled states) from some copies of an initial state. An efficient protocol is known for pure states, but not for mixed states. This provides another motivation for studying and finding ways to fully characterize the simplest non-pure bipartite states (the rank-2 bipartite mixed states).

The notion of the Bloch sphere, also known as the Poincaré sphere, is a very useful geometrical interpretation of a single qubit – namely, of the 2-dimensional Hilbert space $\mathcal{H}_2$ (see Section 2.2 and Figure 2.1). We notice that $\mathcal{H}_2$ is isomorphic to *any* 2-dimensional (complex) *subspace* of a full Hilbert space. Therefore, given any 2-dimensional Hilbert subspace $\mathcal{H}$ and its orthonormal basis $\{|\psi_0\rangle, |\psi_1\rangle\}$, we can define a unique generalized Bloch sphere representing $\mathcal{H}$ (the uniqueness is up to a possible rotation of the sphere; see Section 3.4): we represent $|\psi_0\rangle$ by the north pole and $|\psi_1\rangle$ by the south pole; all their superpositions (the pure states) are on the sphere; and all the pure states' mixtures (the mixed states) are inside the sphere. For example, $\mathcal{H}$ can be the subspace spanned by the eigenstates $|\psi_0\rangle, |\psi_1\rangle$ of a given rank-2 mixed state $\rho = q|\psi_0\rangle\langle\psi_0| + (1-q)|\psi_1\rangle\langle\psi_1|$, as illustrated in Figure 3.1.

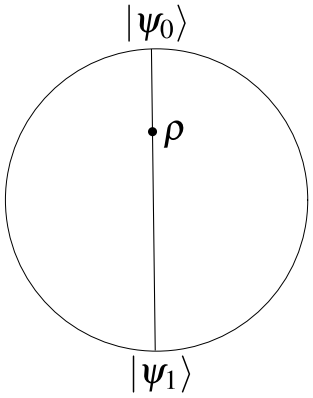

Figure 3.1: **Bloch sphere of the 2-dimensional Hilbert space Span**$\{|\psi_0\rangle, |\psi_1\rangle\}$

We define here the "Bloch-sphere entanglement" of a quantum rank-2 bipartite state. This (informally) means that we define the sets of separable states and of entangled states inside the unique Bloch sphere associated with this quantum state. We provide some examples, and we prove that the five classes we present exhaust all the possibilities of "Bloch-sphere entanglement". We briefly discuss going beyond bipartite states, and we briefly present an interesting exception (from the above classification) for the case of just two qubits.

In Section 3.2 we explain the Peres-Horodecki entanglement criterion. In Section 3.3 we present a weaker entanglement criterion that we will use for proving our claims. In

Section 3.4 we introduce several important properties of Bloch spheres to be used in our proofs. In Section 3.5 we present a classification of all rank-2 states into five classes. In Section 3.6 we present entanglement measures based on the Bloch sphere and on the trace distance. In Section 3.7 we prove that no other classes exist. In Section 3.8 we prove that one of the classes does not exist in a specific case (the two-qubit case). In Section 3.9 we generalize some of our results to multipartite entanglement. In Section 3.10 we describe previous works in this area. In Section 3.11 we conclude.

3.2 The Peres-Horodecki Criterion

Given a system AB represented by the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, and given a mixed state $\rho_{AB} \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$ (namely, ρ_{AB} is a mixture of pure states in $\mathcal{H}_A \otimes \mathcal{H}_B$), we can represent ρ_{AB} as a matrix in the standard (computational) basis $\{|i\rangle_A \otimes |k\rangle_B\}_{i,k}$, as

$$\rho_{AB} = \sum_{i,j,k,l} a_{ijkl} |i\rangle_A \langle j|_A \otimes |k\rangle_B \langle l|_B, \tag{3.1}$$

where the scalars $a_{ijkl} \in \mathbb{C}$ are the matrix elements. (Notice that in the proof of Lemma 3.1, we define $C_{ijkl} \triangleq |i\rangle_A \langle j|_A \otimes |k\rangle_B \langle l|_B$, and thus we can represent ρ_{AB} as a linear combination of C_{ijkl}.)

We define the *partial transpose* of ρ_{AB} with respect to the subsystem B, denoted as $\rho_{AB}^{T_B}$, as

$$\rho_{AB}^{T_B} \triangleq \sum_{i,j,k,l} a_{ijkl} |i\rangle_A \langle j|_A \otimes |l\rangle_B \langle k|_B. \tag{3.2}$$

In other words, we perform the "transpose" operation only on the subsystem B and not on the subsystem A.

The Peres-Horodecki criterion [Per96, HHH96] says that *if* for a state ρ of the system AB, the operator ρ^{T_B} is not positive semidefinite (namely, if it has a negative eigenvalue), *then* ρ is entangled.

It was shown in [HHH96] that for systems of dimensions $2 \otimes 2$, $2 \otimes 3$, or $3 \otimes 2$, ρ is entangled *if and only if* ρ^{T_B} is not positive semidefinite. This was also proved to be true for states of rank 3 or less [HSTT03, CC08]. However, in higher dimensions and higher ranks there are entangled states (that are bound entangled states, namely, their entanglement cannot be distilled) that have a positive partial transpose [HHH96, Hor97, BDM$^+$99].

3.3 A Weaker Entanglement Criterion

We will use this weaker entanglement criterion for proving our claims:

Lemma 3.1. *Let ρ_{AB} be a state of a bipartite system.* ***If*** *there are states $|\phi_A\rangle$, $|\phi_B\rangle$, $|\psi_A\rangle$, and $|\psi_B\rangle$ such that $\langle \phi_A \phi_B | \rho_{AB} | \phi_A \phi_B \rangle = 0$ and $\langle \phi_A \psi_B | \rho_{AB} | \psi_A \phi_B \rangle \neq 0$,* ***then***

ρ_{AB} is entangled.

Proof. Let $\rho = \rho_{AB}$, $|\phi\rangle = |\phi_A \phi_B^\star\rangle$, and $|\psi\rangle = |\psi_A \psi_B^\star\rangle$, where $|\phi_B^\star\rangle$ and $|\psi_B^\star\rangle$ are obtained from $|\phi_B\rangle$ and $|\psi_B\rangle$ by replacing their amplitudes in the standard (computational) basis by their complex conjugates: if $|\phi_B\rangle = \sum_j \alpha_j |j\rangle$, then $|\phi_B^\star\rangle = \sum_j \alpha_j^\star |j\rangle$. We note that $\langle k|\phi_B^\star\rangle = \alpha_k^\star = \langle \phi_B|k\rangle$ and that $\langle \phi_B^\star|l\rangle = \alpha_l = \langle l|\phi_B\rangle$.

We first need a property of ρ^{T_B}. By definition, the partial transpose of $C_{ijkl} = |i\rangle\langle j| \otimes |k\rangle\langle l|$ is $C_{ijkl}^{T_B} = |i\rangle\langle j| \otimes |l\rangle\langle k|$, and the partial transpose ρ^{T_B} of ρ is obtained by a linear extension. Therefore, for C_{ijkl} it holds that

$$\begin{aligned} \langle \phi_A \phi_B^\star| \, C_{ijkl}^{T_B} \, |\psi_A \psi_B^\star\rangle &= \langle \phi_A|i\rangle\langle j|\psi_A\rangle\langle \phi_B^\star|l\rangle\langle k|\psi_B^\star\rangle \\ &= \langle \phi_A|i\rangle\langle j|\psi_A\rangle\langle \psi_B|k\rangle\langle l|\phi_B\rangle \\ &= \langle \phi_A \psi_B| \, C_{ijkl} \, |\psi_A \phi_B\rangle \,, \end{aligned} \tag{3.3}$$

and by linearity,

$$\langle \phi_A \phi_B^\star| \, \rho^{T_B} \, |\psi_A \psi_B^\star\rangle = \langle \phi_A \psi_B| \, \rho \, |\psi_A \phi_B\rangle \,. \tag{3.4}$$

If the condition of the Lemma is satisfied, then $\langle \phi_A \phi_B^\star| \, \rho^{T_B} \, |\phi_A \phi_B^\star\rangle = \langle \phi_A \phi_B| \, \rho \, |\phi_A \phi_B\rangle = 0$ and $\langle \phi_A \phi_B^\star| \, \rho^{T_B} \, |\psi_A \psi_B^\star\rangle = \langle \phi_A \psi_B| \, \rho \, |\psi_A \phi_B\rangle \neq 0$. From Lemma 3.2 it follows that ρ^{T_B} is not positive semidefinite. Therefore, by the Peres-Horodecki criterion, ρ is entangled.□

We declare this Lemma to be a "weaker" criterion because it proves entanglement only for a subclass of all the states satisfying the Peres-Horodecki criterion.

Lemma 3.2. *If a Hermitian operator A is positive semidefinite and $\langle \phi| \, A \, |\phi\rangle = 0$, then $\langle \phi| \, A \, |\psi\rangle = 0$ for all $|\psi\rangle$.*

Proof. Because A is a Hermitian operator, it has a spectral decomposition: $A = \sum_i \lambda_i |i\rangle\langle i|$ with $\lambda_i \geq 0$ (because A is positive semidefinite). It thus holds that

$$0 = \langle \phi| \, A \, |\phi\rangle = \sum_i \lambda_i \langle \phi|i\rangle\langle i|\phi\rangle = \sum_i \lambda_i |\langle \phi|i\rangle|^2. \tag{3.5}$$

Therefore, for any i satisfying $\lambda_i \neq 0$, it must hold that $\langle \phi|i\rangle = 0$. It follows that

$$\langle \phi| \, A \, |\psi\rangle = \sum_i \lambda_i \langle \phi|i\rangle\langle i|\psi\rangle = 0 \tag{3.6}$$

for all $|\psi\rangle$. □

Lemma 3.2 was presented earlier in a conference [BM14, BBM17].

3.4 Properties of Subspaces and Bloch Spheres

In the next sections, we also use the following results, that were also proved in [Hor97, HJW93] and mentioned in [OSU08]:

Lemma 3.3. *Let $\mathcal{H}'$ be a subspace of a Hilbert space $\mathcal{H}$. Let $\rho \in \mathcal{L}(\mathcal{H}')$ (i.e., ρ can be decomposed as a mixture of pure states from $\mathcal{H}'$). If $\rho = \sum_j q_j |\phi_j\rangle\langle\phi_j|$ is a decomposition of ρ with $|\phi_j\rangle \in \mathcal{H}$ and $q_j > 0$, then $|\phi_j\rangle \in \mathcal{H}'$ for all j.*

Proof. Let $\{|\psi_i\rangle\}_{i\in I'}$ be an orthonormal basis of the Hilbert space $\mathcal{H}'$. Since $\mathcal{H}' \subseteq \mathcal{H}$, we can extend this orthonormal basis to an orthonormal basis $\{|\psi_i\rangle\}_{i\in I}$ of $\mathcal{H}$ (where $I' \subseteq I$). Since $\rho \in \mathcal{L}(\mathcal{H}')$, and since $|\psi_i\rangle$ is orthogonal to $\mathcal{H}'$ for all $i \in I \setminus I'$, it holds that $\langle\psi_i| \rho |\psi_i\rangle = 0$ for all $i \in I \setminus I'$.

For all j, because $|\phi_j\rangle \in \mathcal{H}$, we can present $|\phi_j\rangle = \sum_{i\in I} a_{ji}|\psi_i\rangle$, with $a_{ji} = \langle\psi_i|\phi_j\rangle$. Then for all $i \in I \setminus I'$,

$$0 = \langle\psi_i| \rho |\psi_i\rangle = \sum_j q_j \langle\psi_i|\phi_j\rangle\langle\phi_j|\psi_i\rangle = \sum_j q_j |\langle\psi_i|\phi_j\rangle|^2 = \sum_j q_j |a_{ji}|^2. \tag{3.7}$$

Since $q_j > 0$ for all j, this implies that $a_{ji} = 0$ for all j and $i \in I \setminus I'$. Therefore, for all j, it holds that $|\phi_j\rangle = \sum_{i\in I'} a_{ji}|\psi_i\rangle$, which means that $|\phi_j\rangle \in \mathcal{H}'$. □

Corollary 3.4. *If a rank-2 mixed state ρ is inside a specific Bloch sphere, then all the pure states in all of its decompositions lie on the same Bloch sphere.*

Proof. If ρ is inside a specific Bloch sphere that represents the 2-dimensional Hilbert space $\mathcal{H}'$, then it can be represented as a mixture of pure states in $\mathcal{H}'$. Let us be given *any* decomposition of ρ as a mixture of pure states in some Hilbert space $\mathcal{H}$ (that can be assumed, without limiting generality, to have $\mathcal{H}'$ as a subspace), $\rho = \sum_j q_j |\phi_j\rangle\langle\phi_j|$. According to Lemma 3.3, it holds that $|\phi_j\rangle \in \mathcal{H}'$ for all j – namely, all the pure states in this decomposition are in $\mathcal{H}'$, and therefore they are on the same Bloch sphere. □

By using Corollary 3.4, we get:

Corollary 3.5. *If ρ is a rank-2 mixed state, then it lies inside a unique Bloch sphere (the uniqueness is up to a possible rotation of the sphere).*

Proof. ρ lies inside the Bloch sphere that is spanned by its two eigenstates; we now denote this Bloch sphere as $\mathcal{B}$. According to Corollary 3.4, all the other pure states in all the other decompositions of ρ lie on $\mathcal{B}$. Since all the Bloch spheres that contain ρ include at least two linearly independent pure states that are in a decomposition of ρ, and since those pure states are on $\mathcal{B}$ and thus span $\mathcal{B}$ (up to some rotation), we conclude that all the Bloch spheres containing ρ are the same as $\mathcal{B}$ (up to some rotation). □

Corollary 3.6. *If a rank-2 mixed state ρ is separable, then there exist at least two different pure separable states on its unique Bloch sphere.*

Proof. If ρ is separable, then it can be decomposed as a mixture of at least two pure states that are tensor product (separable) states. According to Corollary 3.4, those pure states lie on its unique Bloch sphere (that exists according to Corollary 3.5). □

3.5 Classification of Bloch-Sphere Entanglement

In the rest of this chapter we use Lemma 3.1 (a "weaker entanglement criterion"), Lemma 3.2 (a "positive semidefinite operators condition"), Corollary 3.5 (the "unique-Bloch-sphere corollary"), and Corollary 3.6 (a "separable states condition") in order to provide a classification of Bloch-sphere entanglement. This is based on the following understanding: if ρ is a bipartite rank-2 mixed state that is a mixture of pure states in the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, then according to Corollary 3.5, it lies inside a unique Bloch sphere (the uniqueness is up to a possible rotation); and this Bloch sphere corresponds to a 2-dimensional subspace of $\mathcal{H}_A \otimes \mathcal{H}_B$.

We present five different classes of 2-dimensional subspaces of a bipartite system, that are distinguished by their Bloch-sphere entanglement: (It is sufficient to consider only examples for which $\mathcal{H}_A$ is 2-dimensional ($\mathcal{H}_2$) and $\mathcal{H}_B$ is either 2-dimensional ($\mathcal{H}_2$) or 3-dimensional ($\mathcal{H}_3$).)

1. No entanglement at all

   Example in $\mathcal{H}_2 \otimes \mathcal{H}_2$: $\mathrm{Span}\{|00\rangle, |01\rangle\}$ (Figure 3.2)

2. Entanglement everywhere on and inside the sphere except a line (of separable states) connecting two *orthogonal* pure states on the sphere (e.g., the poles)

   Example in $\mathcal{H}_2 \otimes \mathcal{H}_2$: $\mathrm{Span}\{|00\rangle, |11\rangle\}$ (Figure 3.3)

3. Entanglement everywhere on and inside the sphere except a line (of separable states) connecting two *non-orthogonal* pure states on the sphere

   Example in $\mathcal{H}_2 \otimes \mathcal{H}_2$: $\mathrm{Span}\{|00\rangle, |{+}{+}\rangle\}$ (Figure 3.4)

4. Entanglement everywhere on and inside the sphere except a single separable point on the sphere

   Example in $\mathcal{H}_2 \otimes \mathcal{H}_2$: $\mathrm{Span}\{|00\rangle, \alpha|01\rangle + \beta|10\rangle\}$ with $\alpha\beta \neq 0$ (Figure 3.5 and Proposition 3.7)

5. Entanglement everywhere ("completely entangled subspace")

   Example in $\mathcal{H}_2 \otimes \mathcal{H}_3$: $\mathrm{Span}\left\{\frac{|00\rangle+|11\rangle}{\sqrt{2}}, \frac{|02\rangle+|10\rangle}{\sqrt{2}}\right\}$ (Figure 3.6 and Proposition 3.8)

   Does not exist in $\mathcal{H}_2 \otimes \mathcal{H}_2$. (Proof is given in Section 3.8, as Proposition 3.10.)

Very similar examples can be found in all the bipartite Hilbert spaces (if the dimensions of both subsystems are at least 2), except the example to Class 5, that does not exist in $\mathcal{H}_2 \otimes \mathcal{H}_2$.

The analysis of Classes 1-3 (see Figures 3.2-3.4) is very simple and follows directly from the proof of the general Theorem 3.9. Generally speaking, if two pure separable states exist on the Bloch sphere, then it belongs to one of those classes.

We now analyze the example for Class 4 (see Figure 3.5), a class that we found, yet was also found independently by [RA16a].

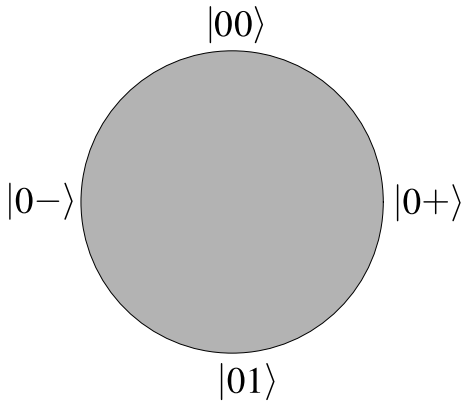

Figure 3.2: **Bloch sphere of the example for Class 1**: all the states on and inside this Bloch sphere are separable.

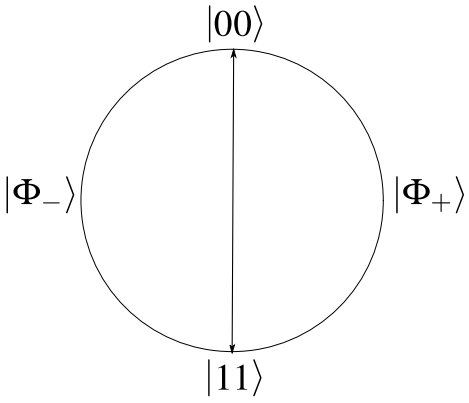

Figure 3.3: **Bloch sphere of the example for Class 2**: all the states along the line connecting $|00\rangle$ and $|11\rangle$ are separable; all the other states on and inside this Bloch sphere are entangled. Any two orthogonal product states can replace $|00\rangle$ and $|11\rangle$.

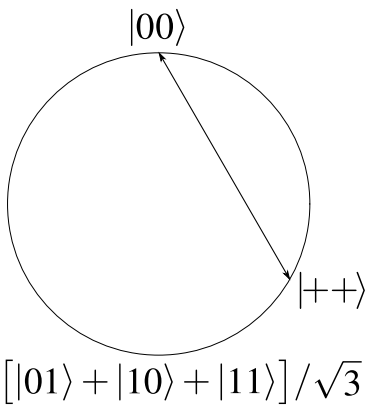

Figure 3.4: **Bloch sphere of the example for Class 3**: all the states along the line connecting $|00\rangle$ and $|{+}{+}\rangle$ are separable; all the other states on and inside this Bloch sphere are entangled. Any two non-orthogonal linearly independent product states can replace $|00\rangle$ and $|{+}{+}\rangle$.

Proposition 3.7. *Let* $|\psi_0\rangle = |00\rangle$ *and* $|\psi_1\rangle = \alpha|01\rangle + \beta|10\rangle$ *with* $\alpha\beta \neq 0$, $|\alpha|^2 + |\beta|^2 = 1$. *The state* $\rho = a_{00}|\psi_0\rangle\langle\psi_0| + a_{01}|\psi_0\rangle\langle\psi_1| + a_{10}|\psi_1\rangle\langle\psi_0| + a_{11}|\psi_1\rangle\langle\psi_1|$ *is separable if and only if* $a_{01} = a_{10} = a_{11} = 0$.

Proof. We look at two possible cases:

1. If $a_{11} \neq 0$, then:

$$\langle 11|\,\rho\,|11\rangle = 0 \tag{3.8}$$
$$\langle 10|\,\rho\,|01\rangle = a_{11}\langle 10|\psi_1\rangle\langle\psi_1|01\rangle = a_{11}\beta\alpha^\star \neq 0 \tag{3.9}$$

   Therefore, according to Lemma 3.1 (the "weaker entanglement criterion"), ρ is entangled.

2. If $a_{11} = 0$, then:

$$\langle\psi_1|\,\rho\,|\psi_1\rangle = a_{11} = 0 \tag{3.10}$$
$$\langle\psi_1|\,\rho\,|\psi_0\rangle = a_{10} \tag{3.11}$$

   Therefore, according to Lemma 3.2 (a "positive semidefinite operators condition"), because ρ is positive semidefinite, it must hold that $a_{10} = 0$. This implies that $a_{01} = a_{10}^\star = 0$. Therefore, $a_{01} = a_{10} = a_{11} = 0$.

We conclude that if ρ is separable, it must hold that $a_{11} = 0$ (otherwise, ρ would be entangled), and thus $a_{01} = a_{10} = a_{11} = 0$. On the other hand, if ρ is entangled, $a_{11} \neq 0$. This concludes our proof. □

Finally, for the example of Class 5 (see Figure 3.6):

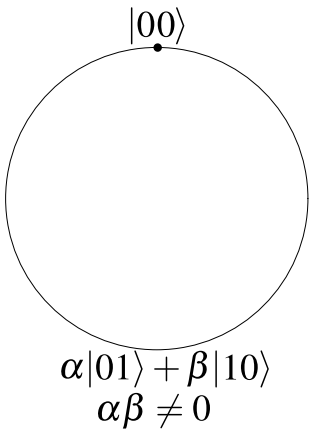

Figure 3.5: **Bloch sphere of the example for Class 4**: only the state $|00\rangle$ is separable; all the other states on and inside this Bloch sphere are entangled.

Proposition 3.8. *Let* $|\psi_0\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ *and* $|\psi_1\rangle = \frac{|02\rangle+|10\rangle}{\sqrt{2}}$. *The state* $\rho = a_{00}|\psi_0\rangle\langle\psi_0| + a_{01}|\psi_0\rangle\langle\psi_1| + a_{10}|\psi_1\rangle\langle\psi_0| + a_{11}|\psi_1\rangle\langle\psi_1|$ *is* <u>*always*</u> *entangled.*

Proof. By using Corollary 3.6 (the "separable states condition"), it is sufficient to prove that all the pure states $|\psi\rangle = \alpha|\psi_0\rangle + \beta|\psi_1\rangle$ are entangled: if all the pure states on the Bloch sphere are entangled, then all the mixed states inside the Bloch sphere are entangled.

Let us look at the state

$$\begin{aligned} |\psi\rangle &= \alpha|\psi_0\rangle + \beta|\psi_1\rangle \\ &= \frac{\alpha}{\sqrt{2}}|00\rangle + \frac{\alpha}{\sqrt{2}}|11\rangle + \frac{\beta}{\sqrt{2}}|02\rangle + \frac{\beta}{\sqrt{2}}|10\rangle \\ &\triangleq \sum_{i,j} \epsilon_{ij}|i\rangle|j\rangle. \end{aligned} \tag{3.12}$$

Assume by contradiction that $|\psi\rangle$ is separable. In this case, there must exist a_0, a_1 and b_0, b_1, b_2 such that $|\psi\rangle = \left(\sum_{i=0}^{1} a_i|i\rangle\right) \otimes \left(\sum_{j=0}^{2} b_j|j\rangle\right)$, and, therefore, $\epsilon_{ij} = a_i b_j$ for all i, j. This means that the equations $\epsilon_{01} = a_0 b_1 = 0$ and $\epsilon_{12} = a_1 b_2 = 0$ must hold.

We notice that if $a_0 = 0$, then $\alpha = \beta = 0$, and that if $b_1 = 0$, then $\alpha = 0$. Therefore, from the equation $\epsilon_{01} = a_0 b_1 = 0$ we deduce that $\alpha = 0$. Similarly, from the equation $\epsilon_{12} = a_1 b_2 = 0$ we deduce that $\beta = 0$. Therefore, we see that $\alpha = \beta = 0$, which is impossible.

We conclude that there are no separable pure states on the Bloch sphere. Therefore, by Corollary 3.6, there cannot be separable mixed states inside the Bloch sphere. □

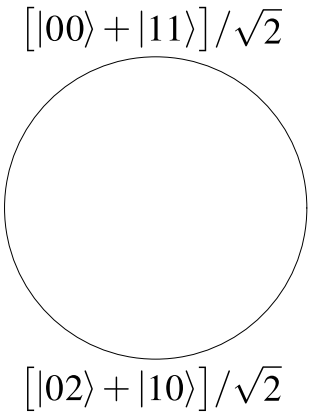

Figure 3.6: **Bloch sphere of the example for Class 5**: all the states on and inside this Bloch sphere are entangled.

3.6 Entanglement Measures inside the Bloch Sphere

Our classification suggests natural ways to measure entanglement inside the Bloch sphere: for example, entanglement may be measured by the Euclidean distance to the closest separable state (e.g., given the Bloch sphere Span$\{|00\rangle, |11\rangle\}$, the closest separable state to the pure state $\alpha|00\rangle + \beta|11\rangle$ is the state $|\alpha|^2|00\rangle\langle 00| + |\beta|^2|11\rangle\langle 11|$) – namely, by twice the *trace distance* to the closest separable state. We note that this entanglement measure, unlike the measures analyzed by [LOSU06, OSU08], vanishes only for separable states. Analyzing the properties of such measures is beyond the scope of this work.

3.7 A Proof that There are Exactly Five Classes of "Bloch-Sphere Entanglement"

Our main goal is to provide a full analysis of the general bipartite case. We prove that the classes we found are the only classes that exist in the bipartite case, for all the rank-2 bipartite states (namely, for all the corresponding 2-dimensional Hilbert spaces):

Theorem 3.9. *Let $\mathcal{H}$ be a 2-dimensional subspace of $\mathcal{H}_A \otimes \mathcal{H}_B$, where $\mathcal{H}_A$ and $\mathcal{H}_B$ are two Hilbert spaces. Then $\mathcal{H}$ belongs to one of the following classes:*

Class 1 *The Bloch ball of $\mathcal{H}$ is completely separable.*

Classes 2+3 *The Bloch ball of $\mathcal{H}$ has one line of separable states, and all the other states are entangled.*

Class 4 *The Bloch ball of $\mathcal{H}$ has one separable point (pure state), and all the other states are entangled.*

Class 5 *The Bloch ball of $\mathcal{H}$ is completely entangled.*

(We note that Class 2 and Class 3 are discussed together, because in both of them the Bloch ball has just one line of separable states.)

Proof. First, assume that there is no separable *mixed* state inside the Bloch ball. This means that there is at most one pure separable state on the Bloch sphere (because if two pure states are separable, then the line connecting them inside the Bloch ball is separable, too). This matches Classes 4 and 5.

Now assume that there is a separable *mixed* state ρ inside the Bloch ball. According to Corollary 3.6 (the "separable states condition"), this means that there are at least two different pure separable states on the Bloch sphere. We denote them by $|\psi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$ and $|\phi\rangle = |\phi_A\rangle \otimes |\phi_B\rangle$.

We note that $|\psi\rangle \ncong |\phi\rangle$ (defining the symbol $\cong$ to be "equality as normalized states, possibly with different global phases"; thus, the symbol $\ncong$ means that the two normalized states are really different, as opposed to states that are equal up to a global phase), which means that $|\psi\rangle$ and $|\phi\rangle$ are linearly independent. Therefore, the Bloch sphere represents the 2-dimensional subspace $\mathrm{Span}\{|\psi\rangle, |\phi\rangle\}$, which means that all the mixed states inside the Bloch ball are of the form:

$$\rho = a_{00}|\psi\rangle\langle\psi| + a_{01}|\psi\rangle\langle\phi| + a_{10}|\phi\rangle\langle\psi| + a_{11}|\phi\rangle\langle\phi| \tag{3.13}$$

If $|\psi_A\rangle \cong |\phi_A\rangle$ or $|\psi_B\rangle \cong |\phi_B\rangle$, then obviously all the states on and inside the Bloch sphere are separable, which matches Class 1.

If $|\psi_A\rangle \ncong |\phi_A\rangle$ and $|\psi_B\rangle \ncong |\phi_B\rangle$, then we prove that only the line connecting $|\psi\rangle$ and $|\phi\rangle$ inside the Bloch ball is separable, and that all the other pure and mixed states in the Bloch ball are entangled. This will match Classes 2+3, and will conclude our proof.

We look at all the mixed states of the form (3.13). If $a_{01} = a_{10} = 0$, then we obviously get a separable state:

$$\rho = a_{00}|\psi_A\rangle\langle\psi_A| \otimes |\psi_B\rangle\langle\psi_B| + a_{11}|\phi_A\rangle\langle\phi_A| \otimes |\phi_B\rangle\langle\phi_B| \tag{3.14}$$

If $a_{10} \neq 0$, then: let $|\overline{\phi_A}\rangle \in \mathcal{H}_A$ satisfy $\langle\phi_A|\overline{\phi_A}\rangle = 0$ and $\langle\psi_A|\overline{\phi_A}\rangle \neq 0$ ($|\overline{\phi_A}\rangle$ always exists, because $|\psi_A\rangle \ncong |\phi_A\rangle$). Similarly, let $|\overline{\psi_A}\rangle \in \mathcal{H}_A$ and $|\overline{\phi_B}\rangle, |\overline{\psi_B}\rangle \in \mathcal{H}_B$ satisfy similar properties (because $|\psi_B\rangle \ncong |\phi_B\rangle$). Then

$$\left\langle \overline{\psi_A}\ \overline{\phi_B} \right| \rho \left| \overline{\psi_A}\ \overline{\phi_B} \right\rangle = 0, \tag{3.15}$$

and

$$\begin{aligned} \left\langle \overline{\psi_A}\ \overline{\psi_B} \right| \rho \left| \overline{\phi_A}\ \overline{\phi_B} \right\rangle &= a_{10}\langle \overline{\psi_A}\ \overline{\psi_B} | \phi_A\phi_B\rangle\langle\psi_A\psi_B|\overline{\phi_A}\ \overline{\phi_B}\rangle \\ &= a_{10}\langle\overline{\psi_A}|\phi_A\rangle\langle\overline{\psi_B}|\phi_B\rangle\langle\psi_A|\overline{\phi_A}\rangle\langle\psi_B|\overline{\phi_B}\rangle \\ &\neq 0. \end{aligned} \tag{3.16}$$

Therefore, by Lemma 3.1 (the "weaker entanglement criterion"), if $a_{10} \neq 0$ (or $a_{01} \neq 0$ – this is equivalent, because $a_{01} = a_{10}^{\star}$), then ρ is entangled.

We conclude that only the line between $|\psi\rangle$ and $|\phi\rangle$ (i.e., the line of states satisfying $a_{01} = a_{10} = 0$) is separable, and that the other states (i.e., the states satisfying $a_{10} \neq 0$ or $a_{01} \neq 0$) are entangled, which matches Classes 2+3. This concludes our proof. □

3.8 A Proof that Class 5 Does Not Exist in the Two-Qubit Case

We have seen that for almost all the bipartite Hilbert spaces, five classes appear. We now show that for the Hilbert space $\mathcal{H}_2 \otimes \mathcal{H}_2$, only four classes exist (Classes 1-4):

Proposition 3.10. *No 2-dimensional subspace of $\mathcal{H}_2 \otimes \mathcal{H}_2$ is completely entangled.*

Proof. This proof follows the methods of [OSU08]. For a two-qubit state $|\psi\rangle = \sum_{i,j} a_{ij}|i\rangle|j\rangle$, the entanglement measure named "concurrence", that is denoted by C, is defined as follows [HW97, Woo01]:

$$C(\psi) = 2|a_{00}a_{11} - a_{01}a_{10}| \tag{3.17}$$

In particular, $C(\psi) = 0$ if and only if $|\psi\rangle$ is separable. (This is not necessarily true for other entanglement measures.)

Let $\mathcal{H} \triangleq \mathrm{Span}\{|\psi_0\rangle, |\psi_1\rangle\}$ be a 2-dimensional subspace of $\mathcal{H}_2 \otimes \mathcal{H}_2$. Let us represent:

$$|\psi_0\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle \tag{3.18}$$

$$|\psi_1\rangle = b_{00}|00\rangle + b_{01}|01\rangle + b_{10}|10\rangle + b_{11}|11\rangle \tag{3.19}$$

We may assume that $C(\psi_1) \neq 0$ (otherwise, $|\psi_1\rangle$ is separable, hence $\mathcal{H}$ cannot be completely entangled). Therefore, the set of separable pure states in $\mathcal{H}$ (if we ignore normalization) is the set of non-normalized states $|\psi_0\rangle + z|\psi_1\rangle$ satisfying the equation

$$C(|\psi_0\rangle + z|\psi_1\rangle) = 0, \tag{3.20}$$

that rewrites as

$$2|(a_{00} + b_{00}z)(a_{11} + b_{11}z) - (a_{01} + b_{01}z)(a_{10} + b_{10}z)| = 0, \tag{3.21}$$

or, removing the absolute value, as

$$2[(a_{00} + b_{00}z)(a_{11} + b_{11}z) - (a_{01} + b_{01}z)(a_{10} + b_{10}z)] = 0. \tag{3.22}$$

This is a quadratic equation in the complex variable z. The coefficient of z^2 is $2[b_{00}b_{11} - b_{01}b_{10}]$, whose absolute value is $C(\psi_1) \neq 0$. Therefore, according to the

fundamental theorem of algebra, there are two solutions $\xi_1, \xi_2 \in \mathbb{C}$ (possibly equal) to this equation. Thus, the non-normalized state $|\psi_0\rangle + \xi_1|\psi_1\rangle$ in $\mathcal{H}$ (and its normalization in $\mathcal{H}$) must be separable. Therefore, there is a separable state in $\mathcal{H}$, and $\mathcal{H}$ cannot be completely entangled. □

3.9 Examples and Analysis of Multipartite Entanglement

For multipartite states, there are several different definitions of separability and entanglement: an m-partite mixed state is "fully separable" if it is a mixture of pure states that are products of m pure states; and it is "separable with respect to a bipartite partition $\mathcal{P}$" (with $\mathcal{P}$ partitioning the m subsystems into two disjoint sets) if the bipartite state corresponding to the partition $\mathcal{P}$ is separable [HHHH09]. For example, the state $|0\rangle_A|\Phi_+\rangle_{BC} \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ is separable with respect to the partition $\{\{1\},\{2,3\}\}$, but is entangled with respect to both partitions $\{\{1,2\},\{3\}\}$ and $\{\{1,3\},\{2\}\}$. Note that even if a state is separable with respect to all the bipartite partitions, it may still be entangled (i.e., not fully separable) [BDM$^+$99].

To illustrate the many existing possibilities for Bloch spheres in the multipartite case, we look at two examples:

1. Span$\{|000\rangle, |111\rangle\}$: the line connecting between the north pole ($|000\rangle$) and the south pole ($|111\rangle$) is fully separable; all the other points are entangled with respect to *any* bipartite partition.

2. Span$\{|000\rangle, |011\rangle\}$: the line connecting between the north pole ($|000\rangle$) and the south pole ($|011\rangle$) is fully separable; all the other points are separable with respect to the bipartite partition $\{\{1\},\{2,3\}\}$, but are entangled with respect to the partitions $\{\{1,2\},\{3\}\}$ and $\{\{1,3\},\{2\}\}$.

The proofs of separability above are direct from the definitions; and the proofs of entanglement are implied by our analysis in the proof of Theorem 3.9.

Moreover, our Theorem 3.9 is true also for the set of *fully separable* states in the multipartite case:

Theorem 3.11. *Let $\mathcal{H}$ be a 2-dimensional subspace of $\mathcal{H}_{A_1} \otimes \cdots \otimes \mathcal{H}_{A_m}$, where $\mathcal{H}_{A_1}, \ldots, \mathcal{H}_{A_m}$ are Hilbert spaces. Then $\mathcal{H}$ belongs to one of the following classes:*

Class 1 *All the states inside the Bloch ball of $\mathcal{H}$ are fully separable.*

Classes 2+3 *The Bloch ball of $\mathcal{H}$ has one line of fully separable states, and all the other states are not fully separable.*

Class 4 *The Bloch ball of $\mathcal{H}$ has one fully separable point (pure state), and all the other states are not fully separable.*

Class 5 *All the states inside the Bloch ball of $\mathcal{H}$ are not fully separable.*

Proof. First, assume that there is no fully separable *mixed* state inside the Bloch ball. This means that there is at most one pure fully-separable state on the Bloch sphere (because if two pure states are fully separable, then the line connecting them inside the Bloch ball is fully separable, too). This matches Classes 4 and 5.

Now assume that there is a fully separable *mixed* state ρ inside the Bloch ball. According to Corollary 3.6 (the "separable states condition"), this means that there are at least two different fully separable pure states on the Bloch sphere. We denote them by $|\psi\rangle = |\psi_{A_1}\rangle \otimes \cdots \otimes |\psi_{A_m}\rangle$ and $|\phi\rangle = |\phi_{A_1}\rangle \otimes \cdots \otimes |\phi_{A_m}\rangle$.

We note that $|\psi\rangle \ncong |\phi\rangle$ (defining the symbol $\cong$ as we did in the proof of Theorem 3.9 above; thus, the symbol $\ncong$ means that the two normalized states are really different, as opposed to states that are equal up to a global phase), which means that $|\psi\rangle$ and $|\phi\rangle$ are linearly independent. Therefore, the Bloch sphere represents the 2-dimensional subspace $\mathrm{Span}\{|\psi\rangle, |\phi\rangle\}$, which means that all the mixed states inside the Bloch ball are of the form:

$$\rho = a_{00}|\psi\rangle\langle\psi| + a_{01}|\psi\rangle\langle\phi| + a_{10}|\phi\rangle\langle\psi| + a_{11}|\phi\rangle\langle\phi| \tag{3.23}$$

If $|\psi_{A_i}\rangle \cong |\phi_{A_i}\rangle$ for all i except one value of i, then obviously all the states on and inside the Bloch sphere are fully separable, which matches Class 1.

If $|\psi_{A_{i_1}}\rangle \ncong |\phi_{A_{i_1}}\rangle$ and $|\psi_{A_{i_2}}\rangle \ncong |\phi_{A_{i_2}}\rangle$ for $i_1 < i_2$, then we prove that given the bipartite partition $\{I_1, I_2\}$ with $I_1 = \{1, \ldots, i_1\}$ and $I_2 = \{i_1 + 1, \ldots, m\}$ (satisfying $I_1 \cup I_2 = \{1, \ldots, m\}$, $I_1 \cap I_2 = \emptyset$, $i_1 \in I_1$, and $i_2 \in I_2$), it holds that only the line connecting $|\psi\rangle$ and $|\phi\rangle$ inside the Bloch ball is fully separable, and that all the other pure and mixed states in the Bloch ball are entangled with respect to the partition $\{I_1, I_2\}$. This will match Classes 2+3, and will conclude our proof.

To prove that the line is fully separable, we notice that any convex combination of fully separable states is fully separable. Therefore, the line connecting $|\psi\rangle$ and $|\phi\rangle$ inside the Bloch ball is fully separable.

To prove that all the other states are entangled with respect to the partition $\{I_1, I_2\}$, we denote $|\psi^{I_1}\rangle = |\psi_{A_1}\rangle \otimes \cdots \otimes |\psi_{A_{i_1}}\rangle$ and $|\psi^{I_2}\rangle = |\psi_{A_{i_1+1}}\rangle \otimes \cdots \otimes |\psi_{A_m}\rangle$; and similarly, we define $|\phi^{I_1}\rangle$ and $|\phi^{I_2}\rangle$. Then, because $i_1 < i_2$, and because $|\psi_{A_{i_1}}\rangle \ncong |\phi_{A_{i_1}}\rangle$ and $|\psi_{A_{i_2}}\rangle \ncong |\phi_{A_{i_2}}\rangle$, it must hold that $|\psi^{I_1}\rangle \ncong |\phi^{I_1}\rangle$ and $|\psi^{I_2}\rangle \ncong |\phi^{I_2}\rangle$. It also holds that $|\psi\rangle = |\psi^{I_1}\rangle \otimes |\psi^{I_2}\rangle$ and $|\phi\rangle = |\phi^{I_1}\rangle \otimes |\phi^{I_2}\rangle$; therefore, according to the proof of the original Theorem 3.9, it holds that all the states outside of the line connecting $|\psi\rangle$ and $|\phi\rangle$ in the Bloch ball (i.e., all the states satisfying $a_{01} \neq 0$ or $a_{10} \neq 0$) are entangled with respect to the partition $\{I_1, I_2\}$. Together with the proof that all the states on that line (i.e., all the states satisfying $a_{01} = a_{10} = 0$) are fully separable, this matches Classes 2+3, and concludes our proof. □

Extensions of Theorem 3.9 to other cases of multipartite entanglement are beyond the scope of this work.

3.10 Previous Works

The existence of completely entangled subspaces has been discussed in many papers before. In particular, this notion was used in [BDM+99] to prove the existence of a huge class of bound entangled states.

Analysis of entangled states in a Hilbert subspace, using *specific* entanglement measures (e.g., the concurrence and the 3-tangle) and Bloch spheres, was done by [LOSU06] and [OSU08]. However, the entanglement measures they choose usually vanish not only for all the separable states, but also for some of the entangled states [OSU08]. Much more recently, [RA16a] and [RA16b] investigated interesting classes in the *same* research direction. In contrast, this chapter analyzes the separability and the entanglement in the Bloch sphere for any rank-2 bipartite state; and, instead of using a specific entanglement measure that *cannot show the entanglement* of some of the entangled states, we fully characterize the set of separable states on and inside the state's Bloch sphere.

3.11 Conclusion

We have found a complete classification of the possible sets of separable states in all the 2-dimensional subspaces of bipartite Hilbert spaces. Our result is general and is not limited to specific entanglement measures or to specific bipartite spaces, but it applies to all the bipartite Hilbert spaces, and it extends to the sets of fully separable states in multipartite spaces. Moreover, the result makes it possible to define natural measures that vanish exactly on the separable states.

Our analysis identifies the set of "Bloch-sphere neighbor states" of any rank-2 state (namely, the set of states in its Bloch sphere). Such Bloch-sphere neighbor states may be useful for various protocols: for example, entanglement purification or error correction protocols may first turn the state into a Bloch-sphere neighbor state of desired properties (e.g., more entangled), and then operate on that Bloch-sphere neighbor state. Those possibilities may be explored by future research.

Other potential applications of our geometrical view include analyzing many possible physical and algorithmic processes defined by using two pure states. Namely, our results and the geometrical intuition they provide may be useful for analyzing the separability and entanglement during processes in which two pure states play important roles. Potential examples, that are left for future research, include the Bloch sphere spanned by an entangled ground state of some Hamiltonian and by the closest pure separable state to this ground state with respect to some entanglement measure, and the Bloch sphere spanned by the initial state and the final state of some quantum algorithm (for example, Grover's algorithm). In those examples (and in many others), the entanglement and separability (and other quantum features) along various paths on and inside the Bloch sphere can be analyzed, and the Bloch sphere itself can be classified.

It may be possible to extend our results into higher-rank mixed states: for example, it is possible to look at "portions" of the higher-rank states (e.g., a non-degenerate rank-3 state defines three Bloch spheres, each corresponding to two out of the three eigenstates); and it is possible to analyze higher-rank states that are ϵ-close ($\epsilon \ll 1$) to rank-2 states.

Another relevant direction for extending our results into higher-rank mixed states is finding ways to characterize the set of separable states in the relevant higher-dimensional Hilbert subspace, *without* having the intuitive geometrical visualization on the Bloch sphere. The definitions of the classes easily extend into higher dimensions (e.g., Classes 2+3 mean that the set of separable states is the set of all mixtures of two linearly independent pure separable states; a possible generalization into higher dimensions is a set of separable states that equals to the set of all mixtures of k linearly independent pure separable states). As a trivial example, the 3-dimensional Hilbert subspace $\mathrm{Span}\{|00\rangle, |01\rangle, |02\rangle\} \subseteq \mathcal{H}_2 \otimes \mathcal{H}_3$ is completely separable, so it is a generalization of Class 1. Lemmas 3.1-3.3 already apply to higher-rank mixed states; Corollaries 3.4-3.6 trivially apply to higher-rank mixed states and to higher-dimensional Hilbert subspaces (without the geometrical visualization on the Bloch sphere); and Proposition 3.10 trivially applies to higher-dimensional Hilbert subspaces of $\mathcal{H}_2 \otimes \mathcal{H}_2$. However, generalizing the examples presented in Section 3.5 (and their corresponding Propositions, 3.7 and 3.8) and the full classification presented in Theorems 3.9 and 3.11 into higher-dimensional Hilbert subspaces is not trivial and is left for future research.

Chapter 4

Security Against Collective Attacks of a Modified BB84 QKD Protocol with Information only in One Basis

In this chapter, we prove the security against collective attacks of a protocol named "BB84-INFO-z" that is slightly different from BB84, and we use the trace distance for making the proof more composable than similar previous security proofs of BB84.

This chapter is based on the published conference paper [BLM17b].

4.1 Introduction

Quantum key distribution (QKD) protocols take advantage of the laws of quantum mechanics, and most of them can be proven secure even against powerful adversaries limited only by the laws of physics. The two parties (Alice and Bob) want to create a shared random key, using an insecure quantum channel and an unjammable classical channel (to which the adversary may listen, but not interfere). The adversary (eavesdropper), Eve, tries to get as much information as she can on the final shared key. The first and most important QKD protocol is BB84 [BB84].

Boyer, Gelles, and Mor [BGM09] discussed the security of the BB84 protocol against collective attacks. Collective attacks [BM97b, BM97a, BBB$^+$02] are a subclass of the joint attacks; joint attacks are the most powerful theoretical attacks. [BGM09] improved the security proof of Biham, Boyer, Brassard, van de Graaf, and Mor [BBB$^+$02] against collective attacks, by using some techniques of Biham, Boyer, Boykin, Mor, and Roychowdhury [BBB$^+$06] (that proved security against joint attacks). In this chapter, too, we restrict the analysis to collective attacks, because security against collective attacks is conjectured (and, in some security notions, proved [Ren08, CKR09]) to imply

security against joint attacks. In addition, proving security against collective attacks is much simpler than proving security against joint attacks.

In many QKD protocols, including BB84, Alice and Bob exchange several types of bits (encoded as quantum systems, usually qubits): INFO bits, that are secret bits shared by Alice and Bob and are used for generating the final key (via classical processes of error correction and privacy amplification); and TEST bits, that are publicly exposed by Alice and Bob (by using the classical channel) and are used for estimating the error rate. In BB84, each bit is sent from Alice to Bob in a random basis (the z basis or the x basis).

In this chapter, we extend the analysis of BB84 done in [BGM09] and prove the security of a QKD protocol we shall name *BB84-INFO-z*. This protocol is almost identical to BB84, except that all its INFO bits are in the z basis. In other words, the x basis is used only for testing. The bits are thus partitioned into three disjoint sets: INFO, TEST-Z, and TEST-X. The sizes of these sets are arbitrary (n INFO bits, n_z TEST-Z bits, and n_x TEST-X bits).

We note that, while this chapter follows a line of research that mainly discusses a specific approach of security proof for BB84 and similar protocols (this approach, notably, considers finite-key effects and not only the asymptotic error rate), many other approaches have also been suggested: see for example [May01, SP00, Ren08, RGK05].

In the other papers ([BM97b, BM97a, BBB$^+$02, BBB$^+$06, BGM09]) that discussed the same approach of security proofs as discussed here, the classical mutual information between Eve and the final key was calculated and bounded, which caused problems with composability (see definition in [Ren08] and in Section 2.4). In contrast to those papers, in this chapter we suggest a method to partially avoid those problems: we calculate and bound the trace distance between any two density matrices Eve may hold. This method is more composable, because it bounds the distance between the *quantum* states of Eve instead of bounding the *classical* information she has (bounding the classical information means, in particular, that we assume that Eve measures at the end of the protocol, while in reality she is not required to measure then, but is allowed to wait until Alice and Bob use the final key). This method is implemented in this chapter for the security proof of BB84-INFO-z; it also directly applies to the BB84 security proof in [BGM09], and it may be extended in the future to show that the BB84 security proofs of [BGM09], [BBB$^+$02], and [BBB$^+$06] prove the composable security of BB84.

The "qubit space", $\mathcal{H}_2$, is a 2-dimensional Hilbert space. The states $|0^0\rangle, |1^0\rangle$ form an orthonormal basis of $\mathcal{H}_2$, called "the computational basis" or "the z basis". The states $|0^1\rangle \triangleq \frac{|0^0\rangle+|1^0\rangle}{\sqrt{2}}$ and $|1^1\rangle \triangleq \frac{|0^0\rangle-|1^0\rangle}{\sqrt{2}}$ form another orthonormal basis of $\mathcal{H}_2$, called "the x basis". Those two bases are said to be *conjugate bases*. (Those notations are useful for us in the current chapter, and they are used in [BGM09] and in [BLM17b]. In the other chapters, $|0^0\rangle, |1^0\rangle, |0^1\rangle, |1^1\rangle$ were denoted by $|0\rangle, |1\rangle, |+\rangle, |-\rangle$, respectively.)

In this chapter, bit strings of some length t are denoted by a bold letter (e.g., $\mathbf{i} = i_1 \dots i_t$ with $i_1, \dots, i_t \in \{0, 1\}$) and are identified to elements of the t-dimensional

$\mathbf{F}_2$-vector space $\mathbf{F}_2^t$, where $\mathbf{F}_2 = \{0,1\}$ and the addition of two vectors corresponds to a XOR operation. The number of 1-bits in a bit string $\mathbf{s}$ is denoted by $|\mathbf{s}|$, and the Hamming distance between two strings $\mathbf{s}$ and $\mathbf{s}'$ is $d_H(\mathbf{s},\mathbf{s}') = |\mathbf{s}+\mathbf{s}'|$.

4.2 Formal Description of the BB84-INFO-z Protocol

Below we describe the BB84-INFO-z protocol used in this chapter.

1. Alice and Bob pre-agree on numbers n, n_z, and n_x (we denote $N \triangleq n + n_z + n_x$), on error thresholds $p_{a,z}$ and $p_{a,x}$, on a linear error-correcting code C with an $r \times n$ parity check matrix P_C, and on a linear key-generation function (privacy amplification) represented by an $m \times n$ matrix P_K. It is required that *all* the $r+m$ rows of the matrices P_C and P_K put together are linearly independent.

2. Alice randomly chooses a partition $\mathcal{P} = (\mathbf{s},\mathbf{z},\mathbf{b})$ of the N bits by randomly choosing three N-bit strings $\mathbf{s},\mathbf{z},\mathbf{b} \in \mathbf{F}_2^N$ that satisfy $|\mathbf{s}| = n, |\mathbf{z}| = n_z, |\mathbf{b}| = n_x$, and $|\mathbf{s}+\mathbf{z}+\mathbf{b}| = N$. Thus, $\mathcal{P}$ partitions the set of indexes $\{1,2,...,N\}$ into three disjoint sets:

   - I (INFO bits, where $s_j = 1$) of size n;
   - T_Z (TEST-Z bits, where $z_j = 1$) of size n_z; and
   - T_X (TEST-X bits, where $b_j = 1$) of size n_x.

3. Alice randomly chooses an N-bit string $\mathbf{i} \in \mathbf{F}_2^N$ and sends the N qubit states $|i_1^{b_1}\rangle, |i_2^{b_2}\rangle, \ldots, |i_N^{b_N}\rangle$, one after the other, to Bob using the quantum channel. Notice that the INFO and TEST-Z bits are encoded in the z basis, while the TEST-X bits are encoded in the x basis. Bob keeps each received qubit in quantum memory, not measuring it yet[1].

4. Alice publicly sends to Bob the string $\mathbf{b} = b_1 \ldots b_N$. Bob measures each saved qubit in the correct basis (namely, if $b_i = 0$ then he measures the i-th qubit in the z basis, and if $b_i = 1$ then he measures it in the x basis).

   The bit string measured by Bob is denoted by $\mathbf{i}^B$. If there is no noise and no eavesdropping, then $\mathbf{i}^B = \mathbf{i}$.

5. Alice publicly sends to Bob the string $\mathbf{s}$. The INFO bits, used for generating the final key, are the n bits with $s_j = 1$, while the TEST-Z and TEST-X bits are the $n_z + n_x$ bits with $s_j = 0$. The substrings of $\mathbf{i},\mathbf{b}$ that correspond to the INFO bits are denoted by $\mathbf{i_s}$ and $\mathbf{b_s}$.

[1] Here we assume that Bob has a quantum memory and can delay his measurement. In practical implementations, Bob usually cannot do that, but is assumed to measure in a randomly-chosen basis (z or x), so that Alice and Bob later discard the qubits measured in the wrong basis. In that case, we need to assume that Alice sends more than N qubits, so that N qubits are finally detected by Bob and measured in the correct basis.

6. Alice and Bob both publish their values of all the TEST-Z and TEST-X bits, and they compare the bit values. If more than $n_z \cdot p_{a,z}$ TEST-Z bits are different between Alice and Bob *or* more than $n_x \cdot p_{a,x}$ TEST-X bits are different between them, they abort the protocol. We note that $p_{a,z}$ and $p_{a,x}$ (the pre-agreed error thresholds) are the maximal allowed error rates on the TEST-Z and TEST-X bits, respectively – namely, in each basis (z and x) separately.

7. Alice and Bob keep the values of the remaining n bits (the INFO bits, with $s_j = 1$) secret. The bit string of Alice is denoted $\mathbf{x} = \mathbf{i_s}$, and the bit string of Bob is denoted $\mathbf{x}^B$.

8. Alice sends to Bob the r-bit string $\boldsymbol{\xi} = \mathbf{x}P_C^{\mathrm{T}}$, that is called the *syndrome* of $\mathbf{x}$ (with respect to the error-correcting code C and to its corresponding parity check matrix P_C). By using $\boldsymbol{\xi}$, Bob corrects the errors in his $\mathbf{x}^B$ string (so that it is the same as $\mathbf{x}$).

9. Alice and Bob compute the m-bit final key $\mathbf{k} = \mathbf{x}P_K^{\mathrm{T}}$.

The protocol is defined similarly to BB84 (and to its description in [BGM09]), except that it uses the generalized bit numbers n, n_z, and n_x (numbers of INFO, TEST-Z, and TEST-X bits, respectively); that it uses the partition $\mathcal{P} = (\mathbf{s}, \mathbf{z}, \mathbf{b})$ for dividing the N-bit string $\mathbf{i}$ into three disjoint sets of indexes (I, T_Z, and T_X); and that it uses two separate thresholds ($p_{a,z}$ and $p_{a,x}$) instead of one (p_a).

4.3 Security Proof of BB84-INFO-z Against Collective Attacks

4.3.1 The General Collective Attack of Eve

Before the QKD protocol is performed (and, thus, independently of $\mathbf{i}$ and $\mathcal{P}$), Eve chooses some collective attack to perform. A *collective attack* is bitwise: each qubit is attacked separately, by using a separate probe (ancillary state) that is attached by Eve and saved by her in a quantum memory. Eve can keep her quantum probes indefinitely, even after the final key is used by Alice and Bob; and she can perform, at any time of her choice, an optimal measurement of all her probes together, chosen based on all the information she has at the time of the measurement (including the classical information sent during the protocol, and including the information she acquires when Alice and Bob use the key).

Given the j-th qubit $|i_j^{b_j}\rangle_{T_j}$ sent from Alice to Bob ($1 \leq j \leq N$), Eve attaches a probe state $|0^E\rangle_{E_j}$ and applies some unitary operator U_j of her choice to the compound system $|0^E\rangle_{E_j}|i_j^{b_j}\rangle_{T_j}$. Then, Eve keeps to herself (in a quantum memory) the subsystem E_j, which is her probe state; and sends to Bob the subsystem T_j, which is the qubit sent from Alice to Bob (which may have been modified by her attack U_j).

The most general collective attack U_j of Eve on the j-th qubit, represented in the orthonormal basis $\{|0^{b_j}\rangle_{T_j}, |1^{b_j}\rangle_{T_j}\}$, is

$$U_j|0^E\rangle_{E_j}|0^{b_j}\rangle_{T_j} = |E_{00}^{b_j}\rangle_{E_j}|0^{b_j}\rangle_{T_j} + |E_{01}^{b_j}\rangle_{E_j}|1^{b_j}\rangle_{T_j} \quad (4.1)$$

$$U_j|0^E\rangle_{E_j}|1^{b_j}\rangle_{T_j} = |E_{10}^{b_j}\rangle_{E_j}|0^{b_j}\rangle_{T_j} + |E_{11}^{b_j}\rangle_{E_j}|1^{b_j}\rangle_{T_j}, \quad (4.2)$$

where $|E_{00}^{b_j}\rangle_{E_j}$, $|E_{01}^{b_j}\rangle_{E_j}$, $|E_{10}^{b_j}\rangle_{E_j}$, and $|E_{11}^{b_j}\rangle_{E_j}$ are non-normalized states in Eve's probe system E_j attached to the j-th qubit.

We thus notice that Eve can modify the original *product state* of the compound system, $|0^E\rangle_{E_j}|i_j^{b_j}\rangle_{T_j}$, into an *entangled state* (e.g., $|E_{00}^{b_j}\rangle_{E_j}|0^{b_j}\rangle_{T_j}+|E_{01}^{b_j}\rangle_{E_j}|1^{b_j}\rangle_{T_j}$). Eve's attack may thus cause Bob's state to become entangled with her probe. On the one hand, this may give Eve some information on Bob's state; on the other hand, this causes disturbance that may be detected by Bob. The security proof shows that the information obtained by Eve and the disturbance caused by Eve are inherently correlated: this is the basic reason QKD protocols are secure.

4.3.2 Results from [BGM09]

The security proof of BB84-INFO-z against collective attacks is very similar to the security proof of BB84 itself against collective attacks, that was detailed in [BGM09]. Most parts of the proof are not affected at all by the changes made to BB84 to get the BB84-INFO-z protocol (changes detailed in Section 4.2 of the current chapter), because those parts assume fixed strings $\mathbf{s}$ and $\mathbf{b}$, and because the attack is collective (so the analysis is restricted to the INFO bits).

Therefore, the reader is referred to the proof in Section 2 and Subsections 3.1 to 3.5 of [BGM09], that applies to BB84-INFO-z without any changes (except changing the total number of bits, $2n$, to N, which does not affect the proof at all), and that will not be repeated here.

We denote the rows of the error-correction parity check matrix P_C as the vectors $v_1, \ldots, v_r$ in $\mathbf{F}_2^n$, and the rows of the privacy amplification matrix P_K as the vectors $v_{r+1}, \ldots, v_{r+m}$. We also define, for every r', $V_{r'} \triangleq \mathrm{Span}\{v_1, ..., v_{r'}\}$; and we define

$$d_{r,m} \triangleq \min_{r \le r' < r+m} d_H(v_{r'+1}, V_{r'}) = \min_{r \le r' < r+m} d_{r',1}. \quad (4.3)$$

For a 1-bit final key $k \in \{0,1\}$, we define $\widehat{\rho}_k$ to be the state of Eve corresponding to the final key k, given that she knows $\boldsymbol{\xi}$. Thus,

$$\widehat{\rho}_k = \frac{1}{2^{n-r-1}} \sum_{\mathbf{x} \Big|_{\mathbf{x} \cdot v_{r+1} = k}^{\mathbf{x} P_C^{\mathrm{T}} = \boldsymbol{\xi}}} \rho_{\mathbf{x}}^{\mathbf{b}'}, \quad (4.4)$$

where $\rho_{\mathbf{x}}^{\mathbf{b}'}$ is Eve's state after the attack, given that Alice sent the INFO bit string $\mathbf{x}$

encoded in the bases $\mathbf{b}' = \mathbf{b_s}$. In [BGM09], the state $\widetilde{\rho}_k$ was also defined: it is a lift-up of $\widehat{\rho}_k$ (which means that $\widehat{\rho}_k$ is a partial trace of $\widetilde{\rho}_k$), in which the states $\rho_{\mathbf{x}}^{\mathbf{b}'}$ appearing in $\widehat{\rho}_k$ are replaced by their purifications (see full definition in Subsection 3.4 of [BGM09]).

In the end of Subsection 3.5 of [BGM09], it was found that (in the case of a 1-bit final key, i.e., $m = 1$)

$$\frac{1}{2}\operatorname{tr}|\widetilde{\rho}_0 - \widetilde{\rho}_1| \leq 2\sqrt{P\left[|\mathbf{C}_I| \geq \frac{d_{r,1}}{2} \;\middle|\; \mathbf{B}_I = \overline{\mathbf{b}'}, \mathbf{s}\right]}, \tag{4.5}$$

where $\mathbf{C}_I$ is the random variable corresponding to the n-bit string of errors on the n INFO bits; $\mathbf{B}_I$ is the random variable corresponding to the n-bit string of bases of the n INFO bits; $\overline{\mathbf{b}'}$ is the bit-flipped string of $\mathbf{b}' = \mathbf{b_s}$; and $d_{r,1}$ (and, in general, $d_{r,m}$) was defined above.

Now, according to [NC00, Theorem 9.2 and page 407], and using the fact that $\widehat{\rho}_k$ is a partial trace of $\widetilde{\rho}_k$, we find that $\frac{1}{2}\operatorname{tr}|\widehat{\rho}_0 - \widehat{\rho}_1| \leq \frac{1}{2}\operatorname{tr}|\widetilde{\rho}_0 - \widetilde{\rho}_1|$. From this result and from inequality (4.5) we deduce that

$$\frac{1}{2}\operatorname{tr}|\widehat{\rho}_0 - \widehat{\rho}_1| \leq 2\sqrt{P\left[|\mathbf{C}_I| \geq \frac{d_{r,1}}{2} \;\middle|\; \mathbf{B}_I = \overline{\mathbf{b}'}, \mathbf{s}\right]}. \tag{4.6}$$

4.3.3 Bounding the Differences Between Eve's States

We define $\mathbf{c} \triangleq \mathbf{i} + \mathbf{i}^B$: namely, $\mathbf{c}$ is the XOR of the N-bit string $\mathbf{i}$ sent by Alice and of the N-bit string $\mathbf{i}^B$ measured by Bob. For each index $1 \leq l \leq N$, $c_l = 1$ if and only if Bob's l-th bit value is different from the l-th bit sent by Alice. The partition $\mathcal{P}$ divides the N bits into n INFO bits, n_z TEST-Z bits, and n_x TEST-X bits. The corresponding substrings of the error string $\mathbf{c}$ are $\mathbf{c_s}$ (the string of errors on the INFO bits), $\mathbf{c_z}$ (the string of errors on the TEST-Z bits), and $\mathbf{c_b}$ (the string of errors on the TEST-X bits). The random variables that correspond to $\mathbf{c_s}$, $\mathbf{c_z}$, and $\mathbf{c_b}$ are denoted by $\mathbf{C}_I$, $\mathbf{C}_{T_Z}$, and $\mathbf{C}_{T_X}$, respectively.

We define $\widetilde{\mathbf{C}_I}$ to be the random variable corresponding to the string of errors on the INFO bits *if Alice had encoded and sent the INFO bits in the x basis* (instead of the z basis dictated by the protocol). In those notations, inequality (4.6) reads as

$$\frac{1}{2}\operatorname{tr}|\widehat{\rho}_0 - \widehat{\rho}_1| \leq 2\sqrt{P\left[|\widetilde{\mathbf{C}_I}| \geq \frac{d_{r,1}}{2} \;\middle|\; \mathcal{P}\right]} = 2\sqrt{P\left[|\widetilde{\mathbf{C}_I}| \geq \frac{d_{r,1}}{2} \;\middle|\; \mathbf{c_z}, \mathbf{c_b}, \mathcal{P}\right]}, \tag{4.7}$$

using the fact that Eve's attack is collective, so the qubits are attacked independently, and, therefore, the errors on the INFO bits are independent of the errors on the TEST-Z and TEST-X bits (namely, of $\mathbf{c_z}$ and $\mathbf{c_b}$).

As explained in [BGM09], inequality (4.7) was not derived for the actual attack $U = U_1 \otimes \ldots \otimes U_N$ applied by Eve, but for a virtual flat attack (that depends on $\mathbf{b}$ and therefore could not have been applied by Eve). That flat attack gives the same states

$\widehat{\rho}_0$ and $\widehat{\rho}_1$ as the original attack U, and gives a lower (or the same) error rate in the conjugate basis. Therefore, inequality (4.7) also holds for the original attack U. This means that, from now on, all our results apply to the original attack U rather than to the flat attack.

So far, we have discussed a 1-bit key. We will now discuss a general m-bit key $\mathbf{k}$. We define $\widehat{\rho}_{\mathbf{k}}$ to be the state of Eve corresponding to the final key $\mathbf{k}$, given that she knows $\boldsymbol{\xi}$:

$$\widehat{\rho}_{\mathbf{k}} = \frac{1}{2^{n-r-m}} \sum_{\mathbf{x} \,\left|\, \substack{\mathbf{x}P_C^{\mathrm{T}} = \boldsymbol{\xi} \\ \mathbf{x}P_K^{\mathrm{T}} = \mathbf{k}}\right.} \rho_{\mathbf{x}}^{\mathbf{b}'} \tag{4.8}$$

Proposition 4.1. *For any two m-bit keys $\mathbf{k}, \mathbf{k}'$,*

$$\frac{1}{2} \operatorname{tr} |\widehat{\rho}_{\mathbf{k}} - \widehat{\rho}_{\mathbf{k}'}| \leq 2m \sqrt{P\left[|\widetilde{\mathbf{C}_I}| \geq \frac{d_{r,m}}{2} \mid \mathbf{c_z}, \mathbf{c_b}, \mathcal{P}\right]}. \tag{4.9}$$

Proof. We define the key $\mathbf{k}_j$, for $0 \leq j \leq m$, to consist of the first j bits of $\mathbf{k}'$ and the last $m - j$ bits of $\mathbf{k}$. This means that $\mathbf{k}_0 = \mathbf{k}$, $\mathbf{k}_m = \mathbf{k}'$, and $\mathbf{k}_{j-1}$ differs from $\mathbf{k}_j$ at most on a single bit (the j-th bit).

First, we find a bound on $\frac{1}{2} \operatorname{tr} |\widehat{\rho}_{\mathbf{k}_{j-1}} - \widehat{\rho}_{\mathbf{k}_j}|$: since $\mathbf{k}_{j-1}$ differs from $\mathbf{k}_j$ at most on a single bit (the j-th bit, given by the formula $\mathbf{x} \cdot v_{r+j}$), we can use the same proof that gave us inequality (4.7), attaching the other (identical) key bits to $\boldsymbol{\xi}$ of the original proof; and we find that

$$\frac{1}{2} \operatorname{tr} |\widehat{\rho}_{\mathbf{k}_{j-1}} - \widehat{\rho}_{\mathbf{k}_j}| \leq 2 \sqrt{P\left[|\widetilde{\mathbf{C}_I}| \geq \frac{d_j}{2} \;\mid\; \mathbf{c_z}, \mathbf{c_b}, \mathcal{P}\right]}, \tag{4.10}$$

where we define d_j as $d_H(v_{r+j}, V_j')$, and $V_j' \triangleq \operatorname{Span}\{v_1, v_2, \ldots, v_{r+j-1}, v_{r+j+1}, \ldots, v_{r+m}\}$.

Now we notice that d_j is the Hamming distance between v_{r+j} and some vector in V_j', which means that $d_j = \left|\sum_{i=1}^{r+m} a_i v_i\right|$ with $a_i \in \mathbf{F}_2$ and $a_{r+j} \neq 0$. The properties of Hamming distance assure us that d_j is at least $d_H(v_{r'+1}, V_{r'})$ for some $r \leq r' < r + m$. Therefore, we find that $d_{r,m} = \min_{r \leq r' < r+m} d_H(v_{r'+1}, V_{r'}) \leq d_j$.

The result $d_{r,m} \leq d_j$ implies that if $|\widetilde{\mathbf{C}_I}| \geq \frac{d_j}{2}$ then $|\widetilde{\mathbf{C}_I}| \geq \frac{d_{r,m}}{2}$. Therefore, inequality (4.10) implies

$$\frac{1}{2} \operatorname{tr} |\widehat{\rho}_{\mathbf{k}_{j-1}} - \widehat{\rho}_{\mathbf{k}_j}| \leq 2 \sqrt{P\left[|\widetilde{\mathbf{C}_I}| \geq \frac{d_{r,m}}{2} \;\mid\; \mathbf{c_z}, \mathbf{c_b}, \mathcal{P}\right]}. \tag{4.11}$$

Now we use the triangle inequality for norms to find

$$\frac{1}{2} \operatorname{tr} |\widehat{\rho}_{\mathbf{k}} - \widehat{\rho}_{\mathbf{k}'}| = \frac{1}{2} \operatorname{tr} |\widehat{\rho}_{\mathbf{k}_0} - \widehat{\rho}_{\mathbf{k}_m}| \leq \sum_{j=1}^{m} \frac{1}{2} \operatorname{tr} |\widehat{\rho}_{\mathbf{k}_{j-1}} - \widehat{\rho}_{\mathbf{k}_j}|$$

$$\leq 2m\sqrt{P\left[|\widetilde{\mathbf{C}_I}| \geq \frac{d_{r,m}}{2} \;\middle|\; \mathbf{c_z}, \mathbf{c_b}, \mathcal{P}\right]}, \tag{4.12}$$

as we wanted. □

The value we want to bound is the expected value of trace distance between two states of Eve corresponding to two final keys. However, we should take into account that if the test fails, no final key is generated, and the distance between all of Eve's states becomes 0 for any purpose. We thus define the random variable $\Delta_{\text{Eve}}^{(p_{a,z},p_{a,x})}(\mathbf{k},\mathbf{k}')$ for any two final keys $\mathbf{k},\mathbf{k}'$:

$$\Delta_{\text{Eve}}^{(p_{a,z},p_{a,x})}(\mathbf{k},\mathbf{k}'|\mathcal{P},\boldsymbol{\xi},\mathbf{c_z},\mathbf{c_b}) \triangleq \begin{cases} \frac{1}{2}\operatorname{tr}|\widehat{\rho}_{\mathbf{k}} - \widehat{\rho}_{\mathbf{k}'}| & \text{if } \frac{|\mathbf{c_z}|}{n_z} \leq p_{a,z} \text{ and } \frac{|\mathbf{c_b}|}{n_x} \leq p_{a,x} \\ 0 & \text{otherwise} \end{cases} \tag{4.13}$$

We need to bound the expected value $\langle\Delta_{\text{Eve}}^{(p_{a,z},p_{a,x})}(\mathbf{k},\mathbf{k}')\rangle$, that is given by:

$$\langle\Delta_{\text{Eve}}^{(p_{a,z},p_{a,x})}(\mathbf{k},\mathbf{k}')\rangle = \sum_{\mathcal{P},\boldsymbol{\xi},\mathbf{c_z},\mathbf{c_b}} \Delta_{\text{Eve}}^{(p_{a,z},p_{a,x})}(\mathbf{k},\mathbf{k}'|\mathcal{P},\boldsymbol{\xi},\mathbf{c_z},\mathbf{c_b}) \cdot p(\mathcal{P},\boldsymbol{\xi},\mathbf{c_z},\mathbf{c_b}) \tag{4.14}$$

Theorem 4.2.

$$\langle\Delta_{\text{Eve}}^{(p_{a,z},p_{a,x})}(\mathbf{k},\mathbf{k}')\rangle \leq 2m\sqrt{P\left[\left(\frac{|\widetilde{\mathbf{C}_I}|}{n} \geq \frac{d_{r,m}}{2n}\right) \wedge \left(\frac{|\mathbf{C}_{T_Z}|}{n_z} \leq p_{a,z}\right) \wedge \left(\frac{|\mathbf{C}_{T_X}|}{n_x} \leq p_{a,x}\right)\right]} \tag{4.15}$$

where $\frac{|\widetilde{\mathbf{C}_I}|}{n}$ *is the random variable corresponding to the error rate on the INFO bits if they had been encoded in the x basis,* $\frac{|\mathbf{C}_{T_Z}|}{n_z}$ *is the random variable corresponding to the error rate on the TEST-Z bits, and* $\frac{|\mathbf{C}_{T_X}|}{n_x}$ *is the random variable corresponding to the error rate on the TEST-X bits.*

Proof. We use the convexity of x^2, namely, the fact that for all $\{p_i\}_i$ satisfying $p_i \geq 0$ and $\sum_i p_i = 1$, it holds that $\left(\sum_i p_i x_i\right)^2 \leq \sum_i p_i x_i^2$. We find that:

$$\begin{aligned}
&\langle\Delta_{\text{Eve}}^{(p_{a,z},p_{a,x})}(\mathbf{k},\mathbf{k}')\rangle^2 \\
&= \left[\sum_{\mathcal{P},\boldsymbol{\xi},\mathbf{c_z},\mathbf{c_b}} \Delta_{\text{Eve}}^{(p_{a,z},p_{a,x})}(\mathbf{k},\mathbf{k}'|\mathcal{P},\boldsymbol{\xi},\mathbf{c_z},\mathbf{c_b}) \cdot p(\mathcal{P},\boldsymbol{\xi},\mathbf{c_z},\mathbf{c_b})\right]^2 && \text{(by (4.14))} \\
&\leq \sum_{\mathcal{P},\boldsymbol{\xi},\mathbf{c_z},\mathbf{c_b}} \left(\Delta_{\text{Eve}}^{(p_{a,z},p_{a,x})}(\mathbf{k},\mathbf{k}'|\mathcal{P},\boldsymbol{\xi},\mathbf{c_z},\mathbf{c_b})\right)^2 \cdot p(\mathcal{P},\boldsymbol{\xi},\mathbf{c_z},\mathbf{c_b}) && \text{(by convexity of } x^2\text{)} \\
&= \sum_{\mathcal{P},\boldsymbol{\xi},\frac{|\mathbf{c_z}|}{n_z}\leq p_{a,z},\frac{|\mathbf{c_b}|}{n_x}\leq p_{a,x}} \left(\tfrac{1}{2}\operatorname{tr}|\widehat{\rho}_{\mathbf{k}} - \widehat{\rho}_{\mathbf{k}'}|\right)^2 \cdot p(\mathcal{P},\boldsymbol{\xi},\mathbf{c_z},\mathbf{c_b}) && \text{(by (4.13))} \\
&\leq 4m^2 \cdot \sum_{\mathcal{P},\boldsymbol{\xi},\frac{|\mathbf{c_z}|}{n_z}\leq p_{a,z},\frac{|\mathbf{c_b}|}{n_x}\leq p_{a,x}} P\left[|\widetilde{\mathbf{C}_I}| \geq \tfrac{d_{r,m}}{2} \mid \mathbf{c_z}, \mathbf{c_b}, \mathcal{P}\right] \cdot p(\mathcal{P},\boldsymbol{\xi},\mathbf{c_z},\mathbf{c_b}) && \text{(by (4.9))}
\end{aligned}$$

$$= 4m^2 \cdot \sum_{\mathcal{P}, \frac{|\mathbf{c_z}|}{n_z} \leq p_{a,z}, \frac{|\mathbf{c_b}|}{n_x} \leq p_{a,x}} P\left[|\widetilde{\mathbf{C}_I}| \geq \tfrac{d_{r,m}}{2} \mid \mathbf{c_z}, \mathbf{c_b}, \mathcal{P}\right] \cdot p(\mathcal{P}, \mathbf{c_z}, \mathbf{c_b})$$

$$= 4m^2 \cdot \sum_{\mathcal{P}} P\left[\left(|\widetilde{\mathbf{C}_I}| \geq \tfrac{d_{r,m}}{2}\right) \wedge \left(\tfrac{|\mathbf{C}_{T_Z}|}{n_z} \leq p_{a,z}\right) \wedge \left(\tfrac{|\mathbf{C}_{T_X}|}{n_x} \leq p_{a,x}\right) \mid \mathcal{P}\right] \cdot p(\mathcal{P})$$

$$= 4m^2 \cdot P\left[\left(|\widetilde{\mathbf{C}_I}| \geq \tfrac{d_{r,m}}{2}\right) \wedge \left(\tfrac{|\mathbf{C}_{T_Z}|}{n_z} \leq p_{a,z}\right) \wedge \left(\tfrac{|\mathbf{C}_{T_X}|}{n_x} \leq p_{a,x}\right)\right] \tag{4.16}$$

as we wanted. □

4.3.4 Proof of Security

Following [BGM09] and [BBB+06], we choose matrices P_C and P_K such that the inequality $\frac{d_{r,m}}{2n} > p_{a,x} + \epsilon$ is satisfied for some ϵ (we will explain in Subsection 4.3.6 why this is possible). This means that

$$\begin{aligned} &P\left[\left(\tfrac{|\widetilde{\mathbf{C}_I}|}{n} \geq \tfrac{d_{r,m}}{2n}\right) \wedge \left(\tfrac{|\mathbf{C}_{T_Z}|}{n_z} \leq p_{a,z}\right) \wedge \left(\tfrac{|\mathbf{C}_{T_X}|}{n_x} \leq p_{a,x}\right)\right] \\ &\leq P\left[\left(\tfrac{|\widetilde{\mathbf{C}_I}|}{n} > p_{a,x} + \epsilon\right) \wedge \left(\tfrac{|\mathbf{C}_{T_X}|}{n_x} \leq p_{a,x}\right)\right]. \end{aligned} \tag{4.17}$$

We will now prove the right-hand-side of (4.17) to be exponentially small in n.

As said earlier, the random variable $\widetilde{\mathbf{C}_I}$ corresponds to the bit string of errors on the INFO bits if they had been encoded in the x basis. The TEST-X bits are also encoded in the x basis, and the random variable $\mathbf{C}_{T_X}$ corresponds to the bit string of errors on those bits. Therefore, we can treat the selection of the indexes of the n INFO bits and the n_x TEST-X bits as a random sampling (after the numbers n, n_z, and n_x *and* the indexes of the TEST-Z bits have all already been chosen) and use Hoeffding's theorem (that is described in Appendix A of [BGM09]).

Therefore, for each bit string $c_1 \ldots c_{n+n_x}$ that consists of the errors in the $n + n_x$ INFO and TEST-X bits *if the INFO bits had been encoded in the x basis*, we apply Hoeffding's theorem: namely, we take a sample of size n without replacement from the population $c_1, \ldots, c_{n+n_x}$ (this corresponds to the random selection of the indexes of the INFO bits and the TEST-X bits, as defined above, given that the indexes of the TEST-Z bits have already been chosen). Let $\overline{X} = \frac{|\widetilde{\mathbf{C}_I}|}{n}$ be the average of the sample (this is exactly the error rate on the INFO bits, assuming, again, that the INFO bits had been encoded in the x basis); and let $\mu = \frac{|\widetilde{\mathbf{C}_I}| + |\mathbf{C}_{T_X}|}{n+n_x}$ be the expectancy of $\overline{X}$ (this is exactly the error rate on the INFO bits and TEST-X bits together). Then $\frac{|\mathbf{C}_{T_X}|}{n_x} \leq p_{a,x}$ is equivalent to $(n+n_x)\mu - n\overline{X} \leq n_x \cdot p_{a,x}$, and, therefore, to $n \cdot (\overline{X} - \mu) \geq n_x \cdot (\mu - p_{a,x})$. This means that the conditions $\left(\frac{|\widetilde{\mathbf{C}_I}|}{n} > p_{a,x} + \epsilon\right)$ and $\left(\frac{|\mathbf{C}_{T_X}|}{n_x} \leq p_{a,x}\right)$ rewrite to

$$\left(\overline{X} - \mu > \epsilon + p_{a,x} - \mu\right) \wedge \left(\frac{n}{n_x} \cdot (\overline{X} - \mu) \geq \mu - p_{a,x}\right), \tag{4.18}$$

which implies $\left(1 + \frac{n}{n_x}\right)(\overline{X} - \mu) > \epsilon$, which is equivalent to $\overline{X} - \mu > \frac{n_x}{n+n_x}\epsilon$. Using

Hoeffding's theorem (from Appendix A of [BGM09]), we get:

$$P\left[\left(\frac{|\widetilde{\mathbf{C}_I}|}{n} > p_{a,x} + \epsilon\right) \wedge \left(\frac{|\mathbf{C}_{T_X}|}{n_x} \leq p_{a,x}\right)\right] \leq P\left[\overline{X} - \mu > \frac{n_x}{n+n_x}\epsilon\right] \leq e^{-2\left(\frac{n_x}{n+n_x}\right)^2 n\epsilon^2} \tag{4.19}$$

In the above discussion, we have actually proved the following Theorem:

Theorem 4.3. *Let us be given $\delta > 0$, $R > 0$, and, for infinitely many values of n, a family $\{v_1^n, \ldots, v_{r_n+m_n}^n\}$ of linearly independent vectors in $\mathbf{F}_2^n$ such that $\delta < \frac{d_{r_n,m_n}}{n}$ and $\frac{m_n}{n} \leq R$. Then for any $p_{a,z}, p_{a,x} > 0$ and $\epsilon_{\text{sec}} > 0$ such that $p_{a,x} + \epsilon_{\text{sec}} \leq \frac{\delta}{2}$, and for any $n, n_z, n_x > 0$ and two m_n-bit final keys $\mathbf{k}, \mathbf{k}'$, the distance between Eve's states corresponding to $\mathbf{k}$ and $\mathbf{k}'$ satisfies the following bound:*

$$\langle \Delta_{\text{Eve}}^{(p_{a,z},p_{a,x})}(\mathbf{k}, \mathbf{k}') \rangle \leq 2R\, n e^{-\left(\frac{n_x}{n+n_x}\right)^2 n\epsilon_{\text{sec}}^2} \tag{4.20}$$

In Subsection 4.3.6 we explain why the vectors required by this Theorem exist.

We note that the quantity $\langle \Delta_{\text{Eve}}^{(p_{a,z},p_{a,x})}(\mathbf{k}, \mathbf{k}') \rangle$ bounds the expected values of the Shannon Distinguishability and of the mutual information between Eve and the final key, as done in [BGM09] and [BBB$^+$06], which is sufficient for proving non-composable security; but it also avoids composability problems: Eve is not required to measure immediately after the protocol ends, but she is allowed to wait until she gets more information; and equation (4.20) bounds the trace distance between any two of Eve's possible states.

4.3.5 Reliability

Security itself is not sufficient; we also need the key to be reliable (namely, to be the same for Alice and Bob). This means that we should make sure that the number of errors on the INFO bits is less than the maximal number of errors that can be corrected by the error-correcting code. We demand that our error-correcting code can correct $n(p_{a,z} + \epsilon_{\text{rel}})$ errors (we explain in Subsection 4.3.6 why this demand is satisfied). Therefore, reliability of the final key with exponentially small probability of failure is guaranteed by the following inequality: (as said, $\mathbf{C}_I$ corresponds to the actual bit string of errors on the INFO bits in the protocol, when they are encoded in the z basis)

$$P\left[\left(\frac{|\mathbf{C}_I|}{n} > p_{a,z} + \epsilon_{\text{rel}}\right) \wedge \left(\frac{|\mathbf{C}_{T_Z}|}{n_z} \leq p_{a,z}\right)\right] \leq e^{-2\left(\frac{n_z}{n+n_z}\right)^2 n\epsilon_{\text{rel}}^2} \tag{4.21}$$

This inequality is proved by an argument similar to the one used in Subsection 4.3.4: the selection of the indexes of the INFO bits and the TEST-Z bits is a random partition of $n + n_z$ bits into two subsets of sizes n and n_z, respectively (assuming that the indexes of the TEST-X bits have already been chosen), and thus it corresponds to Hoeffding's sampling.

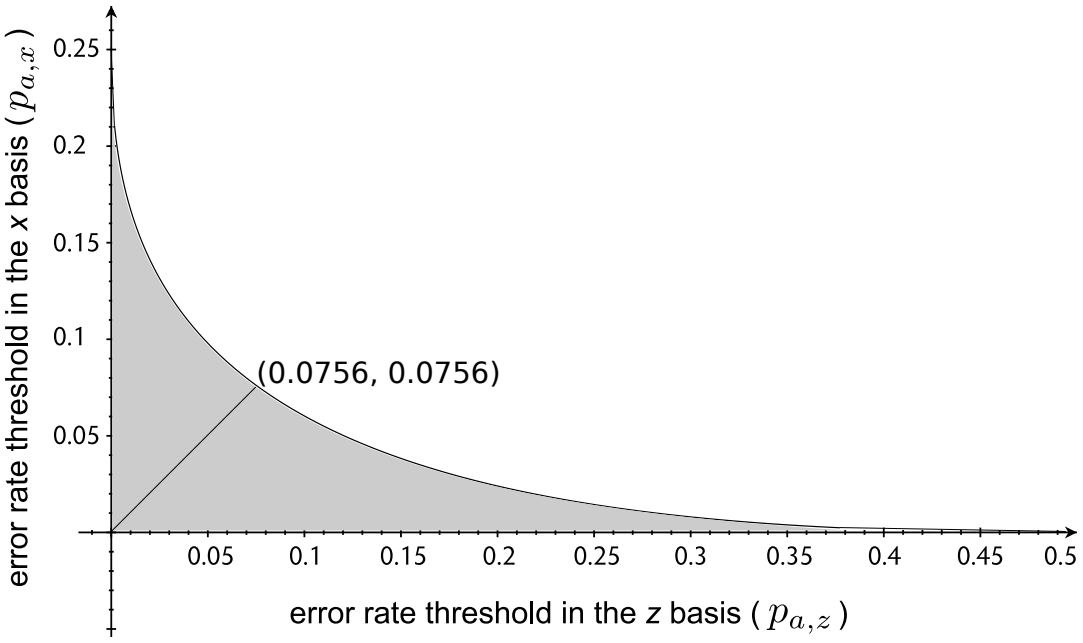

Figure 4.1: **The secure asymptotic error rates zone for BB84-INFO-z** (below the curve)

4.3.6 Security, Reliability, and Error Rate Threshold

According to Theorem 4.3 and to the discussion in Subsection 4.3.5, to get both security and reliability we only need vectors $\{v_1^n, \ldots, v_{r_n+m_n}^n\}$ satisfying both the conditions of the Theorem (distance $\frac{d_{r_n,m_n}}{2n} > \frac{\delta}{2} \geq p_{a,x} + \epsilon_{\text{sec}}$) and the reliability condition (the ability to correct $n(p_{a,z} + \epsilon_{\text{rel}})$ errors). Such families were proven to exist in Appendix E of [BBB$^+$06], giving the bit-rate:

$$R_{\text{secret}} \triangleq \frac{m}{n} = 1 - H_2(2p_{a,x} + 2\epsilon_{\text{sec}}) - H_2\left(p_{a,z} + \epsilon_{\text{rel}} + \frac{1}{n}\right) \tag{4.22}$$

where $H_2(x) \triangleq -x\log_2(x) - (1-x)\log_2(1-x)$.

Note that we use here the error thresholds $p_{a,x}$ for security and $p_{a,z}$ for reliability. This is possible, because in [BBB$^+$06] those conditions (security and reliability) on the codes are discussed separately.

To get the asymptotic error rate thresholds, we require $R_{\text{secret}} > 0$, and we get the condition:

$$H_2(2p_{a,x} + 2\epsilon_{\text{sec}}) + H_2\left(p_{a,z} + \epsilon_{\text{rel}} + \frac{1}{n}\right) < 1 \tag{4.23}$$

The secure asymptotic error rate thresholds zone is shown in Figure 4.1 (it is below the curve), assuming that $\frac{1}{n}$ is negligible. Note the trade-off between the error rates $p_{a,z}$ and $p_{a,x}$. Also note that in the case $p_{a,z} = p_{a,x}$, we get the same threshold as BB84 ([BBB$^+$06] and [BGM09]), which is 7.56%.

4.4 Conclusion

In this chapter, we have analyzed the security of the BB84-INFO-z protocol against any collective attack. We have discovered that the results of BB84 hold very similarly for BB84-INFO-z, with only two exceptions:

1. The error rates must be separately checked to be below the thresholds $p_{a,z}$ and $p_{a,x}$ for the TEST-Z and TEST-X bits, respectively, while in BB84 the error rate threshold p_a applies to all the TEST bits together.

2. The exponents of Eve's information (security) and of the failure probability of the error-correcting code (reliability) are different than in [BGM09], because different numbers of test bits are now allowed (n_z and n_x are arbitrary). This implies that the exponents may decrease more slowly (or more quickly) as a function of n. However, if we choose $n_z = n_x = n$ (thus sending $N = 3n$ qubits from Alice to Bob), then we get exactly the same exponents as in [BGM09].

The asymptotic error rate thresholds found in this chapter allow us to tolerate a higher threshold for a specific basis (say, the x basis) if we demand a lower threshold for the other basis (z). If we choose the same error rate threshold for both bases, then the asymptotic bound is 7.56%, exactly the bound found for BB84 in [BBB$^+$06] and [BGM09].

We conclude that even if we change the BB84 protocol to have INFO bits only in the z basis, this does not harm its security and reliability (at least against collective attacks). This does not even change the asymptotic error rate threshold. The only drawbacks of this change are the need to check the error rate for the two bases separately, and the need to either send more qubits ($3n$ qubits in total, rather than $2n$) or get a slower exponential decrease of the exponents required for security and reliability.

We thus find that the feature of BB84, that both bases are used for information, is not very important for security and reliability, and that BB84-INFO-z (that lacks this feature) is almost as useful as BB84. This may have important implications on the security and reliability of other protocols that, too, use only one basis for information qubits, such as [Mor98] and some two-way protocols [BKM07, ZQL$^+$09].

We also present a better approach for the proof, that uses the quantum distance between two states rather than the classical information. In [BGM09], [BBB$^+$02], and [BBB$^+$06], the classical mutual information between Eve's information (after an optimal measurement) and the final key was calculated (by using the trace distance between two quantum states); although we should note that in [BGM09] and [BBB$^+$06], the trace distance was used for the proof of security of a single bit of the final key even when all other bits are given to Eve, and only the last stages of the proof discussed bounding the classical mutual information. In the current chapter, on the other hand, we use the trace distance between the two quantum states until the end of the proof, which avoids composability problems that existed in the previous works.

Therefore, this proof makes a step towards making [BGM09], [BBB$^+$02], and [BBB$^+$06] prove composable security of BB84 (and, in particular, security even if Eve keeps her quantum states until she gets more information when Alice and Bob use the key, rather than measuring them at the end of the protocol). This approach also applies (similarly) to the BB84 security proof in [BGM09].

We note that this chapter strengthens the security proofs described in [BGM09, BBB$^+$02, BBB$^+$06], both because it slightly generalizes them (from security of BB84 to security of BB84-INFO-z) and because it makes them more composable. Those security proofs have various advantages over other methods to prove security: first of all, they are mostly self-contained, while other security proofs require many results from other areas of quantum information (such as various notions of entropy needed for the security proof of [Ren08, RGK05], and entanglement purification and quantum error correction needed for the security proof of [SP00]); second, they give tight finite-key bounds, unlike several other methods (see details below); and finally, at least in some sense, they are simpler than other proof techniques. On the other hand, their generality and their asymptotic error-rate threshold (7.56%, rather than 11% given by [RGK05, SP00]) are yet to be improved by future research.

Our method for proving security gives explicit and tight finite-key bounds. In contrast to this, the security proof of [SP00] gives only asymptotic results (for infinitely long keys). For the security proof of [Ren08, RGK05], it is proved today that for some protocols (including BB84), one can get tight finite-key bounds that are the same as the ones found by our method [TLGR12]; but at first that security method gave very pessimistic bounds (by using the de Finetti theorem [Ren08, Ren07]), and later, the bounds were improved for several protocols (including BB84) [SR08], but were still not tight (see [TLGR12] for comparison).

We also note that the existence of many different proof techniques is important, because some proofs may be more adjustable to various QKD protocols or to practical scenarios; some proofs may be clearer to different readers with different backgrounds; analyzing the differences between the proofs and between their obtained results may lead to important insights on the strengths and weaknesses of various techniques; and the existence of many proofs makes the security result more certain and less prone to errors.

Chapter 5

Summary

In this research we have used important basic notions of quantum information (entanglement, the Bloch sphere, and the trace distance) for analyzing several research problems, both in quantum information and in quantum cryptography. We have seen the importance of those basic QIP notions from various perspectives.

We have provided a full geometrical analysis of entanglement and separability for all the possible bipartite Bloch spheres – that is, for all the possible 2-dimensional Hilbert spaces. We have seen that the possible sets of separable states in those Bloch spheres belong to exactly five classes, and are not arbitrary convex sets. This finding, while interesting by itself, may also be useful in the future for defining new entanglement measures and for using the "Bloch sphere neighbors" of a rank-2 state in various quantum procedures (e.g., entanglement purification and error correction).

We have also provided a proof of security against collective attacks for a new quantum key distribution (QKD) protocol, named BB84-INFO-z. We have extended an existing simplified security proof of BB84 against collective attacks [BGM09] to also hold against this different protocol. We have also used the trace distance, a geometrical distance corresponding (for qubits) to Euclidean distance on the Bloch sphere, for improving the composability of our security proof: while there are still some technical barriers blocking our proof from reaching the full definition of composable security, our proof attains the most important property of composability (a quantum near-indistinguishability between different states of Eve). Moreover, it applies to the simplified proof of security against collective attacks of [BGM09], but it may extend to the proof of security against joint attacks [BBB$^+$06], which gives a reasonable finite-key analysis and is generally simpler than many of the currently-existing composable security proofs (e.g., [RGK05, Ren08]).

5.1 Open Questions

Some questions raised by this research are left for the future. In particular, the properties of the geometrical entanglement measures defined for Bloch spheres (defining the entanglement measure of a state as its Euclidean distance, that is actually twice the

trace distance, from the closest separable state in the Bloch sphere) are not discussed and are left for future analysis; and so are potential improvements for entanglement distillation and entanglement purification processes.

Other open questions left for the future are various possible extensions of our partly-composable security proof of BB84-INFO-z against collective attacks. It may be extended to joint attacks; it may be extended to fully composable security; it may be extended to other protocols; and it may simplify and unify the currently-existing QKD security proofs. Of course, like the other currently-existing full security proofs of QKD, it does not fully model the realistic systems (which means that realistic systems do not have their full security proved, and may have many loopholes); extending full security proofs to realistic systems is another important open question in the area of security of QKD.

Bibliography

[BB84] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *International Conference on Computers, Systems & Signal Processing, IEEE, 1984*, pages 175–179, Dec 1984.

[BBB+02] Eli Biham, Michel Boyer, Gilles Brassard, Jeroen van de Graaf, and Tal Mor. Security of quantum key distribution against all collective attacks. *Algorithmica*, 34(4):372–388, Nov 2002.

[BBB+06] Eli Biham, Michel Boyer, Oscar P. Boykin, Tal Mor, and Vwani Roychowdhury. A proof of the security of quantum key distribution. *Journal of Cryptology*, 19(4):381–439, Apr 2006.

[BBCM95] Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Ueli M. Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6):1915–1923, Nov 1995.

[BBM17] Michel Boyer, Aharon Brodutch, and Tal Mor. Extrapolated quantum states, void states and a huge novel class of distillable entangled states. *Soft Computing*, pages 1–14, Feb 2017.

[BBP+96] Charles H. Bennett, Gilles Brassard, Sandu Popescu, Benjamin Schumacher, John A. Smolin, and William K. Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Physical Review Letters*, 76:722–725, Jan 1996.

[BBPS96] Charles H. Bennett, Herbert J. Bernstein, Sandu Popescu, and Benjamin Schumacher. Concentrating partial entanglement by local operations. *Physical Review A*, 53:2046–2052, Apr 1996.

[BDF+99] Charles H. Bennett, David P. DiVincenzo, Christopher A. Fuchs, Tal Mor, Eric Rains, Peter W. Shor, John A. Smolin, and William K. Wootters. Quantum nonlocality without entanglement. *Physical Review A*, 59:1070–1091, Feb 1999.

[BDM+99] Charles H. Bennett, David P. DiVincenzo, Tal Mor, Peter W. Shor, John A. Smolin, and Barbara M. Terhal. Unextendible product bases and bound entanglement. *Physical Review Letters*, 82:5385–5388, Jun 1999.

[BGLS07] Cyril Branciard, Nicolas Gisin, Norbert Lütkenhaus, and Valerio Scarani. Zero-error attacks and detection statistics in the coherent one-way protocol for quantum cryptography. *Quantum Information and Computation*, 7(7):639–664, Sep 2007.

[BGM09] Michel Boyer, Ran Gelles, and Tal Mor. Security of the Bennett-Brassard quantum key distribution protocol against collective attacks. *Algorithms*, 2(2):790–807, Jun 2009.

[BKM07] Michel Boyer, Dan Kenigsberg, and Tal Mor. Quantum key distribution with classical Bob. *Physical Review Letters*, 99:140501, Oct 2007.

[BLM17a] Michel Boyer, Rotem Liss, and Tal Mor. Geometry of entanglement in the Bloch sphere. *Physical Review A*, 95:032308, Mar 2017.

[BLM17b] Michel Boyer, Rotem Liss, and Tal Mor. Security against collective attacks of a modified BB84 QKD protocol with information only in one basis. In *Proceedings of the 2nd International Conference on Complexity, Future Information Systems and Risk – COMPLEXIS, 24-26 April, 2017, Porto, Portugal*, pages 23–29, Apr 2017.

[BLMS00a] Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C. Sanders. Limitations on practical quantum cryptography. *Physical Review Letters*, 85:1330–1333, Aug 2000.

[BLMS00b] Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C. Sanders. Security aspects of practical quantum cryptography. In Bart Preneel, editor, *Advances in Cryptology — EUROCRYPT 2000: International Conference on the Theory and Application of Cryptographic Techniques Bruges, Belgium, May 14–18, 2000 Proceedings*, pages 289–299, Berlin, Heidelberg, May 2000. Springer Berlin Heidelberg.

[BM97a] Eli Biham and Tal Mor. Bounds on information and the security of quantum cryptography. *Physical Review Letters*, 79:4034–4037, Nov 1997.

[BM97b] Eli Biham and Tal Mor. Security of quantum cryptography against collective attacks. *Physical Review Letters*, 78:2256–2259, Mar 1997.

[BM11] Michel Boyer and Tal Mor. Comment on "semiquantum-key distribution using less than four quantum states". *Physical Review A*, 83:046301, Apr 2011.

[BM14] Michel Boyer and Tal Mor. Extrapolated states, void states, and a huge novel class of distillable entangled states. In Adrian-Horia Dediu, Manuel Lozano, and Carlos Martín-Vide, editors, *Theory and Practice of Natural Computing: Third International Conference, TPNC 2014, Granada, Spain, December 9-11, 2014. Proceedings*, pages 107–118, Cham, Dec 2014. Springer International Publishing.

[BMS96] Charles H. Bennett, Tal Mor, and John A. Smolin. Parity bit in quantum cryptography. *Physical Review A*, 54:2675–2684, Oct 1996.

[BOHL+05] Michael Ben-Or, Michał Horodecki, Debbie W. Leung, Dominic Mayers, and Jonathan Oppenheim. The universal composable security of quantum key distribution. In Joe Kilian, editor, *Theory of Cryptography: Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12, 2005. Proceedings*, pages 386–406, Berlin, Heidelberg, Feb 2005. Springer Berlin Heidelberg.

[Can01] Ran Canetti. Universally composable security: a new paradigm for cryptographic protocols. In *Foundations of Computer Science, 2001. Proceedings. 42nd IEEE Symposium on*, pages 136–145, Oct 2001.

[CC08] Lin Chen and Yi-Xin Chen. Rank-three bipartite entangled states are distillable. *Physical Review A*, 78:022318, Aug 2008.

[CKR09] Matthias Christandl, Robert König, and Renato Renner. Postselection technique for quantum channels with applications to quantum cryptography. *Physical Review Letters*, 102:020504, Jan 2009.

[FL06] Chi-Hang Fred Fung and Hoi-Kwong Lo. Security proof of a three-state quantum-key-distribution protocol without rotational symmetry. *Physical Review A*, 74:042342, Oct 2006.

[FvdG99] Christopher A. Fuchs and Jeroen van de Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Transactions on Information Theory*, 45(4):1216–1227, May 1999.

[GMD02] A. Galindo and M. A. Martín-Delgado. Information and computation: Classical and quantum aspects. *Reviews of Modern Physics*, 74:347–423, May 2002.

[Gru99] Jozef Gruska. *Quantum computing*. McGraw-Hill London, 1999.

[HHH96] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. Separability of mixed states: necessary and sufficient conditions. *Physics Letters A*, 223(1):1–8, Nov 1996.

[HHH98] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. Mixed-state entanglement and distillation: Is there a "bound" entanglement in nature? *Physical Review Letters*, 80:5239–5242, Jun 1998.

[HHHH09] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of Modern Physics*, 81:865–942, Jun 2009.

[HJW93] Lane P. Hughston, Richard Jozsa, and William K. Wootters. A complete classification of quantum ensembles having a given density matrix. *Physics Letters A*, 183(1):14–18, Nov 1993.

[Hor97] Paweł Horodecki. Separability criterion and inseparable mixed states with positive partial transposition. *Physics Letters A*, 232(5):333–339, Aug 1997.

[HSTT03] Pawel Horodecki, John A. Smolin, Barbara M. Terhal, and Ashish V. Thapliyal. Rank two bipartite bound entangled states do not exist. *Theoretical Computer Science*, 292(3):589–596, Jan 2003.

[HW97] Scott Hill and William K. Wootters. Entanglement of a pair of quantum bits. *Physical Review Letters*, 78:5022–5025, Jun 1997.

[Kra15] Walter O. Krawec. Security proof of a semi-quantum key distribution protocol. In *2015 IEEE International Symposium on Information Theory (ISIT)*, pages 686–690. IEEE, Jun 2015.

[Kra16] Walter O. Krawec. Asymptotic analysis of a three state quantum cryptographic protocol. In *2016 IEEE International Symposium on Information Theory (ISIT)*, pages 2489–2493, Jul 2016.

[LOSU06] Robert Lohmayer, Andreas Osterloh, Jens Siewert, and Armin Uhlmann. Entangled three-qubit states without concurrence and three-tangle. *Physical Review Letters*, 97:260502, Dec 2006.

[LWW+10] Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*, 4(10):686–689, Aug 2010.

[May01] Dominic Mayers. Unconditional security in quantum cryptography. *Journal of the ACM*, 48(3):351–406, May 2001.

[Mor98] Tal Mor. No cloning of orthogonal states in composite systems. *Physical Review Letters*, 80:3137–3140, Apr 1998.

[NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge university press (10th anniversary edition, 2010), 2000.

[OSU08] Andreas Osterloh, Jens Siewert, and Armin Uhlmann. Tangles of superpositions and the convex-roof extension. *Physical Review A*, 77:032310, Mar 2008.

[Per96] Asher Peres. Separability criterion for density matrices. *Physical Review Letters*, 77:1413–1415, Aug 1996.

[PW00] Birgit Pfitzmann and Michael Waidner. Composition and integrity preservation of secure reactive systems. In *Proceedings of the 7th ACM Conference on Computer and Communications Security*, CCS '00, pages 245–254, New York, NY, USA, 2000. ACM.

[RA16a] Bartosz Regula and Gerardo Adesso. Entanglement quantification made easy: Polynomial measures invariant under convex decomposition. *Physical Review Letters*, 116:070504, Feb 2016.

[RA16b] Bartosz Regula and Gerardo Adesso. Geometric approach to entanglement quantification with polynomial measures. *Physical Review A*, 94:022324, Aug 2016.

[Ren07] Renato Renner. Symmetry of large physical systems implies independence of subsystems. *Nature Physics*, 3(9):645–649, Jul 2007.

[Ren08] Renato Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 6(01):1–127, Feb 2008.

[RGK05] Renato Renner, Nicolas Gisin, and Barbara Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Physical Review A*, 72:012332, Jul 2005.

[RP00] Eleanor Rieffel and Wolfgang Polak. An introduction to quantum computing for non-physicists. *ACM Computing Surveys*, 32(3):300–335, Sep 2000.

[SP00] Peter W. Shor and John Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 85:441–444, Jul 2000.

[SR08] Valerio Scarani and Renato Renner. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Physical Review Letters*, 100:200501, May 2008.

[TLGR12] Marco Tomamichel, Charles Ci Wen Lim, Nicolas Gisin, and Renato Renner. Tight finite-key analysis for quantum cryptography. *Nature Communications*, 3(634):1–6, Jan 2012.

[Woo01] William K. Wootters. Entanglement of formation and concurrence. *Quantum Information and Computation*, 1(1):27–44, Jun 2001.

[ZQL+09] Xiangfu Zou, Daowen Qiu, Lvzhou Li, Lihua Wu, and Lvjun Li. Semiquantum-key distribution using less than four quantum states. *Physical Review A*, 79:052312, May 2009.

אחד. אנו מתבוננים בקבוצת הנקודות בכדור בלוך המייצגות מצבים שאינם שזורים (הנקראים "מצבים פריקים") ומוכיחים שקיימות חמש מחלקות אפשריות של קבוצת המצבים הפריקים: הכדור כולו, קו שהוא קוטר, קו שאינו קוטר, נקודה על שפת הכדור, והקבוצה הריקה. אנו נותנים דוגמאות לכדורי בלוך השייכים לכל מחלקה, ומוכיחים שלא קיימות מחלקות אחרות. בנוסף, אנו מציגים אפשרויות להגדרת "מדדי שזירות" שונים מהקיימים היום, שמתאימים ערך 0 לכל המצבים הפריקים וערך גדול מ־0 לכל המצבים השזורים. אחת האפשרויות להגדרת "מדד שזירות" היא באמצעות שימוש ב"מרחק העקבה" של המצב המבוקש מהמצב הפריק הקרוב ביותר. התוצאות שהצגנו עשויות להיות חשובות לצורך מציאת המצב הפריק הקרוב ביותר בכדור (אם קיים) בחישוב מדד זה.

בפיסיקה קוונטית ניתן להגדיר סוגים שונים של מרחקים בין מצבים קוונטיים. אחד המרחקים השימושיים ביותר נקרא מרחק העקבה, והוא חסם מלמעלה על "יכולת ההבחנה" בין המצבים. (למשל: בין שני מצבים אורתוגונליים ניתן להבחין בוודאות, ולכן מרחק העקבה שלהם הוא 1; ובין שני מצבים זהים זה לזה לא ניתן להבחין כלל, ולכן מרחק העקבה שלהם הוא 0.) למרחק העקבה יש שימושים רבים באינפורמציה קוונטית ובהצפנה קוונטית, ובנוסף, יש לו משמעות גאומטרית פשוטה: הוא שווה למחצית המרחק האוקלידי בין המצבים בכדור בלוך.

פרוטוקולי הפצת מפתחות קוונטית מאפשרים לשני משתתפים המפעילים את הפרוטוקול, אליס ובוב, ליצור מפתח סודי אקראי משותף, גם אם מתייצבת מולם יריבה כל־יכולה, איב, בעל יכולת חישוב בלתי־מוגבלת (זוהי משימה בלתי־אפשרית בתקשורת קלאסית). אליס ובוב משתמשים בערוץ קוונטי לא־בטוח (איב יכולה ליירט ולשנות כרצונה את כל המצבים הקוונטיים הנשלחים בערוץ זה) ובערוץ קלאסי מאומת (איב יכולה להאזין לכל המידע הנשלח בו, המורכב מביטים קלאסיים, אך אינה יכולה לשנותו). לפרוטוקול הפצת המפתחות הקוונטית הראשון, של בנט וברסר (הנקרא BB84), וכן למספר פרוטוקולים חשובים נוספים, קיימות הוכחות בטיחות כנגד יריבים חזקים מאוד המבצעים את ההתקפות הכלליות ביותר האפשריות על מימוש תאורטי (אידאלי) של הפרוטוקול. בפרק 4 אנו דנים בפרוטוקול מעט שונה, הקרוי "BB84-INFO-z", ומוכיחים את בטיחותו כנגד מחלקה נרחבת של התקפות (הקרויות "התקפות קיבוציות", או collective attacks). יתרה מכך, אנו משתמשים ב"מרחק העקבה" כדי להפוך את הוכחת הבטיחות שלנו ליותר "ניתנת להרכבה" מהוכחות בטיחות קודמות דומות עבור BB84: כלומר, כדי להתקדם לקראת הוכחה לכך שהמפתח הסודי נשאר סודי גם כאשר אליס ובוב משתמשים בו בפועל כחלק מפרוטוקולים קריפטוגרפיים – למשל, לצורך הצפנה.

תקציר

החוקים הפיסיקליים של תורת הקוונטים מובילים למסקנות לא־אינטואיטיביות ומאפשרים לבצע פעולות וליצור מצבים פיסיקליים שניתן היה לחשוב שהם בלתי אפשריים (למשל: חלקיק עשוי להיות בסופרפוזיציה – למשל, סכום או הפרש – של כמה מיקומים שונים, כמה זמנים שונים, או כמה מצבים שונים). תחום המחקר הנקרא עיבוד אינפורמציה קוונטית חוקר כיצד ניתן לנצל את חוקי תורת הקוונטים לצורך ייצוג אינפורמציה ועיבודה, ומאפשר לפתור בעיות ולבצע משימות שאינן אפשריות (או שהן קשות) במחשבים ובמכשירי תקשורת קלאסיים (כלומר, סטנדרטיים ולא־קוונטיים).

בתזה זו, אנו משתמשים במושגים יסודיים של תורת האינפורמציה הקוונטית (בעיקר שזירות, כדור בלוך ומרחקים גאומטריים בין מצבים קוונטיים) כדי לנתח קשרים של מצבים קוונטיים זה לזה ופרוטוקולי הצפנה קוונטית.

תכונת השזירות היא תכונה חשובה של מצבים קוונטיים. באופן אינטואיטיבי (ולא לגמרי מדויק), שזירות מייצגת קורלציות קוונטיות (ולא קלאסיות) בין מספר מערכות קוונטיות שונות. שזירות היא אחת התופעות הקוונטיות החשובות ביותר, ואין לה הסבר קלאסי. לתופעת השזירות יש שימושים רבים באינפורמציה קוונטית, בתקשורת קוונטית, במחשוב קוונטי, ואף בחקר יסודות תורת הקוונטים עצמה.

חלק מהמצבים הקוונטיים ניתן לייצג באופן גאומטרי על־ידי כדור בלוך: כדור היחידה במרחב האוקלידי התלת־ממדי. המצבים הקוונטיים ה"רגילים", שעליהם פועלים ישירות החוקים של תורת הקוונטים, נקראים מצבים טהורים. בנוסף להם, קיימים מצבים מעורבים: מצב מעורב הוא התפלגות הסתברויות ("עירוב") של מספר מצבים טהורים. בהינתן שני מצבים טהורים שמקיימים תכונה מתמטית חשובה מסוימת ("אורתוגונליות"), ניתן לקבוע אחד מהם בקוטב הצפוני של כדור בלוך ואת השני בקוטב הדרומי שלו, ואז על שפת הכדור (ספירת בלוך) מופיעים כל המצבים הטהורים שהם סופרפוזיציות של שני המצבים המקוריים, ובתוך הכדור מופיעים כל המצבים המעורבים שמערבים שניים (או יותר) מהמצבים הטהורים שעל שפת הכדור. ייצוג גאומטרי זה הוא שימושי ואינטואיטיבי למטרות שונות; מידע נוסף עליו מופיע בפרק 2.

בפרק 3 מוצג ניתוח גאומטרי של השזירות עבור מצבים קוונטיים מסוג מסוים: מצבים מעורבים מדרגה 2. (מצב מעורב "מדרגה 2" הוא עירוב של שני מצבים טהורים.) לכל מצב מעורב מדרגה 2 (מכל מימד), אנו מגדירים כדור בלוך מוכלל שעליו מופיעים שני המצבים הטהורים (ושבתוכו מופיע המצב המעורב) ומנתחים את המצב המעורב ואת המצבים ה"שכנים" שלו בתוך כדור בלוך שהגדרנו. (אנו מוכיחים שכל מצב מעורב מדרגה 2 נמצא בכדור בלוך אחד ויחיד.) כזכור, כל נקודה בתוך כדור בלוך מייצגת מצב מעורב אחד, וכל נקודה על שפת הכדור (הנקראת ספירת בלוך) מייצגת מצב טהור

המחקר נעשה בהנחיית פרופ׳ חבר טל מור, בפקולטה למדעי המחשב.

רוב התוצאות בחיבור זה פורסמו כמאמרים מאת המחבר ושותפיו למחקר בכנסים ובכתבי־עת:

Michel Boyer, Rotem Liss, and Tal Mor. Geometry of entanglement in the Bloch sphere. *Physical Review A*, 95:032308, March 2017.

Michel Boyer, Rotem Liss, and Tal Mor. Security against collective attacks of a modified BB84 QKD protocol with information only in one basis. In *Proceedings of the 2nd International Conference on Complexity, Future Information Systems and Risk – COMPLEXIS, 24-26 April, 2017, Porto, Portugal*, pages 23–29, April 2017.

תודות

ברצוני להודות למנחה שלי, פרופ׳ חבר טל מור, על הדרכתו המועילה, ועל הדיונים, הרעיונות והעזרה במהלך מחקר זה. ברצוני גם להודות לפרופ׳ חבר מישל בואייה על שיתוף פעולה פורה במחקר, דיונים, עזרה, ועזרה טכנית ביצירת התמונות המופיעות בתזה זו.

ברצוני גם להודות לז׳יל ברסר, לג׳ון סמולין, ללואי סלביי, ליוסי וינשטיין, ליאיר רזק, ליובל אליאס, ולאיתי פיירוורקר.

תודה מיוחדת מגיעה למשפחתי.

אני מודה לטכניון על התמיכה הכספית הנדיבה בהשתלמותי.

שזירות ומרחקים גאומטריים באינפורמציה קוונטית ובהצפנה קוונטית

חיבור על מחקר

לשם מילוי חלקי של הדרישות לקבלת התואר
מגיסטר למדעים במדעי המחשב

רותם ליס

הוגש לסנט הטכניון – מכון טכנולוגי לישראל
אייר התשע"ז חיפה מאי 2017

שזירות ומרחקים גאומטריים
באינפורמציה קוונטית
ובהצפנה קוונטית

רותם ליס