RESEARCH WORK

Application of mutually unbiased bases in quantum information

Petr Šulc

Acknowledgements

I would like to thank to prof. Jiří Tolar for support and guidance. I also thank to prof. Jex and prof. Alber for consultations and useful comments.

Contents

Introduction

Quantum cryptography is certainly one the most promising branches of quantum information theory. Since its discovery in 1984, it has been a rapidly evolving field with very promising applications. It has already been experimentally realized by several institutions and more experiments are currently in development. Construction of quantum cryptographic networks and devices presents a big technical challenge, but there are still many aspects of quantum cryptographic protocols that are interesting from the theoretical point of view as well. The nature of quantum cryptography is truly interdisciplinary: it is a fusion of physics, computer science and electronics. In this work, necessary physical and information theoretical background is first given. Then, we present the basic overview of quantum cryptography together with description of possible eavesdropping attacks. Quantum cryptography is then investigated in Hilbert spaces od dimensions higher than 2. Quantum cryptographic protocols are related to the use of *mutually unbiased bases*. The maximal size of a set of mutually unbiased bases in Hilbert spaces of dimension different than prime or a power of prime is still unknown. We therefore consider and compare the generalizations of the two-dimensional protocols to higher dimension, where one generalization uses only 2 mutually unbiased bases and the other one uses the maximal possible number of mutually unbiased bases.

In accordance with cryptographic textbooks, the sending party in the cryptographic protocol will be called Alice and the receiving party will be called Bob. The person who is trying to eavesdrop the communication will be called Eve.

Chapter 1

Quantum states and composite systems

We start with a brief review of description of quantum states by density matrices [1] that is necessary in quantum theory in general and then we focus on composite systems [2] which play very important role in quantum computation and communication in general, since they are used to describe a multiple qubit (or qudit) system.

1.1 Pure and mixed states

Throughout this work, we will only concentrate on the finite dimensional quantum systems, therefore all states will be represented in finite dimensional (complex) Hilbert spaces $\mathcal{H}$. The pure states are represented by vectors in Hilbert spaces. The *bracket* notation introduced by P. A. M. Dirac [3] is used to denote these vectors. In quantum computation and information theory, vectors in two dimensional Hilbert space are called *qubits* and the vectors of standard (*computational*) basis are denoted as

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{1.1}$$

Sometimes we may encounter a different orthonormal basis composed of vectors

$$|+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \qquad |-\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}. \tag{1.2}$$

In a d-dimensional Hilbert space the vectors of standard basis are called *qudits*. Generalizing the notation (1.1) to higher dimensions, they are denoted as $|i\rangle$ where $i \in \{0, 1, \ldots d-1\}$ and $|i\rangle$ is a vector with 1 at the $i+1$-th place and zeros elsewhere. Vectors in three dimensional Hilbert space are called *qutrits*, in four dimensional case *quarts*.

The general description of a quantum state is provided by a density matrix. Here we just briefly summarize the important formulas and properties concerning density matrices

[4] [5]. Suppose we have a density matrix ρ that is assigned to a given quantum state in Hilbert space $\mathcal{H}$. Then:

1. ρ is Hermitian. It is defined as a weighted sum of one-dimensional orthogonal projectors
$$\rho \equiv \sum_i p_i |\psi_i\rangle\langle\psi_i|, \quad p_i \geq 0, \quad \sum_i p_i = 1. \tag{1.3}$$

2. In order for the operator ρ to be normalized, its trace has to be equal to one, because
$$\text{tr}(\rho) = \sum_i p_i \text{tr}\left(|\psi_i\rangle\langle\psi_i|\right) = \sum_i p_i = 1$$
and we naturally assume that the sum of all probabilities is equal to 1.

3. The condition that the eigenvalues of operator ρ play the role of probabilities requires them to be all ≥ 0, meaning that ρ has to be positive.

4. The probability of finding a system described by density matrix ρ in the state $|a\rangle$ is:
$$p_a = \langle a|\rho|a\rangle. \tag{1.4}$$
Formula (1.4) can be rewritten using an orthogonal projector $P_a = |a\rangle\langle a|$. The mean value of this operator will be equal to the probability of measuring state $|a\rangle$:
$$p_a = \langle a|\rho|a\rangle = \text{tr}(\langle a|\rho|a\rangle) = \text{tr}(P_a\rho). \tag{1.5}$$

5. State represented by density matrix ρ is pure if and only if $\text{tr}(\rho^2) = 1$. Otherwise $\text{tr}(\rho^2) < 1$.

1.2 Composite systems

Composite systems are described as tensor products of Hilbert spaces.

1.2.1 Tensor product of Hilbert spaces

Suppose we have Hilbert spaces $\mathcal{V}$ and $\mathcal{W}$. Then we can define a Hilbert space $\mathcal{H}$ as their tensor product, which is denoted as
$$\mathcal{H} = \mathcal{V} \otimes \mathcal{W}.$$
It is a linear span of $|v\rangle \otimes |w\rangle$, where $|v\rangle \in \mathcal{V}$ and $|w\rangle \in \mathcal{W}$. If the set of vectors $|e_j^{\mathcal{V}}\rangle$ and $|e_i^{\mathcal{W}}\rangle$ form orthonormal bases of $\mathcal{V}$ and $\mathcal{W}$, respectively, then the set $|e_j^{\mathcal{V}}\rangle \otimes |e_i^{\mathcal{W}}\rangle$ forms an orthonormal basis of $\mathcal{V} \otimes \mathcal{W}$. In finite dimensional spaces, if $\dim\mathcal{V} = n$ and $\dim\mathcal{W} = m$, then $\dim\mathcal{V} \otimes \mathcal{W} = mn$. The following relations are satisfied in $\mathcal{V} \otimes \mathcal{W}$ by definition:

1. For $\lambda \in \mathbb{C}, |v\rangle \in \mathcal{V}, |w\rangle \in \mathcal{W}$

$$\lambda(|v\rangle \otimes |w\rangle) = (\lambda|v\rangle) \otimes |w\rangle = |v\rangle \otimes (\lambda|w\rangle). \tag{1.6}$$

2. For arbitrary vectors $|v_1\rangle, |v_2\rangle \in \mathcal{V}, |w\rangle \in \mathcal{W}$

$$(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle. \tag{1.7}$$

3. If A and B are weighted shift operators acting in $\mathcal{V}$ and $\mathcal{W}$ respectively, then one can define an operator $A \otimes B$ acting in $\mathcal{V} \otimes \mathcal{W}$ as

$$(A \otimes B)(|v\rangle \otimes |w\rangle) \equiv A|v\rangle \otimes B|w\rangle. \tag{1.8}$$

4. The inner product in $\mathcal{V} \otimes \mathcal{W}$ is defined by using the inner products in $\mathcal{V}$ and $\mathcal{W}$ as

$$\left\langle \sum_i \alpha_i |v_i\rangle \otimes |w_i\rangle \middle| \sum_j \beta_j |\tilde{v_j}\rangle \otimes |\tilde{w_j}\rangle \right\rangle \equiv \sum_{i,j} \overline{\alpha_i}\beta_j \langle v_i|\tilde{v_j}\rangle\langle w_i|\tilde{w_j}\rangle. \tag{1.9}$$

The above definitions can be extended to a tensor product of n Hilbert spaces: $\mathcal{V}_1 \otimes \mathcal{V}_2 \otimes \ldots \otimes \mathcal{V}_n$.

1.2.2 Quantum states in composite spaces

As follows from the previous section, if we have an n-dimensional Hilbert space $\mathcal{H}$ with orthonormal basis

$$|j\rangle, \quad j \in \{0, 1, \ldots, n-1\}$$

then the space $\mathcal{H} \otimes \mathcal{H}$ will have orthonormal basis

$$|i\rangle \otimes |j\rangle, \quad i, j \in \{0, 1, \ldots, n-1\}.$$

It is clear that this approach ca be generalized for higher products as well. Sometimes instead of $|i\rangle \otimes |j\rangle$ a shorter notion is used: $|i\rangle|j\rangle$ or $|ij\rangle$. In the following discussion, we will consider a composite system that is a tensor product of two Hilbert spaces $\mathcal{H}$. A general state of a composite system is described by a density matrix ρ. If we have a mixed quantum state ρ in a composite space $A \otimes B$ and we want to know to what state it corresponds for example in space A, then a procedure called *partial trace* has to be performed. The partial trace over system B is a linear operator defined by the relation

$$\mathrm{tr}_B \left(|j_A\rangle\langle k_A| \otimes |c_B\rangle\langle d_B|\right) \equiv \langle c_B|d_B\rangle |j_A\rangle\langle k_A| \tag{1.10}$$

for any vectors $|j_A\rangle, |k_A\rangle \in A$ and $|c_B\rangle, |d_B\rangle \in B$. For example, if we write out ρ explicitly in the base of $A \otimes B$:

$$\rho = \sum_{i,j=0}^{n-1} p_{ij} |ij\rangle\langle ij|$$

(where $|ij\rangle\langle ij|$ are one-dimensional projectors) and compute the partial trace over system B, we get

$$\rho_A = \mathrm{tr}_B(\rho) = \sum_{i=0}^{n-1} \left(\sum_{j=0}^{n-1} p_{ij} \right) |i\rangle\langle i|.$$

Note that a pure state in a composite system $\mathcal{H}_A \otimes \mathcal{H}_B$ can be a mixed state from a point of view of an observer in system $\mathcal{H}_A$ or $\mathcal{H}_B$.

Bell states and entanglement

Suppose we have a composite system $\mathcal{H} \otimes \mathcal{H}$ where $\mathcal{H}$ is two-dimensional. Then the Bell basis of this composite system is composed of four Bell states:

$$\begin{aligned} |\psi_+\rangle &= \frac{|00\rangle + |11\rangle}{\sqrt{2}} \qquad |\psi_-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \\ |\Phi_+\rangle &= \frac{|01\rangle + |10\rangle}{\sqrt{2}} \qquad |\Phi_-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \end{aligned}$$

The states listed above have an interesting property: they are *entangled*:

Definition 1. A state $|\psi\rangle$ of a composite system $\mathcal{H}_a \otimes \mathcal{H}_b$ is *entangled* if it cannot be expressed as

$$|\psi\rangle = |a\rangle \otimes |b\rangle$$

for any $|a\rangle \in \mathcal{H}_A$ and $|b\rangle \in \mathcal{H}_B$.

Purification

Purification is a mathematical procedure often used in quantum information theory. Suppose we have a mixed state ρ^A in Hilbert space $\mathcal{H}_A$. It is then possible [2] to find a pure state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, where $\mathcal{H}_B$ is an additional Hilbert space and

$$\rho^A = \mathrm{tr}_B \left(|\psi\rangle\langle\psi| \right).$$

The state $|\psi\rangle$ is called *purification* of state ρ^A.

Chapter 2

Quantum information theory

In this chapter, we will briefly present the necessary definitions and theorems from cassical and quantum information theory that are used in quantum cryptography and security analysis of the protocols. We will begin by introduction some notions from classical information theory that are used in the quantum case as well.

2.1 Entropy

2.1.1 Shannon entropy

Entropy enables us to quantify the amount of information. Suppose that message X takes values from the set

$$\mathcal{X} = \{x_i | i = 1 \dots n\}.$$

The occurrence of these elements in the message X is given by a probability distribution p, i. e. every element x_i has its respective probability of appearance which will be denoted as $p(x_i)$ for some $i \in \{1 \dots n\}$. In case of a binary message, the symbols are denoted 0 and 1. Since X takes values according to a given probability distribution, it can be thought of as a random variable. Entropy can be therefore understood as the amount of knowledge that we have about a source that produces messages composed of elements of $\mathcal{X}$ according to a given probability distribution. The following definition of entropy [2] represents the key concept of classical information theory:

Definition 2. Suppose X is a random variable that can take any value from a set $\mathcal{X}$ according to a probability distribution $p(x_1), p(x_2), \dots, p(x_n)$ where $x_i \in \mathcal{X}$. We define *Shannon entropy* of X as

$$H(X) = H\left(p(x_1), p(x_2), \dots, p(x_n)\right) \equiv -\sum_{x \in \mathcal{X}} p(x) \log\left(p(x)\right) \tag{2.1}$$

Please note that by $\log$ we mean the logarithm with base 2 and by definition we put

$$0 \log(0) \equiv 0.$$

For X that takes values from $\mathcal{X}$ with a given probability distribution $p(x)$, we use the notation

$$X \sim (\mathcal{X}, p(x)) \tag{2.2}$$

As an example, consider a source that produces 0 with probability p and 1 with probability $1-p$. The Shannon entropy of such a source is then

$$H(p, 1-p) = -p \log(p) - (1-p) \log(1-p). \tag{2.3}$$

It can be easily seen that $H(p, 1-p)$ achieves its maximum for $p = 0.5$, therefore entropy can be intuitively understood as the measure of our uncertainty about a given source. The entropy (2.3) is referred to as *binary entropy* H_{bin}.

One can easily see that Shannon entropy has the following property for an arbitrary $X \sim (\mathcal{X}, p(x))$:

$$H(X) \geq 0 \text{ and } H(X) = 0 \text{ if and only if } p(x_0) = 1 \text{ for some } x_0 \in \mathcal{X}$$

Joint entropy

Definition 3. For two random variables X and Y, we define the *joint entropy* $H(X, Y)$ as

$$H(X, Y) \equiv -\sum_{x,y} p(x, y) \log\left(p(x, y)\right) \tag{2.4}$$

where x and y correspond to all possible values that X and Y can acquire and $p(x, y)$ is the joint probability distribution. The above definition can be easily extended to a joint entropy of n random variables $X_1, X_2, \ldots X_n$

$$H(X_1, X_2, \ldots X_n) \equiv -\sum_{x_1, x_2, \ldots, x_n} p(x_1, x_2, \ldots, x_n) \log\left(p(x_1, x_2, \ldots, x_n)\right) \tag{2.5}$$

Joint entropy satisfies the inequality

$$H(X, Y) \leq H(X) + H(Y) \tag{2.6}$$

where equality is attained if and only if $p(x, y) = p(x)p(y)$ (i. e. X and Y are independent).

Conditional entropy

Suppose we have two random variables X and Y (which we expect not to be independent) and we would like to express the level of our uncertainty about the variable X on the condition of knowing Y. For such reasons, it is useful to define *conditional entropy*

Definition 4. For two random variables X and Y, we define *entropy of X conditional on knowing Y* as

$$H(X|Y) \equiv H(X,Y) - H(Y) \tag{2.7}$$

where $H(X,Y)$ is the joint entropy of X and Y. Note that $H(X|Y) = H(X)$ if and only if X and Y are independent. It means that if two variables are independent, the knowledge of one of them does not provide any more information about the other one, as one would naturally expect.

The conditional entropy $H(X|Y)$ can be expressed in terms of probabilities as

$$H(X|Y) = \sum_{y \in \mathcal{Y}} p(y) H(X|Y=y) \tag{2.8}$$

where

$$H(X|Y=y) = -\sum_{x \in \mathcal{X}} p(x|y) \log(p(x|y)). \tag{2.9}$$

In the equation, the $p(x|y)$ is the conditional probability of the random variable X being equal to x on the condition of Y being equal to y.

Mutual information

Mutual information quantifies how much have two variables X and Y in common, for example a variable X generated by a sender and transmitted through a wire and variable Y read at the end of the wire. These two are not necessarily equal, because an error may occur during the transmission.

Definition 5. The *mutual information* of two random variables X and Y is

$$I(X,Y) \equiv H(X) + H(Y) - H(X,Y). \tag{2.10}$$

Sometimes [2] notation $H(X{:}Y)$ is used instead of $I(X,Y)$. Note that $I(X,Y) = I(Y,X)$ as one can see from the definition.

Using (2.10) and (2.7) one can derive the following equality:

$$I(X,Y) = H(X) - H(X|Y). \tag{2.11}$$

2.1.2 von Neumann entropy

For completeness, we will present entropy that is related to quantum states. Since quantum states are described by density matrices [1] [5] (and we can assign a density matrix to a pure state as well), we want to find a function of a density matrix with similar properties as Shannon entropy.

Definition 6. For a quantum state described by a density matrix ρ, the *von Neumann entropy* [2] is

$$S(\rho) \equiv -\text{tr}(\rho \log \rho). \tag{2.12}$$

Therefore for a density matrix ρ in an n-dimensional space with eigenvalues denoted as λ_i we see from (2.12) that

$$S(\rho) = -\sum_{i=1}^{n} \lambda_i \log \lambda_i. \tag{2.13}$$

2.2 Distance measures in information theory

2.2.1 Hamming distance

Hamming distance [6] is used in classical information theory to distinguish between two binary messages.

Definition 7. The *Hamming distance* between two messages of the same length is equal to the number of places at which they are not identical.

For example the Hamming distance between two bit strings 00110 and 00011 is 2.

2.2.2 Distances between two probability distributions

Since the value of entropy depends on a given probability distribution for a given random variable with probability distribution function, it is useful to introduce a distance measure between different probability distributions. There are two widely used measures for this purpose.

Definition 8. For two probability distributions $p(x)$ and $q(x)$ where $x \in \mathcal{X}$, we define *trace distance* [2] as

$$D(p,q) \equiv \frac{1}{2} \sum_{x \in \mathcal{X}} |p(x) - q(x)| \tag{2.14}$$

Trace distance is a metric on probability distributions, because it is symmetric and satisfies the triangle inequality

$$D(p,q) \leq D(p,w) + D(q,w)$$

where $p, w,$ and q are some probability distributions on $\mathcal{X}$. The following equation [2] explains the notion of trace distance between two probabilities a little more intuitively:

$$D(p,q) = \max_{S \subset \mathcal{X}} \left| \sum_{x \in S} p(x) - \sum_{x \in S} q(x) \right| \tag{2.15}$$

Another distance measure between two probability distributions is called fidelity.

Definition 9. The *fidelity* of two probability distributions p and q is

$$F(p,q) = \sum_{x \in \mathcal{X}} \sqrt{p(x)q(x)}. \tag{2.16}$$

It is easy to see that fidelity is symmetric but does not satisfy the triangle inequality, therefore it is not a metric.

2.2.3 Distance measures for quantum states

Hamming distance enables to quantify how different are two pieces of information in classical information theory. In quantum information theory, there are two widely used functions that are used to quantify the difference between the quantum states described by density matrices. Since probabilities of measurement outcomes are determined by density matrices (and vice-versa, by knowing probabilities of all possible outcomes in a given basis, one can define a density matrix describing a given quantum states), it seems natural to introduce a generalization of the measures that are used to distinguish between two probability distributions.

Trace distance

Definition 10. Let two quantum states in an n-dimensional quantum space be described by density matrices ρ and σ, respectively. Then the *trace distance* between these two states is

$$D(\rho, \sigma) \equiv \frac{1}{2} \text{tr}\left(|\rho - \sigma|\right) \tag{2.17}$$

where absolute value of an operator A is understood $\sqrt{A^\dagger A}$ [7]. In our simple case of a hermitian matrix $\eta = \rho - \sigma$, $\text{tr}\left(|\eta|\right)$ is just equal to sum of absolute values of its eigenvalues.

Trace distance D between two quantum states is denoted by the same letter as the distance between two probability distributions, but it is clear from the context which one of the two is used.

Fidelity

The notion of fidelity plays a key concept in quantum information theory and is often used to distinguish between two states, although it is not a metric on the space of all density

operators (similarly as the fidelity in the classical information theory). Currently, two different definitions of fidelity are used, we will use the original definition [8]:

Definition 11. The *fidelity* of two quantum states described by density matrices ρ and σ is

$$F(\rho,\sigma) \equiv \left(\mathrm{tr}\left(\sqrt{\rho^{\frac{1}{2}}\sigma\rho^{\frac{1}{2}}}\right)\right)^2. \tag{2.18}$$

Some authors use a little different definition of fidelity:

$$\tilde{F}(\rho,\sigma) \equiv \mathrm{tr}\left(\sqrt{\rho^{\frac{1}{2}}\sigma\rho^{\frac{1}{2}}}\right). \tag{2.19}$$

The connection between these two definitions is $F(\rho,\sigma) = \left(\tilde{F}(\rho,\sigma)\right)^2$.

Since it is quite difficult to see properties of fidelity directly from definition (2.18), we will list its several properties [2] [8] that make the notion of fidelity more clear to understand.

Theorem 1 (Uhlmann's theorem [2])**.** Fidelity of two quantum states in Hilbert space $\mathcal{H}$ that are described by density matrices ρ and σ can be calculated as

$$F(\rho,\sigma) = \max_{|\psi\rangle,|\varphi\rangle} |\langle\psi|\varphi\rangle|^2 \tag{2.20}$$

where $|\psi\rangle, |\varphi\rangle$ are the purifications of ρ and σ into space $\mathcal{H}\otimes\mathcal{H}$ respectively. The maximum is taken over all purifications of ρ and σ into $\mathcal{H}\otimes\mathcal{H}$.

Now it is clear that fidelity is symmetric. Moreover, one can see from (2.20) that the fidelity is bounded between 0 and 1:

$$\forall\rho,\sigma\in\mathcal{H} \quad 0 \le F(\rho,\sigma) \le 1. \tag{2.21}$$

We also see that it is equal to one in case where the two quantum states ρ and σ are identical.

The next equation presents a useful formula that is used to compute fidelity of a mixed state (i.e. a state described by a density matrix ρ) and a pure state $|\varphi\rangle$. By inserting them into (2.18) (and noting that the density matrix of a pure state is the one-dimensional projector $|\varphi\rangle\langle\varphi|$) one gets

$$F\left(|\varphi\rangle,\rho\right) = \left(\mathrm{tr}\left(\sqrt{\langle\varphi|\rho|\varphi\rangle|\varphi\rangle\langle\varphi|}\right)\right)^2 = \langle\varphi|\rho|\varphi\rangle. \tag{2.22}$$

It means that the fidelity of a pure state $|\varphi\rangle$ and a mixed state ρ corresponds to the transition probability. (1.4).

2.3 Quantum cloning

In this section, we investigate the possibilities of copying quantum states.

2.3.1 The no-cloning theorem

The fact that non-orthogonal quantum states cannot be perfectly copied stands at the heart of quantum cryptography. The no-cloning theorem is one of the most important conclusions of quantum information theory. Here we present the theorem and its proof as presented in [9] [2]

Theorem 2. Suppose we have two non-orthogonal pure states $|\varphi\rangle$, $|\psi\rangle$ and a quantum cloning machine, i.e. a device that starts out in some initial quantum state $|i\rangle$ which is transformed, after the unitary evolution, to the state $|\varphi\rangle$ while the original state is preserved. The scheme for the function of this machine is then

$$|\varphi\rangle \otimes |i\rangle \longrightarrow U\left(|\varphi\rangle \otimes |i\rangle\right) = |\varphi\rangle \otimes |\varphi\rangle$$
$$|\psi\rangle \otimes |i\rangle \longrightarrow U\left(|\psi\rangle \otimes |i\rangle\right) = |\psi\rangle \otimes |\psi\rangle$$

Where U is a unitary matrix acting on a composite Hilbert space.

Proof. Let $|\varphi\rangle$ and $|\psi\rangle$ be two different non-orthogonal states $|\psi\rangle$ and $|\varphi\rangle$ which are copied by the cloning machine. The copying proceeds as follows:

$$\begin{aligned} U\left(|\psi\rangle \otimes |i\rangle\right) &= |\psi\rangle \otimes |\psi\rangle \\ U\left(|\varphi\rangle \otimes |i\rangle\right) &= |\varphi\rangle \otimes |\varphi\rangle \end{aligned}$$

Now we take the inner product of the first and second equation and using the fact that unitary matrices preserve the inner product, we obtain

$$\langle\psi|\varphi\rangle \underbrace{\langle i|i\rangle}_{=1} = \left(\langle\psi|\varphi\rangle\right)^2. \tag{2.23}$$

So it is clear that $\langle\psi|\varphi\rangle$ must be equal to either 1 or 0 to fulfill (2.23). These both cases were excluded by the assumption that states $|\varphi\rangle$ and $|\psi\rangle$ were neither identical nor orthogonal. □

Even though the above theorem prevents one from making an identical copy of a quantum state, it is still possible to create approximate copies of quantum states through quantum cloning machines [10]. A universal quantum cloning machine for qudits will be presented in section 4.2.2 with relation to the eavesdropping attack on quantum cryptographic protocol.

2.4 Error correction and quantum error correction

Error correction plays very important role in classical information theory: it is necessary to perform an error correction for example after a transmission of data through a noisy channel. The same problem occurs with quantum states, which can be corrupted during a transmission through a channel.

2.4.1 Classical error correction

We will briefly present the underlying ideas of classical error correction. It is a very important and extensively studied branch of information theory [11].

Three bit code

One of the simplest protections against errors during the transmission of classical bits is encoding the 0 or 1 into so-called logical 0 and logical 1. It means that instead of transmitting 0, three bits are transmitted: 000. The same applies for 1: instead of 1, 111 is transmitted. An error that occurs during the transmission is called a bit flip: an error occurring on bit 0 turns it into 1 and vice-versa. If three identical bits are sent, and error occurs in only one of them, it can still be inferred from the other two what was the original value that was sent. That is, 001 is still interpreted as 0. Therefore, one bit is encoded into three bits and such a code can protect against one bit flip error that occurs during the transmission. If an error occurs during the transmission with probability p (that is with this probability, one bit is flipped during the transmission), then the above code fails to correct an error with probability $p^2(1-p) + p^3 = p^2$ (since the three bit encoding code fails if either two or all three bits are flipped).

Coding theorem

In information theory, we define [11] $[N, K]$ codes:

Definition 12. $[N, K]$ *code* is a code composed of 2^K *codewords* where each one of them is of length that is used to encode N bits, i.e. K bits are transformed into an N bit string (a codeword) that is then sent through a noisy channel and decoded by a decoding algorithm that assigns a bit string of length K to a codeword that was received from the channel. The code's *rate* R is defined as $R = \frac{K}{N}$.

The above three bit code is an example of a $[3, 1]$ code, but more sophisticated methods for constructing codes and correcting transmitted data are available using so-called generator and parity check matrices [2] [11].

The possibilities of error correcting codes are summarized in Shannon's coding theorem [11]:

Theorem 3 (Shannon's noisy channel coding theorem)**.** For a given memoryless channel (that means that the channel that acts the same way every time it is used, i.e. its properties

do not change in time) there exists $C \geq 0$ (called the *channel capacity*) with the following property: For any $\epsilon > 0$ and $\tilde{R} < C$ and for large enough N, there exists a block code of length N and rate $R \leq \tilde{R}$ and a decoding algorithm, such that the maximal *probability of error* p is $\leq \epsilon$. The probability of error p is defined as the maximal probability over all sent messages that the decoded output bits will not be equal to the bits originally sent.

Shannon's theorem in other words states that we can achieve arbitrarily small probability of error. However, such codes may require very large values of N, thus not being very effective.

Random coding

Following the example of the three bit code, it is possible to define more complicated codes that can encode more than one bit. One such possibility is called *random coding* and illustrates how the basic idea of Hamming distance (Definition 7) between two codewords can be used in error correction [11].

Given blocks of length K, we want to generate a codeword of length N. Supposing that the rate $R = \frac{K}{N} < 1 - H(p, 1-p)$ where p is the probability of an error occurring during the transmission, one can use them to transmit K-bit long block. For a fixed parameter q ($0 < q < 1$) we generate randomly 2^K codewords of length N, where the i-th bit will be 0 with probability q and 1 with probability $1 - q$. Of course it is possible that the code-generating algorithm will fail and will generate for example the same codeword for all inputs. However, on average, we should obtain a usable code. During the transmission, several bits get corrupted (and given the probability p of a bit being flipped, one expects Np bit to be flipped on average for large N). Therefore, the Hamming distance of the received message is in average Np from the original codeword. Therefore, one constructs a *Hamming sphere* (a set of all bit strings of length N that have Hamming distance from a given codeword lower or equal to Np) around each codeword. It can be shown that the overlaps between different Hamming spheres will not play significant role in the error correction and that the random coding approach succeeds for any rate $R < 1 - H(p, 1-p)$ [11] [2].

2.4.2 Quantum error correction

It is clear that for quantum error correction, one has to use somewhat different approach. First, for a case of a qubit, during a transmission, the error that can occur to a qubit is expressed through an action of a unitary matrix E

$$|\psi\rangle = E|\psi\rangle. \tag{2.24}$$

Unitary matrix E is a 2×2 matrix and can therefore be expanded in a basis of consisting of identity matrix I and Pauli matrices σ_x, σ_y and, σ_z

$$E = \alpha I + \beta\sigma_x + \gamma\sigma_y + \delta\sigma_z. \tag{2.25}$$

Pauli matrices then correspond to specific errors that can occur during the transmission. Matrices σ_x, σ_y and σ_z correspond to bit flip error, phase flip error and combination of the two respectively. The simplest method for error correction is a generalization of the three-bit code to quantum case [2]. That is, the qubit states $|0\rangle$ and $|1\rangle$ are encoded as

$$\begin{aligned} |0\rangle &\longrightarrow |000\rangle \\ |1\rangle &\longrightarrow |111\rangle \end{aligned}$$

We encode a state $\alpha|0\rangle + \beta|1\rangle$ from space $\mathcal{H}$ as $\alpha|000\rangle + \beta|111\rangle$ in space $\mathcal{H} \otimes \mathcal{H} \otimes \mathcal{H}$. If a bit-flip error occurs to one of the three qubits (by an application of operator σ_x acting in one of the Hilbert space). To correct the bit-flip error that can occurred a measurement operator M is applied. The operator M is characterized by the projectors

$$\begin{aligned} P_1 &= |100\rangle\langle 100| + |011\rangle\langle 011| \\ P_2 &= |010\rangle\langle 010| + |101\rangle\langle 101| \\ P_3 &= |001\rangle\langle 001| + |110\rangle\langle 110| \end{aligned}$$

where each projector corresponds to a bit flip occurring to i-th qubit. For example, if measurement indicates that a bit flip error occurred to second qubit, then it is possible to apply an operator $I \otimes \sigma_x \otimes I$ which will correct actual state from $\alpha|010\rangle + \beta|101\rangle$ to the original state. Note that this approach is done without knowing the values of a and b. If more errors occur (such as phase errors), this procedure fails. It is possible to extend the three-qubit code to so-called *Shor code* [2], which is able to correct phase flip errors as well. The more complex error correcting quantum codes, such as CSS codes are possible to be constructed as well. In general, it is possible to construct an arbitrary quantum code, whose states in Hilbert space $\mathcal{H}^{\otimes n}$ encode k qubits [2] [12]. Such a code can be constructed for a given number of t errors that it has to correct.

2.5 Information reconciliation

2.5.1 Formulation of the task

Information reconciliation is a process of error correction that Alice and Bob perform in order to obtain a shared key. The information reconciliation protocol is done over classical channel, i.e. does not include any manipulation with quantum states. However, the motivation for application of information reconciliation protocols lies in the need to

correct data that were obtained as an outcome of measurement of quantum states. Despite being rather a part of classical information theory, research in the field of information reconciliation protocols was largely stimulated by the needs of quantum cryptography [9].

Now, suppose that Bob and Alice possess a block of bits of randomly generated data that is only partially correlated (due to errors that occurred when Eve sent her data to Bob through an insecure channel). Bob's block will be denoted as B, Alice's block will be denoted as A. The task is therefore for Bob and Alice to establish a common block S by using classical communication over an insecure channel. Because the channel is insecure, they want to reveal as little information as possible to a potential eavesdropper Eve about their final secret key S.

2.5.2 Information reconciliation protocols

There exist several protocols that can be used for information reconciliation [13] [14] [9]. We suppose Alice has a string A and Bob has a string B. These are divided into blocks of length n (n and m are fixed parameters of the information reconciliation protocols). We give an example of an information reconciliation protocol

1. Eve randomly chooses a function (called a hash function) g from a set $\mathcal{G}$ defined as

$$\mathcal{G} = \left\{ g : \{0,1\}^n \to \{0,1\}^m \quad | \quad (\forall x, y \in \{0,1\}^n, x \neq y) \left(p\left(g(x) = g(y)\right) \leq \frac{1}{2^m} \right) \right\} \tag{2.26}$$

   where p denotes probability. It can be proved that such set $\mathcal{G}$ exists for arbitrary choice of parameters m and n [14]. Functions from set $\mathcal{G}$ are called *two universal hash functions*.

2. She computes $g(A)$ and sends her output to Bob, together with the description of function g.

3. Bob chooses a string $\tilde{B}$ from a set $Q = \{D \in \{0,1\}^n \quad | \quad g(D) = g(A)\}$ such that the Hamming distance between B and $\tilde{B}$ is minimal. The string $\tilde{B}$ is now Bob's corrected bit string of length n. Assuming that the bits sent from Alice to Bob get corrupted with probability p (i.e. with this probability, 0 is detected as 1 and vice-versa), the following protocol is an example of information reconciliation procedure [13]:

Information reconciliation protocols are characterized by their:

- *Robustness*, i.e. the probability of failure of the protocol (that means that Bob has no candidate string $\tilde{B}$ that would replace his string B.

- *Probability of error* p_e: p_e is the probability that Bob's final string $\tilde{B}$ will not be equal to Alice's string A
- *Information leakage* I_E: The amount of information that eavesdropper Eve gains on the final shared key between Alice and Bob by listening to the public discussion during the protocol between Bob and Alice.

For the information reconciliation protocol described above, it can be proved [13] that for p_e and I_E being functions of n, one can compute that:

$$\lim_{n \mapsto \infty} p_e = 0$$

and information leak I_E approaches asymptotically $nH(p, 1-p)$.

2.6 Privacy amplification

2.6.1 Motivation

Privacy amplification is an essential part of all key generating protocols. In case eavesdropper Eve has some partial information about the shared key between Alice and Bob, privacy amplification has to be employed in order to decrease Eve's knowledge about the key. We assume that Bob and Alice share a bit string S about which Eve has some amount of information $I_E(S)$. Alice and Bob now must use a public channel in order to establish a final key $\tilde{S}$ from their original key S. Their intention is to create the key $\tilde{S}$ in such a way that Eve's information $I_E\left(\tilde{S}\right)$ can be made arbitrarily small.

2.6.2 Privacy amplification by public discussion protocol

The privacy amplification protocol uses the set of two universal hash functions $\mathcal{G}$ as defined in (2.26). The string is divided into blocks of length n, a previously agreed parameter. The protocol then proceeds as follows:

1. Bob and Alice agree on the parameter $m \in \mathbf{N}, m < n$ of the protocol.
2. Alice chooses randomly a two universal hash function $g \in \mathcal{G}$. She tells Bob which function she chose.
3. Alice and Bob compute $g(S_i)$ where S_i is the i-th block of their key S. The output $\tilde{S}_i = g(S_i)$ is a m-bit long part of the final key $\tilde{S}$. Note that since $n > m$, the new key will be shorter than the original one. This is the price they have to pay for lowering Eve's information about their key.
4. Alice and Bob apply steps 2 and 3 for all blocks.

The next theorem states that Bob and Alice can establish a secret key through this protocol [15]:

Theorem 4. For all positive ϵ and γ, there is a positive α such that if Alice and Bob share a random n-bit string S, which Eve receives through a channel with error probability ϵ (i. e. Eve is eavesdropping the distribution of the original key S between Alice and Bob and she has the probability ϵ of getting the right bit). Then using the privacy amplification by public discussion protocol, choosing

$$m = \lfloor (H(\epsilon, 1-\epsilon) - \gamma)\, nS \rfloor$$

and sufficiently large n, Eve's expected information about the final key is $I_E\left(\tilde{S}\right) \leq 2^{-\alpha n}$

Therefore Bob and Alice can make Eve's information exponentially small.

2.7 Important theorems

We will present two important theorems [16] [17] that will be required in the following sections.

Theorem 5. Suppose that Alice and Bob share a (not perfectly) correlated secret key, about which Eve has some partial information. The whole situation can be described through a probability distribution function $P(\alpha, \beta, \epsilon)$, where α, β, ϵ correspond to Alice's, Bob's and Eve's values respectively. Bob and Alice can establish a shared secret key through error correction and privacy amplification protocols if

$$I(A,B) \geq I(A,E) \quad \text{or} \quad I(A,B) \geq I(B,E)$$

where $I(A,B)$ is the mutual information about the key between Alice and Bob and as defined in (2.10), and $I(A,E)$ and $I(B,E)$ is the mutual information about the key between Alice and Eve or Bob and Eve respectively.

The theorem states an important criterion: Bob's and Alice's mutual information about the final key has to be higher than Eve's.

The next theorem by Hall [17] poses limitations in terms of mutual information:

Theorem 6. Let $I(A,B)$ and $I(A,E)$ denote the mutual information (about the state sent by Alice) between Alice and Bob and Alice and Eve respectively. $|\psi_B^i\rangle$ and $|\psi_E^j\rangle$ ($j \in 0, \ldots, n-1$) denote the eigenvectors of observables that correspond to measurement performed by Bob and Eve, respectively. Now the following inequality holds:

$$I(A,B) + I(A,E) \leq 2\log(nc) \tag{2.27}$$

where c is defined as

$$c = \max_{i,j \in \{0,\ldots,n-1\}} \left(\left| \langle \psi_B^i | \psi_E^j \rangle \right| \right)$$

The theorem puts an upper bound on the information that Bob and Eve are able to obtain from Alice's state. The increase in Bob's information necessarily limits the amount of information accessible for Eve.

Chapter 3

Quantum Cryptography

3.1 Classical cryptography

Quantum cryptography is currently the only known protocol with a provable security [9]. The security of currently used public key cryptographic protocol RSA [18] is considered to be secure on (unproved) conjectures that some computational operations are too difficult (i.e. take too much time) to be performed on classical computers (such security is called computational security). The construction of a quantum computer would enable cracking the RSA in small amount of time and make it completely useless. The current encryption standard for symmetric cipher AES (Advanced Encryption Standard) will be weakened (i.e. cracked more easily) by the possible invention of a quantum computer.

Fortunately, what quantum computers take away, quantum cryptography provides. Quantum cryptography presents a provably secure method of information transmission. The security of quantum cryptography depends on the *Vernam cipher*.

3.2 Vernam cipher

The Vernam cipher [19] (originally invented for usage in electrical telegraphs) provides an absolutely secret way of communication. Suppose Alice has a message M of letters from n-symbol alphabet and each symbol is assigned a number from 0 to $n-1$. For example 0 and 1 in the case of a binary message. Then she has a random key generating device that generates a random message K of the same length as message M. The encrypted message E is computed in the following way: If M_i denotes the i-th letter in message, then

$$\forall i \quad E_i = M_i + K_i \mod n.$$

The encrypted message E is received by Bob, who also possesses the key K (It has been delivered to him previously). The decryption can be done only with the key K available as:

$$\forall i \quad M_i = E_i - K_i \mod n.$$

We assume that

1. The key K is randomly generated
2. K is used only once
3. K has the same length as the encrypted message M

Then message M cannot be obtained without knowing the key K. This fact was first noticed and proved by Claude Shannon [20], who pointed out that the eavesdropper doesn't obtain any new information about the message M by knowing the encrypted message E (i.e. all messages that can be sent have their respective probabilities of being sent, then knowing E does not change the probabilities of which message could have been sent). Vernam cipher is sometimes referred to as *one-time pad* because of the fact that the key is used only once for the encryption.

Vernam cipher enables us to send any message if we are able to provide a way in which Alice and Bob can obtain the same random generated key of the same length as the message that Alice is sending without revealing the key to anybody else. This is exactly what are quantum cryptographic protocols doing: equipping Alice and Bob with the same randomly generated key K which is then used to encrypt a message. The message can be sent through a public channel, because nobody can decipher it without having the key. So, instead of *quantum cryptographic protocols*, the name *quantum key generating protocols* is more appropriate.

3.3 BB84 protocol

The first proposed (and experimentally realized) quantum cryptographic protocol is called BB84 after its inventors (Bennett and Brassard [21]).

We suppose that Alice and Bob are equipped with a quantum channel that can transmit quantum states (optical fiber transmitting single photons, for example). In the discussion we will first assume that all the communication equipment is perfect, i. e. no error occurs during the transmission due to detectors, optical fibers, etc.) The goal of this protocol is to equip Alice and Bob with a randomly generated binary key of length n. In case their communication is eavesdropped, they abort the communication. Therefore, the highest damage Eve can do is prevent them from communicating. They are also equipped with a public channel which reliably transforms all information, but information passing through it is accessible to everybody (insecure phone line, communication through internet etc.). Moreover, Alice has a random number generator that generates 0 or 1 with equal probability. We assume that Alice and Bob can trust their equipment, that means that Eve has no 'hidden' backdoor, cannot influence the function of random generator, nor detectors etc.

1. Alice generates two random numbers. If the first is 0, then she sends one of the states from the standard (computational) basis. Which one is sent depends on the second number (*bit*) that she generates. If it is 0, she sends $|0\rangle$, otherwise she sends $|1\rangle$. In case the first generated number was one, Alice will use the second basis composed of vectors $|+\rangle$ and $|-\rangle$. (defined in (1.2)). If the second number is 1, she sends $|+\rangle$, otherwise she sends $|-\rangle$. To summarize, upon generating two numbers, Alice sends

$$\begin{aligned} 00 &\longrightarrow |0\rangle \\ 01 &\longrightarrow |1\rangle \\ 11 &\longrightarrow |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \\ 10 &\longrightarrow |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \end{aligned}$$

   The first bit therefore serves to choose a basis, the second one is the part of the generated key.

2. Bob randomly chooses in which basis he will do his projective measurement. If he generates 0, then he measures in the standard basis. Otherwise he measures in the $\{|+\rangle, |-\rangle\}$ basis. With the probability $\frac{1}{2}$ Bob measures in the same basis in which Alice chose to encode her second bit and therefore gets the correct result. By measurement we suppose that if for example he decides to measure in the first basis, he makes a projective measurement with projector $P = |0\rangle\langle 0|$. If the photon (or whatever the sent quantum state is) passes through, he assumes that the state originally sent was $|0\rangle$). Note that if he chooses the wrong basis (for example the standard basis if the original state was $|+\rangle$), he receives the correct bit sent by Alice only with probability $\frac{1}{2}$. He stores the value he measured as a part of the generated key.

3. Alice and Bob repeat the send-receive procedure (steps 1 and 2) $4n$ times.

4. Alice publicly announces (i.e. communicates it to Bob via a public channel) which bits she used for choosing the encoding basis (that is the first bit from the pair generated in step 1). Bob responds (again through a public channel) in which cases he measured in the correct basis. This should be in approximately $2n$ cases for large n. They discard the bits of the key in which Bob used wrong basis to perform the measurement. In ideal case (no eavesdropping) Bob and Alice would share a key of length $2n$.

5. Alice chooses randomly n bits of the key and announces them publicly. Bob compares them with his own bits. They compute the so-called qubit error rate

$$\text{QBER} = \frac{t}{n} \tag{3.1}$$

that is the number of errors t over n. Based on the result, they either decide whether they abort the protocol or whether they proceed top the next step. The actual QBER below which the protocol should be interrupted will be discussed below.

6. Alice and Bob perform information reconciliation (see section 2.5) procedure and then privacy amplification (described in section 2.6). This leaves them with the final key.

We will first assume the (non-realistic) scenario of noiseless channel with perfect equipment, i.e. all the errors that occurred during the communication are attributed to an eavesdropper. The simplest attack that Eve could perform is called *intercept-resend* attack. The name of the attack is quite self-explanatory: Eve intercepts the communication and performs a measurement on the qubit sent by Alice. Of course she does not want Alice and Bob to know that their communication is eavesdropped and she therefore has to resend another qubit to Bob so that he would not become suspicious. Since Eve has no idea in which basis the qubit was sent, she has chance $\frac{1}{2}$ of picking the wrong basis. Recall that if she has the wrong basis, she has probability of $\frac{1}{2}$ of measuring the wrong qubit. Then she resends the qubit in the different basis than in the one in which Bob performs measurement. He therefore has the chance $\frac{1}{2}$ of detecting the different qubit than the one which Alice sent (and the same chance of detecting the right one). To summarize, the intercept-resend strategy has the probability $\frac{1}{2}\frac{1}{2} = \frac{1}{4}$ of introducing an error into to the communication. Therefore, approximately 25% of final key will have errors introduced by Eve. The randomly selected check bits should also include some errors and therefore Bob and Alice are able to tell whether their protocol is intercepted or not with a sufficiently high probability: they can increase the probability of detecting an error in their sample by making it larger than n bits. With perfect equipment, Bob and Alice know that their communication was intercepted in case they have QBER higher than 0%. However, even if protocol is intercepted, they still may be able to establish a secure key via privacy amplification protocol, if they fulfil the requirements of Theorem 5. In case Eve gains too much information (i.e. they are not able to perform privacy amplification), the protocol is aborted.

This is the basic idea behind the quantum cryptographic protocols. Of course, this model was simplified. In real life situations, there will always be some errors caused by the imperfections of detectors and errors that occur during the transmission of qubits. Therefore, information reconciliation step is necessary for Bob and Alice to introduce

some error correction. The following privacy amplification then reduces Eve's information to a level required by the needs of Alice and Bob. The decision whether they abort protocol or establish a private key via privacy amplification depends on the measured error rate QBER. We will see that this number depends on the type of attack that Eve uses: for example the simple intercept-resend strategy (which produces on average 25% disturbance) is not the most effective that Eve can employ. Therefore, the analysis of security and robustness of quantum protocols is more complicated. We will therefore analyze the security of BB84 protocol in greater detail in next sections. The maximum disturbance (i.e. the error rate QBER) up to which it is still possible to establish a secure key is called *robustness* of the protocol.

The outcome of random sampling test performed by Alice and Bob places a probability bound on the number of errors that remain in the n-bit set. It can be proven that [2]

Theorem 7. The probability p_e that for any given $1 > \delta > 0$ there is less then δn errors in check bits and more than $(\delta + \epsilon)n$ errors in the remaining bits is lower than $e^{-O(\epsilon^2 n)}$ for large n.

It is important to point out that from the scheme of the protocol, one can also see that if Eve gains power over the qubit channel as well as of the public channel, she can pretend to be Bob and establish communication with Alice. Then Eve pretends to Bob that she is Alice and establishes a secure key with him. She then accepts the message from Alice and resends it to Bob using their mutual key. To prevent this, Alice and Bob have to posses some pre-shared secret (a secret passphrase, for example) that then verifies their identity to make sure that they are indeed communicating with each other. Therefore, the most accurate name for quantum cryptographic protocols is not really quantum key generating protocols, but *quantum secret-growing protocol* [9].

3.4 Security analysis

3.4.1 Security criterion

We begin with a security criterion for quantum cryptographic protocols [2]:

Definition 13. The quantum key distribution protocol is *secure*, if for any chosen parameters $s > 0$ and $l > 0$ and for any eavesdropping strategy, the protocol either aborts or it succeeds with probability at least $1 - O(2^{-s})$ and guarantees that Eve's mutual information with the final key $I_E(K)$ is less that 2^{-l}. The key generated by the protocol is then used for the encryption by Vernam cipher, so it is also required for the final key to be random.

3.4.2 Eavesdropping attacks

We will give the categories of possible attacks and then analyze security against them. The possible Eve's attack are:

- **Individual attack**
  In this type of attack, Eve is able to manipulate only one qubit of the protocol at a time. The simplest subcategory of this type of attack is *intercept-resend attack*, which was already described in section 3.3. It requires Eve to measure in some basis that she chooses and then resending a new qubit. These were the first attacks taken into account at the beginning of quantum cryptography [22]. Nowadays, *cloning* attacks are considered as much better strategy for Eve to employ. The attack consists of applying a cloning machine onto the sent qubit. Eve attaches an ancilla to every passing qubit and waits until Bob performs his measurement. This gives her some information about his outcome. Closer examinations of this kind of attack will be given below.

- **Coherent attack**
  In this scenario, Eve is assumed to be able to manipulate several qubits at a time, allowing her therefore wider range of operations she may perform. A subclass called *collective attacks* allows Eve to manipulate a larger (but fixed) number of qubits at a time, assuming that the total number of sent qubits n is much larger. The most general type of coherent attacks are *joint attacks*, which pose no limitation at the total number of qubits manipulated at a time.

3.4.3 Security of BB84

The security of the BB84 protocol was proved for example in [12]. They claim that the protocol is secure (that means it fulfils the requirements of Definition 13) if Alice and Bob achieve the QBER lower than 11% We will use a different approach to show the robustness of BB84 protocol [9], but we will reach the same conclusion as [12].

We will exploit Theorems 6 and 5 in our analysis. As stated in Theorem 5, one can successfully obtain a secret key through error correction procedure and privacy amplification if the Eve's mutual information with Bob's or Alice's key is lower than Alice's and Bob's mutual information on the key.

Alice and Bob's mutual information

From now on, we will attribute all errors that occur during the transmission to Eve. Bob and Alice simply consider all errors as disturbances caused by Eve's attack on their protocol. We also suppose that the number n is large. We will now examine how much disturbance are the protocols able to withstand. We will now compute Alice's and Bob's mutual information $I(A, B)$. Using the formula (2.11), we first compute $H(A)$ (the entropy of the source, defined in (2.1)). Alice generates her bits randomly, both 0 and 1 with equal probability $\frac{1}{2}$. We therefore have

$$H(A) = -\left(\frac{1}{2}\log\frac{1}{2} + \frac{1}{2}\log\frac{1}{2}\right) = 1. \tag{3.2}$$

The disturbance $\mathcal{D}$ is a probability of an occurrence of error during the transmission (and it should correspond to measured quantum bit error rate QBER for large n). Note that if a qubit is corrupted with a probability $\mathcal{D}$, the expected number of errors should be around $\mathcal{D}n$ (again assuming large n). In our computation of mutual information, we consider only those qubits which were measured by Bob in the correct basis. If he uses the incorrect one, the bit is discarded and does not form part of the key. The conditional entropy is then

$$H(B|A) = \sum_{x \in \mathcal{X}} p(x) H(B|Y = x) = -2\frac{1}{2}\left((1-\mathcal{D})\log(1-\mathcal{D}) + \mathcal{D}\log\mathcal{D}\right). \tag{3.3}$$

Combining (3.2) and (3.3), we get

$$I(A,B) = H(A) - H(B|A) = 1 + \left((1-\mathcal{D})\log(1-\mathcal{D}) + \mathcal{D}\log\mathcal{D}\right). \tag{3.4}$$

for the case of one qubit. Because the key (before the information reconciliation and privacy amplification procedure) consists of approximately n bits, the mutual information is then

$$I^n(A,B) = n(1 + ((1-\mathcal{D})\log(1-\mathcal{D}) + \mathcal{D}\log\mathcal{D})) \tag{3.5}$$

Next, it is necessary to compute $I(A,E)$, the amount of mutual information between Alice and Eve. This number of course depends on the type of attack that Eve uses. We want to have an unconditional proof of security, that is a proof against all types of operations that Eve could possibly use. Because of the symmetry of the BB84, it can be shown [23] that the threshold for the sum of mutual informations in Theorem 6 is

$$I(A,B) + I(A,E) \leq 2n \log\left(2\frac{1}{\sqrt{2}}\right). \tag{3.6}$$

Together with the requirement of Theorem 5 that $I(A,B) > I(A,E)$, we can arrive to the final bound by inserting the (3.4) and (3.5) into the above equation and solving the equation numerically one gets the bound 11%. Therefore, if the disturbance is lower than 11%, one can establish the private key as stated by Theorem 5. The Theorem 7 is used to place a probabilistic bound on the unchecked qubits in terms of maximal number of remaining errors, then the error correcting procedure and privacy amplifiaction establish a key that is secure by the means of security requirement with Eve's information made as small as required.

The maximal tolerated disturbance was derived for an attack that attacks fixed number of bits at a time. However, the bound obtained through this approach is equal to the bound obtained by different approaches which place no limitation on the type of the attack nor the number of qubits manipulated at a time [12] [23].

The specific analysis of the robustness of the quantum protocols against quantum-cloning and intercept-resend attacks will be further analyzed in connection with general-

ization of quantum key distribution protocol BB84 to d-dimensional Hilbert spaces. The results for BB84 will then be a special case for $d = 2$.

3.5 Mutually unbiased bases in BB84 protocol

Note that the bases used in BB84 are mutually unbiased, that is, the inner product of any two vectors $|u\rangle$ and $|v\rangle$ from different bases is

$$|\langle u|v\rangle| = \frac{1}{\sqrt{d}}$$

where d is the dimension of Hilbert space, 2 in the case of BB84.

Note that the use of mutually unbiased basis ensures that if Eve uses different basis than Alice, her two outcomes will have equal probability $\frac{1}{2}$. The definition together with important theorems about mutually unbiased bases is given in appendix A.

3.6 EPR-based protocol

The EPR protocol was first introduced by A. Ekert [24]. The EPR-based protocols are based on the exchange of the Bell states. They generally proceed in the following way:

1. Alice prepares an entangled state

$$|\psi_+\rangle = \frac{|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B}{\sqrt{2}}. \tag{3.7}$$

   She keeps the qubit in space $\mathcal{H}_A$ and sends the second one to Bob (whose Hilbert space is $\mathcal{H}_B$). Alternatively, the entangled state can be prepared by a third party and the respective qubits can be sent to Bob and Alice. Alice and Bob receive $2n$ states this way.

2. Alice and Bob select half (that is n) of their qubits and perform a measurement. They both publicly announce their outcome. They count the number of errors. If more than t errors occur, they abort the protocol (where t is predetermined parameter).

3. Alice and Bob would now ideally be left with n entangled states $|\psi_+\rangle^{\otimes n}$. However, their communication could have suffered several errors from eavesdropping, imperfect equipment or noisy channel. They measure the remaining n bits in a t-errors quantum correcting code $[n, k]$, which leaves them with final entangled state $|\psi_+\rangle^{\otimes k}$ for some $k < n$.

4. Alice then performs a measurement on the remaining qubits and from the output of her measurement ($|0\rangle$ or $|1\rangle$, both outcomes have probability $\frac{1}{2}$). Alice knows

immediately what will be the outcome of Bob's measurement, because the qubit was entangled. The outcome of Alice's and Bob's measurement are random and correlated and therefore this procedure generates a random key as required for the one-time pad encryption. Note that in this case the randomness of the key follows from the equal probability of measuring either 0 or 1.

Alternatively, Bob and Alice could have performed the measurement and then employ the classical error correction and privacy amplification procedures. The security of the protocol is proved for the robustness (the number of errors occurring) equal to 11% [12]. The above protocol can be modified in order to correspond to the BB84 scheme, and therefore the proof of the security of above scheme also implies security of BB84.

Chapter 4

Quantum cryptography in d-dimensional Hilbert spaces

Since quantum information and computation theory was studied with relation and comparison to classical information theory, it was natural to consider qubits in two dimensional Hilbert spaces. The use of higher dimensional Hilbert spaces in quantum information theory came to interest only recently, when several schemes for quantum key distribution have been proposed [25] [26] [27]. We will describe the generalization of BB84 protocol to d-dimensional Hilbert spaces and its robustness against intercept-resends and cloning machine attacks [28] [29]. Note that all the results are valid for $d = 2$ as well, so BB84 is just a special case of the presented protocols.

4.1 Generalization of BB84 to higher dimensions

The generalization of BB84 to d dimensional Hilbert space is quite straightforward. We consider two possible generalizations:

- 2-*bases protocol*
  In the case of the 2-bases protocol, it proceeds exactly the same way as BB84: In step one, Alice randomly chooses between two mutually unbiased bases (it is a consequence of Theorem 9 in Appendix A that one can always find at least three mutually unbiased bases in arbitrary dimension higher than one). Then she randomly generates a number from 0 to $d-1$ and encodes it as a state $|\psi_j^k\rangle$, where k denotes the used basis (either 1 or 2) and j denotes the randomly genrated symbol from 0 to $d-1$ to which the state corresponds.

- $d+1$ *bases protocol*
  In this version of protocol, Alice first randomly chooses between $d+1$ mutually unbiased bases and then encodes a randomly generated symbol as one of the d states in the given basis. Note that in this version of protocol, Bob has a probability of

choosing the correct basis $\frac{1}{d+1}$, so therefore higher number of dits has to be dropped because of use of wrong basis. The two-dimensional version of this protocol with three mutually unbiased basis (typically the bases of eigenvectors of Pauli matrices) is called *six-state protocol*. Unlike the 2 bases protocol, it is not proved whether it is possible to find $d + 1$ mutually unbiased bases for arbitrary dimension d. Such construction is known only if d equals prime or a power of prime (see appendix A).

The steps of privacy amplification and error correction proceed in similar way as in the case of BB84 but they have to be modified in a way that instead of symbols 0 and 1, they work on symbols $0, 1, \ldots, d-1$.

Next, we will describe how is the is robustness of these protocols computed and compare the advantages of using higher dimensions and the differences between 2 and $d + 1$ versions of the protocol.

4.2 Security analysis

Following the Theorem 5, we can now consider the robustness of 2-state and $d + 1$-state protocols. First, we need to compute the Alice's and Bob's mutual information $I_d(A, B)$ where d denotes the dimension of used Hilbert space. $I_d(A, B)$ is derived in a similar way as for the two-dimensional case. First, we compute the entropy of the source, i.e. of the states randomly generated and sent by Alice

$$H(A) = -\sum_{i=0}^{d-1} \frac{1}{d} \log \frac{1}{d} = \log d. \tag{4.1}$$

Next, we compute the conditional entropy of Bob. Note that the probability of error is denoted $\mathcal{D}$. We consider only the cases in which Bob and Alice choose the same basis. If no error occurs (with probability $1 - \mathcal{D}$), then Bob detects correctly the state. In the other case, we assume that all other possible outcomes are equiprobable, as well as it is assumed that the final outcomes of his measurement are equally distributed among all the possible d outcomes. The conditional entropy of Bob's key in relation to the value sent by Alice is

$$H(A|B) = -(1-\mathcal{D}) \log(1-\mathcal{D}) - \frac{\mathcal{D}}{d-1} \log \frac{\mathcal{D}}{d-1} \tag{4.2}$$

where the $\mathcal{D}$ stands for the probability of error. The previous equation is then obtained by using (2.8). Then we get the mutual information as [28]

$$I_d(A, B) = H(A) - H(A|B) = \log d + (1-\mathcal{D}) \log(1-\mathcal{D}) + \mathcal{D} \log \frac{\mathcal{D}}{d-1}. \tag{4.3}$$

In the next section, we will consider the intercept-resend attack in a d-dimensional Hilbert space.

4.2.1 Intercept-resend attack

As was described before, Eve's strategy in intercept-resend attack is to guess randomly which base Alice uses and then resend her result to Bob. Therefore, if we assume that m is the total number of bases (we consider 2 or $d+1$), Eve introduces a disturbance:

$$\mathcal{D}_m^d = \left(1 - \frac{1}{m}\right)\left(1 - \frac{1}{d}\right) \tag{4.4}$$

where d is the dimension of the Hilbert space. Note that the above equation follows from the fact that an error is introduced if Eve guesses incorrectly Alice's basis (which happens with probability $1-\frac{1}{m}$) and when Bob measures the incorrect value as a result of receiving a state resent by Eve in a wrong basis (probability of which is $1-\frac{1}{d}$, because the two bases are mutually unbiased and therefore all d outcomes are equiprobable)

Eve's mutual information on the key sent by Alice is

$$I_m^d(A,E) = \frac{\log(d)}{m}. \tag{4.5}$$

The above equation is obtained in the following way: using again the formulas (2.11) and (2.8) to compute mutual information, we note that Eve can obtain one of dm possible results (depending on which basis she uses and what is the outcome). So, in the summation in (2.8) y goes over all possible dm states, whereas x in (2.9) goes over all possible d values that could have been sent by Alice with a given conditional probability $p(x|y)$. The use of mutually unbiased bases makes the computation quite easy: one of the bases over which the summation is done is identical to Alice's, then one of the conditional probabilities will be equal to 1 (because if Eve chose the same basis, she obtains the correct state out of d total states in the basis), other states from the basis will have conditional probability 0. In case of the remaining $m-1$ bases, the conditional probability is always equal to $\frac{1}{d}$ because of the fact that all Eve's possible outcomes are equiprobable (which follows from mutual unbiasedness of used bases).

If the quantity $I(A,B) - I(A,E) \geq 0$ (with $\mathcal{D}$ substituted from (4.4)), then Bob and Alice can establish a secret key (according to Theorem 5). This quantity for the cases when $m = 2$ and $m = d+1$ in various dimensions d is plotted in figure 4.1. The values for the case that uses the maximal number of mutually unbiased bases is plotted only for d equal to prime or power of a prime. The quantity $I(A,B) - I(A,E)$ i always higher than zero for the case when $m = d+1$ while for the two-bases version of the protocol, it is greater than zero for dimensions greater or equal to twelve.

4.2.2 Universal cloning machine attack

The most effective individual attack that for $d = 2$ is universal quantum cloning machine (UQCM) attack [28]. This fact is not proved yet for higher dimesions, but so far it is the

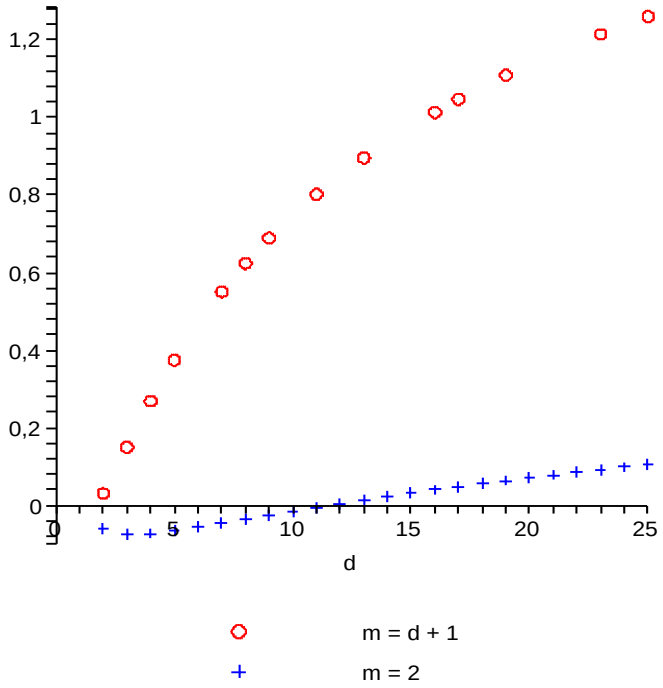

Figure 4.1: I(A,B) - I(A,E) for a given dimension d in the case of intercept-resend attack

best individual attack known. For the UQCM attack, Eve uses a cloning machine on state that is transmitted. We begin with a description of universal quantum cloning machnine.

Universal quantum cloning machine

Here we present a brief description of universal quantum cloning machines [30] for arbitrary dimension d of Hilbert space. Universal quantum cloning machine produces three outputs, one of them is sent to Bob, the two remaining (with subscripts E and M) are kept by Eve. In case the two output states kept by Eve are identical, the cloning machine is symmetric, otherwise it is asymmetric. The action of a universal quantum cloning machine on a quantum state $|\psi\rangle_A$ in d-dimensional Hilbert space is

$$|\psi\rangle \longrightarrow \sum_{m,n=0}^{d-1} a_{m,n} U_{m,n} |\psi\rangle \otimes |\Psi_{m,d-n}\rangle_{EM} \tag{4.6}$$

where $a_{m,n}$ are coefficients satisfying

$$\sum_{m,n=0}^{d-1} |a_{m,n}|^2 = 1 \tag{4.7}$$

and $U_{m,n}$ are operators acting on the state $|\psi\rangle$ as

$$U_{m,n}|\psi\rangle = \sum_{k=0}^{d-1} e^{2\pi i\left(\frac{kn}{d}\right)}|k+m\rangle\langle k|\psi\rangle \tag{4.8}$$

where the addition $k+m$ is taken modulo d.
$|\Psi_{m,d-n}\rangle$ are entangled qudits, generalizations of Bell states to higher dimensions:

$$|\Psi_{m,d-n}\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{2\pi i\left(\frac{kn}{d}\right)}|k\rangle_E \otimes |k+m\rangle_M \tag{4.9}$$

where the addition $k+m$ is again understood modulo d. Note that the output of UQCM is a state in Hilbert space $\mathcal{H}\otimes\mathcal{H}_E\otimes\mathcal{H}_M$ which is a tensor product of three d-dimensional Hilbert spaces. The first subspace corresponds to the state that is sent to Bob, the other two subspaces (states in these subspaces were denoted with subscripts E and M) correspond to the states that are kept by Eve.
By performing a partial trace over the systems $\mathcal{H}_E$ and $\mathcal{H}_M$, we find out that a mixed state that is received by Bob is equal to

$$\rho_B = \sum_{m,n=0}^{d-1} |a_{m,n}|^2 \, |\phi_{m,n}\rangle\langle\phi_{m,n}| \tag{4.10}$$

where

$$|\phi_{m,n}\rangle = U_{m,n}|\psi\rangle$$

The coefficients $a_{m,n}$ can be expressed as elements of a $d\times d$ matrix a:

$$a = \begin{pmatrix} v & x & \cdots & x \\ x & y & \cdots & y \\ \vdots & \vdots & \ddots & \vdots \\ x & y & \cdots & y \end{pmatrix} \tag{4.11}$$

where x, y and v are real parameters. In order to satisfy the condition (4.7), these parameters must fulfil the equation

$$v^2 + 2(d-1)x^2 + (d-1)^2y^2 = 1 \tag{4.12}$$

Two basis scheme

First we consider a case when two basis are used. One basis will be the standard basis

$$\mathcal{B} = \{|k\rangle \quad | \quad k = 0, 1, \ldots, d-1\} \tag{4.13}$$

and the second basis will be constructed as its dual under discrete Fourier transform (i.e. by a multiplication of vectors of standard basis by the Sylvester matrix as presented in (A.7)):

$$|\tilde{l}\rangle = S|l\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{\frac{2\pi i}{d} kl} |k\rangle. \tag{4.14}$$

The complementary dual basis is then

$$\mathcal{F} = \left\{ |\tilde{l}\rangle \quad | \quad l = 0, 1, \ldots, d-1 \right\} \tag{4.15}$$

It is clear that these two basis are mutually unbiased.

In this version of the protocol, Eve chooses between one of the two bases to encode the part of the key that she sends. We now suppose she chooses the standard basis $\mathcal{B}$ and sends a state $|k\rangle$. We first note that the state $|\phi_{m,n}\rangle$ in the equation (4.10) is

$$|\phi_{m,n}\rangle = U_{m,n}|k\rangle = e^{\frac{2\pi i}{d} kn} |k+m\rangle \tag{4.16}$$

and therefore we obtain that fidelity of the sent state and state ρ_B received by Bob is then according to equation (2.22) equal to

$$F_{\mathcal{B}} = \langle k|\rho_b|k\rangle = \sum_{n=0}^{d-1} |a_{0,n}|^2 \tag{4.17}$$

For the second case, when Eve chooses a state $|\tilde{l}\rangle$ from the dual basis $\mathcal{F}$, the fidelity $F_{\mathcal{F}}$ of ρ_B is then computed similarly as in the previous case and one obtains

$$F_{\mathcal{F}} = \langle \tilde{l}|\rho_b|\tilde{l}\rangle = \sum_{m=0}^{d-1} |a_{m,0}|^2 \tag{4.18}$$

Because coefficients $a_{m,n}$ are symmetric in m,n, we get that in terms of parameters x and v

$$F_B = F_{\mathcal{F}} = F_{\mathcal{B}} = v^2 + (d-1)x^2. \tag{4.19}$$

Note that the fidelity F_B is equal to Bob's probability of detecting the state that was originally sent by Alice, because the formula for computation of fidelity is equal to the formula for computing the transition probability (1.4) between the state and the density matrix. Therefore F_B is the probability of detecting the correct state, then $1 - F_B$ is equal to disturbance $\mathcal{D}$, because it will correspond to the probability of errors that occur during the transmission as a result of the cloning machine attack. Then, substituting $\mathcal{D}$ by $1 - F_B$

in equation (4.3), one gets

$$I_d(A,B) = \log d + F_B \log(F_B) + (1-F_B)\log\frac{(1-F_B)}{d-1}. \tag{4.20}$$

Eve's strategy is to wait with her measurement until the bases that were used for encoding are announced by Alice and the incorrect basis are discarded. It can be shown [28] that in this scheme, Eve's fidelity is equal to

$$F_E = \frac{F_B}{d} + \frac{(d-1)(1-F_B)}{d} + \frac{2}{d}\sqrt{(d-1)F_B(1-F_B)} \tag{4.21}$$

where F_B is Bob's fidelity (4.19). Eve attains the maximal information on Alice's state if the parameters of the cloning machine are set as [28]:

$$x = \sqrt{\frac{F_B(1-F_B)}{d-1}}, \quad y = \frac{1-F_B}{d-1}, \quad v = F_B. \tag{4.22}$$

Eve then performs her measurement in the basis that Eve used. Eve's fidelity F_E is therefore a function of Bob's fidelity F_B which depends on the parameters of the cloner. Eve's information is given by the same expression as Bob's (4.20). Eve's mutual information with Alice is then given by the same expression as Bob's (4.20), only with the exception that F_B is replaced by Eve's fidelity F_E

$$I_d(A,E) = \log d + F_E \log(F_E) + (1-F_E)\log\frac{(1-F_E)}{d-1}. \tag{4.23}$$

If Eve measures different state than the one originally sent by Alice, she gets one of the $d-1$ remaining ones, each with equal probability $\frac{1-F_E}{d-1}$. Therefore, the limiting point for the possibility of extraction of a secret key is when the $I_d(A,E) = I_d(A,B)$, that is when Eve's information equals to Bob's which implies that their fidelities are equal as well:

$$F_B = F_E = \frac{1}{2}\left(1 + \frac{1}{\sqrt{d}}\right). \tag{4.24}$$

Therefore, the maximal tolerable disturbance of the two-basis scheme against cloning machine attack is

$$\mathcal{D}_2^{\text{clone}}(d) = 1 - F_B = \frac{1}{2} - \frac{1}{2\sqrt{d}}. \tag{4.25}$$

where the subscript and superscript denote the fact that it is a disturbance for 2 basis protocol in case of quantum cloning machine.

d+1 basis scheme

In the $d+1$ basis scheme, the universal asymmetric cloner's coefficients $a_{m,n}$ are given by

$$a_{m,n} = \alpha\delta_{m,0}\delta_{n,0} + \frac{\beta}{d} \tag{4.26}$$

that is, taking the matrix (4.11), it means that $x = y = \frac{\beta}{d}$ and $v = \frac{\beta}{d} + \alpha$ and the normalization relation reduced to

$$\alpha^2 + \frac{2\alpha\beta}{\sqrt{d}} + \beta^2 = 1 \tag{4.27}$$

and the transformed state $|k\rangle$ sent by Alice is transformed by the cloning machine as [30] [28]

$$|k\rangle \longrightarrow |k\rangle_B \left(\frac{\alpha}{\sqrt{d}} \sum_{l=0}^{d-1} |l\rangle_E |l\rangle_M + \frac{\beta}{d} |k\rangle_E |k+m\rangle_M \right) + \sum_{m=1}^{d-1} |k+m\rangle \left(\frac{\beta}{\sqrt{d}} |k\rangle_E |k+m\rangle_M \right). \tag{4.28}$$

The properties of the transformation are given by parameters α and β. The Bob's fidelity (4.19) is now

$$F_B^{d+1} = 1 - \frac{d-1}{d}\beta^2. \tag{4.29}$$

Eve's strategy is to wait until Alice and Bob announce publicly the used basis and then she performs measurement of her states in the correct basis. If her two outcomes disagree, the outcome state of the cloner must have been the second term in equation (4.28). and therefore Eve learns Bob's error m (as a difference of her tow measured values) and also the correct value of k. This happens with probability $1 - F_B^{d+1}$. Therefore, the probability of Eve getting two equal outcomes is equal to F_B^{d+1} in which case she has probability $\frac{(\alpha+\beta)^2}{d}$ of measuring the same state as the one that goes to Bob (she gets the same value of k). The remaining probability of measuring of one of the incorrect possible $d-1$ values is then $\frac{d-1}{d}\alpha^2$, which means that Eve's fidelity (equal to probability of measuring correctly the output state) is then

$$F_E^{d+1} = 1 - \frac{d-1}{d}\alpha^2. \tag{4.30}$$

The Alice's and Bob's mutual information is given by (4.20), with Bob's fidelity F_B^{d+1} given by (4.29). Mutual information of Alice and Eve depends on the measurement outcome of Alice's measurement. In the case that she measures Bob's error m different than zero, she now exactly the value of k sent by Alice. The mutual information is then

$$I(A, E|m \neq 0) = \log d. \tag{4.31}$$

In the second case, the mutual information is given by

$$I(A,E|m=0) = \log d + \frac{(\alpha+\beta)^2}{dF_B^{d+1}} \log\left(\frac{(\alpha+\beta)^2}{dF_B^{d+1}}\right) + (d-1)\frac{\alpha^2}{d}\log\left(\frac{\alpha^2}{d}\right). \quad (4.32)$$

The average mutual information is then

$$I(A,E) = F_B^{d+1} I(A,E|m=0) + (1-F_B^{d+1}) I(A,E|m\neq 0) \quad (4.33)$$

which can be expressed with the help of Eve's fidelity (4.30) and (4.27) as

$$I(A,E) = \log d + (F_B^{d+1}+F_E^{d+1}-1)\log\left(\frac{F_B^{d+1}+F_E^{d+1}-1}{F_B^{d+1}}\right) + (1-F_E^{d+1})\log\left(\frac{1-F_E^{d+1}}{d-1}\right). \quad (4.34)$$

Now, according to Theorem 5, we have to solve the equation

$$I(A,B) - I(A,E) = 0. \quad (4.35)$$

In order to obtain the threshold disturbance against the cloning machine attack

$$\mathcal{D}_{d+1}^{\text{clone}} = 1 - F_B^{d+1},$$

we substitute from equations (4.29) (4.30) (4.27). Numerical solutions for d from 2 to 25 are plotted in figure 4.2. The circled points in the figure correspond to the dimensions equal to primes or powers of primes[1]. The comparison with 2-bases protocol for dimension d ranging from 2 to 50 is plotted in figure 4.3, where only values for dimension of prime or power of a prime are plotted for the case of $d+1$ basis protocol. One can see that the threshold disturbance against the cloning machine attacks as described in this and previous section is higher for $d+1$ bases protocol, but for d greater than 16, 2-bases protocol becomes more advantageous, i.e. more robust against the cloning machine attack.

[1]Only for d equal to primes or their powers, we know the construction of $d+1$ mutually unbiased bases

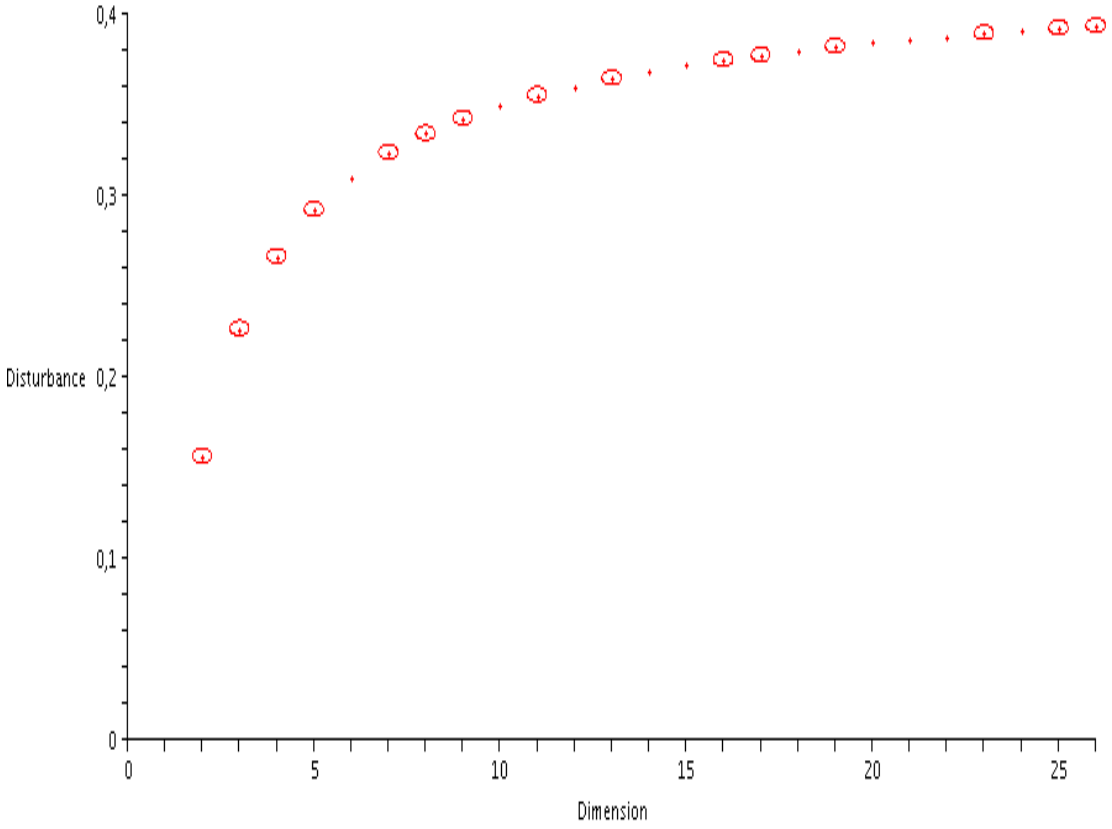

Figure 4.2: Threshold disturbance for a given dimension d against cloning attack in $d+1$ bases protocol

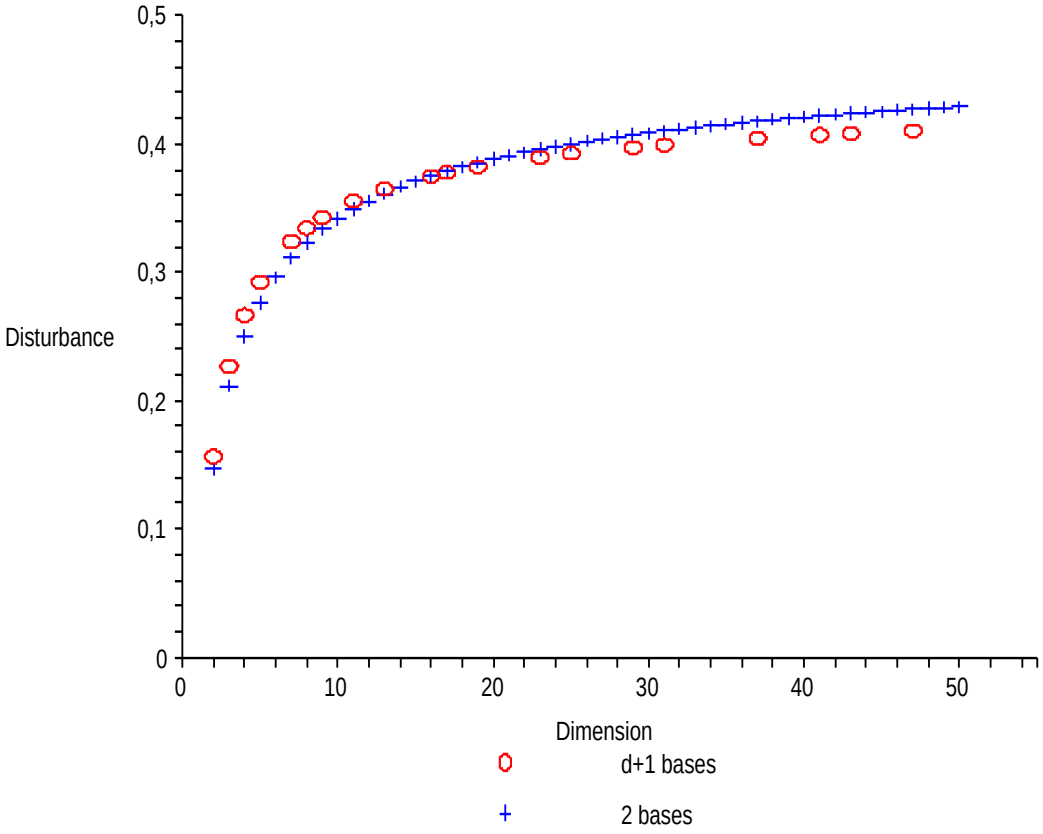

Figure 4.3: Disturbance in 2 and $d+1$ bases protocols in quantum cloning machine attack

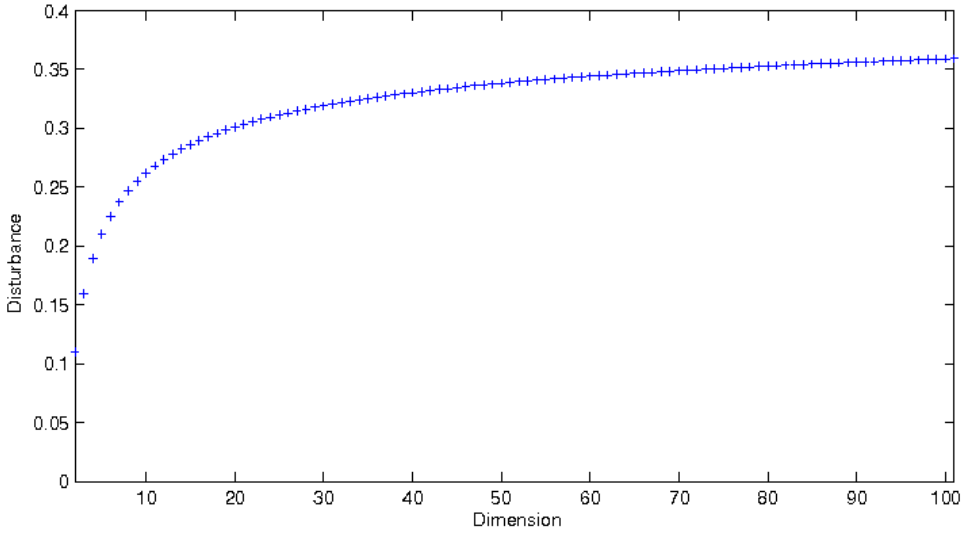

Figure 4.4: Threshold disturbance for a given dimension

4.2.3 Finite coherent attacks

Generalizing the steps from section 3.4.3 to d-dimensional protocols, according to Theorem 6

$$I(A,B) + I(A,E) \leq \log d. \tag{4.36}$$

Following the condition given by Theorem 5, we have the condition

$$I(A,B) > \frac{1}{2}\log d \tag{4.37}$$

which yields, after substituting from (4.20) for $I(A,B)$,

$$F_B \log\left(\frac{1}{F_B}\right) + (1-F_B)\log\left(\frac{d-1}{1-F_B}\right) < \frac{1}{2}\log d. \tag{4.38}$$

Solving this equation for a fixed d, one can obtain the maximal tolerated disturbance $\mathcal{D} = 1 - F_B$ for such a protocol. The results computed numerically for d from 2 to 100 are plotted in figure 4.4. As d increases, so does the disturbance $\mathcal{D}$, with the limit

$$\lim_{d\to\infty} \mathcal{D}^{\text{coh}} = \frac{1}{2}. \tag{4.39}$$

4.2.4 Comparison of the $d+1$-bases protocol and 2-bases protocol

As was stated in previous section, the 2 bases protocol is less advantageous for dimensions lower than 19. Therefore, for example the variation of BB84 protocol in two-dimensional

Hilbert space that uses three bases (so called six-state protocol) is more robust against cloning machine attack than the original BB84 protocol. Another characteristic of the protocol is its rate, that is the number of use of the communication channel per a bit (or dit) of the final key. The rate is obviously inversely proportional to the number of bases that the protocol is using (because if the protocol uses more bases, Bob has a smaller chance of selecting the correct one). From this point of view, the 2-bases protocols are certainly more advantageous.

Values from figures 4.4 and 4.3 are shown in the following table (for selected dimensions):

d	$\mathcal{D}_2^{\text{clone}}$ (%)	$\mathcal{D}_{d+1}^{\text{clone}}$ (%)	$\mathcal{D}^{\text{coh}}$ (%)
2	14.64	15.64	11.00
3	21.13	22.67	15.95
5	25.00	29.23	20.99
8	32.32	33.44	24.70
13	36.13	36.48	27.82
16	37.50	37.50	28.97
17	37.87	37.77	29.28
19	38.53	38.23	29.85
23	39.57	38.96	30.75
25	40.00	39.25	31.13

It is not known whether the quantum cloning machine attack is the most powerful individual attack that Eve might use in higher dimensions than two. But in terms of the cloning attack as described in previous sections, The $d+1$-basis scheme presents little advantage and is certainly more difficult to realize technically. Therefore, from the point of view of the cloning machine attacks, the existence of the maximal number of mutually unbiased bases in all dimensions would not bring a significant enhancement in the terms of the security of quantum cryptographic protocols based on BB84 scheme.

Nevertheless, the question of the maximal number of mutually unbiased bases in composite dimensions still remains an open and interesting question.

4.3 Concluding remarks

The area of quantum information theory and quantum cryptography is already large enough for a book, so this work presented a selection of topics and quantum cryptographic protocols and eavesdropping attacks, especially concentrating on BB84 protocol and its generalization to higher dimensions and utilisation of a maximal set of mutually unbiased bases in those dimensions. Following the approach of [29] [28], we investigated the robustness of $d+1$ and 2 bases protocols against universal cloning machine attacks.

Appendix A

Mutually unbiased bases

In this appendix, we briefly describe mutual unbiased bases and mention their known properties and also refer to unsolved problems about their existence and construction. The proofs of the presented theorems are provided in [31], [32] or in articles cited there.

Let us start with the definition of mutually unbiased bases:

Definition 14 (Mutually unbiased bases)**.** Two orthonormal bases

$$\{|u_i\rangle | i = 1, 2, \ldots, N\} \quad \text{and} \quad \{|v_j\rangle | j = 1, 2, \ldots, N\}$$

in an N-dimensional complex Hilbert space are *mutually unbiased* if inner products between all possible pairs of vectors with one vector from each basis have the same magnitude $\frac{1}{\sqrt{N}}$:

$$|\langle u_i|v_j\rangle| = \frac{1}{\sqrt{N}} \; \forall i, j \in \{1, 2, \ldots, N\} \tag{A.1}$$

Definition 15 (Set of mutually unbiased bases)**.** A set of d bases is called mutually unbiased if every two different bases from the set are mutually unbiased with respect to each other.

One of interesting properties of these bases is that a measurement over one basis provides maximum uncertainty as to the outcome of a measurement in a basis that is unbiased with respect to the first one (because all N possible outcomes will have equal probabilities $\frac{1}{N}$). This property was first noted by Schwinger [33]. The first attempt to use these bases in a state determination was made by Ivanović[34], who also provided an explicit construction of $N+1$ mutually unbiased bases for odd prime number dimensional Hilbert spaces. The idea of using mutually unbiased bases for quantum system state determination was further developed by Wootters [35] and Wootters and Fields ([36]). In [36], they presented a construction of $N + 1$ mutually unbiased bases in an arbitrary prime power $p^a = N$-dimensional Hilbert space and also demonstrated that they form a complete set of measurements for state determination which is optimal [36].

A.1 Minimal and maximal number of mutually unbiased bases

We shall first prove two theorems (that are given in [36] and [37]) that limit the maximal and minimal possible number of mutually unbiased bases that can exist in a given N-dimensional Hilbert space.

Theorem 8. In an N-dimensional Hilbert space, there cannot be more than $N+1$ mutually unbiased bases.

To formulate next theorem, we shall use the fact given in section A.3 that it is possible to find a set of $N+1$ mutually unbiased bases in a Hilbert space of dimension equal to an arbitrary power of a prime number. We will now assume that we are able to find such a set for arbitrary power of a prime p. Then we can easily prove the following theorem:

Theorem 9. Let $\mathcal{H}$ be an N- dimensional Hilbert space $\mathcal{H}$, where

$$N = p_1^{m_1} p_2^{m_2} \dots p_r^{m_r}$$

is a factorization of N into distinct primes p_i. Then the minimal number of mutually unbiased bases in $\mathcal{H}$ is

$$\min\left\{p_1^{m_1}+1, p_2^{m_2}+1, \dots, p_r^{m_r}+1\right\}.$$

A.2 Construction of mutually unbiased bases for prime dimensions

It can be easily verified that the set of eigenvectors of Pauli matrices form a set of mutually unbiased bases:

$$\begin{gathered} \{|0\rangle, |1\rangle\} \\ \left\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\} \\ \left\{\frac{|0\rangle+i|1\rangle}{\sqrt{2}}, \frac{|0\rangle-i|1\rangle}{\sqrt{2}}\right\} \end{gathered}$$

Therefore, they form a maximal set of 3 mutually unbiased bases in a two-dimensional Hilbert space. The construction of such a set of bases in higher dimensions can be understood as a generalization of this property. The set of mutually unbiased bases for any odd prime dimension p was first discovered by Ivanović [34]. For a p-dimensional Hilbert

space he gave the set of $p+1$ mutually unbiased bases:

$$\begin{aligned}
|\psi\rangle_j^{(0,k)} &= \delta_{jk}, \\
|\psi\rangle_j^{(1,k)} &= \frac{1}{\sqrt{p}} e^{\frac{2\pi i}{p}(j+k-1)^2}, \\
&\vdots \\
|\psi\rangle_j^{(n,k)} &= \frac{1}{\sqrt{p}} e^{\frac{2\pi i}{p} n(j+k-1)^2}, \\
&\vdots \\
|\psi\rangle_j^{(p-1,k)} &= \frac{1}{\sqrt{p}} e^{\frac{2\pi i}{p}(p-1)(j+k-1)^2}, \\
|\psi\rangle_j^{(p,k)} &= \frac{1}{\sqrt{p}} e^{\frac{2\pi i}{p}(jk)},
\end{aligned}$$

where $|\psi\rangle_j^{(n,k)}$ denotes the j-th component of the k-th vector in n-th basis. The first basis is the standard (or canonical) basis. Every basis from the set is orthonormal. The mutual unbiasedness follows from the Gauss sums of number theory [38]:

$$\left| \sum_{i=1}^{p} e^{\frac{2\pi}{p}(ai^2+bi)} \right| = \frac{1}{\sqrt{p}} \qquad a, b \in \mathbb{N}, a \neq 0, a \neq \pm kp, \quad k \in \mathbb{N}, p \text{ odd prime.} \tag{A.2}$$

Namely, the magnitude of the inner product of two vectors $|\psi\rangle^{(n,k)}$ and $|\psi\rangle^{(m,l)}$ taken from m-th and n-th basis, respectively, ($m \neq n,\ \ m, n \neq 0$) is of the form (A.2). The case when one of the vectors is taken from the standard basis is trivial.

We shall now have a look at one possible approach (presented in [39] and independently derived with a group theoretical approach in [31]) to derive the $N+1$ mutually unbiased bases for any prime dimension N. This approach uses unitary operators P_N, Q_N which are defined for a finite N-dimensional Hilbert space, with an orthonormal basis $B = \{|0\rangle, |1\rangle, \ldots |N-1\rangle\}$, by the relations

$$Q_N|j\rangle = \omega_N^j |j\rangle, \tag{A.3}$$

$$P_N|j\rangle = |j+1 \mod N\rangle. \tag{A.4}$$

Here ω_N is the primitive N-th root of unity $e^{\frac{2\pi i}{N}}$. The unitary operators P_N and Q_N are represented by unitary matrices:

$$Q_N = \text{diag}\left(1, \omega_N, \omega_N^2, \cdots, \omega_N^{N-1}\right) \tag{A.5}$$

and

$$P_N = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & & & \ddots & & \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \tag{A.6}$$

In finite dimensional quantum mechanics, the unitary matrices P_N and Q_N play the roles of exponential operators of position and momentum in the coordinate representation [40]. The analogue of the Fourier transformation for these operators, which allows us the transition from the coordinate representation (corresponding to the above matrix forms) to the momentum representation, is given by the unitary Sylvester matrix S:

$$S_{jk} = \frac{\omega_N^{jk}}{\sqrt{N}}. \tag{A.7}$$

The following relations are then fulfilled:

$$S^{-1} P_N S = Q_N^{-1} = Q_N^{N-1} = Q_N^{\dagger}, \quad S^{-1} Q_N S = P_N \tag{A.8}$$

Therefore, one can see that the bases composed of eigenvectors of Q_N and P_N respectively will be mutually unbiased, because where $|j\rangle$ (a j-th vector from standard basis) is an eigenvector of Q_N (and of $Q_N^{\dagger}$ as well) and therefore $S|j\rangle$ will be an eigenvector of P_N. Now, using the definition (A.7) of S, it can be seen that

$$|\langle j|S|k\rangle| = \left| \sum_i^N \left\langle \frac{1}{\sqrt{N}} \omega^{ij} |i\rangle \middle| |k\rangle \right\rangle \right| = \frac{1}{\sqrt{N}}$$

We will now state an important theorem:

Theorem 10 ([39] [31])**.** The bases composed of eigenvectors of operators

$$\left\{ Q_N, P_N, P_N Q_N, P_N Q_N^2, \ldots, P_N Q_N^{N-1} \right\} \tag{A.9}$$

are mutually unbiased with respect to each other and form therefore a maximal set of $N+1$ mutually unbiased bases.

A.3 Mutually unbiased bases for powers of primes

The first construction of mutually unbiased bases for dimension $N = p^a$, p prime, was presented by Wootters and Fields [36]. We will present here the formulas for completeness. They are different for powers of 2 and powers of odd primes.

A.3.1 Odd prime powers

Suppose that $N = p^a, \quad p \neq 2$. Than one of the $N+1$ mutually unbiased bases is the standard basis

$$|\psi\rangle_j^{(0,k)} = \delta_{jk}$$

and the other N bases will be given by

$$|\psi\rangle_j^{(n,k)} = \frac{1}{\sqrt{N}} e^{\frac{2\pi i}{p}\mathrm{tr}(nj^2+jk)}, \quad n = 1, 2, \ldots, N \tag{A.10}$$

where j denotes the j-th component of the k-th vector in n-th base and $\mathrm{tr}(\alpha)$ is defined as

$$\mathrm{tr}(\alpha) = \sum_{i=0}^{p^{a-1}} \alpha^i.$$

The fact that such bases are mutually unbiased is demonstrated in [36] and [37]

A.3.2 Even prime powers

For a systems of dimension N equal to 2^n, we can define 2^n bases whose vectors will be in a form

$$|\psi\rangle_j^{(n,k)} = \frac{1}{\sqrt{2^n}} e^{\frac{2\pi i}{4}\mathrm{tr}(n+2k)j}. \tag{A.11}$$

It is obvious that they will be mutually unbiased with respect to the standard basis. For the proof that these bases are mutually unbiased with respect to each other, we refer to [37] and [36].

A.4 Outlook

The question whether it is possible to construct the maximal possible number of $N+1$ mutually unbiased bases in N-dimensional complex Hilbert spaces for arbitrary N, not only for N equal to primes or powers of primes. So far, even attempts to construct more than the minimal number of existing mutually unbiased bases guaranteed by the Theorem 9 have been unsuccessful. It is conjectured that one cannot construct a set of more than 3 mutually unbiased bases for $N = 6$ [41].

Bibliography

[1] U. Fano, *Description of states in quantum mechanics by density matrix and operator techniques*, Reviews of Modern Physics, Vol. 29, No. 1, 1957, 74-93

[2] M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2003

[3] P. A. M. Dirac, *The Principles of Quantum Mechanics*, Oxford University Press, Oxford, 1958

[4] J. Formánek, *Úvod do kvantové teorie*, Academia, Praha, 2004

[5] J. von Neumann, *Mathematical Foundations of Quantum Mechanics*, Princeton University Press, Princeton, 1996

[6] R. K. Bock, W. Krischer, *The Data Analysis BriefBook*, Springer, 1998

[7] J. Blank, P. Exner, M. Havlíček, *Lineární operátory v kvantové fyzice*, Karolinum, Praha, 1993

[8] R. Jozsa, *Fidelity for Mixed Quantum States*, Journal of Modern Optics, Vol. 41, Issue 12, 1994, 2315 - 2323

[9] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, *Quantum cryptography*, Reviews of Modern Physics, Vol. 74, 2002

[10] N. J. Cerf, *Pauli Cloning of a Quantum Bit*, Physical Review Letters, Vol. 84, No 19, 2000, 4497-4500

[11] D. J. MacKay, *Information Theory, Inference and Learning Algorithms*, Cambridge University Press, 2003

[12] P. W. Shor, J. Preskill, *Simple proof of security of the BB84 quantum key distribution protocol*, Phys. Rev. Lett. 85, 2000, 441-444

[13] G. Brassard, L. Savail, *Secret-key reconciliation by public channel*, Lecture Notes in Computer Science, Vol. 765, 1994, 410-421

[14] R. Renner, *Security of Quantum Key Distribution*, Diss. ETH No. 16242, arXiv:quant-ph/0512258v2

[15] C. H. Bennett, G. Brassard, C. Crepeau, U. Maurer, *Generalized Privacy Amplification*, IEEE Transactions on Information Theory, Vol. 41, No. 6, November 1995, 1915-1923

[16] I. Csiszzár, J. Körner, *Broadcast Channels with confindential messages*, IEEE Transactions on Information Theory,Vol. IT-24, No. 3, 1978, 339-348

[17] M. J. W. Hall, *Information exclusion principle for complementary observables*, Phys. Rev. Lett., Vol. 74, 1995, 3307-3311

[18] R. L. Rivest, A. Shamir, L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM, Vol. 21, Issue 2, 1978, 120 - 126

[19] G. S. Vernam, *Cipher printing telegraph systems for secret wire and radio telegraphic communications*, J. Amer. Inst. Elec. Eng., Vol 55, 1926, 109-115

[20] C. Shannon, *Communication Theory of Secrecy Systems*, Bell System Technical Journal, Vol. 28, 1949, 656–715

[21] C. H. Bennett, G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, Proceedings of IEEE International Conference on Computers, 1984

[22] N. Lütkenhuas, *Security against eavesdropping in quantum cryptography*, Physical Review A, Vol. 54, No.1, 1996, 97-111

[23] D. Mayers, *Unconditional Security in Quantum Cryptography*, Journal of the ACM, Vol. 48, No. 3, 2001, 351-406

[24] A. K. Ekert, *Quantum cryptography based on Bell's theorem*, Physical Review Letters, Vol. 67, 1991, 661-663

[25] M. Bechmann-Pasquinucci, W. Tittel, *Quantum cryptography using larger alphabets*, Phys. Rev. Lett. A, Vol. 61, 2000,

[26] H. Bechmann-Pasquinucci, A. Peres, *Quantum Cryptography with 3-State Systems*, Phys. Rev. Lett., Vol. 85, No. 15, 2000, 3313-3316

[27] G. M. Nikolopoulos, G. Alber, *Security bound of two-basis quantum-key-distribution protocols using qudits*, Physical Review A 72, 2005, 032320

[28] N. J. Cerf, M. Bourennane, A. Karlson, N. Gisin, *Security of Quantum Key Distribution Using d-Level Systems*, Phys. Rev. Lett. Vol. 88, No. 12, 2002

[29] M. Bourennane, A. Karlsson, G. Björk, N. Gisin, N. Cerf, *Quantum key distribution using multilevel encoding*, J. Phys. A: Math. Gen, Vol 35, 2002, 10065-10076

[30] V. Bužek, M. Hillery, *Universal Optimal Cloning of Arbitrary Quantum States: From Qubits to Quantum Registers*, Phys. Rev. Lett., Vol. 81, 1998,5003-5006

[31] P. Šulc, *Optimal determination of states of d-level quantum systems*, Bachelor's Thesis, FNSPE, CTU, 2006

[32] P. Šulc, J. Tolar, *Group theoretical construction of mutually unbiased bases in Hilbert spaces of prime dimensions*, arXiv:quant-ph/0708.4114v1

[33] J. Schwinger, *Unitary operator bases*, Proc. Natl. Acad. Sci. 46, 1960

[34] I. D. Ivanović, *Geometrical description of quantum state determination*, Journal of Physics A, 14 (1981), no.12, pp. 3241 - 3245

[35] W. K. Wootters, *Quantum mechanics without probability amplitudes*, Foundations of Physics, Vol. 16, No. 4, 1986, 391-405

[36] W. K. Wootters, B.D. Fields, *Optimal State-Determination by Mutually Unbiased Measurements*, Annals of Physics 191 (1989), 363-381

[37] A. Klappenecker, M. Rötteler, *Constructions of Mutually Unbiased Bases*, Lecture Notes in Computer Science, vol. 2984, Springer, 2004, arXiv:quant-ph/0401155

[38] T. Nagell, *Introduction to Number Theory*, Wiley, New York, 1951.

[39] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, F. Vatan, *A new proof for the existence of mutually unbiased bases*, Algorithmica 34, 2002, arXiv:quant-ph/0103162

[40] P. Šťovíček, J. Tolar, *Quantum Mechanics in a Discrete Space-time*, Rep. Math. Phys. 20, 1984, 157-170

[41] M. Grassl, *On SIC-POVMs and MUBs in dimension 6*, arXiv:quant-ph/0406175