

A unified description of cryptosystems: From classical to quantum protocols

Giuseppe De Riso

Dipartimento di Fisica "E. R. Caianiello"

Università degli Studi di Salerno

Via Giovanni Paolo II 132

84084 Fisciano (SA)

Italy

Marialaura Noce *

Dipartimento di Matematica

Università degli Studi di Salerno

Via Giovanni Paolo II 132

84084 Fisciano (SA)

Italy

Abstract

The launch of quantum computing has created new challenges in the field of cryptography. Nowadays this field of research is extremely active in physics, mathematics and computer science. In this paper we present an overview of the most common classical and quantum protocols. The former are usually defined through a 5-uple given by a plaintext space, a ciphertext space, an encryption and decryption space, an encryption function and a decryption function. Here, we show how to unify quantum and classical protocols by using the same formalism of the 5-uple mentioned above.

Subject Classification: (2020) 81P94.

Keywords: Quantum cryptography, Cryptography.

1. Introduction

Cryptography is the study of techniques to send messages in a way that only the parties involved can read the message. The process

* E-mail: mnoce@unisa.it

of sending a secret message is called *encryption*. The *encryption key* is needed to transform the plaintext into cipher text. Once the message has been received, to be converted into the original, is used a process called *decryption*. The most important aspect of security and exchange of message is based on *keys* that the sender and recipient use. Namely, classical cryptography is mainly based into two classes: secret (or symmetric) key cryptography and public key (or asymmetric) cryptography.

The former is the most traditional exchange of messages. Secret key cryptography works in such a way that the two parties, say Alice and Bob, share a key, which only they know. With this key they are able to encrypt and decrypt their messages. So far, private key cryptosystems have several problems, for example the difficulty to distribute and share the key, and to communicate in a private channel. On the other hand, in public key cryptography a shared secret key does not need to be established prior to communication in public key cryptography. Here Alice and Bob have both a private key (which will be secret) and then they have a public key that can be distributed freely.

The security of public key cryptography protocols is based on the difficulty to solve certain mathematical problems, for example the integer factorization or the discrete logarithm problem. For this reason, public key cryptography could be vulnerable to attacks. In 1994 Shor provided a quantum algorithm that solves these problems in polynomial time [12]. After Shor's quantum algorithm, researchers in many areas of mathematics were motivated to find alternative methods in the era of *post-quantum cryptography*, that is public-key cryptography based on problems other than factorizing integers and compute discrete logarithms. Among others, possible candidates are: lattice-based cryptography, code-based cryptography and group-based cryptography. About the latter, we mention that in the last decades several families of groups were suggested as platforms for cryptographic protocols (e. g. polycyclic groups [7], right-angled Artin groups [5], and Engel groups [9]; see also [8] for an overview of the topic).

In this scenario, another way to send secure messages was developed by the advent of *quantum cryptography*, which uses laws of physics, and more precisely principles of quantum mechanics, to send secure messages. Contrary to classic cryptography, in which the security of the encryption is based on finding the correct key, the security of quantum cryptography is based on sending messages in a quantum channel that cannot be hacked.

To this end, in the last decades, many different approaches related to novel cryptographic algorithms were developed. Among others, we

mention chaotic cryptosystems based on the dynamic lookup table that were used for securing text data and images over the network. In 2019, it was introduced an improved and alternate version of this, see [13]. Finally, in 2020 the QuantQueryEXP implements an eminent technique based on queries implementing quantum techniques. This gave a better accuracy in complexity over any conventional algorithm to achieve supremacy in quantum computing. More precisely, the QuantQueryEXP has an accuracy of 90.43%, [10].

In this paper, we present the most important quantum cryptosystems from a new point of view. More precisely, it is known that to define formally a classical cryptosystem one needs to define a plaintext space, a ciphertext space, an encryption and decryption space, an encryption function and a decryption function. Here, we apply the same formalism to define a quantum cryptosystem.

2. Preliminaries

2.1 Definition of a cryptosystem

An *alphabet* A is a non-empty set, whose elements are called *letters* or *symbols*. For $m \geq 2$, a *word* over A is an element of A^m , where A^m denotes the canonical Cartesian product of m copies of A . In other terms, a word is a finite sequence of letters of A . We write ε to denote the trivial word, thus, for example, $A^0 = \{\varepsilon\}$. The length of a word w is denoted by $|w|$, and the trivial has length 0. The set of all words is $A^* = \bigcup_{m \geq 0} A^m$. The *concatenation* of two words $x = a_1 \dots a_m$ and $y = b_1 \dots b_n$ in A^* is a binary operation that gives $xy = a_1 \dots a_m b_1 \dots b_n \in A^{m+n}$. The concatenation is associative, so, as a consequence, A^* is a monoid, that is called the *free monoid* generated by A . We recall that monoid is a set with an associative binary operation and an identity element (in our case, the identity element is ε). A *formal language* L is a subset of A^* .

Let A, B be two alphabets. A *cryptosystem* is a 5-tuple $(\mathcal{P}, \mathcal{C}, k, \mathcal{E}, \mathcal{D})$, where:

- $\mathcal{P} \subseteq A^*$ is the *plaintext space*. The elements of $\mathcal{P}$ are called *plaintexts*.
- $\mathcal{C} \subseteq B^*$ is the *ciphertext space*. The elements of $\mathcal{C}$ are called *ciphertexts*.
- Let $\mathcal{K}$ and $\mathcal{K}'$ be two nonempty sets. Then $k : \mathcal{K} \rightarrow \mathcal{K}'$ is a bijective map called the *key correspondence*. The sets $\mathcal{K}$ and $\mathcal{K}'$ are the *encryption* and *decryption key space*, respectively.

- $\mathcal{E} = \{e_k \mid k \in \mathcal{K}\}$ is the family of all *encryption functions* e_k . For $k \in \mathcal{K}$, the map e_k is

$$\begin{aligned} e_k : \mathcal{P} &\rightarrow \mathcal{C} \\ p &\mapsto c. \end{aligned}$$

- $\mathcal{D} = \{d_k \mid k \in \mathcal{K}\}$ is the family of all *decryption functions* d_k .

For $k \in \mathcal{K}$, the map d_k is

$$\begin{aligned} d_k : \mathcal{C} &\rightarrow \mathcal{P} \\ c &\mapsto p. \end{aligned}$$

In the classical definition of a cryptosystem, we often assume that $A = B$, $\mathcal{P} = A^*$, and k is the identity map. Furthermore, to avoid ambiguity during the decryption process, we require that the encryption functions e_k are injective for any $k \in \mathcal{K}$. In other words, for any $p, p' \in \mathcal{P}$ with $p \neq p'$, we must have $e_k(p) \neq e_k(p')$. This condition, together with the definitions of e_k and d_k , implies that for every $k, k' \in \mathcal{K}$ there exist an encryption function $e_k \in \mathcal{E}$ and a decryption function $d_{k'} \in \mathcal{D}$ such that $d_{k'}(e_k(p)) = p$. In other words, is $d_{k'} = e_k^{-1}$.

2.2 Fundamentals of quantum mechanics

To understand how quantum cryptosystems work, in this section we survey the aspects of quantum mechanics. For a complete introduction on the topic see, for example, [6].

2.2.1 Measurement

The state of a quantum system is described by a state vector $|\psi\rangle$ in a complex Hilbert space $\mathcal{H}$, so that we can identify quantum states with vectors in $\mathcal{H}$. A physical quantity for the system is represented by a self-adjoint operator $A = A^\dagger$ on $\mathcal{H}$ and it is called *observable*. If A has a discrete spectrum, a generic state of $\mathcal{H}$ can be thus written as:

$$|\psi\rangle = \sum_{i=1}^n c_i \psi_i\rangle,$$

where n is the dimension of $\mathcal{H}$ (eventually n can be infinite), $c_i = \langle \psi_i | \psi \rangle$ are complex numbers, and $|\psi_i\rangle$ are eigenfunctions of the self-adjoint operator A , forming a complete orthonormal base $\{|\psi_i\rangle\}_{i=1, \dots, n}$ for $\mathcal{H}$. From now on, we will assume that the state $|\psi\rangle$ is normalized. We note that a

measurement of an observable A in the quantum state $|\psi\rangle$ can only give one of the eigenvalues λ_i of A with probability $p_i = |c_i|^2$. Now, we define the following operator $P_i = \psi_i \psi_i$. It is easy to check that such an operator has the following properties:

- normality and idempotence: $P_i P_j = \delta_{ij} P_j$;
- completeness: $\sum_{i=1}^n P_i = I$, where I is the identity operator.

As a consequence, P_i is a *projection* operator. According to quantum mechanics, the effect of a measurement of an observable on the system is the *collapse* of the wave function, namely a projection of the state vector $|\psi\rangle$ onto the subspace spanned by the eigenfunctions of $A|\psi_i\rangle$:

$$|\psi_i\rangle = \frac{P_i |\psi\rangle}{\sqrt{\langle\psi|P_i|\psi\rangle}}.$$

Therefore, the probability to obtain such state as consequence of the measurement of the observable is given by $p_i = |c_i|^2 = \langle\psi|P_i|\psi\rangle$. We remark that this process is irreversible and causes loss of information about the state of the system before the measurement.

2.2.2 Heisenberg Uncertainty Principle

Let now consider two observables for a system, described by the operators A and B . The *commutator* of A and B is defined as $[A, B] = AB - BA$. If $[A, B] = 0$ the observables are said to be *compatible* and they share a complete set of common eigenvectors, implying that we can measure with arbitrary precision A and B simultaneously. Otherwise, if $[A, B] \neq 0$ the observables are said to be *incompatible* and an uncertainty relation holds:

$$\sigma_A^2 \sigma_B^2 \geq \left| \frac{1}{2i} \langle\psi|[A, B]|\psi\rangle \right|^2.$$

Here, $\sigma_Q^2 = \langle Q^2 \rangle - \langle Q \rangle^2$ is the variance of the observable associated with Q , over a given state $|\psi\rangle$. This inequality implies that A and B do not share a common set of complete eigenvectors and cannot be measured simultaneously or in sequence with arbitrary precision: the more we know about the value of A , the less we know about the value of B and vice versa.

2.2.3 Quantum Entanglement

Let us consider two non interacting single particle systems with Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$. The overall Hilbert space is given by the *tensor product* $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. For example, if we consider two level systems we have $\dim \mathcal{H}_{AB} = 4$. Let $\{|0\rangle_A, |1\rangle_A\}$ and $\{|0\rangle_B, |1\rangle_B\}$ be orthonormal bases for $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively. Thus, a canonical basis for $\mathcal{H}_{AB}$ is

$$|0\rangle_A \otimes |1\rangle_A \otimes |0\rangle_B \otimes |1\rangle_B = |0\rangle_A \otimes |0\rangle_B \otimes |0\rangle_A \otimes |1\rangle_B \otimes |1\rangle_A \otimes |0\rangle_B \otimes |1\rangle_A \otimes |1\rangle_B.$$

The most general state of the system is then given by $|\psi\rangle = \sum_{i,j=0}^1 c_{ij}^{AB} |i\rangle_A \otimes |j\rangle_B$ where the c_{ij}^{AB} are complex coefficients such that $\sum_{i,j=0}^1 |c_{ij}^{AB}|^2 = 1$.

A state $|\psi\rangle \in \mathcal{H}_{AB}$ is said to be *separable* if and only if it can be written as the tensor product

$$|\psi\rangle = |\phi\rangle \otimes |\varphi\rangle,$$

where $|\phi\rangle = \sum_{i=0}^1 c_i^A |i\rangle_A$ and $|\varphi\rangle = \sum_{j=0}^1 c_j^B |j\rangle_B$ are single particle states. In other words the state is separable only if there exists some complex coefficients c_i^A, c_j^B such that $c_i^A c_j^B = c_{ij}^{AB}$. If these coefficients do not exist the state is said to be *non separable* or *entangled*. From now on we will use the simplified notation $|\phi\varphi\rangle$ for $|\phi\rangle \otimes |\varphi\rangle$.

Now suppose we perform a basis change on the entangled state. It can be shown that the resulting state is also an entangled state of the same form as the starting one. Some important entangled states for the space $\mathcal{H}_{AB}$ are represented by the *EPR states* or *Bell states*, defined as

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \quad |\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \quad |\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \quad |\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}.$$

The set $\{|\beta_{ij}\rangle\}_{i,j \in \{0,1\}}$ is an orthonormal basis for $\mathcal{H}_{AB}$, known as the *Bell basis*. The Bell states play a key role in quantum information theory: they are the simplest example of *maximally entangled* pure states, in the sense that they maximally violate the *CHSH inequality*, [3].

Let us now consider a two particle system described by the state $|\beta_{00}\rangle$, and let us suppose that one particle is sent to Alice and the other one to Bob. If Alice performs a measurement, obtaining the state $|0\rangle_A$ ($|1\rangle_A$), as a consequence of the structure of $|\beta_{00}\rangle$, Bob's particle will collapse in the state $|0\rangle_B$ ($|1\rangle_B$). Moreover, this collapse will occur instantaneously after Alice's measurement, no matter how far the particles are. Due to this property, the entangled states have profound and counterintuitive implications in physics, and this feature represents a precious tool to realize quantum cryptographic protocols.

3. Quantum cryptosystems

In this section we rewrite the QKD protocols using the formalism applied to the definition of classical cryptosystems. To this end, we first recall the description of each protocol, and then we describe how they work by using the formalism of classic cryptosystem. We always suppose that Alice and Bob want to send to each other a secret message through a secure channel. More precisely, they want to generate and share a secret key that can be used in a public key cryptographic scheme.

3.1 *Protocols based on Heisenberg's Uncertainty Principle*

Here, we present the most important protocols known by using Heisenberg's Uncertainty Principle, i. e. the BB84 and the B92. We note that in both cases, there are two channels are used, namely:

- a *quantum channel* that permits Alice and Bob to exchange a sequence of qbits;
- a *classical channel* which handles "classical" information.

3.1.1 The BB84 protocol

The BB84 [2], named after Bennett and Brassard, is the first quantum key distribution protocol. This protocol may be described in two steps: the first one by using a quantum channel, while the second one by using a classical channel. To better describe this protocol, we will use in each step an example to understand how the BB84 works.

- Alice and Bob choose two orthonormal bases.
- Alice constructs a sequence of bits, each of them associated to a vector of the basis.
- Alice prepares a random sequence of quantized polarized light, i. e. the aforementioned photon states, and sends it to Bob.
- Bob receives the photons and measures them using a random sequence of bases.
- There are two possibilities for the results of the measurement of Bob:
 - If the basis that Bob chooses is equal to the one of Alice, then Bob obtains a bit representing the information;
 - Otherwise a random result is obtained and he loses information.

The second step uses the classical channel and works as follows:

- Bob sends the bases he used (but not the results he has obtained).
- Alice tells to Bob what are the cases in which the bases coincide.
- Bob keeps only the equal bases and discards the others. In this way he gets the secret key.

We conclude this introduction on the BB84 protocol by pointing out that the security of the protocol is based on the fact that it relies on the quantum property that information gain is only possible at the expense of disturbing the signal if the two states one is trying to distinguish are not orthogonal (see [11, No-Cloning Theorem]) and an authenticated public classical channel.

Now, we present the BB84 protocol by using the classical cryptosystem formalism.

Let us consider a 2 level system, which defines a 2-dimensional Hilbert space $\mathcal{H}$ an Hilbert space $\mathcal{H}$. Let X, Y be two orthonormal bases for this space:

$$X = \{|x_1\rangle, |x_2\rangle\}, \langle x_i | x_j \rangle = \delta_{ij},$$

$$Y = \{|y_1\rangle, |y_2\rangle\}, \langle y_i | y_j \rangle = \delta_{ij}.$$

Formally, given an integer $n \geq 1$, let

- $\mathcal{P} = \mathcal{C} = \{|x_1\rangle, |x_2\rangle, |y_1\rangle, |y_2\rangle\}^n$: the plaintext and the cyphertext are represented by a string of length n of the state vectors of the basis chosen for the description of the qbit. Each state vector is associated with a binary value

$$|x_1\rangle \leftrightarrow 0 \quad |x_2\rangle \leftrightarrow 1 \quad |y_1\rangle \leftrightarrow 0 \quad |y_2\rangle \leftrightarrow 1;$$

- $\mathcal{K} = \{X, Y\}^n$: the key space is a string of length n of the bases chosen by Alice for the description of the system;
- for each qbit, the encryption function $e_k(p)$ is the projection operator $P_A = |A\rangle \langle A|$ such that

$$P_A |\psi\rangle = c_A |A\rangle \quad |A\rangle \in \mathcal{C},$$

where $|\psi\rangle$ is the state of the system before the encoding process (i.e. a measurement), $|A\rangle$ is the state of the system after the encoding

process, $|c_A|^2 = |\langle A | \psi \rangle|^2$ gives the probability to obtain such state after the measurement;

- for each qbit, the decryption function $d_k(c)$ is the projection operator $P_B = |B\rangle \langle B|$ such that

$$P_B |A\rangle = c_B |B\rangle \quad |B\rangle \in \mathcal{P};$$

where $|A\rangle$ is the state of the system before the decoding process (i.e. a measurement), $|B\rangle$ is the state of the system after the decoding process, $|c_B|^2 = |\langle B | A \rangle|^2$ gives the probability to obtain such state after the measurement.

The decoding process is achieved successfully only if

$$P_A = P_B$$

for every bit of the string, i.e. only if Alice and Bob choose the same measurement basis. In this case we have $|c_B|^2 = 1$ and the measurement gives the same state sent by Alice, with no loss of information. In the other case, since the measurement process is subject to the probabilistic behaviour of the system, there is no certainty that the information sent matches the information received and the bit must be discarded. It should be noted that if initially Alice and Bob shared the basis string used for the coding, this would be a simple symmetric cipher with the basis string as key.

3.1.2 The B92 protocol

The B92 protocol [1] is a “minimal” version of BB84 using any two non orthogonal states. As in the case of the BB84, this protocol has two main steps, over a quantum and a classical channel. The first step takes place over a quantum channel:

- Alice and Bob choose two orthonormal bases for the qbit description.
- Alice associates a binary value to a random state of the first basis and the second one to a random state of the second basis;
- Alice constructs a sequence of bits and prepares the states of the qbits according to the fixed bit sequence. Then sends them to Bob.
- Bob receives the qbits and measures them using randomly the remaining two non orthogonal vectors of the chosen bases;

- The measurement outcome depends upon the chosen basis:
 - if the measurement basis is different from Alice's, then Bob will get a bit representing the information;
 - Otherwise no bit is revealed and the information is lost.

The second step takes place over a classical channel:

- Bob tells Alice in which case the measurement was successful (without revealing the sequence of bases he used);
- Bits not measured by Bob are discarded.

We now rewrite the above protocol using the classical cryptosystems formalism.

Let us consider two mutually non orthonormal bases both spanning the 2-dimensional Hilbert space of a single qbit, namely

$$R = \{|x_0\rangle, |x_1\rangle\}, \langle x_i | x_j \rangle = \delta_{ij}$$

$$D = \{|y_0\rangle, |y_1\rangle\}, \langle y_i | y_j \rangle = \delta_{ij}.$$

Given an integer $n \geq 1$, let:

- $\mathcal{P} = \mathcal{C} = \{|x_i\rangle, |y_j\rangle\}^n$: plaintext and ciphertext are represented by a string of length n of state vectors. The vectors chosen for the encryption must be non orthogonal.
- $\mathcal{K} = \{R, D\}^n$: the key space is a string of length n of the bases chosen by Alice for the description of the system;
- for each qbit the encryption function $e_k(p)$ is the projection operator $P_A = |A\rangle \langle A|$ such that

$$P_A |\psi\rangle = c_A |A\rangle \quad |A\rangle \in \mathcal{C}$$

where $|\psi\rangle$ is the state of the system before the encoding process, $|A\rangle$ is the state of the system after the measurement, $|c_A|^2 = |\langle A | \psi \rangle|^2$ gives the probability to obtain such state after a measurement;

- for each qbit, the decryption function $d_k(c)$ is the projection operator $P_B = |B\rangle \langle B|$ such that

$$P_B |A\rangle = c_B |B\rangle \quad |B\rangle \in \mathcal{P}^\perp;$$

where $|A\rangle$ is the state of the system before the decoding process (i.e. a measurement), $|B\rangle$ is the state of the system after the decoding

process, $|c_B|^2 = |\langle B|A \rangle|^2$ gives the probability to obtain such state after the measurement.

The decoding process is achieved successfully only if

$$P_B |A\rangle \neq 0$$

for every qbit of the string, i.e. only if Alice and Bob choose two different bases for the measurement. In this case the bit is revealed and information is obtained: Bob can recognize exactly the initial state of the qbit, thus his binary value. Otherwise the qbit is not measured and his initial state remains unknown. It should be noted that for the communication to be successful the exact value of the measured qbit is irrelevant. The only request is a positive measurement outcome.

3.2 *Protocols based on quantum entanglement*

Here we present Eckert's protocol, that relies on the perfect correlation between entangled states.

3.2.1 Eckert's protocol

The E91 protocol [4], named after Eckert's work, is a QKD protocol which uses entangled states for the communication of a secret key between two parties. As the other protocols discussed, there are two main phases, over a quantum and a classical channel.

In the first phase:

- Alice and Bob choose three orthonormal non mutually orthogonal basis for the qbit description.
- Alice, Bob or a trusted third party creates a Bell's state $|\beta_{ij}\rangle$. The structure of the state is fixed during the whole protocol.
- One particle of the pair is sent to Alice, the other to Bob. Separately and independently, they perform a measurement on the qbit received using one of the three above basis. The first to take a measurement gets information about the qbit state and makes the joint system to collapse in the corresponding state. However, depending upon the basis choice for the second measurement there are two possibilities:
 - if the second basis is equal to the first, the measurements will be perfectly correlated;
 - otherwise a random result is obtained.

In the second phase:

- Alice and Bob communicate over a classical channel the measurement basis used (but not the results).
- when the basis are equal, a key bit is obtained, otherwise the bit is discarded (but can be used to detect eavesdroppers).

Now we rewrite the above protocol using the classical cryptosystem formalism. Let

$$A = \{|a_0\rangle, |a_1\rangle\} \quad B = \{|b_0\rangle, |b_1\rangle\} \quad C = \{|c_0\rangle, |c_1\rangle\},$$

be three mutually non orthogonal bases for the Hilbert space of a single qbit. Let us consider a two qbits system, which defines an Hilbert space $\mathcal{H}_{AB}$ with $\dim \mathcal{H}_{AB} = 4$. If we choose the same basis for the description of both qbits, then

$$E \otimes E = \{|e_0 e_0\rangle, |e_0 e_1\rangle, |e_1 e_0\rangle, |e_1 e_1\rangle\} \quad E \in \{A, B, C\}$$

is a basis for $\mathcal{H}_{AB}$. Let now prepare the overall system in a maximally entangled state, i.e. a Bell state:

$$|\beta_{ij}\rangle = \frac{|e_0 e_j\rangle + (-1)^i |e_1 e_{1-j}\rangle}{\sqrt{2}}.$$

The Eckert protocol is formalized as follows. Given an integer $n \geq 1$:

- $\mathcal{P} = \mathcal{C} = \{|e_i e_j\rangle\}^n$: the plaintext and ciphertext are strings of length n of the states vectors used for the description of both qbits. Each single particle state is associated to a binary value:

$$|e_0\rangle \leftrightarrow 0 \quad |e_1\rangle \leftrightarrow 1 \quad e = \{a, b, c\}.$$

In the state $|e_i e_j\rangle$, the first label refers to Alice's particle, the second to Bob's particle. Thus they represent the information bits of Alice and Bob.

- $\mathcal{K} = \{A, B, C\}^n$: the key space is a string of length n of the basis randomly chosen during the first measurement of the entangled pair. Suppose that Alice and Bob measure particle A and B , respectively, at different times t_1 and $t_2 \geq t_1$. We will use the labels T_1 and T_2 to identify the results of first and second measurements, respectively.
- For each entangled pair, the encryption function $e_k(p)$ is the single particle projection operator $P_{T_1} = |T_1\rangle \langle T_1|$, $|T_1\rangle \in E$ which acts only

on the first or second particle of the system depending on who is the first to take a measurement between Alice and Bob. The effect is:

$$P_{T_1} |\beta_{ij}\rangle = c_{T_1} |T_1 e_j\rangle \quad |T_1 e_j\rangle \in \mathcal{C},$$

$$P_{T_1} |\beta_{ij}\rangle = c_{T_1} |e_i T_1\rangle \quad |e_i T_1\rangle \in \mathcal{C}.$$

where $|\beta_{ij}\rangle$ is the state vector of the composite system before the encryption process (i. e. before the measurement), $|T_1 e_j\rangle$ and $|e_i T_1\rangle$ are the state vectors of the composite system after the decryption process, $|c_{T_1}|^2$ gives the probability to obtain such state after the first measurement.

- For each entangled pair, the decryption function $d_k(c)$ is the single particle projection operator $P_{T_2} = |T_2\rangle \langle T_2|$ which acts only on the first or second particle of the system depending on who is the second to take a measurement between Alice and Bob. The effect is:

$$P_{T_2} |T_1 e_j\rangle = c_{T_2} |T_1 T_2\rangle \quad |T_1 T_2\rangle \in \mathcal{P},$$

$$P_{T_2} |e_i T_1\rangle = c_{T_2} |T_2 T_1\rangle \quad |T_2 T_1\rangle \in \mathcal{P}.$$

where $|T_1 e_j\rangle$ and $|e_i T_1\rangle$ are the state vectors of the composite system before the decryption process (i.e. before the measurement), $|T_1 T_2\rangle$ and $|T_2 T_1\rangle$ are the state vectors of the composite system after the decryption process, $|c_{T_2}|^2$ gives the probability to obtain such state after the second measurement.

The decryption process is achieved successfully only if

$$P_{T_1} = P_{T_2}$$

for each pair of qbits i.e. only if Alice and Bob choose the same measurement basis. In this case we have $|c_{T_2}|^2 = 1$ and the second measurement is perfectly correlated or anticorrelated with the first one depending on the chosen Bell's state. On the other hand, if the second measurement is performed in a different basis, the outcome is random and there is no correlation between the two results. As a consequence the acquired bit must be discarded. We note that the ciphertext is "generated" only when the first measurement is performed and the message can be considered encrypted only for the user who measure the particle last. Finally, if the measurements are made simultaneously, i.e. if $t_1 = t_2$, the key generation

process can be considered truly random: it is impossible to decide when the message has been encrypted or decrypted.

References

- [1] C. H. Bennett, Quantum cryptography using any two nonorthogonal states, *Phys. Rev. Lett.* 68 (1992May), 3121-3124.
- [2] C. H. Bennett and Gilles Brassard, Quantum cryptography: Public key distribution and coin tossing, *Theoretical Computer Science* 560 (2014Dec), 7-11.
- [3] J. F. Clauser, M. A. Horne, Abner Shimony, and Richard A. Holt, Proposed experiment to test local hidden-variable theories, *Phys. Rev. Lett.* 23 (1969Oct), 880-884.
- [4] Artur K. Ekert, Quantum cryptography based on bell's theorem, *Phys. Rev. Lett.* 67 (1991Aug), 661-663.
- [5] R. Flores, D. Kahrobaei, and T. Koberda, Algorithmic problems in right-angled Artin groups: Complexity and applications, *Journal of Algebra* 519 (2019), 111-129.
- [6] D. J. Griffiths and D. F. Schroeter, Introduction to Quantum Mechanics, 3rd ed., Cambridge University Press, 2018.
- [7] J. Gryak and D. Kahrobaei, The status of polycyclic group-based cryptography: A survey and open problems, *Groups Complexity Cryptology* 8 (2016), 171-186.
- [8] D. Kahrobaei, R. Flores, and M. Noce, Group-based cryptography in the Quantum Era, *Notices of the American Mathematical Society* 70 no. 5 (2023), pp. 752-763.
- [9] D. Kahrobaei and M. Noce, Algorithmic problems in engel groups and cryptographic applications, *International Journal of Group Theory* 9 (2020), no. 4, 231-250.
- [10] I. S. Kaushik, G. Deepak, and A. Santhanavijayan, QuantqueryEXP : A novel strategic approach for query expansion based on quantum computing principles, *Journal of Discrete Mathematical Sciences and Cryptography* 23 (2020), no. 2, 573-584.

- [11] J. L. Park, The concept of transition in quantum mechanics, *Foundations of Physics* 1 (1970), 23-33.
- [12] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J. Comput.* 26 (1997), no. 5, 1484-1509.
- [13] D. K. Verma, M. Rani, R. K. Tyagi, and B. B. Sagar, Baptista chaotic cryptosystem based on alternate superior dynamic lookup table, *Journal of Discrete Mathematical Sciences and Cryptography* 22 (2019), no. 8, 1383-1392.
- [14] D. Kahrobaei, M. Noce, E. Rordaro, Applications of Automaton Groups in Cryptography, preprint arXiv:2306.10522 [math.GR] (2023).
- [15] D. Kahrobaei, R. Flores, M. Noce, M. Habeeb, C. Battarbee, Applications of Group Theory in Cryptography: Post-quantum group-based cryptography, *The Mathematical Surveys and Monographs* series of the American Mathematical Society, in press.

Received May, 2022

Revised September, 2022