Indonesian Journal of Electrical Engineering and Computer Science
Vol. 7, No. 2, August 2017, pp. 542 ~ 550
DOI: 10.11591/ijeecs.v7.i2.pp542-550

Quantum Key-Policy Attribute-Based Encryption

Gabriela Mogos
Department of Computer Science, Stefan Procopiu Technical College, Calea Chisinaului 132bis, Iasi, 700179, Romania
Corresponding author, e-mail: gabi.mogos@gmail.com

Abstract

Attribute-Based Encryption is a relatively new concept in the field of cryptography, and it allows only the authorized entities to decrypt a message. This type of encryption is the mechanism by which the users may encrypt and decrypt data based on user attributes. This paper proposes the first quantum alternative of the scheme Key-Policy Attribute Based Encryption, where the information, the encryption/decryption key, and the attributes are made of qutrits.

Keywords*: qutrits, entanglement, encryption, decryption, attribute-based encryption*

1. Introduction

Human society undergoes at present one of the deepest transformation in its entire existence, which is the transfer of common activities in another space, the so-called cyberspace, which removes the frontiers, the notion of distance, and which brings flexibility, rapidity, and efficiency. Today we can speak about the remote access of information resources, contracts signed between persons who do not meet on a face to face basis, electronic payment systems, systems of funds transfer and electronic network commerce, etc.

The architectural complexity, and the topological distribution of networks lead to an uncontrolled growth of the multitude of users with free access to the resources of the network - files, database, routers, etc., that is why we can speak of a network vulnerability manifested on various levels. Therefore, a crucial aspect of computer networks is security of information. Consequently, there is a need to identify the users located far away, and, also, a need of security and authenticity, at all the architectural levels of the networks. The purpose of the act of communication is to transport the information among the individuals forming the society by various ways and modalities, in such a way as to assure the integrity, and eventually the confidentiality of communication. Communication implies the information transmission among entities located at various levels, and their heterogeneity (people - calculation systems - communication lines) implies the prioritizing infrastructure. Each level of the infrastructure is capable to understand only the information coming in an encoded form, according to their needs.

Cryptography is a set of standards and protocols for the encryption of data and messages to be more securely stored and sent. Cryptography is the basis for many security services and mechanisms from the Internet. It uses mathematical methods to transform the data, to prevent them to be seen and to get their content altered. Cryptography can be used to assure the data integrity and secrecy; to verify the source of the data and of the messages using digital signatures and certificates.

The explicit purpose of cryptography is to make it difficult or impossible for a third party to access the protected information. Cryptography helps in getting a more secure communication, even when the transmission environment is not to be trusted.

The fundamental purpose of cryptography is:

1. *Confidentiality*: the assurance that nobody can read the message except the sender;
2. *Data integrity*: it realizes the protection of the data of their alteration or manipulation (insertions, delays etc.) by unauthorized persons;
3. *Authentication*: it implies the possibility to identify the source of the information and of the entity (person, computer terminal);
4. *Non-repudiation*: which prevents the refusal to admit previous declarations or actions.

Received May 1, 2017; Revised July 11, 2017; Accepted July 27, 2017

The concept of Attribute-Based Encryption (ABE) was proposed for the first time by Amit Sahai and Brent Waters [1] and later by Vipul Goyal, Omkant Pandey, Amit Sahai and Brent Waters [2]. This is a type of encryption with public key, where a user's secret key and the cyphertext depend on attributes.

The decryption of the cyphertext is possible only when the set of attributes of the user key matches the cyphertext attributes. A crucial security characteristic of attribute-based encryption is collusion-resistance: an enemy who owns several keys should be able to access the data only if at least one of the individual keys guarantees the access. A user's data can be encrypted and stored on the internet. The disadvantage of traditional encryption schemes is the fact that these data can be only roughly distributed, which allows any user who owns a decryption key to decrypt the data.

Attribute-Based Encryption is a new vision of encryption, going beyond such traditional restrictions, by which to allow the access control based on policies.

For example, in an institution there are various functions for the employees: accountant, secretary, manager, general manager, etc. Based on the employees' degrees, they can or they cannot have access to the encrypted data.

Consequently, if one has the function *x*, for example, and has certain attributions: *a, b, c*, let us suppose they are encoded in attributes *1* and *2*, and therefore, one has *2* attributes forming an access structure, which means one can have access to message decryption.

The stages of the classical scheme of Attribute-Based Encryption [2] are as follows:

a. *Setup*: Input: security parameter *s*; Output: public key *PK* and master key *MK*.
b. *Key generator*: Input: master key *MK* and attributes *S*; Output: private key *SK*.
c. *Encryption*: Input: public key *PK*, text *T* and access structure *A*; Output: cyphertext *CT*.
d. *Decryption*: Input: cyphertext *CT*, public key *PK*; Output: text *T*.

Lately, there has been a significant progress in ABE scheme construction, efficient from various points of view, and for specific functionalities. Up to present, there are two types of Attribute-Based Encryption: one is based on key policy, *Key-policy Attribute-Based Encryption*, and the other is based on crypto-text policy, *Cyphertext-policy Attribute-Based Encryption*.

In the case of *Key-policy Attribute-Based Encryption*, the owner of the data generates a master key. With the help of the master key, the owner encrypts the data, so an encrypted text is labelled with a set of attributes. The private key used for data decryption has a tree-based access structure associated, showing which cyphertext can be decrypted by the key. The tree-based access structure contains leaves, which are associated with the attributes. A user can decrypt the cyphertext when the attributes associated to the cyphertext satisfy the key access structure [2].

In the case of *Cyphertext-policy Attribute-Based Encryption*, a user's private key is associated with a set of attributes. When a party encrypts the message, an attribute-based access structure is specified, and this access structure is associated to the cyphertext. A user can decrypt the encrypted text when his/her attributes go through the access structure of the cyphertext [3].

In the past two decades, quantum secure communication developed rapidly. Quantum key distribution is one of the important braches in quantum secure communication. Many researchers have studied Quantum key distribution and proposed some important ideas and protocols [4-6]. At the same time, there has been an interesting progress recently regarding quantum-resistant anonymous digital signatures [7].

Even if were studied issues related to ensuring security in a network [8], the Attribute-Based Encryption problem in quantum version was not yet discussed.

In this paper, we present a Quantum Key-policy Attribute-Based Encryption method. In our scheme, there is requirement of a central authority, the information is encoded in qutrits [9] and the authentication between the central authority and the user is based on entanglement swapping phenomenon. The proposed scheme is constructed starting from the classical method, and, is the first key-policy Attribute-Based Encryption system in quantum version.

2. Quantum Key-Policy Atribute-Based Encryption

The qutrit [9] replaces the classical trit, and it is the unit of information in ternary quantum computing. A qutrit is represented as a unit vector in state space, which is a complex three-dimensional vector space (three-dimensional Hilbert space), H(3).

In the computing basis, the basis vectors (or the basis states) in H(3) using Dirac notation, are written: $|1\rangle, |2\rangle$ and $|3\rangle$, where $|1\rangle = (1,0,0)^T, |1\rangle = (0,1,0)^T$ and $|1\rangle = (0,0,1)^T$. An arbitrated vector $|H\rangle$ in H(3) can be expressed as a linear combination:

$$|\psi\rangle = c_1|1\rangle + c_2|2\rangle + c_3|3\rangle$$

where $c_1, c_1, c_1 \in \boldsymbol{C}$ and $|c_1|^2 + |c_2|^2 + |c_3|^2 = 1$.

The real number $|c_i|^2$ is the probability that the state vector $|\Psi\rangle$ be found in the basis of measurement *i*. As was said earlier, the proposed is based on the phenomenon of entanglement, an extraordinary quantum phenomenon, discovered in 1934 by Einstein-Podolsky-Rosen [10].

2.1. Definition and Classification of Entangled Quantum States

The proposed Quantum Key-policy Attribute-Based Encryption scheme will use different types of entanglement, and for the beginning, we will comment a little about them.

A mathematical description of the "entanglement" was offered by Werner in 1984 [11], extending the principle of inseparability: *If two systems interacted in the past, it is possible to find the whole system in a state which could not be written as an entanglement of state product*. This principle leads to a general definition of the entangled states.

A state $|\Psi\rangle$ is entangled or inseparable if and only if it cannot be written as a convex combination of state product:

$$\Psi^{AB} \neq \sum_i p_i \Psi_i^A \otimes \Psi_i^B$$

with $\sum_i p_i = 1$.

On the contrary, the bi-partite states that allow the factorization in the terms of a combination of state product are *separable*. The easiest example of the state separability is: $\Psi = \Psi^A \otimes \Psi^B$.

2.1.1. Bi-Partite Systems

Two quantum systems labeled *A* and *B* are in a quantum correlation - entangled - if the compound state Ψ^{AB} cannot be factorized as a sum of the state product:

$$\Psi^{AB} \neq \sum_i p_i \Psi_i^A \otimes \Psi_i^B$$

with $\sum_i p_i = 1$.

The compound state $|\Psi\rangle^{AB}$ is entangled if and only if it cannot be factorized in two separate states $|\Psi\rangle^A$ and $|\Phi\rangle^B$ respectively:

$$|\Psi\rangle^{AB} = |\Psi\rangle^A \otimes |\Phi\rangle^B$$

All the states $|\Psi\rangle^{AB}$ of the compound systems form a set S. Generally, these states are entangled, and very rarely are separable.

For example, for two two-level systems *1* and *2* whose states can be written in the orthonormal basis $\{|\uparrow\rangle, |\downarrow\rangle\}$, any of their compound state can be written in the bases with four orthogonal states $|\uparrow\uparrow\rangle, |\downarrow\downarrow\rangle, |\uparrow\downarrow\rangle, |\downarrow\uparrow\rangle$.

Together, these basis states generate a Hilbert four-dimensional space. However, these bases are not unique, other orthonormal bases, called *Bell bases*, are also possible, as follows:

$$\begin{cases} |\Psi^{\pm}\rangle = \dfrac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle \pm |\downarrow\uparrow\rangle) \\ |\Phi^{\pm}\rangle = \dfrac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle \pm |\downarrow\downarrow\rangle) \end{cases}$$

2.1.2. Tri-Partite Systems

The bi-partite entangled states can be extended to three parts. Similarly, we can define an entangled tri-partite state if and only if we cannot write it as the sum of products of the tri-partite state (Figure 1).

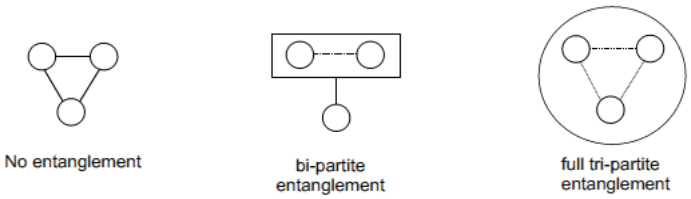

Figure 1. Types of entanglement in tri-partite systems

A state is called fully tri-partite entangled if and only if the decomposition:

$$\Psi = \sum_i p_i \Psi_i \text{ where } p_i \geq 0, \sum_i p_i = 1$$

exists for all the states Ψ_i and is factorizable in state products of at least two parts.

This definition excludes the totally separable states $\Psi = \Psi_A \otimes \Psi_B \otimes \Psi_C$ and the bi-partite states $\Psi = \Psi_{AB} \otimes \Psi_C$.

2.1.3. N-Partite Systems

Seevinck and Uffink [12] [13] extended the study for the case of *N* systems. Suppose we have an *N*-partite system described by a Hilbert space $H = H_1 \otimes H_2 \ldots \otimes H_N$.

A general state Ψ of this system is called fully *N*-partite entangled if and only if the following factorization:

$$\Psi = \sum_i p_i \Psi_i \text{ with } p_i \geq 0, \sum_i p_i = 1$$

exists for all the states Ψ_i and is factorizable in state products of at least *N* parts.

An example of an *N*-state which is fully *N*-partite entangled, is the generalized state Greenberger-Horne-Zeilinger:

$$\Psi_{GHZ}^N = \frac{1}{\sqrt{2}}(|\uparrow\uparrow \cdots \uparrow\rangle + |\downarrow\downarrow \cdots \downarrow\rangle)$$

An *N* - partite state is called *M* - partite entangled (M < N) if and only if there is a factorization as follows:

$$\Psi = \sum_i p_i \Psi_i^{K_1^{(1)}} \otimes \ldots \otimes \Psi_i^{K_{r_i}^{(i)}}$$

For each $i, K_1^{(1)}, \ldots, K_{r_i}^{(i)}$ are some partitions *{1,... ,N}* in a subset disjunction r_i, and each subset $K_j^{(i)}$ contains maximum *M* elements; but no factorization is possible when all these subsets contain less than *M* elements.

All *M* - partite entangled *N* - particles with M < N are called *non-fully entangled states* or *partially separable states*.

An example is the *N* - state which is made of *(N - 1)* - partite entangled, that is a tri-partite entangled state with four particles:

$$|\Psi\rangle = |\uparrow\rangle \otimes |\Psi_{GHZ}^3\rangle$$

2.2. Quantum Key-Policy Attribute-Based Encryption

Attribute-Based Encryption (ABE) has the main purpose to assure an access and security control. This can only be performed when the user and the server are in a field of confidence. Attribute-Based Encryption (ABE) takes a step forward and defines the receiver's identity by a set of attributes.

Consequently, the messages can be encrypted based on subsets of attributes (Key-policy ABE), or based on defined policies by sets of attributes (Cyphertext-policy ABE). Somebody should be able to decrypt an encrypted text when they possess a key with "proper attributes", the user keys being always sent by a trusted party (Figure 2).

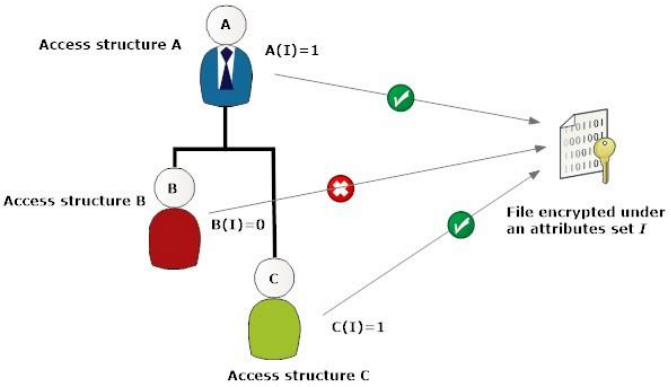

Figure 2. Key-Policy Attribute-Based Encryption scheme

Will be considered a Key-Policy Attribute-Based Encryption scheme, where the encrypted text is associated to a set of attributes, and a tree access structure (Figure 3) is associated to the user's decryption key. When the cyphertext with attributes satisfies the tree access structure, only the user can decrypt the cyphertext.

Were considered that Attribute-Based Encryption scheme is supervised by a Certification Authority (CA) who will have a defining role in the process of encryption/decryption.

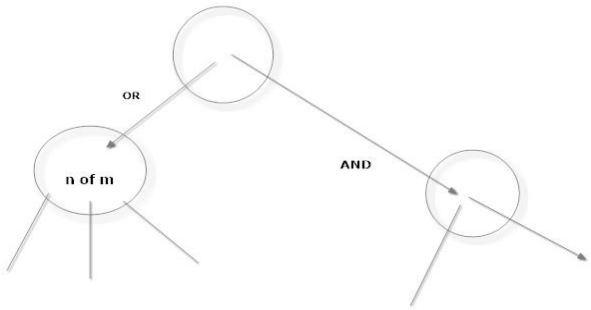

Figure 3. The access tree structure

In the proposed scheme, the text, the Certification Authority (CA) key, as well as the set of attributes are made of qutrits, and the AND and OR constructions from the tree access structure are made with the help of the entanglement performed among the qutrits. The study does not analyse the modality of obtaining the cryptographic keys, it presents the Key-Policy Attribute-Based Encryption (ABE) procedure in quantum version.

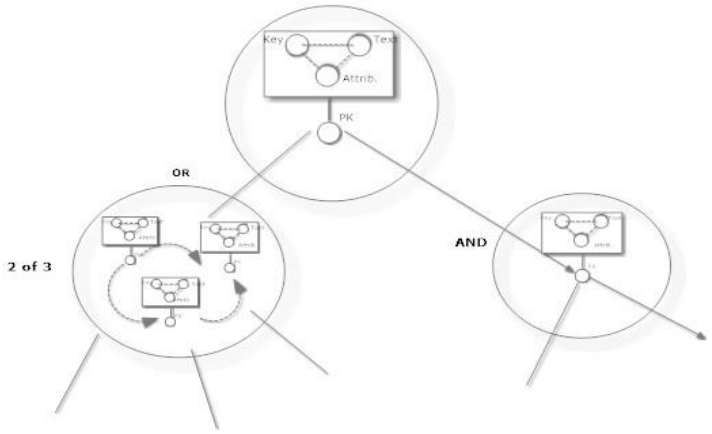

Figure 4. The Quantum Key-Policy Attribute-Based Encryption model

The stages of the scheme are the following (Figure 4):

1. *Keys generation*. The Certification Authority (CA) will generate a sequence of qutrits, half of which will form the secret key *S*, and the other half will form the public key *P*.
2. *Access structure generation*. To realise the access structure, the Certification Authority (CA) will make an entanglement GHZ (entangled three-particle states) between qutrits of attribute *A*, to link a piece of information to the other under the shape of a tree (the access tree).
3. *Text encryption*. To build the access rights, the text will be encrypted using a maximal entanglement of GHZ type among the qutrits of the secret key *S*, of the attribute existing in the access structure *A*, and of the text *T*. The entanglement previously resulted will be combined with a public key *P* (Figure 5).

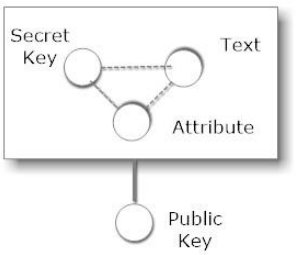

Figure 5. The encryption structures

The obtained state is:

$$|\Psi\rangle_{PSTA} = |\Psi\rangle_P \otimes |\Psi\rangle_{STA}$$

where:

$$|\Psi\rangle_P = \alpha|1\rangle_P + \beta|2\rangle_P + \gamma|3\rangle_P$$

with α, β, γ complex numbers satisfying the relation: $|\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1$, it is an attribute qutrit, and the state of GHZ entanglement is:

$$|\Psi\rangle_{STA} = \frac{1}{\sqrt{3}}(\alpha|111\rangle_{STA} + \beta|222\rangle_{STA} + \gamma|333\rangle_{STA})$$

The decryption implies the extraction of text qutrit *T*, and for this it is necessary to perform a projective measurement of the state $|\Psi\rangle_{PSTA}$ using Bell bases obtained from the attribute qutrit *A*, and of the public key *P*.

The generalized form of these Bell states is written as [14]:

$$|\Psi_{AB}\rangle^{mn} = \frac{1}{\sqrt{D}} \sum_{k=0}^{D-1} e^{\frac{2\pi imk}{D}} |k\rangle_A |(k-m)\ mod\ D\rangle_B$$

where *m, n* - enumerate states $|\Psi_{AB}\rangle^{mn}$, *k* - vectors of states *A, B* and *D* is the dimension of Hibert space associated to the quantum system.

Consequently, the 3^2 = 9 possible states where the system with the state $|\Psi\rangle_{PSTA}$ may collapse, are the following:

$$\frac{1}{3}|\Psi_{11}\rangle_{PA}(\alpha|11\rangle_{ST} + \beta|22\rangle_{ST} + \gamma|33\rangle_{ST})$$
$$\frac{1}{3}|\Psi_{12}\rangle_{PA}(\alpha|22\rangle_{ST} + \beta|33\rangle_{ST} + \gamma|11\rangle_{ST})$$
$$\frac{1}{3}|\Psi_{13}\rangle_{PA}(\alpha|33\rangle_{ST} + \beta|11\rangle_{ST} + \gamma|22\rangle_{ST})$$
$$\frac{1}{3}|\Psi_{21}\rangle_{PA}(\alpha|11\rangle_{ST} + e^{\frac{4\pi i}{3}}\beta|22\rangle_{ST} + e^{\frac{2\pi i}{3}}\gamma|33\rangle_{ST})$$
$$\frac{1}{3}|\Psi_{31}\rangle_{PA}(\alpha|11\rangle_{ST} + e^{\frac{2\pi i}{3}}\beta|22\rangle_{ST} + e^{\frac{4\pi i}{3}}\gamma|33\rangle_{ST})$$
$$\frac{1}{3}|\Psi_{22}\rangle_{PA}(\alpha|22\rangle_{ST} + e^{\frac{4\pi i}{3}}\beta|33\rangle_{ST} + e^{\frac{2\pi i}{3}}\gamma|11\rangle_{ST})$$
$$\frac{1}{3}|\Psi_{32}\rangle_{PA}(\alpha|22\rangle_{ST} + e^{\frac{2\pi i}{3}}\beta|33\rangle_{ST} + e^{\frac{4\pi i}{3}}\gamma|11\rangle_{ST})$$
$$\frac{1}{3}|\Psi_{23}\rangle_{PA}(\alpha|33\rangle_{ST} + e^{\frac{4\pi i}{3}}\beta|11\rangle_{ST} + e^{\frac{2\pi i}{3}}\gamma|22\rangle_{ST})$$
$$\frac{1}{3}|\Psi_{33}\rangle_{PA}(\alpha|33\rangle_{ST} + e^{\frac{2\pi i}{3}}\beta|11\rangle_{ST} + e^{\frac{4\pi i}{3}}\gamma|22\rangle_{ST})$$

These Bell bases obtained from the pairs *(P, A)* needed for the measurements of the leaves of the access tree are, also, part of the public key. We suppose that in the public key the Bell-based projection $|\Psi_{11}\rangle_{PA}$ is indicated. In this case, qutrits *T* and *S* will collapse in the state:

$$|\Psi\rangle_{ST} = \frac{1}{3}(\alpha|11\rangle_{ST} + \beta|22\rangle_{ST} + \gamma|33\rangle_{ST})$$

To measure the text qutrit *T*, the help of the Certification Authority (CA) who possesses the secret key *S* will be needed.

Mutually unbiased bases [15] [16] will be used to measure the state $|\Psi\rangle_{ST}$. They are obtained starting from the basis $\{|1\rangle, |2\rangle, |3\rangle\}$ by applying discrete Fourier transformations.
Were obtained:

1). Basis $\{|\varphi_1'\rangle, |\varphi_2'\rangle, |\varphi_3'\rangle\}$, where

$$|\varphi_1'\rangle = \frac{1}{\sqrt{3}}(|1\rangle + |2\rangle + |3\rangle)$$
$$|\varphi_2'\rangle = \frac{1}{\sqrt{3}}(|1\rangle + e^{2\pi i/3}|2\rangle + e^{4\pi i/3}|3\rangle)$$
$$|\varphi_3'\rangle = \frac{1}{\sqrt{3}}(|1\rangle + e^{4\pi i/3}|2\rangle + e^{2\pi i/3}|3\rangle)$$

2). Basis $\{|\varphi_1^{"}\rangle, |\varphi_2^{"}\rangle, |\varphi_3^{"}\rangle\}$:

$$|\varphi_1^{"}\rangle = \frac{1}{\sqrt{3}}(e^{2\pi i/3}|1\rangle + |2\rangle + |3\rangle)$$
$$|\varphi_2^{"}\rangle = \frac{1}{\sqrt{3}}(|1\rangle + e^{2\pi i/3}|2\rangle + |3\rangle)$$

$$|\varphi_3^{"}\rangle = \frac{1}{\sqrt{3}}(|1\rangle + |2\rangle + e^{2\pi i/3}|3\rangle)$$

3). Basis $\{|\varphi_1^{"'}\rangle, |\varphi_2^{"'}\rangle, |\varphi_3^{"'}\rangle\}$:

$$|\varphi_1^{"'}\rangle = \frac{1}{\sqrt{3}}(e^{4\pi i/3}|1\rangle + |2\rangle + |3\rangle)$$

$$|\varphi_2^{"'}\rangle = \frac{1}{\sqrt{3}}(|1\rangle + e^{4\pi i/3}|2\rangle + |3\rangle)$$

$$|\varphi_3^{"'}\rangle = \frac{1}{\sqrt{3}}(|1\rangle + |2\rangle + e^{4\pi i/3}|3\rangle)$$

Suppose that the basis chosen is $\{|\varphi_1'\rangle, |\varphi_2'\rangle, |\varphi_3'\rangle\}$, $|\Psi\rangle_{ST}$ can be expressed as follows:

$$|\Psi\rangle_{TS} = \frac{1}{3}[\frac{1}{\sqrt{3}}|\varphi_1'\rangle_S(\alpha|1\rangle_T + \beta|2\rangle_T + \gamma|3\rangle_T) + \frac{1}{\sqrt{3}}|\varphi_2'\rangle_S(\alpha|1\rangle_T + e^{-2\pi i/3}\beta|2\rangle_T + e^{-4\pi i/3}\gamma|3\rangle_T) +$$
$$+\frac{1}{\sqrt{3}}|\varphi_3'\rangle_S(\alpha|1\rangle_T + e^{-4\pi i/3}\beta|2\rangle_T + e^{-2\pi i/3}\gamma|3\rangle_T)]$$

If the result of the measurement will be $|\varphi_1'\rangle_S$, then the state $|\Psi\rangle_{ST}$ will collapse towards $\alpha|1\rangle_T + \beta|2\rangle_T + \gamma|3\rangle_T$, which represents the state of text qutrit *T*.

If the result of the measurement performed by the Certification Authority (CA) is $|\varphi_2'\rangle_S$, then the state $|\Psi\rangle_{ST}$ will collapse in $\alpha|1\rangle_T + e^{-2\pi i/3}\beta|2\rangle_T + e^{-4\pi i/3}\gamma|3\rangle_T$.

The text qutrit *T* will be reconstructed by applying the operator:

$$O_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e^{2\pi i/3} & 0 \\ 0 & 0 & e^{4\pi i/3} \end{pmatrix}$$

If the result of the measurement is $|\varphi_3'\rangle_S$, then the state $|\Psi\rangle_{ST}$ will collapse in $\alpha|1\rangle_T + e^{-4\pi i/3}\beta|2\rangle_T + e^{-2\pi i/3}\gamma|3\rangle_T$.

To obtain the text qutrit *T*, we apply the operator:

$$O_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e^{4\pi i/3} & 0 \\ 0 & 0 & e^{2\pi i/3} \end{pmatrix}$$

For the cases of the other projection bases is similar, to obtain the text qutrit *T* is necessary to apply one of the operators O_1 and O_2, respectively.

According to the attributes (from the access structure), users can obtain the information destined to them.

3. Security analysis

The security of the method is quantified by the easiness with which an intruder could decipher the text encrypted.

It can presume that an intruder tries to substitute the user of the system, the one whom the text is sent to. The intruder may use the public key to begin the decryption, but, unfortunately, he/she will need the help of Certification Authority to apply the private key.

The first obstacle met by the intruder will be the authentication with the Certification Authority (CA). Taking into account that the procedure of authentication is based on entanglement-swapping, it will be impossible for the intruder to trick the Certification Authority, which will lead to the failure of his/her plan.

However, the most unpleasant situation is when the authority proves to be dishonest.

In this case, the whole system is compromised, being necessary to replace the authority, and to restart the entire process..

4. Conclusion

In this paper, we present the first Quantum Key-Policy Attribute-Based Encryption scheme.

Starting from the classical scheme, were considered the information is encoded in qutrits and the generation of access structure is based on the phenomenon of entanglement. We believe that the proposed work can be considered a start for study the Key-Policy Attribute-Based Encryption scheme for quantum version.

The security of the quantum scheme is assured mainly by the existence of the quantum properties by the work with qutrits, any intervention over a tri-dimensional quantum system being easily discovered.

Furthermore, the schema proposes the use of an authentication between the Certification Authority (CA) and the user is based on entanglement swapping, and, different users' attribute private keys cannot be combined to give correct decryption, which avoids the collusion threat of different users.

References

[1] A Sahai and B Waters, "Fuzzy Identity-Based Encryption". *EUROCRYPT*, Aarhus. 2005: 457-473.
[2] V Goyal, O Pandey, A Sahai and B Waters. "Attribute-based encryption for fine-grained access control of encrypted data". *CCS'06*, New York. 2006: 89-98.
[3] J Bethencourt, A Sahai and B Waters. "Ciphertext-Policy Attribute-Based Encryption". *SP'07*. 2007: 321-334.
[4] AM Abbas, A Goneid and S El-Kassas. "Privacy Amplification in Quantum Cryptography BB84 using Combined Universal-Truly Random Hashing". *International Journal of Information and Network Security (IJINS)*. 2014; 3(2): 98-115.
[5] VK Jha and P Srivastava. "A Theoretical Model of Multi-user QKD Network as the Extension of E91 Protocol". *International Journal of Information and Network Security (IJINS)*. 2013; 2(4): 311-321.
[6] XH Li, FG Deng and HY Zhou. *Phys. Rev. A 78*. 022321. 2008.
[7] E Ghadafi. "Stronger security notions for decentralized traceable attribute-based signatures and more efficient constructions". *CT-RSA*, Springer. 2015: 391–409.
[8] D Huang, S Zhu, D Song and Y Guo. "Network Coding-Based Communications via the Controlled Quantum Teleportation". *Indonesian Journal of Electrical Engineering and Computer Science*. 2013; 11(2): 827-838.
[9] A Melikidze, VV Dobrovitski, HA De Raedt, MI Katsnelson and BN Harmon. "Parity effects in spin decoherence". *Physical Review B 70*. 014435. 2004.
[10] A Einstein, B Podolsky and N Rosen. "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?". *Physical Review*. 1935; 47: 777-780.
[11] RF Werner. "Quantum States with Einstein-Podolsky-Rosen Correlations Admitting a Hidden-Variable Model". *Physical Review A*. 1989; 40(8): 4277-4281.
[12] J Uffink. "The joint measurement problem". *International Journal of Theoretical Physics*. 1994; 33: 199-212.
[13] M Seevinck and G Svetlichny. "Bell-type inequalities for partial separability in N-particle systems and quantum mechanical violations". *Physical Review Letters 89*. 060401. 2002.
[14] XS Liu, GL Long, DM Tong and F Li. "Theoretically efficient high-capacity quantum-key-distribution scheme". *Physical Review A*. 2002; 65(3): id. 032302.
[15] ID Ivanovic. *Journal of Physics A: Math. Gen*. 1981; 14: 3241.
[16] WK Wootters. *Found. Physics*. 1986; 16: 391.