Ciphertext-Policy Attribute-Based Encryption using Quantum Multilevel Secret Sharing Scheme

Gabriela Mogos, *Member, IAENG*

***Abstract*—The current society, with a rapidly multiplying data volume, offered new valences and created new opportunities to develop cryptography. Public-key cryptosystems are the most important contribution of modern cryptography.**

Attribute-based encryption corresponds to the public key cryptography, and enables plain text access only if the user has all the attributes which the original text was encrypted with. There are two types of Attribute-based encryption: Key-Policy Attribute-Based Encryption and Ciphertext-Policy Attribute-Based Encryption.

The basic idea of Ciphertext-policy Attribute-based encryption scheme is that a cryptotext is associated to an access policy. In Ciphertext-Policy Attribute-Based Encryption the authorization is included in the encrypted data, and only users who satisfy the associated policy can decrypt the data. Data can be encrypted without knowing the number of users who can decrypt, but only specifying the policy enabling the decrypt.

This paper proposes a quantum version of a Ciphertext-Policy Attribute-Based Encryption method. Our version is conceptually close to the classical one, dealing with quantum multilevel secret sharing scheme to encrypt quantum states and with access structures, for decryption.

***Index Terms*—qubit, attributes, quantum secret sharing scheme.**

I. Introduction

In all areas, information and data must be confidential and the access to them must be controlled and restricted to protect against risks such as: data loss; unfair competition; errors that threatening the activity of the company; others' inappropriate use, etc.

The security of a company means not only the access to the information inside the company, but also the access from outside the company by malicious people or by the competition. The security of the access to information is an important aspect to be considered in case of implementation of a data sharing solution [18].

In Ciphertext-policy Attribute-based encryption (CP-ABE) scheme, the basic idea is that a cryptotext is associated to an access policy. Each decryption key is connected to a set of attributes. The users will be able to access the information only if the set of attributes associated to their secret key satisfies the cryptotext access policy. Restricting the users to get access to the data is called access policy.

The Ciphertext-policy Attribute-based encryption scheme (fig.1) includes 4 steps: *Setup, Encryption, Key Generation* and *Decryption*.

Each step is presented as follows:

1) *Setup*. A security parameter and the number of attributes are used to obtain the master key and the private key. The master key is used to generate the private key, and the public key (public parameter) is used in encryption.
2) *Key Generation*. By using the master key and the set of user attributes describing the key, the secret key is generated.
3) *Encryption*. The text is encrypted under the access tree structure. The public key, and the specific access structure are used to obtain a ciphertext.
4) *Decryption*. For the ciphertext decryption, the public key and the private key specific to the set of attributes are used. The ciphertext is decrypted when the set of attributes satisfies the access structures.

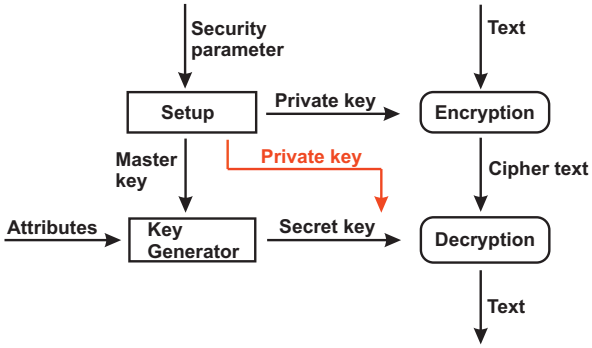

Fig. 1. The Ciphertext-Policy Attribute Based Encryption scheme.

The concept of Ciphertext-policy Attribute-based encryption was proposed by Goyal et al.[10], in 2006. The first scheme of Ciphertext-policy Attribute-based encryption was presented in 2007 by Bethencourt et al.[1]. Cheung and Newport [3] demonstrated the security of Ciphertext-policy Attribute-based encryption scheme where the AND gates of the access tree had positive and negative attributes. This scheme was subsequently improved by Nishide et al.[15] and Emura et al.[5], introducing multi-value attributes.

In 2008 and 2009, respectively, Goyal et al.[10] and Liang et al.[13] proposed a bounded tree structure, proving how easily Key-policy Attribute-based encryption can be transformed into Ciphertext-policy Attribute-based encryption, by using the so-called universal access tree.

Different types of access tree structure have been proposed: a general access tree structure [12]; an access control by a linear secret sharing scheme matrix over the attributes [22]; an access tree which supporting AND gates without bilinear pairings [23], etc.

This paper introduces a quantum analog of classical Ciphertext-policy Attribute-based encryption method and shows how the multilevel secret sharing scheme can be integrated into it.

The paper is organized as follows: Section II is a short introduction on quantum secret sharing scheme, Section III

Manuscript received January 11, 2018; revised August 16, 2018.

G. Mogos is with the Prince Sultan University, College for Women, Riyadh, KSA, e-mail: gabi.mogos@gmail.com.

proposes our Ciphertext-policy Attribute-based encryption scheme featuring the encoding and decoding of secrets, Section IV presents some aspects of the security of the proposed scheme and Section V gives concluding remarks.

II. Quantum secret sharing

A classical sharing scheme consists in dividing a secret in sub-secrets and distributing them to a number of users. The secret can be reconstructed only by certain groups of users, a priori established, forming the (authorised) access structure of the sharing scheme.

Secret sharing schemes were introduced independently by Blakley [2] and Shamir [17], as a solution for storing cryptographic keys. Blakley method considers the secret as a point in the *N*-dimensional hyperplane space, and Shamir proposes the polynomial interpolation method to find the secret.

The classic schemes present two types of sets of participants: authorised - who can reconstitute the secret together, and unauthorised - those who cannot reconstitute the secret. The family of authorised sets is called *access structure*. Several access structures are proposed in the literature.

Simmons [19] introduced the multilevel and compartmented scheme to model the secret recovery in certain practical situations where accountability is not uniformly distributed on the set of all participants.

In the multipartite access structure, a set of participants is organized on levels, and each participant on the same level has the same role inside the access structure. The levels create a hierarchical structure. All the participants on a certain level *i* can recover the secret.

A hierarchical access structure is a multipartite access structure, where a threshold *k* is assigned to each level l_i, and the secret can be reconstructed when there are at least *k* users belonging to all the levels lower or equal to l_i. The access structure can be seen as a graph. This graph is structured on levels, like a tree (fig.2).

On the *(k, n)* threshold secret sharing protocol there are *n* participants and each will receive parts of the secret, so that any *k* participants can recover the secret (i.e. they are authorised), and a number of participants lower than *k* will not be able to obtain any secret information. To improve the efficiency of the secret sharing scheme, the ramp secret sharing scheme was proposed [21].

In *(k, L, n)* ramp secret sharing scheme, the secret can be decrypted by *k* parties, but a number of *k-L* or lower of parties can obtain no information.

Quantum secret sharing is the quantum version of the classical secret sharing protocol, where a dealer distributes a secret to a set of participants, and only certain sub-sets of participants can collaborate to recover it.

The quantum version of the secret sharing scheme was proposed by Hillery [11] and Gottesman [8], and consists in the fact that the secret is encoded in the multipartite quantum state. Each participant in the protocol receives a subpart of the quantum system. The secret can be reconstituted by the collaboration of some of the participants.

Cleve et al.[4] proposed an efficient construction of all threshold schemes and introduced the quantum access structure. Adam Smith [20] studied in detail the quantum access structure to design a quantum secret sharing, Gheorghiu [6] offered a systematic way to determine the access structure, while Gottesman [9] defined a maximal quantum access structure.

The quantum ramp secret sharing scheme was proposed by Ogawa et al. [16]. In weighted threshold secret sharing scheme, a positive value is assigned to each user, and the secret can be reconstructed only if the sum of all values assigned to the users exceeds a certain threshold [14]. The proposed scheme uses an access structure.

An access structure is a hierarchical structure when the set of all the attributes associated to the information is divided in disjoint levels. For example, level *i* contains n_i attributes. The users who possess the same attributes are called users of the same type (e.g. for a company they can be: the manager(s), the assistant manager(s), the accountant(s), the administrator(s), etc).

In a classical Ciphertext-policy Attribute-based encryption scheme, a ciphertext is generated by encrypting a message under an access policy, which is defined over attributes.

In our Ciphertext-policy Attribute-based encryption scheme, the text encryption is performed by a multilevel secret sharing scheme. Consequently, the information is partitioned in subsets placed on different access levels, according to their importance. The access structure has the form of a graph state.

III. Quantum Ciphertext-policy Attribute-based encryption scheme

The basic idea of Ciphertext-policy Attribute-based encryption scheme is that a cryptotext is associated to an access policy. Each decryption key is connected to a set of attributes. The users will be able to access the text only if the set of attributes associated to their secret key satisfies the access policy of the ciphertext. The access control scheme is supervised by an authority.

The paper presents a quantum analog of classical the Ciphertext-policy Attribute-based encryption scheme, where the information is encoded by bi-dimensional quantum systems, qubits.

The scheme proposes to use the multilevel quantum secret sharing method in the encryption and decryption processes. The scheme works as follows:

1) An authority needs to establish a specific access control policy to a quantum secret. Therefor, the authority divides the secret in subparts (partial secrets), attaches an attribute to each partial secret, and creates a hierarchical structure on levels according to the importance of their content. The implementation of the multilevel secret sharing scheme consists in the implementation of a sequence of independent threshold schemes on each level [7].
2) The authority assigns a secret key to each user. According to the type of user, the key will be calculated based on the attributes, in order to satisfy the access tree of the secret (partial secrets).
3) The proposed model uses for encryption the multilevel secret sharing scheme based on a sequence of independent threshold schemes on each level. A threshold *k* is associated to each access level. The family of authorised sets is called *access structure*.

The access to information is made according to the user attributes. The users can access certain parts of information only if their decryption key contains attributes satisfying the respective access policy.

The implementation of the secret sharing scheme for an access structure on multiple levels can be performed as follows:

1) The first (k_1, L_1, n_1) threshold scheme (L_1 scheme) for the level l_1 is conceived, where k_1 is the threshold, representing the number of attributes which can enable the access, L_1 is the number of quantum states from the information of the level, n_1 is the number of attributes corresponding to level l_1. This corresponds to the first level of the access structure.
2) The (k_2, L_2, N_2) threshold scheme (L_2 scheme) for level l_2 is built as an extension of l_1.
3) The (k_3, L_3, N_3) threshold scheme (L_3 scheme) for level l_3 is constructed as an extension of l_2.
4) The process continues up to the threshold scheme (L_n scheme) for level l_n, and is constructed by extending the threshold scheme of level l_{n-1}.

A. Construction of Shares

For the (k, L, n) threshold secret sharing scheme, Ogawa et al.[16] and Zhang et al.[24] show that the encoding of a quantum secret may be performed by using unique values $x, y \in \mathbb{Z}_d$, and, a quantum secret $|s_1, ..., s_L\rangle$ can be transformed into:

$$\frac{1}{\sqrt{d^{k-L}}} \sum_{c \in C} |f_c(x_1), ..., f_c(x_n)\rangle \tag{1}$$

where d is dimensional complex linear spaces, $C = \{(c_1, ...c_k) \in \mathbb{Z}_d | \forall i \in \{1, ..., L\}, c_i = s_i\}$ is the set of polynomial coefficients 2^{nd} over $\mathbb{Z}_d$.

To establish a specific access control policy, the authority divides the secret in partial secrets and attaches attributes to each. Then, the authority holds the partial secrets on levels (fig.2), starting from level *1*, a general access level, to the highest level, where a small number of users have access.

There are users who can access the information from many levels. The implementation of multilevel secret sharing scheme means the implementation of a sequence of independent threshold schemes on each level.

Given the (k_1, L_1, n_1) threshold secret sharing scheme corresponding to level *1*, where L_1 is the number of quantum systems forming the secret, k_1 is the number of attributes which need to be satisfied to access the secret, n_1 is the total number of attributes assigned to the secret (forming the access structure). The polynomial associated to the scheme is the following:

$$f_c(x)|_1 = c_{1,1} + c_{2,1}x_1^1 + ... + c_{k-1,1}x_1^{k-1} \tag{2}$$

Let us consider a level l where $L = 2, k = 3, n = 4$ and d is a prime number representing the dimension of complex linear space. The quantum secret on the level l (partial secret) s has d^L dimensions.

According to the schemes proposed by Shamir, Ogawa et al. and Zhang et al., we consider the values $x = |x_1, ..., x_n\rangle \in \mathbb{Z}_{11}$ and $y = |y_1, ..., y_L\rangle \in \mathbb{Z}_{11}$, the dimension of complex linear space $d = 11$, and, the secret s selected as an arbitrary element from $\mathbb{Z}_{11}$.

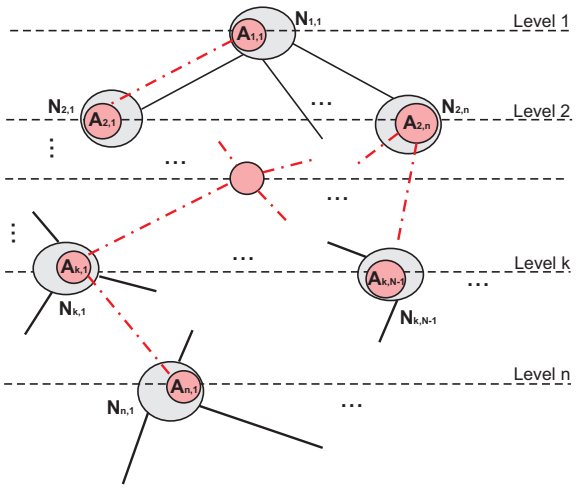

Fig. 2. Multi-level structure of the access tree ($A_{i,l}$-attributes per level, $N_{i,l}$-quantum systems per level).

A polynomial of 2^{nd} degree is generated, with coefficients in $\mathbb{Z}_{11}$: $f(x) = c_0 + c_1x^1 + c_2x_1^2$.

For example, we choose the public values $x = |2, 1, 5, 9\rangle \in \mathbb{Z}_{11}$ and $y = |1, 3\rangle \in \mathbb{Z}_{11}$. The quantum secret has $d^L = 11^2 = 121$ dimensions.

Given the secret $x = |1, 9\rangle \in \mathbb{Z}_{11}$, the set of coefficients of the polynomial of 2^{nd} degree was determined, for which $f(|y\rangle) = |s\rangle$ over $\mathbb{Z}_{11}$.

$$A = \{(0,0,1), (4,6,2), (4,2,6), (7,9,7), (1,6,5), (2,1,9), (5,8,10), (6,3,3), (8,4,0), (10,5,8), (9,10,4), (6,3,3), (8,4,0), (10,5,8), (9,10,4)\} \tag{3}$$

The polynomial is evaluated for each set of coefficients in $x = |2, 1, 5, 9\rangle \in \mathbb{Z}_{11}$. Given the coefficients $(0, 0, 1)$, we calculate $mod 11$:

$$\begin{aligned} 0 + 0 \cdot 2 + 1 \cdot 4 &= 4 \\ 0 + 0 \cdot 1 + 1 \cdot 1 &= 1 \\ 0 + 0 \cdot 5 + 1 \cdot 25 &= 3 \\ 0 + 0 \cdot 9 + 1 \cdot 81 &= 4 \end{aligned} \tag{4}$$

The state obtained is $|4, 1, 3, 4\rangle \in \mathbb{Z}_{11}$.

For the entire set C of coefficients, the encoding of the secret s was obtained by the following superposition:

$$\begin{aligned} |\Psi\rangle = \frac{1}{\sqrt{11}}(&|4,1,3,4\rangle + |2,1,7,0\rangle + |10,1,10,2\rangle + \\ &+ |9,1,7,6\rangle + |0,1,2,9\rangle + |7,1,1,3\rangle + |6,1,9,7\rangle + \\ &+ |2,1,8,1\rangle + |5,1,6,0\rangle + |8,1,4,10\rangle + |1,1,5,5\rangle) \end{aligned} \tag{5}$$

B. Secret Reconstruction

Only a certain set of attributes assigned to the secret key enables the access to all the information on each level. More specifically, in order to gain access to information, a certain attribute must satisfy the access tree.

Using the independent *(k, L, n)* threshold secret sharing scheme to rebuild the secret *s*, the number of parts must be equal to the threshold *k*. The interpolation method is used by applying Vandermonde matrix.

Given the system of linear equations:

$$\begin{aligned} &c_0 + c_1 x_{1,1} + .. + c_{k-1} x_{1,k-1}^{k-1} = y_1 \\ &c_0 + c_1 x_{2,1} + .. + c_{k-1} x_{2,k-1}^{k-1} = y_2 \\ &\cdots \\ &c_0 + c_1 x_{k-1,1} + .. + c_{k-1} x_{k-1,k-1}^{k-1} = y_{k-1} \end{aligned} \quad (6)$$

Using matrices, the system of equations can be written as follows:

$$\begin{pmatrix} 1 & \cdots & x_{1,k-1}^{k-1} \\ \vdots & \ddots & \vdots \\ 1 & \cdots & x_{k-1,k-1}^{k-1} \end{pmatrix} \begin{pmatrix} c_1 \\ \vdots \\ c_{k-1} \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_{k-1} \end{pmatrix} \quad (7)$$

where $V = \begin{pmatrix} 1 & \cdots & x_{1,k-1}^{k-1} \\ \vdots & \ddots & \vdots \\ 1 & \cdots & x_{k-1,k-1}^{k-1} \end{pmatrix}$ is Vandermonde matrix.

To rebuild the secret, i.e. the values of the polynomial coefficients, the following formula should be applied:

$$\begin{pmatrix} c_1 \\ \vdots \\ c_{k-1} \end{pmatrix} = \begin{pmatrix} 1 & \cdots & x_{1,k-1}^{k-1} \\ \vdots & \ddots & \vdots \\ 1 & \cdots & x_{k-1,k-1}^{k-1} \end{pmatrix}^{-1} \begin{pmatrix} y_1 \\ \vdots \\ y_{k-1} \end{pmatrix} \quad (8)$$

$$\begin{pmatrix} c_0 & \cdots & c_{k-1} \end{pmatrix} = \\ = \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ x_{1,k-1}^{k-1} & \cdots & x_{k-1,k-1}^{k-1} \end{pmatrix}^{-1} \begin{pmatrix} y_1 & \cdots & y_{k-1} \end{pmatrix} \quad (9)$$

In our case, for $k = 3$, $x = |2,1,5,9\rangle \in \mathbb{Z}_{11}$, the Vandermonde matrix *M* has the following form:

$$M_{(2,1,5)} = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 1 & 5 \\ 2^2 & 1^2 & 5^2 \end{pmatrix} mod 11 = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 1 & 5 \\ 4 & 1 & 3 \end{pmatrix} \quad (10)$$

with $M \cdot M^{-1} = I$, where *I* = unitary matrix.

It is verified that:

$$\begin{pmatrix} 4 & 1 & 3 \end{pmatrix} M_{(2,1,5)}^{-1} = \begin{pmatrix} 4 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 2 & 1 & 5 \\ 4 & 1 & 3 \end{pmatrix} = \\ = \frac{1}{10} \begin{pmatrix} 4 & 1 & 3 \end{pmatrix} \begin{pmatrix} -2 & -2 & 4 \\ 3 & -1 & -3 \\ -2 & 3 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \end{pmatrix} \quad (11)$$

Consequently, having the coefficients of the polynomial of 2^{nd} degree, the secret $f(|1,3\rangle) = |1,9\rangle \in \mathbb{Z}_{11}$ was rebuilt. The original secret has now been reconstructed in the first 3 qubits. Also, the procedure can be done without the threshold *k*.

C. Multiple levels access

The entire secret is divided in partial secrets, which are distributed on *N* levels, polynomials associated with all the *N*-schemes corresponding to the levels, as follows:

$$\begin{cases} f_c(|x_i\rangle)|_1 = |s_i\rangle|_1 \\ \vdots \\ f_c(|x_i\rangle)|_N = |s_i\rangle|_N \end{cases} \quad (12)$$

where $i = \overline{1,n}$.

What happens if the user has the permission to access multiple levels? In this case, the user will access a total information calculated as the concatenation of all partial secrets belonging to the user access levels.

Assuming a user has access to level 1, level 2 and level 3, the information after decryption is obtained by concatenating the secrets of levels 1, 2 and 3:

$$|S\rangle_{1,2,3} = |s\rangle_1 \otimes |s\rangle_2 \otimes |s\rangle_3 = |s\rangle_1 |s\rangle_2 |s\rangle_3 = |s_1 s_2 s_3\rangle \quad (13)$$

D. Security of the scheme

In Ciphertext-policy Attribute-based encryption scheme, each secret key is associated to a set of attributes, and an access structure on attributes is associated to each ciphertext. The decryption is performed if and only if the user's set of attributes satisfies the ciphertext access structure.

Traditional secret sharing schemes assume that the arbiter is an accountable third party; however, a dishonest arbiter may send incorrect attributes to the users, components from which the secret will not be reconstructed. High levels of confidentiality and accountability must be ensured to keep users' secret keys in a unique and well-guarded location, where a single failure is enough. In addition, it is also very important to prevent the loss or the exposure of the keys.

Ciphertext-policy Attribute-based encryption based on quantum multilevel secret sharing scheme has the advantage of offering encryption for level and inter-level, the attributes being defined so that any type of user may be distinguished from the others, because there are also users who use combinations of attributes for decryption.

IV. Conclusions

This paper proposes a Ciphertext-policy Attribute-based encryption scheme based on quantum multilevel secret sharing scheme. The model uses for encryption the multilevel secret sharing scheme based on a sequence of independent threshold schemes on each level, and for decryption a set of attributes associated to the secret key. Thereby, the quantum secret sharing scheme is based on its classical analogue, the secret is encoded into evaluations of polynomials and a decoding method, the secret can be reconstructed given any k shares. The security of this proposal remains an open problem.

References

[1] J. Bethencourt, A. Sahai, and B. Waters, "The cpabe toolkit", http://acsc.csl.sri.com/cpabe/.

[2] G. R. Blakley, "Safeguarding cryptographic keys", *National Computer Conference*, volume 48 of American Federation of Information Processing Societies Proceedings, pp.313-317, 1979.

[3] L. Cheung, C. C. Newport, "Provably secure ciphertext policy abe", *ACM Conference on Computer and Communications Security*, pp.456-465, 2007.

[4] R. Cleve, D. Gottesman, H. K. Lo, "How to share a quantum secret", *Physical Review Letters*, 83(3), pp.648-651, 1999. DOI 10.1103/PhysRevLett.83.648.

[5] K. Emura, A. Miyaji, A. Nomura, K. Omote, M. Soshi, "A ciphertext-policy attribute-based encryption scheme with constant ciphertext length", *Lecture Notes in Computer Science*, vol.5451, pp.13-23, Springer, Heidelberg, 2009.

[6] V. Gheorghiu, B. C. Sanders, "Accessing quantum secrets via local operations and classical communication", *Physical Review A*, 88, 022340, 2013.

[7] H. Ghodosi, J. Pieprzyk, and R. Safavi-Naini, "Secret Sharing in Multilevel and Compartmented Groups", *Lecture Notes in Computer Science*, Information Security and Privacy Third Australasian Conference, ACISP'98, pp.367-378, 1998
[8] D. Gottesman, "Theory of quantum secret sharing", *Physical Review A*, 61(4), 042, 311, 2000. DOI 10.1103/ PhysRevA.61.042311.
[9] D. Gottesman, "Theory of Quantum Secret Sharing", *Physical Review A, 61, 042311*, 2000.
[10] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute Based Encryption for Fine-Grained Access Control of Encrypted Data", *ACM Conference on Computer and Communications Security (ACM CCS)*, 2006.
[11] M. Hillery, V. Buzek, and A. Berthiaume, "Quantum Secret Sharing", *Physical Review A*, 59, 1829, 1999.
[12] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, W. Jonker, "Mediated Ciphertext-Policy Attribute-Based Encryption and Its Application", *International Workshop on Information Security Applications*, pp.309-323, 2009.
[13] X. Liang, Z. Cao, H. Lin, D. Xing, "Provably secure and efficient bounded ciphertext policy attribute based encryption", *Proceedings of the 2009 ACM Symposium on Information, Computer and Communications Security - ASIACCS 2009*, Sydney, Australia, 2009.
[14] P. Morillo, C. Padro, G. Saez, J. L. Villar, "Weighted threshold secret sharing schemes", *Information Processing Letters 70*, pp. 211-216, 1999.
[15] T. Nishide, K. Yoneyama, K. Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures", *Lecture Notes in Computer Science*, vol.5037, pp.111-129, Springer, Heidelberg, 2008.
[16] T. Ogawa, A. Sasaki, M. Iwamoto, H. Yamamoto, "Quantum secret sharing schemes and reversibility of quantum operations", *Physical Review A*, 72(3), 032,318, 2005. DOI 10.1103/PhysRevA.72.032318.
[17] A. Shamir, "How to share a secret", *Communications of the ACM*, 22(11):612-613, 1979.
[18] W. R. Simpson, "Secure Identity for Enterprises", *IAENG International Journal of Computer Science*, vol. 45, no.1, pp.142-152, 2018.
[19] G. Simmons, "How to (Really) Share a Secret", Advances in Cryptology – Proceedings of CRYPTO '88, vol. 403 of *Lecture Notes in Computer Science*, pp.390-448, Springer-Verlag, 1990.
[20] A. Smith, "Quantum Secret Sharing for General Access Structures", e-print quant-ph/0001087.
[21] H. Yamamoto, "Secret sharing system using (k, l, n) threshold scheme", *Electronics and Communications in Japan*, 69(9), pp.46–54, 1986. DOI 10.1002/ecja.4410690906.
[22] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization", *Cryptology ePrint Archive*, Report 2008/290, 2008.
[23] J. Zhang, F. Zhang, "Linear threshold verifiable secret sharing in bilinear groups", *International Journal of Grid and Utility Computing*, Vol. 4, Nos. 2/3, pp.212-218, 2013
[24] P. Zhang, R. Matsumoto, "Quantum Strongly Secure Ramp Secret Sharing", *Quantum Information Processing*, arXiv:1404.5749v3, 2014.

Gabriela Mogos (M'2009) is from Romania. She received her MSc in Computer Science and BSc. in Physics from Alexandru Ioan Cuza University of Iasi, Romania. She earned her PhD in Informatics in 2010 at Alexandru Ioan Cuza University of Iasi, Romania. Her research interests are driven by a strong desire to bridge computer science and quantum physics and to design new quantum algorithms and quantum cryptographic protocols. Also, her interest was directed in embedding the quantum-safe equipment in large networks, simultaneously with the development of the software applications, to gradually replace the existing classical equipment which becomes vulnerable.

Dr. Gabriela Mogos has over 40 publications, 4 books, and she was main investigator and co-investigator in international and national research projects. She is IAENG, IEEE and IET Member.