First Steps Towards Post-Quantum Attribute-Based Encryption

Victoria Aguilar Díaz
MACIMTE, U. Rey Juan Carlos
C\Tulipán, s\n, 28933 Móstoles, Madrid.
v.aguilard.2019@alumnos.urjc.es

María Isabel González Vasco
MACIMTE, U. Rey Juan Carlos
C\Tulipán, s\n, 28933 Móstoles, Madrid.
mariaisabel.vasco@urjc.es

***Abstract*—Today, both industry and academia doubtless agree on the need for cryptographic constructions withstanding attacks from adversaries which have (some kind of) access to quantum computing resources. Currently, the NIST standarization process for so-called *post-quantum* tools for encryption and signatures is reaching its final phase; maybe due to this fact, there is increasing interest in finding new quantum-resistant versions for a plethora of cryptographic designs. In this paper, we briefly survey the basic topics involved in a potential post-quantum proposal for attributed based encryption, giving an intuitive presentation of the topic and concluding with the sketch of a few informal ideas towards a construction based on codes.**

***Index Terms*—post-quantum cryptography, attribute-based encryption, code-based encryption.**

I. Introduction

Traditional constructions of Public Key Encryption (PKE) schemes are designed in order to restrict the decryption ability to a certain legitimate user (characterized by its knowledge of a secret key). However, with the emergence of complex application scenarios, a need of designing encryption systems allowing for a more fine-grained decryption arbitrage has arose. For instance, distributed systems require access control structures for encrypted data, which is stored in external servers that could be corrupted. On of the main tools for addressing this problem are so-called *Attribute-Based Encryption (ABE) schemes*. In an ABE scheme, users private keys and/or ciphertexts are linked to a set of descriptive attributes, so that each ciphertext can only be decrypted by those users holding the right set of attributes. The first ABE construction was proposed by Sahai and Waters in [25].

In the literature, three different types of ABE can be found, depending on the type of access control they allow for: Key-Policy Attribute-Based Encryption (KP-ABE), Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and Multi-Authority Attribute-Based Encryption (MA-ABE). The main difference between KP-ABE and CP-ABE lies in whether the access policy is linked with the private key (KP) or with the ciphertext (CP). In turn, MA-ABE, achieves similar functionalities without the assumption that a unique external server must be trusted for creating and storing secret keys (which is needed in general for CP-ABE and KP-ABE).

Sooner or later, quantum computers will indeed be a serious threat to many cryptographic systems that currently protect our communications. When this happens, we will need some new quantum-safe cryptographic systems. The area of *Post-Quantum* Cryptography focuses on the search of such new systems, assuming that honest users are still classical, and thus quantum adversaries (to some extent) still interact classically with the system.

In order to derive post-quantum constructions, it is crucial to base the security of a cryptographic design on a computational problem which is not known to be solved easily by quantum algorithms. A few areas have been identified as most promising to this respect: Hash-Based Cryptography, Multivariate Cryptography, Isogeny-Based Cryptography, Code-Based Cryptography and Lattice-Based Cryptography [11]. In this note, we briefly discuss our first steps towards deriving post-quantum ABE schemes. To this aim, we briefly review the basics of ABE, and sketch some ideas towards code-based post-quantum ABE, using as starting point a post-quantum Identity Based Encryption Scheme (IBE) proposed by Gaborit et al [11] at Crypto 2017.

II. Attribute-Based Encryption: Classical Constructions

ABE schemes are constructed under different assumptions matching a wide variety of application scenarios (see, for instance, the classification of ABE from [21]). As mentioned in the introduction, in this note we will stick to the traditional classification based on the type of access control of the scheme, giving raise to three variants: Ciphertext-Policy Attribute-Based Encryption (CP-ABE), Key-Policy Attribute-Based Encryption (KP-ABE) and Multi-Authority Attribute-Based Encryption (MA-ABE). We provide a brief description of each of these schemes.

A KP-ABE scheme is built with respect to a finite attribute universe (AT), which we assume to be publicly known. It involves a (trusted) authority $\mathcal{A}$, interacting with several users from a finite set $\mathcal{U}$ through four algorithms/processes (all assumed to be polynomial time):

1) $\mathsf{Setup}(\lambda)$: Executed by $\mathcal{A}$, given a security parameter $\lambda \in \mathbb{N}$, outputs a master key pair $(MPK,\ MSK)$. It is assumed that the master public key MPK is made accessible to all users in $\mathcal{U}$ while only $\mathcal{A}$ holds MSK.
2) $\mathsf{Key.Gen}(MSK,\mathcal{P})$: Executed by $\mathcal{A}$, given MSK and a policy $\mathcal{P}$ (which can be understood as a collection of designated sets of attributes), outputs a corresponding secret key $SK_{\mathcal{P}}$.
3) $\mathsf{Encrypt}(MPK,M,\mathsf{at})$: Executed by a sender on input a message M, the master public key MPK and an attribute set at, outputs ciphertext CT.
4) $\mathsf{Decrypt}(MPK,SK_{\mathcal{P}},CT)$: Executed by a user on input CT, MPK, and $SK_{\mathcal{P}}$, outputs M (provided that the policy $\mathcal{P}$ is consistent with $SK_{\mathcal{P}}$) or $\perp$.

The first construction of this type was proposed in 2006 by Goyal et al. in [13]. In this scheme, they achieved an encryption tool with fine-grained access control, in which only users complying with the designated access policy, will be able pass through the decryption mechanism. Each key policy is defined as a tree access structure in which each node consist of AND or OR gate, and the leaves are the different attributes. Thus, any set of attributes that satisfy the tree can decrypt a ciphertext. After that, other constructions have been proposed, recent examples are those of 2011 by Attrapadung et al. [2], or the one by J.Han et al. [15], proposed in 2012. The first one describes a KP-ABE scheme allowing for *non-monotonic access structures* (that is, may contain negated attributes) and with constant ciphertext size. The second proposal follows the structure of a KP-ABE but it is a decentralized scheme.

A. Ciphertext-Policy ABE

The main disadvantage of KP-ABE is that the access policy is built into the users private key, so senders have less control on who can actually decrypt. Moreover, a trusted authority is assumed to handle (generate and store) secret keys. Thus, if this authority is compromised, data confidentiality will be compromised in the same way. Finally, these schemes can be affected by collusion attacks, where users collide in order to (jointly) decrypt messages they should not be able to decrypt individually. In order to overcome these hardships, CP-ABE was introduced from different set-up assumptions.

In 2007 Bethencourt et al. [4] introduced the notion Ciphertext-Policy ABE. At this, data confidentiality is preserved even if the trusted authority is compromised. In a CP-ABE scheme, the private key will be labeled with a set of attributes, and a concrete access policy will be linked directly with each ciphertext. As a result, a user will only be able to decrypt the ciphertext if his attributes satisfy the ciphertext's access policy.

As in the case of KP-ABE, a CP-ABE scheme consists on four algorithms/processes as follows:

1) Setup: Executed by an authority $\mathcal{A}$, takes as input the security parameter and outputs a master public key MPK and a master secret key MSK.
2) Key.Gen(MSK,at): Executed by $\mathcal{A}$, takes as input the master secret key MSK and a set of attributes $\mathsf{at} \subseteq \mathsf{AT}$. It outputs a private key SK_{at}.
3) Encrypt(MPK,M,$\mathcal{P}$, AT): Executed by the data owner, takes as input the public key MPK, a message M, and an access policy $\mathcal{P}$ over the universe of attributes AT. Outputs a ciphertext CT (which can be assumed to implicitly contain the policy $\mathcal{P}$).
4) Decrypt(MPK,CT,SK_{at}): Executed by a user holding the secret key SK_{at}, takes as input the master public key MPK and a ciphertext CT (linked to an access policy $\mathcal{P}$). If the set at of attributes satisfies the access policy $\mathcal{P}$, it outputs a message M (otherwise, it outputs an error message).

The main and most recent weakness related to CP-ABE is that so-called *temporal attributes* are not well handled by this scheme. Temporal attributes are those used in dynamic environments, in which attributes may change over time. Furthermore, this scheme is also not very suitable for dealing with the problem of attribute-user revocation without relying on an authority [1]. As in the KP-ABE schemes, trusting an authority raises again in a security problem, and CP-ABE schemes have to deal with the collusion attack problem in the same way. There exists recent works [35], [28], [19], [7], [14] with which it is pretended to solve that drawbacks.

B. Waters CP-ABE.

As an illustrative (classical, surely vulnerable to quantum adversaries) example, look at the work of Brent Waters [31]. Waters develops an ABE construction reducing its security proof to the hardness of solving the so-called Decisional Parallel Bilinear Diffie-Hellman Exponent (PBDHE) problem (see the paper for more information). In his scheme, he uses an access structure over the ciphertext, implementing this way a policy on the set of attributes. During Setup, a group $\mathcal{G}$ of prime order p and generator g are chosen. Then, a random set of elements of $\mathcal{G}$ is selected, each linked to a concrete attribute. Finally, two exponents α, a are chosen uniformly at random, defining a corresponding bilinear map. The public key consists then of generator g, the bilinear map, g^a and the set mentioned before, while the master secret key is the group element g^α. In the encryption step, once an access structure for the set of attributes is defined, a ciphertext for a given message is constructed from the public key and this access structure. More precisely, this access structure consists on a matrix M and a function ρ in that way that the function ρ associates each row of M with an attribute. The Key.Gen algorithm generates a secret key for a selected user set of attributes using the master secret key. Then, the Decrypt algorithm takes the secret key and the ciphertext with its access structure. Using the reconstruction method linked to the reconstruction phase in the related linear secret sharing scheme, it decrypts and rebuild the message.

The security proof of this scheme is based on reducing the problem of breaking it to that of solving the PBDHE problem, e.g., if the decisional PBDHE assumption holds, then a polynomial time adversary will never be able to break the system. As PBDHE is considered a hard computational problem, the security of the scheme is established.

C. Multi-Authority ABE

An effective form to minimize the trusting problem of single KP-ABE and CP-ABE is to replace the single authority with multiple ones for disjoint attributes management, yielding a Multi-Authority ABE (MA-ABE) scheme. Indeed, it is much harder for an adversary to compromise data confidentiality if sensitive information is stored in a distributed manner. The first construction of MA-ABE was made by Chase in 2007 [6], and it builds on top of a KP-ABE generic design. In this scheme, senders are forced to specify for each authority k a set of attributes monitored by a central authority and a (threshold) parameter d_k. A ciphertext may then only be decrypted by a user if he has at least d_k attributes associated to each authority. Moreover, two variants are proposed. One allows the sender to determine how many attributes are required by each authority for each ciphertext, while the other asks him to specify a number D such that

a user can only access to decryption step if he has enough attributes from at least D authorities.

The main drawback of MA-ABE are again collusion attacks; indeed, a set of non-authorized users should not be able to combine their secret keys to decrypt a ciphertext. To prevent these type of attacks, two requirements must be met: on one hand every user must have a Global Identifier (GID), and further, a central authority must generates each secret key on input the corresponding GID. Nevertheless, this central authority can be corrupted, so trusting it could be a serious drawback. There are some recent works trying to solve these problems, such as [36], [9], [33] and [18] which use pseudorandom functions shared among the multiple authorities to randomize users' GIDs.

III. ATTRIBUTE-BASED ENCRYPTION: POST-QUANTUM PARADIGM

The security of all classic public key cryptosystems are primarily based on the difficulty of solving certain number theoretic problems, which will no longer be secure once quantum computing is possible. As a result, the need of finding another problems not solved presently even with quantum computers arises. The most promising areas of cryptography used to develop quantum-resistant algorithms are Hash-Based Cryptography, Multivariate Cryptography, Isogeny-Based Cryptography, Code-Based Cryptography and Lattice-Based Cryptography (see [5, 17]). In this note, we restrict our attention to Code-Based Cryptography, which seems more akin to ABE constructions.

In this section, we propose some ideas to construct a post quantum ABE scheme based on codes. In order to understand the basics of cryptographic constructions based on codes, we need to briefly review the fundamentals of coding theory.

A. Code-based cryptography

Let us start with some very basic definitions from Coding Theory.

Definition III-A.1 (Linear Code). A $[n,k]_q$ linear code $\mathcal{C}$ is a linear subspace over $\mathbb{F}_q$ of length n and dimension k. The elements of the code are called *codewords*.

If $q=2$ we say that it is a binary code, an then it usually omits the subscript q saying this is a $[n,k]$ linear code. Thus, a codeword of a q-ary code is a string of n bits.

The *weight* of a codeword is the number of its elements that are nonzero and the *distance* between two codewords is the Hamming distance between them, similarly, the *support* of a codeword $c \in \mathcal{C}$ is the set of positions in which the non-zero elements appear and is denoted $supp(c)$.

Definition III-A.2 (Minimum Distance). The minimum distance of a linear code $\mathcal{C}$, denoted d_{min}, is the minimum distance of its codewords:

$$d_{min} = min_{c\in\mathcal{C}, c\neq 0} w_H(c).$$

Definition III-A.3 (Generator matrix and parity-check matrix). Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a linear code of dimension k. If $G \in \mathbb{F}_q^{k\times n}$ is a basis matrix of $\mathcal{C}$, i.e.,

$$\mathcal{C} = \{\mathbf{uG} : \mathbf{u} \in \mathbb{F}_q^k\},$$

then we say that $\mathbf{G}$ is a *Generator Matrix* for $\mathcal{C}$. Therefore, $\mathcal{C}$ has an encoding map $f : \mathbb{F}_q^k \to \mathbb{F}_q^n$, which is $\mathbf{u} \to \mathbf{uG}$. If $\mathcal{C}$ is the kernel of a matrix $\mathbf{H} \in \mathbb{F}_q^{(n-k)\times k}$, i.e.,

$$\mathcal{C} = ker(\mathbf{H}) = \{\mathbf{v} \in \mathbb{F}_q^n : \mathbf{Hv^T} = 0\}$$

then we say that $\mathbf{H}$ is a *Parity-Check Matrix* of $\mathcal{C}$. It follows that $\mathbf{GH}^T = 0$.

One of the most relevant family of codes in cryptography are so-called *error-correcting-codes*. An error-correcting code (ECC) is an encoding scheme that transmits messages in such a way that the message sent can be recovered even if there are transmission errors, as long as they are somehow limited. There are two main categories within ECC:

1) **Block codes**: act on fixed-size blocks (packets) of bits or symbols of predetermined size. Practical block codes can generally be hard-decoded in polynomial time (with respect to block length), i.e., block codes are typically decoded with so called *hard-decision decoders*, using a special dedicated algorithm [23].
2) **Convolutional codes**: act on bit or symbol strings of arbitrary length.

Finally, we briefly summarize here some of the main computational problems in coding theory. The majority of the computational problems in coding theory are related to the decoding procedure, that is, to the problem of efficiently retrieving encoded information from a noisy observation.

Problem (Minimum Distance Decoding (MDD)). Let $\mathcal{C}$ be a $[n,k]_q$ linear code. Given a received word $\mathbf{r}$ and an integer w, find a codeword $\mathbf{c} \in \mathcal{C}$ such that $d_H(\mathbf{r}, \mathbf{c}) \leqslant w$. If no such codeword exists in $\mathcal{C}$, output $\perp$.

Problem (Computational Syndrome Decoding (CSD)). Let $\mathcal{C}$ be a $[n,k]_q$ linear code. Given a $(n-k)\times k$ parity-check matrix $\mathbf{H}$ for $\mathcal{C}$, a syndrome $\mathbf{s} \in \mathbb{F}_q^{n-k}$ and an integer $w > 0$, find a word $\mathbf{e} \in \mathbb{F}_q^n$ such that $\mathbf{He^T} = \mathbf{s}$ and $w_H(\mathbf{e}) \leqslant w$. If no such word exists, output $\perp$. $\mathbf{s}$ is said to be the *syndrome* of a word $\mathbf{e}$.

Problem (Minimum Distance Problem (MDP)). Let $\mathcal{C}$ be a $[n,k,d_{min}]_q$ linear code. Given an integer $w > 0$, find a codeword $\mathbf{c} \in \mathcal{C}$ such that $w_H(\mathbf{c}) = w$. If no such codeword exists in $\mathcal{C}$, output $\perp$.

In a seminal work by Vardy (see [29]) it is proven that the decision problem associated to MDP is actually NP-complete. Furthermore, for many reasons decoding linear codes is a fundamental problem in coding theory and many cryptographic systems have as a result been constructed from related decoding problems in linear codes. It is considered a very hard problem in general and most encodings are not known to have an efficient decoding procedure. The first general decoding algorithm proposed in this context was Plain Information-Set Decoding (Plain-ISD) algorithm, proposed by McEliece in [20]. But there exists more recent algorithms currently used. Some examples are Stern's Algorithm [27], Finiasz-Sendrier decoding [10] or Ball-Collision Decoding [3]. They are all super-polynomial and provide helpful information towards fixing parameters in real implementations.

Error-correcting-codes are particularly useful for exploiting the hardness of decoding problems in public key cryptog-

raphy, as the correction method sometimes allows for the construction of a trapdoor – linked to a secret key for decoding/decrypting (see, for instance [5], [24]). The first code-based Public Key cryptosystem was proposed by McEliece in 1978 [20] using binary Goppa codes. This kind of cryptosystem is suitable for use in multi-user communication networks, but has an important disadvantage, the key size. In 1986 Niederreiter published a variant of McEliece's scheme using so-called Generalized Reed-Solomon codes, trying to improve on McElieces' proposal (see [22]). At this, he presented some improvements concerning to encryption and decryption cost, and also introduced a generic method to reduce the size of public keys in code-base schemes. However, a few years later some cryptanalysis techniques as [26] in 1992 and [32] in 2010 were published and Niederreiter scheme was broken. Nevertheless, McEliece cryptosystem still remains unbroken for general cases, and there is no hope for finding significant improvements in cryptanalysis through quantum computation. As a result, code-based cryptosystems are considered as reliable candidates for post-quantum PKE schemes, despite the (still unsolved) issue of large key sizes. It is worth noting that if we check out the list of works that have passed to the round three of NIST Post-Quantum Cryptography Standardization, we can view a work based on codes. That work is the classic McEliece scheme. Then, it supposes a little confirmation that Code-Based Cryptography is a suitable option for constructing Post-Quantum PKE schemes. For these reasons, the cryptographic community has not stopped putting forward new code-based constructions, such as [30]. In 2016 Yongge Wang proposed a PKE scheme based on Random Linear Code-Based cryptography. This scheme is thought to be secure against currently existing attacks over code-based cryptosystems, as filtration and algebraic attacks.

IV. Towards new Post-Quantum ABE from Coding Theory

A reasonable starting point towards a post-quantum ABE is trying to adapt an existing post-quantum IBE, in the same fashion as it is done in the papers [8], [34] and [16].

A. Gaborit's IBE

In [11], Gaborit et al. put forward a new PKE scheme and an IBE scheme based on so-called *Rank Metric problems*. In a nutshell, the PKE proposals are based on the hardness of decoding a random linear code without a trapdoor function generated with the code. Then, an IBE scheme is proposed, from the assumption that it is hard to actually decode without that trapdoor.

Gaborit et al.'s construction adapts a signature scheme named RankSign [12], to construct the trapdoor function in order to transform his PKE design in an IBE. To this aim, a trapdoor function f_A associated to a matrix A is defined as follows:

$$f_A : \mathbb{F}_{q^m}^{n-k} \times \mathbb{F}_{q^m}^{n} \to \mathbb{F}_{q^m}^{n} \quad (s, e) \longmapsto sA + e$$

The matrix A will be generated with a trapdoor T in such a way that from a random $p \in \mathbb{F}_{q^m}^{n}$, T may be recover the tuple $(s, e) = f_A^{-1}(p)$, where e is a word and s its syndrome. This is done following the same ideas behind RankSign, which uses to this aim a family of codes with an efficient decoding algorithm based on LRPC decoding one. LRPC decoding algorithm takes as input the parity-check matrix H of a code, a trapdoor T and a syndrome s, that is the hash value of some string (for example the hash of an identity in the IBE of Gaborit), and output the word corresponding to that syndrome, satisfying $s = He$. As a result, this solves an instance of the so-called Rank-Metric Syndrome Decoding problem (formally defined below). Thus, applying RankSign with a trapdoor like we just defined, we can generate a secret key as described in Gaborit IBE, that is, a syndrome corresponding to a user identity.

As mentioned above, this decoding algorithm solves a variant of the syndrome decoding problem for the rank metric. Then, systems such as of Gaborit's, base its security in the Rank-Metric Syndrome Decoding Problem (RSD), which we can formulate as follows:

Problem (Rank-Metric Syndrome Decoding Problem). Let H be a full-rank $(n-k) \times n$ matrix over $\mathbb{F}_{q^m}$ with $k \leqslant n$, $s \in \mathbb{F}_{q^m}^{n-k}$ and w an integer. Find $x \in \mathbb{F}_{q^m}^{n}$ such that $rank(x) = w$ and $Hx = s$.

We can sketch Gaborit et al's IBE proposal as follows:

Let RankPKE.Enc and RankPKE.Dec the encryption and decryption algorithms from Gaborit et al's PKE (RankPKE). Let $\mathcal{H}$ be a hash function assume to behave as a random oracle.

1) IBE.Setup(d): choose a tuple of parameters (n, m, k, d, t) linked to (a hard instance of the) RSD problem. Now, the keys will be derived from a the triplet of matrices $(P, (R|H), Q)$ where H is a parity-check matrix of an $[n, k]$-code of weight d over $\mathbb{F}_{q^m}$, R is chosen at random from $\mathbb{F}_{q^m}^{(n-k)\times t}$, and P, Q are chosen at random from $GL_{n+t}(\mathbb{F}_q)$. Let A be a full-rank $(k+t) \times (n+t)$ matrix over $\mathbb{F}_{q^m}$ such that $H^{'} A^T = 0$ with $H^{'} = P(R|H)Q$, and set $T := (P, Q)$. Let G be a generator matrix of a public code $\mathcal{C}^{'}$ which can decode efficiently. Return $mpk = (A, G)$ and $msk = T$.
2) IBE.KeyDer(mpk, msk, id): compute $p = \mathcal{H}(id)$ and $(s, e) = f_A^{-1}(p)$ using the trapdoor T. Store (id, s) and return s as secret key for id.
3) IBE.Enc(id, mpk m): with p, return
$$c = RankPKE.Enc((A, p, G), m).$$
4) IBE.Dec(s, c): return $RankPKE.Dec(s, c)$.

Summing up, during the set up phase, the scheme generates a parity-check matrix H' from another parity-check matrix H with a set of three random matrices P, R and Q, Then, decoding the hash of the identity of a user with the trapdoor as in [12], the secret key for this identity is obtained. Finally, it encrypts and decrypts as in RankPKE.

B. Ideas Towards ABE

Now, we can take the first steps in order to construct a CP-ABE scheme based on codes. Our main first idea is to use some mechanism, as a Secret Sharing (SS) scheme, to split the public and secret keys of our ABE scheme into as many shares as attributes we decide. In this way, when generating his secret key, each user will obtain as many shares as correct attributes

he holds (if we shall mimic Gaborit's approach, the syndrome s would be the secret to share). In addition, the set of shares could be linked with a threshold value that will control the minimum of attributes that have to be owned in order to decrypt. Then, messages are encrypted in such a way that only users holding a sufficient number of correct attributes may retrieve the secret key and decrypt. The question now is how to design an efficient key generation algorithm compatible with such strategy. Another idea could be to use Secret Sharing in a similar manner, but for distributing the trapdoor T itself in shares.

V. Final Remarks

With the emergence of quantum computing, code-based cryptography seems to hold promise for the development of ABE schemes. We think it is a reasonable goal to try to construct an ABE scheme on the basis of an IBE scheme based on codes. Still, a lot remains to be done towards this goal. One possible way to get a middle-point solution would be to consider different limitations to the adversarial quantum resources (such as bounding his memory or limiting his quantum-access to the random oracles involved).

Acknowledgements

We are grateful to Javier Herranz for sharing his insight and experience in the topic and helping us identifying relevant related papers. We are also grateful for the anonymous referees from the RECSI Progam Committee. M.I.G.V.'s work is funded by the NATO Science for Peace and Security Programme, grant number G5448 and by MINECO under Grant MTM2016-77213-R.

References

[1] Ruqayah R Al-Dahhan et al. "Survey on revocation in ciphertext-policy attribute-based encryption". In: *Sensors* 19.7 (2019), p. 1695.

[2] Nuttapong Attrapadung, Benoît Libert, and Elie De Panafieu. "Expressive key-policy attribute-based encryption with constant-size ciphertexts". In: *International Workshop on Public Key Cryptography*. Springer. 2011, pp. 90–108.

[3] Daniel J Bernstein, Tanja Lange, and Christiane Peters. "Smaller decoding exponents: ball-collision decoding". In: *Annual Cryptology Conference*. Springer. 2011, pp. 743–760.

[4] John Bethencourt, Amit Sahai, and Brent Waters. "Ciphertext-policy attribute-based encryption". In: *2007 IEEE symposium on security and privacy (SP'07)*. IEEE. 2007, pp. 321–334.

[5] Johannes Buchmann and Jintai Ding. *Post-Quantum Cryptography: Second International Workshop, Proceedings*. Vol. 5299. Springer Science & Business Media, 2008.

[6] Melissa Chase. "Multi-authority attribute based encryption". In: *Theory of Cryptography Conference*. Springer. 2007, pp. 515–534.

[7] Hui Cui et al. "Key Regeneration-Free Ciphertext-Policy Attribute-Based Encryption and Its Application". In: *Information Sciences* (2020).

[8] Vanesa Daza et al. "Extensions of access structures and their cryptographic applications". In: *Applicable Algebra in Engineering, Communication and Computing* 21.4 (2010), pp. 257–284.

[9] Enting Dong et al. "Large universe multi-authority attribute-based PHR sharing with user revocation". In: *International Journal of Computational Science and Engineering* 19.3 (2019), pp. 376–386.

[10] Matthieu Finiasz and Nicolas Sendrier. "Security bounds for the design of code-based cryptosystems". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2009, pp. 88–105.

[11] Philippe Gaborit et al. "Identity-based encryption from codes with rank metric". In: *Annual International Cryptology Conference*. Springer. 2017, pp. 194–224.

[12] Philippe Gaborit et al. "RankSign: an efficient signature algorithm based on the rank metric". In: *International Workshop on Post-Quantum Cryptography*. Springer. 2014, pp. 88–107.

[13] Vipul Goyal et al. "Attribute-based encryption for fine-grained access control of encrypted data". In: *Proceedings of the 13th ACM conference on Computer and communications security*. 2006, pp. 89–98.

[14] Dezhi Han, Nannan Pan, and Kuan-Ching Li. "A traceable and revocable ciphertext-policy attribute-based encryption scheme based on privacy protection". In: *IEEE Transactions on Dependable and Secure Computing* (2020).

[15] Jinguang Han et al. "Privacy-preserving decentralized key-policy attribute-based encryption". In: *IEEE Transactions on Parallel and Distributed Systems* 23.11 (2012), pp. 2150–2162.

[16] Javier Herranz, Fabien Laguillaumie, and Carla Ràfols. "Constant size ciphertexts in threshold attribute-based encryption". In: *International Workshop on Public Key Cryptography*. Springer. 2010, pp. 19–34.

[17] Kateryna Isirova and Oleksandr Potii. "Requirements and Security Models for Post-Quantum Cryptography Analysis". In: *Proceedings of the PhD Symposium at 13th International Conference on ICT in Education, Research, and Industrial Applications*. 2017, pp. 36–41.

[18] Jiguo Li et al. "A decentralized multi-authority ciphertext-policy attribute-based encryption with mediated obfuscation". In: *Soft Computing* 24.3 (2020), pp. 1869–1882.

[19] Huijie Lian, Qingxian Wang, and Guangbo Wang. "Large Universe Ciphertext-Policy Attribute-Based Encryption with Attribute Level User Revocation in Cloud Storage". In: *International Arab Journal of Information Technology* 17.1 (2020), pp. 107–117.

[20] R. J. McEliece. "A Public-Key Cryptosystem Based On Algebraic Coding Theory". In: *Deep Space Network Progress Report* 44 (1978), pp. 114–116.

[21] Saravana Kumar Na, Rajya Lakshmi GV, and Balamurugan Ba. "Enhanced Attribute Based Encryption for Cloud Computing." In: *Procedia Computer Science* 46 (2015), pp. 689–696.

[22] Harald Niederreiter. “Knapsack-type cryptosystems and algebraic coding theory”. In: *Problems of Control and Information Theory* 15.2 (1986), pp. 159–166.

[23] Kennedy Offor. “Performance analysis of soft-decision and hard-decision decoding for error dependent power saving Viterbi decoder for mobile devices”. In: *International Journal of Engineering Research & Technology* 1 (June 2012).

[24] Raphael Overbeck and Nicolas Sendrier. “Code-based cryptography”. In: *Post-quantum cryptography*. Springer, 2009, pp. 95–145.

[25] Amit Sahai and Brent Waters. “Fuzzy identity-based encryption”. In: *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2005, pp. 457–473.

[26] Vladimir M Sidelnikov and Sergey O Shestakov. “On insecurity of cryptosystems based on generalized Reed-Solomon codes”. In: *Discrete Mathematics and Applications* 2.4 (1992), pp. 439–444.

[27] Jacques Stern. “A method for finding codewords of small weight”. In: *International Colloquium on Coding Theory and Applications*. Springer. 1988, pp. 106–113.

[28] Yi-Fan Tseng, Chun-I Fan, and Chih-Wen Lin. “Provably Secure Ciphertext-Policy Attribute-Based Encryption from Identity-Based Encryption.” In: *Journal of Universal Computer Science* 25.3 (2019), pp. 182–202.

[29] A. Vardy. “The intractability of computing the minimum distance of a code”. In: *IEEE Transactions on Information Theory* 43 (1997), pp. 1757–1766.

[30] Yongge Wang. “Quantum resistant random linear code based public key encryption scheme RLCE”. In: *2016 IEEE International Symposium on Information Theory (ISIT)*. IEEE. 2016, pp. 2519–2523.

[31] Brent Waters. “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization”. In: *International Workshop on Public Key Cryptography*. Springer. 2011, pp. 53–70.

[32] Christian Wieschebrink. “Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes”. In: *International Workshop on Post-Quantum Cryptography*. Springer. 2010, pp. 61–72.

[33] Xixi Yan et al. “Privacy-preserving multi-authority attribute-based encryption with dynamic policy updating in PHR”. In: *Computer Science and Information Systems* 16.3 (2019), pp. 831–847.

[34] Mark Zhandry. “Secure identity-based encryption in the quantum random oracle model”. In: *International Journal of Quantum Information* 13.04 (2015), p. 1550014.

[35] Leyou Zhang et al. “Hidden ciphertext policy attribute-based encryption with fast decryption for personal health record system”. In: *IEEE Access* 7 (2019), pp. 33202–33213.

[36] Xiao Zhang et al. “Multi-authority attribute-based encryption scheme with constant-size ciphertexts and user revocation”. In: *Concurrency and Computation: Practice and Experience* 31.21 (2019), e4678.