A New Code-Based Cryptosystem

Fedor Ivanov[1](✉), Grigory Kabatiansky[2], Eugeny Krouk[3],
and Nikita Rumenko[1]

[1] National Research University Higher School of Economics, Moscow, Russia
fivanov@hse.ru
[2] Skolkovo - Institute of Science and Technology (Skoltech), Moscow, Russia
[3] National Research University Higher School of Economics, Moscow, Russia

Abstract. Unlike most papers devoted to improvements of code-based cryptosystem, where original Goppa codes are substituted by some other codes, we suggest a new method of strengthening which is code-independent. We show (up to some limit) that the security of the new code-based cryptosystem is much closer to the hardness of maximum likelihood decoding than in the original McEliece cryptosystem.

Keywords: McEliece cryptosystem · Code-based cryptography · Key size reduction · Information-set decoding · Maximum likelihood decoding · Bounded distance decoding

1 Introduction

In 1976 W. Diffie and M. Hellman proposed the concept of public-key cryptography concept [1]. To construct this public-key cryptosystem one needs to construct a one-way trap-door function. To achieve this, a hard computational problem should be selected, which nevertheless has simple solutions in some special cases. It is supposed that an eavesdropper who desires to "break" the system, i.e. compute the correspondent plaintext from a given ciphertext, has to solve this hard problem, while a legitimate user, using the corresponding private key, obtains the simple special instance of the hard problem and solves it for decryption.

However, to break the system one may not search for a solution to the hard problem being used, but tries to recover hidden secrets or to construct an equivalent system that produces the same encryption-decryption instead. If the construction of an equivalent system is computationally feasible, this leads to breaking the system without solving the initial hard problem. Such an attack on Merkle-Hellman cryptosystem [2] was given by A. Shamir [3], and in code-based cryptography the most famous analogous example of attack was given in [4] to break McEliece cryptosystem [5] based on modified Reed-Solomon codes proposed in [6].

McEliece cryptosystem is the oldest and most popular code-based cryptosystem. It was proposed in 1978 and it uses irreducible Goppa codes [7]. It relies

M. Baldi et al. (Eds.): CBCrypto 2020, LNCS 12087, pp. 41–49, 2020.
https://doi.org/10.1007/978-3-030-54074-6_3

on NP-hardness of *maximum likelihood decoding* (*MLD* for short) for general linear codes, i.e., the hardness of finding the nearest codeword regarding the Hamming distance for a given received vector [24]. Since there are some classes of codes such as Reed-Solomon (RS), Bose–Chaudhuri–Hocquenghem (BCH), Goppa, Low-Density Parity-Check (LDPC) codes that have polynomial-time decoding algorithms, they can be used in the construction of the corresponding trap-door function. The main idea underlying in the McEliece cryptosystem is to hide a given structured code with a simple decoding algorithm (secret key), hence presenting it as a random code (open key) for which a simple decoder is unknown. The main point of our improvement is the following. The security of the McEliece cryptosystem is not based on the NP-hardness of the MLD problem, since in the frame of the McEliece cryptosystem only errors of weight up to $d/2$ must be corrected, where d is the minimal code distance of the underlying code. Such algorithms are called *half minimal distance decoding*, or *HMD decoding*. Note that it is unknown if HMD decoding is NP-hard (or not). The best known estimates for the complexity of HMD decoding can be found in [9,10]. We hence propose a new cryptosystem, that relies more on the hardness of the MLD problem than the original McEliece cryptosystem. For the best estimates of the complexity of ML (i.e., minimum distance) decoding see [11].

There is no known effective quantum algorithm to break the McEliece cryptosystem but nevertheless it gains no wide practical usage mainly because of the very large size of its public key. For example, in the original paper by McEliece [5] the public key has size of order 250 Kbits.

There were many attempts to attack or to improve the original McEliece cryptosystem, see [12]. The main idea for improvements is to substitute the original Goppa code that is used in McEliece cryptosystem with some other code with a specific structure that allows to reduce the key size. For instance in [13] Goppa codes were substituted by subfield subcodes of quasi-cyclic generalized Reed-Solomon codes. Similar instances based on QC-LDPC codes and LDGM codes (Low-Density Generator Matrices) were proposed in [15–21].

Also it should be mentioned that there are some frameworks for code-based cryptography, where authors do not only exchange the secret code within the McEliece cryptosystem. For instance, see [22–25].

The new code-based cryptosystem proposed in this paper forces the eavesdropper to correct seemingly random errors and gives another way to shrink public key sizes due to shorter codes.

The structure of the paper is the following: we start from the standard McEliece cryptosystem, then we describe a "prototype" cryptosystem which has nice mathematical structure but unfortunately provides gain compared with the original McEliece, and finally we propose a new scheme with better parameters.

2 McEliece Cryptosystem

2.1 Design

In the following we recall how the McEliece cryptosystem works. There are two users Alice and Bob, where Bob wants to send a k bit message m to Alice. Alice takes a $k \times n$ generator matrix G of some linear (n, k)-code C with the minimal code distance $d(C) \geq 2t + 1$, which has an efficient decoding algorithm Φ, correcting t errors. The matrix G is a secret, known only to Alice, and the code C is called the *secret code*.

Alice constructs a *public* matrix $G_{pub} = SGP$, where a $k \times k$ nonsingular matrix S and a $n \times n$ permutation matrix P are chosen randomly from the corresponding ensembles and they are also keeping as secrets.

Bob sends to Alice the following *ciphertext* y

$$y = mG_{pub} + e, \tag{1}$$

where e is a vector of weight t which is *randomly* generated by Bob. Alice reveals the message m by the following chain of simple calculations:

$$y' := yP^{-1} = mG_{pub}P^{-1} + eP^{-1} = m'G + e', \tag{2}$$

where $m' = mS, \quad e' = eP^{-1}$ and $wt(e') = wt(e) = t$, since P is a permutation matrix. Then Alice applies the decoding algorithm Ψ to the vector $y' = m'G + e'$ and receives $\Psi(y') = m'$ and finally finds $m := m'S^{-1}$.

Any other user will deal either with the problem of correcting t errors of a random looking linear code C_{pub} with generator matrix G_{pub} or with the problem of reconstructing the code structure from its public-key matrix, these attacks are called *structural attacks*. In the original paper [5] irreducible Goppa codes [7] were chosen as the family of codes for the scheme. In particular, it was suggested to use Goppa code of length $n = 1024$ dimension $k = 524$ and minimum distance $d = 101$, hence $t = 50$.

Later H. Niederreiter proposed a cryptosystem [6], which is based on solving a syndrom equation and in some sense is dual to the McEliece scheme. These two schemes have equivalent security [26] and we restrict our consideration to the McEliece type schemes.

2.2 Decoding Attacks on McEliece Cryptosystem

An attacker (or eavesdropper) $\mathcal{E}$ve tries to find a vector $\hat{e}$ such that

$$y - \hat{e} \in C_{pub}. \tag{3}$$

If $\hat{e} = e$ then (3) holds and $\mathcal{E}$ finds the message m from $mG_{pub} = y - \hat{e}$.

Note that for $\hat{e} \neq e$ the Eq. (3) does not hold. Indeed, let $y - \hat{e} \in C_{pub}$. Since $y - e \in C_{pub}$ we have that $e - \hat{e} \in C_{pub}$. The *public* code C_{pub} is equivalent to the code C, therefore its distance $d(C_{pub}) \geq 2t + 1$, but $wt(e - \hat{e}) \leq wt(e) + wt(\hat{e}) = 2t$ and hence $\hat{e} = e$.

In the worst case $\mathcal{E}$ve must try $\binom{n}{t}(q-1)^t$ vectors $\hat{e}$ over $\mathbb{F}_q$, and on average it takes half of this value, which is nevertheless a huge number for any reasonable code parameters.

Much more effective is the attack based on *Information Set Decoding* (ISD). This attack was already mentioned in the initial security analysis of McEliece [5] and further developed in numerous papers, see [12] and references there. There are different interpretations and modifications of the initial ISD algorithm. Several different improvements have been proposed, such as ball-collision decoding [12] and improvements based on generalized birthday approaches. For instance, in paper [9] the complexity of ISD was reduced to $\tilde{\mathcal{O}}(2^{0.054n})$ and in [10] the complexity exponent is $\tilde{\mathcal{O}}(2^{0.0494n})$ which is the currently the best result.

In the following we recall the basic properties of ISD algorithms. Goal of ISD algorithms is to recover the message m from a given vector $y = m\hat{G} + e$, where $\hat{G}$ is a generator matrix of an (n,k) code $\hat{C}$ with minimal distance $d \geq 2t+1$ and $wt(e) \leq t$.

Let I be a k-subset of the coordinates set $[n] := \{1, 2, \ldots, n\}$ such that I is an information set of $\hat{C}$ and $\hat{G}_I$ be the submatrix of $\hat{G}$ consisting of columns indexed by I. In the same way let e_I be the vector consisting of coordinates of the vector e indexed by I. ISD algorithms work in the following way:

1. Randomly choose an information set I.
2. Find a codeword $\hat{c}$ such that $\hat{c}_I = y_I$
3. Check if $wt(\hat{c} - y) = t$. If Yes then output the message corresponding to the codeword $\hat{c}$. Else return to Step 1.

Observe that, if one assumes that the support of the error vector is disjoint from the information set, then the corresponding probability P_k that chosen k coordinates are error-free is

$$P_k = \frac{\binom{n-t}{k}}{\binom{n}{k}} = \frac{\binom{n-k}{t}}{\binom{n}{t}}, \tag{4}$$

and hence the the average number of required iterations is of order $\dfrac{\binom{n}{t}}{\binom{n-k}{t}}$, which is significantly less than the complexity of the brute-force attack.

In the next section we will describe a "prototype" of a new cryptosystem.

3 The "Prototype" Code-Based Cryptosystem

Let C be a linear (n,k)-code with the minimum distance $d(C) \geq 2t+1$, which has an efficient decoding algorithm Φ, correcting t errors. We also assume that C belongs to some rather big family of codes (like Goppa codes in the original McEliece cryptosystem). Alice takes $k \times n$ generator matrix G of this code C. The matrix G as well as the code C are secrets, known only to Alice, and we call code C is called the *secret code*.

Alice constructs *two* public matrices, namely $G_{pub} = GM$, where M is a randomly chosen $n \times n$ non-singular matrix, and $E_{pub} = (C_n + P)M$, where P is a randomly chosen $n \times n$ permutation matrix and C_n is $n \times n$ matrix which rows are codewords of the code C, i.e. $C_n = UG$ for some random $n \times k$ matrix U. We put some additional restriction on joint choice of matrices P and C_n later, in order to avoid structural attacks. Matrices P and C_n are kept secret.

Bob sends to Alice the following *ciphertext* y

$$y = mG_{pub} + eE_{pub} = (mG + e(C_n + P))M, \tag{5}$$

where e is a vector of weight t *randomly* generated by Bob. Alice reveals the message m by the following chain of calculations:

$$y' := yM^{-1} = mG + e(C_n + P) = m'G + e', \tag{6}$$

where $m' = m + eU,\ \ e' = eP$ and $wt(e') = wt(e) = t$, since P is a permutation matrix, then Alice applies the decoding algorithm Ψ to the vector $y' = m'G + e'$, which outputs the *error vector* e', hence Alice knows $e = e'P^{-1}$ and finally finds m, for instance, from $mG_{pub} = y - eE_{pub}$, see (5).

3.1 First Attack or Why Matrix E_{pub} Must be Singular

Let us show that if the matrix E_{pub} is non-singular then the new scheme can be attacked the same way as the original McEliece scheme. Indeed, if $E_{pub} = (C_n + P)M$ is non-singular then Eve can compute vector $\tilde{y} := yE_{pub}^{-1}$. Hence, according to (5),

$$\tilde{y} = (mG_{pub} + eE_{pub})E_{pub}^{-1} = mG(C_n + P)^{-1} + e = m\tilde{G} + e, \tag{7}$$

where $\tilde{G} = G(C_n + P)^{-1}$ can be considered as a generator matrix of some linear (n, k)-code $\tilde{C}$. It is easy to see that the Eq, (7) cannot have more than one solution for a given $\tilde{y}$. Hence, the code $\tilde{C}$ has distance at least $2t + 1$ and ISD algorithms can be applied. Moreover, we shall show that codes C and $\tilde{C}$ are permutation equivalent and thus to break our scheme in the case where E_{pub} is invertible is the same as to break the McEliece cryptosystem.

Remark 1. To prove that codes C and $\tilde{C}$ are equivalent recall that the rows of the matrix C_n are of the form uG (for some k-tuple u) since they are vectors of the code C and it would be convenient to represent matrix C_n as UG, where U is the corresponding $n \times k$ matrix.

Let us start from the following obvious equality

$$G(I_n + P^{-1}UG) = (I_k + GP^{-1}U)G,$$

and hence

$$(I_k + GP^{-1}U)^{-1}G = G(I_n + P^{-1}UG)^{-1}. \tag{8}$$

By the definition $\tilde{G} = G(UG + P)^{-1}$ and thus

$$\tilde{G} = G(P(P^{-1}UG + I_n))^{-1} = G(P^{-1}UG + I_n)^{-1}P^{-1} = (I_k + GP^{-1}U)^{-1}GP^{-1}.$$

Hence, we proved that $\tilde{G} = (I_k + GP^{-1}U)^{-1}GP^{-1}$, and therefore codes C and $\tilde{C}$ are permutation equivalent (if matrix $(I_k + GP^{-1}U)^{-1}$ exists).

3.2 How to Make Matrix $\boldsymbol{E_{pub}}$ Singular

The matrix $E_{pub} = (C_n + P)M$ is singular iff matrix $C_n + P$ is singular since matrix M is non-singular. Let us show how to construct many singular matrices of the form $C_n + P$. Note that w.l.o.g. we can restrict our consideration to the case $C_n + I_n$ and then transform the obtained singular matrices to the desired ones of the form $\breve{C}_n + P$, where $\breve{C}_n = C_nP$.

Let us first, for simplicity, consider the binary case. Let $\mathbf{c} = (c_1, \ldots, c_n) \in C$ be a codeword of the Hamming weight w and let $c_{j_1}, \ldots, c_{j_w}$ be its w nonzero coordinates. Construct rows $\mathbf{c}^i$ of C_n in the following way: rows not indexed by $J = supp(c)$ will be taken randomly, and the rest of the rows are chosen in such a way that

$$\sum_{j \in J} \mathbf{c}^j = \mathbf{c}. \tag{9}$$

Denote by $B_n = C_n + I_n$ and let $\mathbf{b}^i = \mathbf{c}^i + \delta_i$ be the i-th row of the matrix B, where $\delta_i = (\delta_{i,1}, \ldots, \delta_{i,n})$ and $\delta_{i,j}$ is the Kronecker delta. Then $\sum_{j \in J} \mathbf{b}^j = \mathbf{0}$ and thus the matrix $B_n = C_n + I_n$ is singular.

In the general case one should replace Eq. (9) on

$$\sum_{j \in J} c_j \mathbf{c}^j = -\mathbf{c} \tag{10}$$

and then $\sum_{j \in J} c_j \mathbf{b}^j = \mathbf{0}$ and thus the matrix $B_n = C_n + I_n$ is singular.

Obviously the number of solutions of Eq. (9) equals to $q^{k(w-1)}$, since say first $w - 1$ vectors $\mathbf{c}^j$ can be chosen as arbitrary codevectors, and the last one is chosen uniquely according to (9). Hence the total number of matrices constructed according to (9) for a given nonzero codeword c equals to $q^{k(n-1)}$, among total number q^{kn} $n \times n$ matrices, whose rows are vectors of the code C.

3.3 Second Attack Based on Parity-Check Matrix $\boldsymbol{H_{pub}}$

Unfortunately, there is another attack which shows that the "prototype" cryptosystem can be successfully attacked at least by ISD algorithms.

Namely, Eve computes a parity-check matrix H_{pub} for the generator matrix G_{pub}, i.e. $G_{pub}H_{pub}^T = H_{pub}G_{pub}^T = 0$. Let H be a parity-check matrix for the code C, i.e. $GH^T = 0$. Then it is easy to see that $H_{pub}^T = M^{-1}H^TS^T$, where S

is some non-singular $r \times r$-matrix and $r = n - k$. After that Eve multiplies both parts of Eq. (5), where $C_n = UG$, from the right side with H_{pub}^T and receives

$$\tilde{y} := yH_{pub}^T = (mG + e(UG + P))MM^{-1}H^TS^T = ePH^TS^T = e\tilde{H}^T. \quad (11)$$

Hence (11) is a usual syndrome equation for the code $\tilde{C}$ with parity-check matrix $\tilde{H} = SHP^T$. Since obviously codes C and $\tilde{C}$ are permutation equivalent and the "prototype" cryptosystem is not more secure that the ordinary McEliece system but even worse its public keys are at least twice as large.

4 The New Code-Based Cryptosystem

In order to improve the "prototype" system we shall make the structure of the matrix E_{pub} more complicated. Namely, let $E_{pub} = WD(C_n + P)M$, where $(C_n + P)M$ is the same as for the prototype, D is a randomly chosen $n \times n$ diagonal matrix with t non-zero elements on the diagonal, and W is random $n \times n$ non-singular matrix. Alice forms two *public* matrices: $k \times n$ matrix $G_{pub} = GM$ and $n \times n$ matrix $E_{pub} = WD(C_n + P)M$.

Bob sends to Alice the following *ciphertext* y

$$y = mG_{pub} + eE_{pub} = (mG + eWD(C_n + P))M, \quad (12)$$

where e is a vector *randomly* generated by Bob. Let us stress that the vector e does not bear any restriction on its weight. Recall that C_n can be represented as $C_n = UG$, where U is the appropriate $n \times k$ matrix, and Alice reveals the message m by the following chain of calculations:

$$y' := yM^{-1} = mG + eWD(UG + P) = m'G + e'P, \quad (13)$$

where $m' = m + eWDU, \quad e' = (eW)D$. Note that $wt(e') \leq t$, since D is a diagonal matrix of "weight" t. Then as for the prototype Alice applies the decoding algorithm Ψ to the vector $y' = m'G + e''$, where $e'' = e'P$, which outputs "error vector" e''. Hence Alice knows $e' = e''P^{-1}$, thereafter subsequently finds eWD, then $eWDC_n$ and finally finds m, for instance, from $mG_{pub} = y - eE_{pub}$, see (12).

It is straightforward to check that both attacks described for the "prototype" system do not work for the new system. Indeed, matrix E_{pub} has rank t, since matrix D has rank t, and thus the first attack cannot be applied.

For the second attack Eve multiplies both parts of Eq. (12) from the right side on $H_{pub}^T = M^{-1}\tilde{H}^T$, where $\tilde{H}$ is some parity-check matrix of the code C. She receives the following equation

$$yH_{pub}^T = (mG + eWD(UG + P))MM^{-1}\tilde{H}^T = eWDP\tilde{H}^T = (eWDP)\tilde{H}^T \quad (14)$$

which is a usual syndrome equation for a code with parity-check matrix $\tilde{H}$ and hence Eve can find vector $eWDP$ of weight t but she cannot "extract" from it the vector e since all three multipliers W, D and P are unknown to her.

The new cryptosystem forces Eve to apply brute-force attacks which have complexity at least $\binom{n}{t}$ *trials*.

Consider the following example

Example 1. Let C be an irreducible Goppa code of length $n = 256$ and rate $R = 1/2$, i.e. with $k = 128$ and $t = 16$. Then the number of trials is $\binom{16}{256} > 2^{100}$ and the public key length is $128 \times 256 + 256^2 = 3 \times 2^{15}$.

5 Conclusion

In this paper we considered a new modification of the well-known McEliece cryptosystem in which we transform an error vector of weight t (or $\leq t$) to an error vector of arbitrary weight.

References

1. Diffie, W., Hellman, M.: New directions in cryptography. IEEE Trans. Inf. Theory **22**(6), 644–654 (1976)
2. Merkle, R., Hellman, M.: Hiding information and signatures in trapdoor knapsacks. IEEE Trans. Inf. Theory **24**(5), 525–530 (1978)
3. Shamir, A.: A polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem. IEEE Trans. Inf. Theory **30**(5), 699–704 (1984)
4. Sidelnikov, V.M., Shestakov, S.O.: On encryption based on generalized reed solomon codes. Discrete Math. Appl. **2**(4), 439–444 (1992)
5. McEliece, R.J.: A public-key cryptosystem based on algebraic Coding Theory. DSN Progress Report 42–44, pp. 114–116 (1978)
6. Niederreiter, H.: Knapsack-type cryptosystems and algebraic coding theory. Prob. Control Inf. Theory **15**, 159–166 (1986)
7. Goppa, V.D.: A new class of linear correcting codes. Problemy Peredachi Informatsii **6**(3), 24–30 (1970)
8. Berlekamp, E.R., McEliece, R.J., van Tilborg, H.C.A.: On the inherent intractability of certain coding problems. IEEE Trans. Inform. Theory **24**, 384–386 (1978)
9. May, A., Meurer, A., Thomae, E.: Decoding random linear codes in $\tilde{\mathcal{O}}(2^{0.054n})$. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 107–124. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-25385-0_6
10. Becker, A., Joux, A., May, A., Meurer, A.: Decoding random binary linear codes in $2^{n/20}$: how $1 + 1 = 0$ improves information set decoding. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 520–536. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29011-4_31
11. Barg, A., Krouk, E., van Tilborg, H.: On the complexity of minimum distance decoding of long linear codes. IEEE Trans. Inf. Theory **45**(5), 1392–1405 (1999)
12. Bernstein, D.J., Lange, T., Peters, C.: Attacking and defending the McEliece cryptosystem. In: Buchmann, J., Ding, J. (eds.) PQCrypto 2008. LNCS, vol. 5299, pp. 31–46. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-88403-3_3

13. Berger, T.P., Cayrel, P.-L., Gaborit, P., Otmani, A.: Reducing key length of the McEliece cryptosystem. In: Preneel, B. (ed.) AFRICACRYPT 2009. LNCS, vol. 5580, pp. 77–97. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-02384-2_6
14. Von Maurich, I., Güneysu, T.: Lightweight code-based cryptography: QC-MDPC McEliece encryption on reconfigurable devices, In 2014 Design, Automation and Test in Europe Conference and Exhibition (DATE), pp. 1–6 (2014)
15. Baldi, M., Chiaraluce, F., Garello, R., Mininni, F.: Quasi-cyclic low-density parity-check codes in the McEliece cryptosystem. In: 2007 IEEE International Conference on Communications, pp. 951–956 (2007)
16. Baldi, M.: LDPC codes in the McEliece cryptosystem: attacks and countermeasures, In: NATO Science for Peace and Security Series–D: Information and Communication Security. LNCS, vol. 23, pp. 160–174 (2009)
17. Baldi, M., Bodrato, M., Chiaraluce, F.: A new analysis of the McEliece cryptosystem based on QC-LDPC codes. In: Ostrovsky, R., De Prisco, R., Visconti, I. (eds.) SCN 2008. LNCS, vol. 5229, pp. 246–262. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-85855-3_17
18. Baldi, M., Bambozzi, F., Chiaraluce, F.: On a family of circulant matrices for quasi-cyclic low-density generator matrix codes. IEEE Trans. Inf. Theory **57**(9), 6052–6067 (2011)
19. Baldi, M., Bianchi, M., Chiaraluce, F.: Security and complexity of the McEliece cryptosystem based on quasi-cyclic low-density parity-check codes. IET Inf. Secur. **7**(3), 212–220 (2013)
20. Baldi, M., Bianchi, M., Chiaraluce, F.: Optimization of the parity-check matrix density in QC-LDPC code-based McEliece cryptosystems. In: Workshop on Information Security Over Noisy and Lossy Communication Systems (IEEE ICC 2013) (2013)
21. Misoczki, R., Tillich, J.P., Sendrier, N., Barreto, P.S.: MDPC-McEliece: new McEliece variants from moderate density parity-check codes. In: 2013 IEEE International Symposium on Information Theory, pp. 2069–2073 (2013)
22. Alekhnovich, M.: More on average case vs approximation complexity. In: 44th Annual IEEE Symposium on Foundations of Computer Science, Proceedings, pp. 298–307 (2003)
23. Baldi, M., Bianchi, M., Chiaraluce, F., Rosenthal, J., Schipani, D.: A variant of the McEliece cryptosystem with increased public key security. In: Proceedings of WCC 2011 - Seventh Workshop on Coding and Cryptography, no. 7, pp. 173–182. HAL-Inria (2011)
24. Berlekamp, E., McEliece, R.J., Van Tilborg, H.: On the inherent intractability of certain coding problems. IEEE Trans. Inf. Theory **24**(3), 384–386 (1978)
25. Khathuria, K., Rosenthal, J., Weger, V.: Encryption scheme based on expanded Reed-Solomon codes. Advances in Mathematics of Communications (2019)
26. Li, Y.X., Deng, R.H., Wang, X.M.: On the equivalence of McEliece's and Niederreiter's public-key cryptosystems. IEEE Trans. Inf. Theory **40**(1), 271–273 (1994)