2023 XVIII International Symposium Problems of Redundancy in Information and Control Systems (REDUNDANCY) | 979-8-3503-8152-8/23/$31.00 ©2023 IEEE | DOI: 10.1109/Redundancy59964.2023.10330197

McEliece-type cryptosystem based on correction of errors and erasures

Evgenii Krouk*, Grigory Kabatiansky†, Cedric Tavernier‡
* Higher School of Economics, Moscow Institute of Mathematics and Electronics, Russia
† Skolkovo Institute of Science and Technology, Russia
‡ Hensoldt France
ekrouk@hse.ru, g.kabatyansky@skoltech.ru, tavernier.cedric@gmail.com

***Abstract*—Recently, a modification of the classical McEliece cryptosystem has been proposed by introducing an auxiliary matrix, by which an artificial error vector is multiplied. The system was broken. In this work, we propose a simpler attack on the system, and at the same time, we propose a generalization of the system, free from the identified shortcomings. We assume that the new scheme is at least as secure as McEliece's cryptosystem.**

I. Description of some previous constructions

Let us start by recalling the classical McEliece cryptosystem [1]. There is an (n, k)-code C with the minimal code distance $d \geq 2t+1$, which can effectively correct t errors. In the original paper [1] it was proposed to take an irreducible Goppa code with the following parameters: $n = 1024,\ k = 524,\ t = 50$.

Alice chooses one of many irreducible Goppa $(1024, 524)$-codes with a generator $k \times n$-matrix G (it is well-known that the number of irreducible Goppa codes grows exponentially with t, and there is the explicit formula for this number, see [2], but less is known about the number of nonequivalent Goppa codes, see [3]). It is important to note that for Goppa codes there are known decoding algorithms correcting errors and erasures with small, i.e., polynomial, complexity.

Then Alice generates two random matrices: $k \times k$ nonsingular matrix A and $n \times n$ permutation matrix P and made publicly accessible the following $k \times n$ matrix $G_{pub} = AGP$. The matrices A, G, P, as well as a particular choice of Goppa polynomial and the corresponding $(1024, 524)$-code, are kept secret.

When user Bob wants to send Alice some secret information, represented as a binary vector $\mathbf{m} = (m_1, \ldots, m_k)$, he generates a random vector $\mathbf{e} = (e_1, \ldots, e_n)$ of the Hamming weight $wt(\mathbf{e}) = t$ (or at most t) and transmits over an open channel the encrypted vector $\mathbf{y}$, where

$$\mathbf{y} = \mathbf{m}G_{pub} + \mathbf{e} \tag{1}$$

Alice can reveal $\mathbf{m}$ via next simple steps: firstly evaluating $\mathbf{y}' = \mathbf{y}P^{-1}$, then decoding $\mathbf{y}' = \mathbf{m}'G + \mathbf{e}'$, where $\mathbf{m}' = \mathbf{m}A$, by correcting the corresponding error $\mathbf{e}' = \mathbf{e}P^{-1}$, with the result of decoding to the vector $\mathbf{m}'$, and finally outputs $\mathbf{m} = \mathbf{m}'A^{-1}$.

So far, neither structural attacks on McEliece's cryptosystem, nor attacks through decoding, starting from McEliece's proposal to use *Information Set Decoding* (ISD for short), have been successful, see [4] for a detailed review. Based on 45 years of successful countering various attacks on the McEliece cryptosystem, this system is considered secure even against attacks by quantum computers.

A lot of papers on McEliece cryptosystem were published, see [4], mainly in line of the original McEliece's idea with the usage of other families of codes, other attacks, etc., but one thing stayed untouched, namely, introducing an artificial error $\mathbf{e}$ of some limited Hamming weight into ciphertext, or, equivalently, in "syndrome form", introduced by H.Niedderraiter [5].

In this article, we propose a new generalization of McEliece's cryptosystem based on Alice's correction of not only errors, but also erasures. In our opinion, this can strengthen the system.

Let us note that the original McEliece cryptosystem is not symmetric with respect to the vectors $\mathbf{m}$ and $\mathbf{e}$. Therefore the following encryption map was proposed in [6]

$$\mathbf{y} = \mathbf{m}G_{pub} + \mathbf{e}E_{pub}, \tag{2}$$

where the $n \times n$-matrix E_{pub} should be properly chosen. We assume that the matrix E_{pub} is nonsingular. Then for the attacker Eve to find $\mathbf{m}$ from equation (2) means to decode the code C_{pub} with the generator matrix G_{pub} but with error vector $\mathbf{e}' := \mathbf{e}E_{pub}$ which Hamming weight can be much greater than $wt(\mathbf{e})$.

This modification appeared in [6] with the following choice of public matrices:

$$G_{pub} := GM,\ E^{(0)}_{pub} = WD(UG + P)M,$$

where M and W are random nonsingular $n \times n$-matrices, P is an $n \times n$ permutation matrix, U is an $n \times k$ matrix with its rank less than k, and an $n \times n$ diagonal matrix D with $r(D)$ ones on its main diagonal, which plays an especially important role in our constriction.

This E_{pub} selection was broken pretty quickly in [7], [8]. Below we will show with much simpler arguments why the attack from [7], [8] works, and at the same time we will analyze how to avoid this attack and some other attacks, which will lead us to a new, better choice of the matrix E_{pub}

in (2). Let's first describe the system of [6] in its strongest form.

Initialization stage. Alice randomly chooses the following binary matrices and kept them secretly :

$k \times n$ matrix G, which is a generator matrix of a *random* linear (n, k)-code C with the minimal distance $d = d(C)$;

nonsingular $n \times n$ matrices M and W;

$n \times n$ permutation matrix P;

$n \times k$ matrix U of the rank less than k;

$n \times n$ diagonal matrix D with $r(D)$ ones on its main diagonal, where $r(D) < d$.

Based on it Alice forms two *public* matrices:

$k \times n$ matrix $G_{pub} := GM$ and $n \times n$ matrix $E^{(0)}_{pub} := WD(UG + P)M$.

Encryption. Bob sends to Alice a k-bits plaintext message $\mathbf{m}$ via the following ciphertext $\mathbf{y} = \mathbf{m}G_{pub} + \mathbf{e}E^{(0)}_{pub}$, where $\mathbf{e}$ is an arbitrary binary vector of dimension n.

Let us show how erasure correction occurs. Alice evaluates $\mathbf{z} := \mathbf{y}M^{-1}$ and then solves the corresponding decoding problem

$$\mathbf{z} = \mathbf{m}G + \mathbf{e}WD(UG + P) = \mathbf{c}' + \mathbf{e}', \tag{3}$$

where $\mathbf{c}' = (\mathbf{m} + \mathbf{e}WDU)G$ and $\mathbf{e}' = \mathbf{e}WDP$. The Hamming weight of $\mathbf{e}'$ is at most $r(D)$ and moreover Alice knows $r(D)$ coordinates of $\mathbf{e}'$, which can only be nonzero. Therefore Alice erases these $r(D)$ positions and then solves the corresponding decoding problem of correction $r(D)$ erasures, i.e. she finds vectors $\mathbf{c}'$ and $\mathbf{e}' = \mathbf{e}WDP$ what can be done for *arbitrary* linear code, since correction of erasures is just to solve the corresponding system of linear equations with $r(D)$ unknown variables and it can be done with at most n^3 complexity. From $\mathbf{c}' = \mathbf{m}'G$ Alice can find $\mathbf{m}' = \mathbf{m} + \mathbf{e}WDU$ and since she knows $\mathbf{e}WD = \mathbf{e}'P^{-1}$ she gets $\mathbf{m} = \mathbf{m}' + \mathbf{e}WDU$.

But Eve can also find $\mathbf{m}$, without even knowing what is M and which positions could be erased. Namely, Eve solves the following system of n linear equations

$$\mathbf{y} = \mathbf{m}G_{pub} + \mathbf{e}E^{(0)}_{pub}, \tag{4}$$

with $n+k$ unknown variables, which are coordinates of vectors $\mathbf{m}$ and $\mathbf{e}$. It is a priori known that this linear system has at least one solution. The system can be solved in polynomial time, e.g. in $O(n^3)$ time. Let $\mathbf{m}, \mathbf{e}$ and $\mathbf{m}', \mathbf{e}'$ be two solution of equation (4) and $\mathbf{m} \neq \mathbf{m}'$. Then both plaintexts $\mathbf{m}$ and $\mathbf{m}'$ could be sent by Bob as

$$\mathbf{y} = \mathbf{m}G_{pub} + \mathbf{e}E^{(0)}_{pub} = \mathbf{m}'G_{pub} + \mathbf{e}'E^{(0)}_{pub}, \tag{5}$$

and Alice cannot resolve this Buridan's ass paradox. It means that there could be many solutions of the system (4) but they can differ only in $\mathbf{e}$ part, not in $\mathbf{m}$ part. Indeed, it follows from (5) that

$$\mathbf{m}G_{pub} + \mathbf{e}E^{(0)}_{pub} = \mathbf{m}'G_{pub} + \mathbf{e}'E^{(0)}_{pub}$$

and hence

$$(\mathbf{m} + \mathbf{m}')G = (\mathbf{e} + \mathbf{e}')WD(UG + P)$$

Thus

$$(\mathbf{m} + \mathbf{m}' + (\mathbf{e} + \mathbf{e}')WDU)G = (\mathbf{e} + \mathbf{e}')WDP \tag{6}$$

Because of the matrix D the vector $(\mathbf{e} + \mathbf{e}')WDP$ has the Hamming weight at most $d - 1$ and therefore the codevector $(\mathbf{m} + \mathbf{m}' + (\mathbf{e} + \mathbf{e}')WDU)G = 0$. Thus $(\mathbf{e} + \mathbf{e}')WDP = 0$ and then $(\mathbf{e} + \mathbf{e}')WD = 0$ since P is a permutation. Hence $(\mathbf{m} + \mathbf{m}')G = 0$, or $\mathbf{m} = \mathbf{m}'$.

Thus, Eve can find the plaintext $\mathbf{m}$ in no more than n^3 time, and the system is broken. The proposed explanation for why the line attack works follows the ideas suggested in [7], [8] but is much simpler. Note that introducing the constraint $wt(\mathbf{e}) = t$ does not help, since Eve is not required to look only for solution of equation (4) with a bounded Hamming weight.

II. The new code-based cryptosystem

In this section we describe and give some cryptoanalysis of the system, which was proposed at CBCrypto 2023. The corresponding encryption map has the following form

$$\mathbf{y} = \mathbf{m}G_{pub} + \mathbf{e}E_{pub} = \mathbf{m}GM + \mathbf{e}(WD(UG + P) + P')M, \tag{7}$$

where P, P' are two permutation $n \times n$ matrices randomly chosen in such a way that the matrix $WDP + P'$ is nonsingular. The error vector $\mathbf{e}$ is chosen as a random vector of the Hamming weight t, where $r(D) + 2t < d = d(C)$. As the particular choice of system's parameters we shall consider $t = d/3,\ r(D) = \frac{d}{3} - 1$.

Let us first show how Alice can decrypt $\mathbf{y}$. Alice evaluates $\mathbf{z} := \mathbf{y}M^{-1}$ and then solves the corresponding decoding problem

$$\mathbf{z} = \mathbf{m}G + \mathbf{e}(WD(UG + P) + P') = \mathbf{c}' + \mathbf{e}' + \mathbf{e}_{eras}, \tag{8}$$

where $\mathbf{c}' = \mathbf{m}'G$, $\mathbf{m}' = \mathbf{m} + \mathbf{e}WDU$, $\mathbf{e}' = \mathbf{e}P'$ and $\mathbf{e}_{eras} = \mathbf{e}WDP$. Alice knows $r(D)$ coordinates of $\mathbf{e}_{eras}$, which can only be nonzero, and by erasing these $r(D)$ positions she transforms solving of (9) to the decoding of the code C in presence of $r(D)$ erasures and at most t errors, induced by $\mathbf{e}'$. As the result of decoding Alice knows codevector $\mathbf{c}'$ and hence she knows $\mathbf{m}'$ and

$$\mathbf{z} + \mathbf{c}' = \mathbf{e}_{eras} + \mathbf{e}' = \mathbf{e}(WDP + P')$$

Then $\mathbf{e} = (\mathbf{z} + \mathbf{c}')(WDP + P')^{-1}$ and Alice finds $\mathbf{m} = \mathbf{m}' + \mathbf{e}WDU$.

It is rather clear that trying to solve equation (7) directly does not look promising due to the unknown random matrix M, what leads to decoding a random code C_{pub} with a random error vector $\mathbf{e}' := \mathbf{e}E_{pub}$. Therefore, more feasible attacks should try to get rid of the matrix M. Let us consider the

following attacks of such type.

If matrix E_{pub} is nonsingular then Eve evaluates $E_{pub}^{-1} = M^{-1}(WD(UG+P)+P')^{-1}$ and considers the following decoding problem

$$\mathbf{y}' := \mathbf{y}E_{pub}^{-1} = \mathbf{m}G' + \mathbf{e}, \tag{9}$$

where $G' = G(WD(UG+P)+P')^{-1}$. This equation looks very similar to the original McEliece system encryption map with just a difference that matrix $(WD(UG+P)+P')^{-1}$ is not a permutation matrix and has more complicated structure. Nevertheless, in order to avoid this attack let us assume additionally that the matrix E_{pub} is singular, i.e., that the matrix $WD(UG+P)+P'$ is singular.

Another attack of Eve works in the following way. She evaluates an $(n-k)\times n$-matrix H_{pub} such that $G_{pub}H_{pub}^T$=0, i.e., evaluates a parity-check matrix for the code C_{pub} with generator matrix G_{pub}. It is easy to verify that $H_{pub}^T = M^{-1}H^T$, where H is some parity-check matrix for the code C. Then Eve evaluates the syndrome $\mathbf{s} = yH_{pub}^T$ and tries to solve the following equation

$$\mathbf{s} = \mathbf{m}G_{pub}H_{pub}^T + \mathbf{e}E_{pub}H_{pub}^T = \mathbf{e}\hat{H}^T, \tag{10}$$

where $\hat{H}^T := E_{pub}H_{pub}^T = (WD(UG+P)+P')MM^{-1}H^T = (WDP+P')H^T$. This equation can be considered as syndrome equation for the code $\hat{C}$ with the parity-check matrix $\hat{H}$. Note that there is an obstacle for Eve in this way, namely, the code $\hat{C}$ is not equivalent to the code C as it is for McEliece system. The minimal distance of the code $\hat{C}$ is unknown and moreover very probably it is approximately the same as the distance of a random (n,k)-code what is twice less than the distance of the initial good code, like Goppa code.

These simple attacks show that we cannot make significant use of the fact that M is an unknown random matrix. Therefore, we confine ourselves to the case which will be discussed in the next section, when M is just a permutation matrix $\mathcal{P}$.

III. McEliece type cryptosystem based on errors and erasures correction

Consider the encryption map (7) in its particular and simplified form when $M = \mathcal{P}$ is a random permutation $n \times n$ matrix

$$\mathbf{y} = \mathbf{m}AG\mathcal{P} + \mathbf{e}(WD(UG+P)+P')\mathcal{P}, \tag{11}$$

where A is a nonsingular $k \times k$ matrix (we did not use the matrix A in our previous consideration, since because of random matrix M we can considered G as an *arbitrary* generating matrix of the code C). Recall that the error vector $\mathbf{e}$ is chosen as a random vector of the Hamming weight t, where $r(D)+2t < d = d(C)$. For $r(D)=0$ and $t = \frac{d-1}{2}$ this is the McEliece system, for $r(D) = d-1$ and $t=0$ this is the system of [6]. We recommend to chose $r(D) \approx t \approx d/3$.

In order to make clearer the similarities and differences between this system and the McEliece system, let us rewrite equation (11) in the following form

$$\mathbf{y} = \mathbf{c} + \mathbf{e}' + \mathbf{e}'' = \mathbf{c} + \mathbf{e}_{total}, \tag{12}$$

where $\mathbf{c} = \mathbf{m}AG\mathcal{P} \in \mathcal{P}(C)$, $\mathbf{e}' = \mathbf{e}P'\mathcal{P}$ $\mathbf{e}'' = \mathbf{e}WD(UG+P)\mathcal{P}$ and $\mathbf{e}_{total} = \mathbf{e}' + \mathbf{e}''$.

The Hamming weight of the error $\mathbf{e}'$ is the same as of $\mathbf{e}$, i.e., equals t, but the weight of $\mathbf{e}''$ can be large, on average about $n/2$. Indeed, $\mathbf{e}'' = \mathbf{e}WDUG + \mathbf{e}WDP$, where the weight of $\mathbf{e}WDP$ is at most $r(D)$ (and $r(D)/2$ in average since matrix W is random). Denote rows of the matrix UG, which are codevectors of the code C, as $\mathbf{c}_1, \ldots, \mathbf{c_n}$, and denote by C' the code generated by these vector, i.e. C' is the linear span of $\mathbf{c}_1, \ldots, \mathbf{c_n}$. Then the vector $\mathbf{e}WDUG = \sum_{i\in I}\mathbf{c}_i$, where I is the set of nonzero coordinates of the vector $\mathbf{e}WD$. Hence in average it is the sum of $r(D)/2$ randomly chosen codevectors $\mathbf{c}_i$. We may assume that $wt(\mathbf{e}WDUG)$ is about $n/2$ in average.

In the next section we give an explicit construction of the matrix U code that guarantees that the weight of the vector $\mathbf{e}WDUG$ *always* is large enough what allows to give enough good lower bound on the weight of $\mathbf{e}_{total}$, i.e., that solving the decoding problem (12) is much more complicated than for the original McEliece scheme.

IV. On the right choice of the matrix U

Let us consider a vector $\mathbf{e}WDUG$ as $\mathbf{g}UG$, where $\mathbf{g} = \mathbf{e}WD$, and hence the Hamming weight $wt(\mathbf{g}) \le r(D)$. Therefore it is sufficient to construct $n \times n$-matrix UG with property that sum (modulo 2) of any $r(D)$ or fewer columns UG has a sufficiently large Hamming weight, say, at least T. Let us denote rows of UG as $\mathbf{f}_1, \ldots, \mathbf{f}_n$. And let denote by C' the subcode of the code C which is their linear span.

Then the desired property can be reformulated as follows: for any subset I such that $|I| \le r(D)$ the inequality holds

$$wt(\sum_{i\in I}\mathbf{f}_i) \ge T \tag{13}$$

This problem in fact is actually already known as superimposed codes in Hamming space, see [9]. Below we recall the construction of [9], which is at least asymptotically optimal.

For a chosen (n,k,d)-code C and chosen parameters $r(D)$ and t, such that $r(D)+2t < d$, we firstly find n vectors $\mathbf{h}_1, \ldots, \mathbf{h}_n$ of the minimal possible dimension m with the property that any $r(D)$ of these vectors are linearly independent. Saying in other words, we need to find a linear $(n, n-m)$-code with the minimal distance at least $r(D)+1$. Then columns of a parity-check matrix $\mathcal{H}$ of this code is a desired set $\{\mathbf{h}_1, \ldots, \mathbf{h}_n\}$.

As the next step we choose an m-dimensional subcode C' of the code C with sufficiently large the minimal code distance $T = d(C')$. And let vectors $\mathbf{v}_1, \ldots, \mathbf{v_m}$ be a basis of C'.

979-8-3503-8152-8/23/$31.00 ©2023 IEEE

It was proposed in [9] to set

$$\mathbf{f}_i := \sum_{j=1}^{m} h_{ij}\mathbf{v}_j \tag{14}$$

Or, saying in words, it was proposed to encode vectors $\mathbf{f}_i$ by the code C'. To prove (13) consider

$$\mathbf{F} := \sum_{i\in I}\mathbf{f}_i = \sum_{i\in I}(\sum_{j=1}^{m} h_{ij}\mathbf{v}_j) = \sum_{j=1}^{m}(\sum_{i\in I} h_{ij})\mathbf{v}_j \tag{15}$$

Then $\mathbf{F}\neq 0$ since vectors $\mathbf{v}_1,\ldots,\mathbf{v_m}$ form a basis and at least one of parentheses is nonzero because any of $r(D)$ vectors $\mathbf{h}_j$ are linearly independent. On the other hand, $\mathbf{F}\in C'$ and thus $wt(\mathbf{F})\geq t$. Q.E.D.

Hence this construction gives us rows of UG as $\mathbf{f}_1,\ldots,\mathbf{f}_n$, and then U can be recovered. In fact, we do not need the matrix U explicitly, but only the matrix UG.

V. Examples

.

Example 1. Consider as (n,k,d)-code C a primitive BCH code with parameters $n=255,\ k=191$ and $d=17$. Let us choose $r(D)=6$ and $t=5$. Then any 6 columns of a parity-check matrix $\mathcal{H}$ must be linearly independent, i.e., let $\mathcal{H}$ be an 24×255 parity-check matrix of a primitive $(255,231,7)$ BCH code, correcting triple errors. Now we need to choose an 24-dimensional subcode C' of the code C with sufficiently large the minimal code distance T. Let again take a BCH code of length 255 correcting 30 errors, i.e., the minimal code distance $T=61$. Proper calculations, see [2], show that the dimension of the code is 25, and hence we choose 24 linearly independent vectors of this code as $\mathbf{v_1},\ldots,\mathbf{v_{24}}$.

Hence the Hamming weight of the vector $\mathbf{e}WDUG\geq 61$. And the total weight of the error $\mathbf{e}_{total}$ which Eve have to correct is at least $61-6-5=50$, what is many times larger than bounded-distance decoding can do. Indeed, there are approximately $2^{255h(\frac{50}{255})}=2^{255\times 0.714}=2^{172}$ different error vectors of the weight 50. On the other hand, there are 2^{64} different syndromes. Thus, in average there are 2^{108} different errors of the weight 50 with the same syndrome. And all of them looks for Eve enough good...

So, the complexity of finding plain text via decoding is huge. On the other hand, this is only a toy example, to show that the considered attack doesn't work, because the number of possible errors $\binom{255}{5}$ is small and just a straight-forward attack brakes the system with complexity approximately $2^{33}\times 2^{14}$. The next example allows to avoid this attack by making weight of $\mathbf{e}$ larger.

Example 2. Consider BCH code of length $n=255$, correcting 11 errors, i.e., with the minimal code distance $d=33$ and $r=132$ parity-check bits. Let us choose $r(D)=10$ and $t=11$. Then any 10 columns of a parity-check matrix $\mathcal{H}$ must be linearly independent, hence let $\mathcal{H}$ be an 40×255 parity-check matrix of a primitive $(255,215,11)$ BCH code, correcting five errors. Next we choose an 40-dimensional subcode C' of the code C with sufficiently large the minimal code distance T. Let again take a BCH code of length 255 correcting 28 errors, i.e., with the minimal code distance $T=57$. Proper calculations, see [2], show that the dimension of the code is 41, and then we choose 40 linearly independent vectors of this code as $\mathbf{v}_1,\ldots,\mathbf{v}_{40}$.

Hence the Hamming weight of a vector $\mathbf{e}WDUG\geq 57$. And the total weight of the error $\mathbf{e}_{total}$, which Eve have to correct, is at least $57-10-11=36$, what is three times larger than bounded-distance decoding can guarantee. Evaluation similar to what was done in Example 1 shows that there are approximately $2^{255h(\frac{36}{255})}=2^{255\times 0.586}=2^{149}$ different error vectors of the weight 36. On the other hand, there are 2^{132} different syndromes. Thus, there are at least 2^{17} different errors of the weight 57 with the same syndrome. Of course, these numbers are not as impressive as in the first example. But that's because we're looking at Alice's worst case scenario. Let's consider the most likely case instead.

Let us do the corresponding probabilistic analysis. Namely, return to the equation (12) and even assume that Eve knows the permutation $\mathcal{P}$ (this knowledge obviously destroys the ordinary McElice system). Then Eve can rewrite equation (12) in the following form

$$\mathbf{y}' := \mathbf{y}\mathcal{P}^{-1} = \mathbf{c}+\mathbf{E}+\hat{\mathbf{e}} = \mathbf{c}+\mathbf{e}_{total}, \tag{16}$$

where $\mathbf{c}=\mathbf{m}AG\in C$, $\hat{\mathbf{e}}=\mathbf{e}(P'+WDP)$, $\mathbf{E}=\mathbf{e}WDUG$ and $\mathbf{e}_{total}=\mathbf{E}+\hat{\mathbf{e}}$. Thus Eve needs to find the codevector $\mathbf{c}$ from "received" vector $\mathbf{y}'=\mathbf{c}+\mathbf{e}_{total}$ and let us estimate the error weight $wt(\mathbf{e}_{total})$. It was proved that $wt(\mathbf{E})\geq 57$. Hence we need to estimate the intersection of supports of vectors $\mathbf{E}$ and $\hat{\mathbf{e}}$. Let us consider the vector $\mathbf{e}$ as fixed and matrices W,P,P' as random (recall that P,P' are permutations). Then the vector $\hat{\mathbf{e}}$ is the sum of two random vectors, one of the them $\mathbf{e}P'$ of weight 11 and another one $\mathbf{e}WDP$ of weight between 1 and 10. Let us simplify the corresponding calculations and assume that vectors $\mathbf{e}WDP+\mathbf{e}P'$ is a randomly permuted vector (since permutations P and P' independent) of the weight 16 (what is true in average). Then the probability

$$\mathcal{P} = Pr\{|supp(\mathbf{e}WDP+\mathbf{e}P')\cap supp(\mathbf{E})|\geq\Delta\} \tag{17}$$

can be expressed in the following way

$$\mathcal{P} = \frac{\sum_{i=\Delta}^{1} 6\binom{57}{i}\binom{198}{16-i}}{\binom{255}{16}} \tag{18}$$

For example, when $\Delta=9$, then $\mathcal{P}<0.01$ and hence with probability 0.99 $wt(\mathbf{e}_{total})\geq 57-8+(16-8)=57$. Thus Eve typically have to search among approximately $2^{255h(\frac{57}{255})}=2^{255\times 0.7765}=2^{178}$ different error vectors of the weight 57. On the other hand, there are 2^{132} different syndromes. Thus, there are at least 2^{46} different errors with the same syndrome. Additionally, checking of each vector takes roughly $n^2=2^{16}$ operations. In total it gives complexity 2^{62}, what it is rather pessimistic estimation, we think.

Since $t = 11$ then the number of possible errors of this weight is $2^{255h(11/255)=2^{65}}$, plus we should count that checking of each error takes at least 11×255 operations, so totally it gives complexity 2^{76}.

Remark. We prefer BCH-codes to Goppa codes, because BCH-codes poses the nested structure when C' is a subcode of the code C.

VI. Conclusion

Our study focuses on a recently proposed generalization of the classical McEliece cryptosystem. We suggested a new modification of the error vector, which is specially introduced into the encryption procedure. Namely, the resulting error vector is obtained by multiplying a random vector of the weight t on the corresponding ublic matrix. The structure of this public matrix allows to make part of the error vector as an artificial code vector, which can easily be found by the legitimate recipient and at the same time it is one of the main obstacles for an attacker to decrypt a message. The given simplified analysis shows that the new system can shorten the public key while maintaining secrecy.

VII. Funding

The research of G.A.Kabatiansky was carried at Skolkovo Institute of Science and Technology and supported by the Russian Science Foundation (project no. 23-11-00340) was carried out at the expense of the Russian Science Foundation, project no. 22-41-02028.

References

[1] R.J.McEliece, "A public-key cryptosystems based on algebraic coding theory," *DSN Progress Report* , vol. 42-44, pp. 114-116, 1978.

[2] MacWilliams,F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. 1st edn. Elsevier (1978)

[3] Bocong Chen and Guanghui Zhang, "The number of extended irreducible binary Goppa codes", DOI:10.48550/arXiv.2204.02083

[4] V. Weger, N. Gassner, and J. Rosenthal,"A Survey on Code-based Cryptography," *arXiv:2201.07119*, 2022.

[5] H. Niederreiter, "Knapsack-type cryptosystems and algebraic coding theory". *Prob. Control Inf. Theory*, vol. 15, pp. 159–166, 1986.

[6] Ivanov, F., Kabatiansky, G., Krouk, E., Rumenko, N., "A New Code-Based Cryptosystem". *In: Baldi, M., Persichetti, E., Santini, P. (eds) Code-Based Cryptography. CBCrypto 2020. Lecture Notes in Computer Science, vol 12087. Springer, Cham*, pp 41-49, 2020.

[7] Y. Lee, J. Cho, Y. -S. Kim and J. -S. No, "Cryptanalysis of the Ivanov-Kabatiansky-Krouk-Rumenko Cryptosystems," *in IEEE Communications Letters,* vol. 24, no. 12, pp. 2678-2681, Dec. 2020

[8] TSC Lau, CH Tan, "Polynomial-time plaintext recovery attacks on the IKKR code-based cryptosystems", *Advances in Mathematics of Communications*, Vol. 17, no 2, pp. 353-366, 2023.

[9] Ericson T. and Levenshtein V.I. "Superimposed codes in the Hamming space", *IEEE Trans. Inform. Theory*. 1994. V. 40. № 6. P. 1882-1893.