G. P. Nagy, S. El Khalfaoui, Towards the security of McEliece's cryptosystem based on Hermitian subfield subcodes, *Prikl. Diskr. Mat. Suppl.*, 2021, Issue 14, 168–175

DOI: https://doi.org/10.17223/2226308X/14/39

## ЛИТЕРАТУРА

1. *Hayes J. P.* A graph model for fault-tolerant computing system // IEEE Trans. Comput. 1976. V. C.-25. No. 9. P. 875–884.
2. *Богомолов А. М., Салий В. Н.* Алгебраические основы теории дискретных систем. М.: Наука, 1997. 368 с.
3. *Абросимов М. Б.* Графовые модели отказоустойчивости. Саратов: Изд-во Сарат. ун-та, 2012. 192 с.
4. *Разумовский П. В., Абросимов М. Б.* Построение цветных графов без проверки на изоморфизм // Изв. Сарат. ун-та. Нов. сер. Сер. Математика. Механика. Информатика. 2021. Т. 21. Вып. 2. С. 267–277.
5. *Harary F. and Hayes J. P.* Edge fault tolerance in graphs // Networks. 1993. V. 23. P. 135–142.

UDC 004.453.2 DOI 10.17223/2226308X/14/39

# TOWARDS THE SECURITY OF McEliece's CRYPTOSYSTEM BASED ON HERMITIAN SUBFIELD SUBCODES[1]

G. P. Nagy, S. El Khalfaoui

The purpose of this paper is to provide a comprehensive security analysis for the parameter selection process, which involves the computational cost of the information set decoding algorithm using the parameters of subfield subcodes of 1-point Hermitian codes.

**Keywords:** *code-based cryptography, McEliece Cryptosystem, Hermitian subfield subcodes, Schur square dimension.*

## 1. Introduction

Recently, there has been a big amount of research addressed to quantum computers that use quantum mechanical techniques to solve hard computational problems in mathematics [1]. The existence of these powerful machines threaten many of the public-key cryptosystem that are widely in use [2]. McEliece [3] introduced the first code-based public-key cryptosystem in 1978. The crucial issues in cryptography today is to reduce the key size and improve the security level of the McEliece cryptosystem, which is a promising cryptographic scheme for the post-quantum era [4]. Error correcting codes, used in code-based cryptographic protocols, must have efficient decoding algorithms. A rich class of such codes is the family algebraic-geometric (AG) codes, their subcodes and subfield subcodes. This includes the generalized Reed — Solomon codes, the alternant codes, the binary Goppa codes and BCH codes. See [5] for a survey on the decoding of AG codes.

The authors of [6 – 8] provided polynomial-time attacks against the McEliece cryptosystem that relies either on AG codes or on their subcodes. In general, evaluation codes do not behave like random codes which demonstrate the quite range of attacks proposed against the McEliece cryptosystem based on AG codes. The approach given in [6, 8] is inspired by the so-called *filtration attacks* that rely on computing the Schur product that make AG codes distinguishable form random ones. Wieschebrink [9] used this observation to provide an attack against McEliece scheme based on subcodes of GRS codes [10]. Many attacks have been founded on this argument, and have employed a

[1] Project no. 2018-1.2.1-NKP-2018-00004 has been implemented with the support provided from the National Research, Development and Innovation Fund of Hungary, financed under the 2018-1.2.1-NKP funding scheme.

combination of powerful techniques such as the filtration method, an error-correcting pair (ECP) or an error-correcting array (ECA), that lead to a key recovery attack or a blind reconstruction of a decoding algorithm [6, 8, 11]. These vulnerabilities are based on two operations: *Schur product* and *s-closure*. In some cases, the *Schur filtration method* can expand the latter to develop an efficient decoding algorithm.

The purpose of this paper is to provide a comprehensive security analysis for the parameter selection process, which involves the computational cost of the information set decoding (ISD) algorithm using Hermitian subfield subcode parameters. Our approach focuses on the optimal parameters that improve the key size for a given security level. Furthermore, due to practical considerations, the key size of several parameter selections is compared to that of the classical McEliece cryptosystem submitted to NIST [4] for the same security level. Besides, we identify the Hermitian subfield subcodes parameters that achieve a Schur square dimension roughly equal to that of random codes. This technique is employed in the so-called distinguisher attack, that allows the attacker to determine the Schur square dimension of the code used as a public key.

## 2. Preliminaries

Let $q$ be a prime power. A *$q$-ary linear code* of length $n$ is a linear subspace $\mathcal{C} \leqslant \mathbb{F}_q^n$. The dimension of $\mathcal{C}$ is denoted by $k$, $\mathcal{C}$ is usually given by its $n \times k$ *generator matrix* $G$, or its $n \times (n-k)$ *parity check matrix* $H$:

$$\mathcal{C} = \{Gx : x \in \mathbb{F}_q^k\} = \{y \in \mathbb{F}_q^n : H^T y = 0\}.$$

The *minimal distance* of $\mathcal{C}$ is $d(\mathcal{C}) = \min\{\mathrm{wt}(x) : x \in \mathcal{C} \setminus \{0\}\}$, where $\mathrm{wt}(x)$ denotes the *Hamming weight* of the vector $x$. If $2t < d(\mathcal{C})$, then for each $y \in \mathbb{F}_q^n$, there is at most one pair $x, e \in \mathbb{F}_q^n$ of vectors such that $x \in \mathcal{C}$, $\mathrm{wt}(e) \leqslant t$ and $y = x + e$. Define the map $D_{\mathcal{C},t} : \mathbb{F}_q^n \to \mathcal{C} \cup \{*\}$ by $y \mapsto x$ if the decomposition $y = x + e$ exists, and $y \mapsto *$ otherwise. We call $D_{\mathcal{C},t}$ a *nearest neighbor decoding* of $\mathcal{C}$, correcting up to $t$ errors. In general, known nearest neighbor decoding algorithms have exponential time complexity in the size of the input $G, t, y$. The seminal result by Berlekamp, McEliece and van Tilborg [12] shows that the decoding problem is NP-complete even for the binary case $q = 2$. The simplest general decoding technique is called *information set decoding* (ISD), with goes back to an old algorithm of Prange [13]. This algorithm has time complexity

$$C_{\text{Prange}}(n, k, t) = \binom{n}{t} \Big/ \binom{n-k}{t} C_{\text{Gauss}}(n, k, q),$$

where $C_{\text{Gauss}}(n, k, q)$ is the time complexity of the Gauss — Jordan elimination of a $k \times n$ matrix over $\mathbb{F}_q$. There are many improvements of Prange's algorithms, but all known variants have the same asymptotic behavior, see [14] and the references therein.

Let us fix the parameters $n, k, t$ and $q$. The McEliece cryptographic scheme [3], or in general code-based cryptosystems has a $[n, k, t]_q$ linear code $\mathcal{C}$ as public key, and an efficient decoding algorithm $D_{\mathcal{C},t}$ as private key. Usually, $\mathcal{C}$ is given by a generator matrix

$$G = \begin{bmatrix} I_k \\ G_0 \end{bmatrix}$$

in systematic form, that is, the key size is

$$k(n-k)\lceil \log_2(q) \rceil.$$

The plain text message $m \in \mathbb{F}_q^k$ is encrypted to $c = Gm + e \in \mathbb{F}_q^n$, where $e$ is a random element of weight $t$ in $\mathbb{F}_q^n$. The security of the scheme relies on two facts:

1) To prevent a *message recovery attack,* the parameters $n, k, t$ and $q$ must be chosen such that the time complexity of ISD exceeds a given level $L$ of security. This level is usually measured in bits, and corresponds to the time complexity of breaking an $L$-bits symmetric-key block cipher, like AES. Since it is not the purpose of this paper to give a detailed cryptanalysis of symmetric-key block ciphers, we interpret this condition as
$$\binom{n}{t}\Big/\binom{n-k}{t} > 2^L.$$
2) To prevent a *key recovery attack,* it should not be possible to give an efficient decoding algorithm for $\mathcal{C}$. At this point, we not only assume the knowledge of $G$, but also the technique that was used to construct $\mathcal{C}$ from a given family of codes. In the classic McEliece proposal, $G = PG_1S$, where $G_1$ is the generator matrix of the binary Goppa code $\Gamma(\mathcal{L}, g)$. Here, $g = g(X)$ is a polynomial over $\mathbb{F}_q$ with no repeated roots, $\mathcal{L}$ is an ordered $n$-tuple of distinct elements of $\mathbb{F}_q$ that are no roots of $g$, $P$ is a random $n \times n$ permutation matrix, and $S$ is a random $k \times k$ invertible matrix; $\mathcal{L}, g, P, S$ are parts of the private key; they are supposed to be kept secret for a long period of time.

The second requirement implies that the public key $\mathcal{C}$ must be indistinguishable from a random subspace of $\mathbb{F}_q^n$. In general, distinguishing attacks do not necessarily lead to message or key recovery attacks. However, often they do, and cryptosystems must resist to distinguishing attacks.

## 3. The Schur product distinguisher

We briefly introduce some notions on attack techniques that allow us to describe some important results stated in [6].

**Definition 1.** Given two elements $a = (a_1, \ldots, a_n)$ and $b = (b_1, \ldots, b_n)$ in $\mathbb{F}_q^n$, the *Schur product* is the component-wise
$$a * b = (a_1b_1, \ldots, a_nb_n)$$
product on $\mathbb{F}_q^n$. For two linear subspaces $A, B \subseteq \mathbb{F}_q^n$, their Schur product is the linear subspace
$$A * B = \mathrm{Span}_{\mathbb{F}_q}\{a * b : a \in A \text{ and } b \in B\}.$$
If $B = A$, then $A * A$ is denoted as $A^{*2}$, and we define $A^{*t}$ by induction for any positive integer $t$.

One of the main results in [15] is that when the length $n$ is such that $n \geqslant k(k+1)/2$, the dimension of the square of the random code $C$ is exactly $k(k+1)/2$, with probability tending to 1 as $n - k(k+1)/2$ approaches infinity. More precisely, we define $\mathcal{F}(n, k)$ as the family of linear codes of length $n$ and dimension $k$. Let $n : \mathbb{N} \longrightarrow \mathbb{N}$ be such that $n(k) \geqslant k(k+1)/2$. Then there exits a constant $\gamma \in \mathbb{R}$ such that, for all large enough $k$,
$$\Pr\left(\dim C * C = \frac{k(k+1)}{2}\right) \geqslant 1 - 2^{\gamma(n(k)-k(k+1)/2)},$$
where $C$ is chosen uniformly at random from $\mathcal{F}(n(k), k)$. This observation serves as a useful distinguisher between random linear subspaces and those with a rich algebraic structure.

**Definition 2.** Let $\mathcal{C}$ be an $[n, k]_q$ linear code. We say that $\mathcal{C}$ is *s-good*, if
$$\dim(\mathcal{C} * \mathcal{C}) = \dim(\mathcal{C}^\perp * \mathcal{C}^\perp) = n.$$

## 4. Algebraic-geometric codes: constructions and parameters

Algebraic-geometric codes are linear error-correcting codes constructed from algebraic curves over finite fields. They are defined by *evaluating functions* or by using *residues of differentials*. Their parameters can be derived from well-known theorems of algebraic geometry. Our notation and terminology on algebraic plane curves over finite fields, their function fields, divisors and Riemann — Roch spaces are standard, see for instance [16].

Let $\mathcal{X}$ be an algebraic curve, i.e., an affine or projective variety of dimension one, which is absolutely irreducible and nonsingular, and whose defining equations are (homogeneous) polynomials with coefficients in $\mathbb{F}_q$. Let $g = g(\mathcal{X})$ be the genus of $\mathcal{X}$, $\mathbb{F}_q(\mathcal{X})$ denotes the function field of $\mathcal{X}$. A *divisor* $D$ of $\mathcal{X}$ is a formal sum $D = n_1P_1 + \ldots + n_kP_k$, where $n_1, \ldots, n_k \in \mathbb{Z}$ and $P_1, \ldots, P_k$ are places of $\mathbb{F}_q(\mathcal{X})$. If $n_1 \ldots, n_k \geqslant 0$, then $D \succeq 0$. If $D, E$ are two divisors and $D - E \succeq 0$, then $D \succeq E$. For a non-zero function $f$ in the function field $\mathbb{F}_q(\mathscr{X})$ and a place $P$, $v_P(f)$ stands for the order of $f$ at $P$. If $v_P(f) > 0$, then $P$ is a zero of $f$, while if $v_P(f) < 0$, then $P$ is a pole of $f$ with multiplicity $-v_P(f)$. The *principal divisor* of a non-zero function $f$ is $\mathrm{Div}(f) = \sum\limits_P v_P(f)P$.

For a divisor $D$, the associated Riemann — Roch space $\mathscr{L}(D)$ is the vector space

$$\mathscr{L}(D) = \{f \in \mathbb{F}_q(\mathcal{X}) \setminus \{0\} : \mathrm{Div}(f) \succeq -D\} \cup \{0\}.$$

The dimension $\ell(D)$ of $\mathscr{L}(D)$ is given by the Riemann-Roch Theorem [16, Theorem 1.1.15]:

$$\ell(D) = \ell(W - D) + \deg D - g + 1,$$

where $W$ is a canonical divisor. We denote the set of *differentials* on $\mathcal{X}$ by $\Omega$. The *differential space* of the dividor $D$ is

$$\Omega(D) = \{dh \in \Omega : \mathrm{Div}(dh) \succeq A\} \cup \{0\}.$$

In the following, $P_1, P_2, \ldots, P_n$ are pairwise distinct places on $\mathcal{X}$, and $D$ is the divisor $D = P_1 + \ldots + P_n$. Let $G$ be another divisor with support disjoint from $D$. We define two types of AG codes, the *functional* and the *differential codes*, respectively:

$$\begin{aligned} C_L(D, G) &= \{(f(P_1), \ldots, f(P_n)) : f \in \mathscr{L}(G)\}, \\ C_\Omega(D, G) &= \{(\mathrm{res}_{P_1}(\omega), \ldots, \mathrm{res}_{P_n}(\omega)) : \omega \in \Omega(G - D)\}. \end{aligned}$$

These codes are dual to each other, and $C_\Omega(D, G) = C_L(D, K + D - G)$ for an well-chosen canonical divisor $K$. The Riemann — Roch theorem enables us to estimate the dimension and the minimum distance of AG codes:

$$\dim(C_L(D,G)) \begin{cases} \geqslant \deg(G) - g + 1, & 0 \leqslant \deg(G) \leqslant 2g - 2, \\ = \deg(G) - g + 1, & 2g - 2 \leqslant \deg(G) \leqslant n, \\ \leqslant \deg(G) - g + 1, & n \leqslant \deg(G) \leqslant n + 2g - 2. \end{cases}$$

The minimum distance of a functional code is at least its *designed minimum distance*

$$\delta_L = n - \deg(G).$$

AG codes have polynomial time decoding algorithms, that can correct up to $t = (\delta_L - g)/2$ errors [5]. However, they are vulnerable to Schur filtration attacks. In particular, AG codes are far from being s-good. The following proposition is derived from [17, Theorem 6].

**Proposition 1.** Let $G$ and $G'$ be two divisors on the curve $\mathcal{X}$ both with disjoint support with the divisor $D$ and such that $\deg G \geqslant 2g+1$ and $\deg G' \geqslant 2g$. Then

$$C_L(D,G) * C_L(D,G') = C_L(D,G+G').$$

In particular,

$$\dim(C_L(D,G)^{*2}) \leqslant 2\dim(C_L(D,G)) + g - 1.$$

Let $\mathcal{C}$ be a linear subspace of the functional code $C_L(D,G)$. The Schur filtration attack constructs an effective decoding algorithm using a system of linear subspaces

$$W_{i,j} = \{z \in \mathbb{F}_q^n : z * \mathcal{C}^{*i} \leqslant \mathcal{C}^{*j}\}.$$

Here, $i,j \geqslant 1$ may be arbitrary. Clearly, if $i<j$, then $\mathcal{C}^{*(j-i)} \leqslant W_{i,j}$.

## 5. Subfield subcodes of 1-point Hermitian codes

Reed — Solomon codes form a well-known subclass of AG codes. In this section, we present the construction of Hermitian codes, another subclass of interest. Let $\mathscr{H}_q$ be a Hermitian curve over a finite field $\mathbb{F}_{q^2}$. In affine coordinates, $\mathscr{H}_q$ is given by the equation

$$\mathscr{H}_q : Y^q + Y = X^{q+1}.$$

It is a non-singular curve, and its genus is $g = q(q-1)/2$ by the genus formula. $\mathscr{H}_q$ has one point $P_\infty = (0:1:0)$ at infinity, and $q^3$ affine rational points $P_1,\ldots,P_{q^3}$. This makes the class of Hermitian curves interesting since they attain the maximal number of rational points for Hasse — Weil bound [18]. Such curves are called $\mathbb{F}_{q^2}$*-maximal.* Xing and Stichtenoth [19] showed that for fixed $q$, the genus of a $\mathbb{F}_{q^2}$-maximal curve is $\leqslant q(q-1)/2$, and equality holds if and only if $\mathcal{X}$ is isomorphic to $\mathscr{H}_q$.

**Definition 3.** Let $s$ be a positive integer. The $\mathbb{F}_{q^2}$-linear code $C_L(D, sP_\infty)$ of length $n = q^3$ is called a *Hermitian 1-point code.*

In general, it is a hard computational problem to determine a bases of the Riemann — Roch space $\mathscr{L}(D)$. For 1-point divisors $D = sP_\infty$ of the Hermitian curve, such a basis is given in [18, Theorem 10.4]. The dual of $C_L(D, sP_\infty)$ is a 1-point Hermitian code too, with parameter

$$s^\perp = n + 2g - 2 - s = q(q^2 - q - 1) - s.$$

Clearly, 1-point Hermitian codes form an increasing series of linear subspaces of $\mathbb{F}_{q^2}^n$.

Let $m$ be a positive integer and $r = q^m$. Let $\mathcal{C}$ be a linear $[n,k,t]$ code over $\mathbb{F}_r$. The $\mathbb{F}_r/\mathbb{F}_q$ subfield subcode of $\mathcal{C}$ is defined as

$$\mathcal{C}|_{\mathbb{F}_q} = \mathcal{C} \cap \mathbb{F}_q^n.$$

The true dimension $k^*$ of $\mathcal{C}|_{\mathbb{F}_q}$ is hard to determine, but the bound

$$k^* \geqslant n - m(n-k)$$

is straightforward. Any algorithm that can decode up to $t$ errors of $\mathcal{C}$ can be used to correct up to $t$ errors of the subfield subcode $\mathcal{C}|_{\mathbb{F}_q}$.

In this paper, we examine the class

$$C_q(s) = C_L(D, sP_\infty)|_{\mathbb{F}_q}$$

of Hermitian subfield subcodes, and propose their usage in code-based cryptosystems. In [20], we determined the true dimension of $C_q(s)$ for some specific values of $s$. In [21], we conducted an experimental study to analyze the true dimension of $C_q(s)$ for $q \leqslant 16$, and concluded that the datasets can be best approximated by the extreme value distribution.

Here, our focus is on the resistance of $C_q(s)$ to the Schur distinguishing attack. We determine the parameters such that the key size is significantly smaller than in the classic McEliece scheme. Notice that the Schur filtration technique may be used for key recovery attacks on subfield subcodes of AG codes, as well, provided the degree $m$ of the field extension, and the genus of the underlying algebraic curve are small. In our case, $m = 2$ is small, but the genus is the largest possible with fixed field $\mathbb{F}_{q^2}$ and maximal length $n$.

**Proposition 2.** Let $q$ be a prime power and let $C_q(s) = C_L(D, sP_\infty)|_{\mathbb{F}_q}$ be a 1-point Hermitian subfield subcode. There are positive integers $a_q, b_q$ such that $C_q(s)$ is s-good if and only if $a_q \leqslant s \leqslant b_q$.

We conducted numerical experiments to determine the values $a_q, b_q$ for $q \leqslant 16$, see Table 1. The results motivate the following conjecture.

**Open problem 1.** Let $q$ be a prime power and let $C_q(s) = C_L(D, sP_\infty)|_{\mathbb{F}_q}$ be a 1-point Hermitian subfield subcode. Then $\dim(C_q(s)^\perp * C_q(s)^\perp) = q^3$ if and only if $s \leqslant q^3 - q - 1$.

Table 1

**Interval bounds for s-goodness**

| $q$ | 4 | 5 | 7 | 8 | 9 | 11 | 13 | 16 |
|---|---|---|---|---|---|---|---|---|
| $a_q$ | 45 | 72 | 192 | 315 | 400 | 720 | 1 176 | 2 295 |
| $b_q$ | 59 | 119 | 335 | 503 | 719 | 1 319 | 2 183 | 4 079 |

## 6. Comparative of Hermitian subfield subcodes to McEliece cryptosystem: key size and security level

The National Institute of Standards and Technology (NIST) has recently begun a selection process to standardize asymmetric cryptosystems resistant to quantum computer attacks [4]. Code-based cryptosystems are promising candidates for NIST selection.

In this section, we analyse the computational cost of solving the ISD problem for various sets of parameters relevant to post-quantum cryptography. To do so, we consider classical McEliece cryptosystem variants built on Goppa codes. The parameters for cryptosystems reported in [22] are designed to be comparable to the computational cost required to break AES-128 (Category 1), AES-192 (Category 3), and AES-256 (Category 5). The Tables 2 and 3 summarize the code parameters of Classical McEliece cryptosystem submitted to NIST round 2-code-based cryptosystems, and those of 1-point Hermitian subfield subcodes $C_q(s)$ (code length $n$, dimension $k$, and error-capability $t$), as well as the computational cost of Prange's ISD algorithm, expressed as $\log_2$ (bit operations) with the public key size.

Table 2

**Classic McEliece cryptosystem**

| **Classic McEliece** | $n$ | $k$ | $t$ | Prange complexity | Key size (bit) |
|---|---|---|---|---|---|
| Category 1 | 3 488 | 2 720 | 64 | 142.78 | 2 088 960 |
| Category 3 | 4 608 | 3 360 | 96 | 184.89 | 4 193 280 |
| Category 5 | 6 688 | 5 024 | 128 | 262.35 | 8 359 936 |
| | 6 960 | 5 413 | 119 | 263.44 | 8 373 911 |
| | 8 192 | 6 528 | 128 | 300.14 | 10 862 592 |

Table 3

**McEliece cryptosystem based on s-good 1-point Hermitian subfield subcodes**

| | Code Type | $n$ | $k$ | $t$ | Prange complexity | Key size (bit) |
|---|---|---|---|---|---|---|
| Category 1 | $C_{11}(1\,174)$ | 1 331 | 927 | 78 | 142.33 | 1 123 524 |
| Category 3 | $C_{13}(2\,039)$ | 2 197 | 1 735 | 79 | 185.89 | 3 206 280 |
| | $C_{16}(3\,980)$ | 4 096 | 3 634 | 58 | 187.40 | 6 715 632 |
| Category 5 | $C_{13}(1\,861)$ | 2 197 | 1 398 | 168 | 263.01 | 4 468 008 |
| | $C_{16}(3\,874)$ | 4 096 | 3 422 | 111 | 300.65 | 9 225 712 |

## REFERENCES

1. *Arute F., Arya K., Babbush R, et al.* Quantum supremacy using a programmable superconducting processor. Nature, 2019, vol. 574(7779), pp. 505–510.
2. *Shor P.* Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput., 1997, vol. 26, pp. 1484–1509.
3. *McEliece R. J.* A Public-Key Cryptosystem Based on Algebraic Coding Theory. Jet Propulsion Lab, 1978. DSN Progress Report 44. pp. 114–116.
4. Post-Quantum Cryptography. `http://csrc.nist.gov/projects/post-quantum-cryptography`. Updated: March 25, 2020.
5. *Høholdt T., and Pellikaan R.* On the decoding of algebraic-geometric codes. Special Issue on Algebraic Geometry Codes. IEEE Trans. Inform. Theory, 1995, vol. 41, no. 6, part 1, pp. 1589–1614.
6. *Couvreur A., Márquez-Corbella I., and Pellikaan R.* Cryptanalysis of McEliece cryptosystem based on algebraic geometry codes and their subcodes. IEEE Trans. Inform. Theory, 2017, vol. 63(8), pp. 5404–5418.
7. *Couvreur A., Márquez-Corbella I., and Pellikaan R.* Cryptanalysis of public-key cryptosystems that use subcodes of algebraic geometry codes. Coding Theory and Applications. Cham, Springer, 2015, pp. 133–140.
8. *Couvreur A., Otmani A., and Tillich J.-P.* Polynomial time attack on wild mceliece over quadratic extensions. IEEE Trans. Inform. Theory, 2016, vol. 63(1), pp. 404–427.
9. *Wieschebrink C.* Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes. Intern. Workshop Post-Quantum Cryptogr., Berlin, Springer, 2010, pp. 61–72.
10. *Berger T. P. and Loidreau P.* How to mask the structure of codes for a cryptographic use. Des. Codes Cryptogr., 2005, vol. 35(1), pp. 63–79.
11. *Couvreur A., Gaborit P., Gauthier-Umaña V., et al.* Distinguisher-based attacks on public-key cryptosystems using Reed —- Solomon codes. Des. Codes Cryptogr., 2014, vol. 73(2), pp. 641–666.
12. *Berlekamp E. R., McEliece R. J., and van Tilborg H. C. A.* On the inherent intractability of certain coding problems. IEEE Trans. Inform. Theory, 1978, vol. IT-24(3), pp. 384–386.
13. *Prange E.* The use of information sets in decoding cyclic codes. IRE Trans. Inform. Theory, 1962, vol. 8(5), pp. 5–9.
14. *Canto Torres R. and Sendrier N.* Analysis of information set decoding for a sub-linear error weight. LNCS, 2016, vol. 9606,pp. 144–161.
15. *Cascudo I., Cramer R., Mirandola D., and Zémor G.* Squares of random linear codes. IEEE Trans. Inform. Theory, 2015, vol. 61(3), pp. 1159–1173.
16. *Stichtenoth H.* Algebraic Function Fields and Codes. Graduate Texts in Math., Berlin, Springer Verlag, 2009, vol. 254, 355 p.
17. *Mumford D.* Varieties defined by quadratic equations. Questions on Algebraic Varieties. C.I.M.E. Summer Schools, vol. 51. Berlin; Heidelberg, Springer, 2010, pp. 29–100.

18. *Menezes A. J., Blake I. F., Gao X., et al.* Applications of Finite Fields. Kluwer Intern. Series Engin. Computer Sci., Boston, MA, Kluwer Academic Publishers, 1993, vol. 199. 218 p.

19. *Xing C. P. and Stichtenoth H.* The genus of maximal function fields over finite fields. Manuscripta Math., 1995, vol. 86(2), pp. 217–224.

20. *El Khalfaoui S. and Nagy G. P.* On the dimension of the subfield subcodes of 1-point Hermitian codes. Adv. Math. Commun., 2021, vol. 15(2), pp. 219–226.

21. *Nagy G. P. and Khalfaoui S. E.* Estimating the dimension of the subfield subcodes of Hermitian codes. Acta Cybernetica, 2020, vol. 24(4), pp. 625–641.

22. *Baldi M., Barenghi A., Chiaraluce F., et al.* A finite regime analysis of information set decoding algorithms. Algorithms, 2019, vol. 12(10), p. 209.