DOI 10.15276/imms.v12.no4.280
UDC 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 12 (2022), No. 4, pp. 280-287

McELIECE CRYPTOSYSTEM BASED ON QUATERNARY HAMMING CODES

D.A. Isakov, A.V. Sokolov

National Odesa Polytechnic University
Ukraine, Odesa, 65044, Shevchenko Ave., 1, radiosquid@gmail.com

The operation of modern information protection systems is largely based on asymmetric cryptographic algorithms that allow encrypted information to be transmitted over an open communication channel without the need for prior key exchange. Modern asymmetric cryptographic algorithms are based on the use of such one-sided functions as factorization of large prime numbers and discrete logarithms, which require significant computational costs for their use, and are not resistant to promising quantum cryptanalysis attacks. Existing modifications of these cryptographic algorithms based on elliptic curves are also characterized by some significant drawbacks: many robust elliptic curves are currently patented, and algorithms on elliptic curves often require the use of powerful physical generators of truly random numbers. The solution to these problems is the use of the McEliece cryptographic system, which is based on the problem of decoding complete linear codes. Despite the prevailing performance of this system and its resistance to promising quantum cryptanalysis attacks, such a shortcoming as the large length of its public key has led to the fact that it is not often used in practice. In this paper, new families of Hamming (n,k)-codes in extensions of extended Galois fields are proposed and it is shown that on the basis of these codes a McEliece cryptosystem can be built, which is characterized by a much smaller size of the public key while providing a comparable number of generator matrices of the code so providing the comparable value of the protection levels number. The possibility of applying cascade Hamming codes on the extensions of extended Galois fields is shown, which makes it possible to obtain protection against the Sidelnikov attack. The proposed cryptosystem can be recommended for practical use in applications that require high speed (for example, mobile devices, IoT devices, and embedded systems), as well as significant cryptographic strength, including protection against promising quantum attacks.
Keywords: asymmetric cryptography, McEliece cryptographic system, Hamming codes, quaternary logic.

Introduction and statement of the problem

Asymmetric cryptographic algorithms are a crucial element of modern information protection systems, that largely determines their effectiveness and performance [1]. Today the use of asymmetric cryptography makes it possible to solve such basic tasks of information protection systems as key distribution, user authentication, confirmation of message authorship, protection of the software, etc.

Among the most widespread in practice [2] asymmetric cryptographic algorithms, it is necessary to note the Diffie-Hellman key distribution system, as well as RSA and El-Gamal full-fledged asymmetric cryptographic algorithms, which are based on the task of the complexity of factorization of large numbers and calculation of discrete logarithms. Despite the breakthrough nature of these cryptographic algorithms and their indisputably high importance in the tasks of ensuring the security of modern information technologies, they are characterized by some significant drawbacks, including high computational complexity of encryption/decryption algorithms, strict requirements for key information, vulnerability to promising quantum cryptanalysis attacks [3]. The computational complexity of these asymmetric cryptographic algorithms significantly limits their use on modern resource-constrained platforms: mobile devices, IoT (Internet of Things) devices, UAV (Unmanned Aerial Vehicles), and also leads to the fact that everywhere in practical

information transmission systems, asymmetric cryptographic algorithms are used once to exchange a key information, after which encryption of the main data arrays is performed using faster symmetric cryptographic algorithms.

The existence of effective quantum algorithms [4] for the factorization of big numbers and calculation of discrete logarithms, as well as the significant pace of development of quantum computers, is a quite real threat to the security of asymmetric cryptographic algorithms based on these computationally complex problems, which led to the appearance of modifications of the Diffie-Hellman, RSA, and El-Gamal cryptographic algorithms based on the elliptic curves [5]. Nevertheless, even these modifications are characterized by some significant drawbacks: the computational complexity remains high, not all elliptic curves provide a sufficient level of security, many robust elliptic curves are currently patented, algorithms on elliptic curves often require the use of powerful physical generators of truly random numbers, which leads to the complication and increase in the cost of the devices on which they are used.

As leading modern research shows, one of the powerful solutions of post-quantum cryptography, which is characterized by a significant reduction in computational complexity (and, therefore, is potentially suitable for use on resource-constrained devices), is crypto-code constructions [6], among which the McEliece cryptosystem is the most widely used solution. This cryptosystem is characterized by a lower level of computational complexity when compared to RSA and El-Gamal [7] cryptographic algorithms and a much higher level of resistance to quantum cryptanalysis attacks. Nevertheless, despite its advantages, the classical McEliece cryptographic system is characterized by a large amount of key information, which is necessary to achieve a sufficient level of cryptographic strength, which significantly limits its use in practice.

The *purpose* of this paper is to reduce the size of the public key in the McEliece cryptographic system while preserving its cryptographic strength using quaternary Hamming codes.

Quaternary Hamming codes based on the extensions of extended Galois fields

Hamming error-correcting codes are linear codes for the binary alphabet with code distance $d = 3$, which allow detecting double and correcting single errors [8]. Today, Hamming codes are quite well-researched and widely used in practice. However, despite the significant scientific results obtained in the theory of error-correcting coding for classes of binary linear codes, a large number of issues related to the application of non-binary codes remain unsolved. The conceptual idea of quaternary Hamming codes was introduced in [9].

The performed research shows that Hamming codes can be constructed not only for the extended Galois field $GF(2^2)$, but also for the extensions of the extended Galois fields $GF(q^r)$, $q = 2^u, u = 2,3,...$ which were introduced in [10, 11]. This fact allows us to talk about the existence of new families of Hamming codes in the extensions of extended Galois fields. For example, let the Galois field $GF(q^r)$, where r is the number of parity symbols in the Hamming code being constructed. Then the parameters of the code will be determined by the following ratios: the total number of codeword symbols $n = \frac{q^r - 1}{q - 1}$, the number of data symbols $k = \frac{q^r - 1}{q - 1} - r$, the number of errors detected by the code $f = 2$, the number of errors corrected by the code $t = 1$.

In this paper, we consider an extended Galois field $GF(2^2)$, the arithmetic of which can be constructed according to the only existing primitive irreducible polynomial $f(x) = x^2 + x + 1$ of degree $\deg(f(x)) = 2$. We provide the tables of addition and

multiplication in the Galois field $GF(2^2) = GF(4)$, the arithmetic of which is determined by the previously mentioned polynomial.

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

,

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

. (1)

Considering relation (1), we can talk about the existence of new families of Hamming codes based on the extension of extended Galois field $GF(4^r)$ the first of which has the following parameters: (5, 3), (21, 18), (85, 81) for $r = 2,3,4$. These codes can be specified using a parity-check matrix H, which is determined by the following relation

$$H = [H_{r,k} \mid I_{r,r}], \tag{2}$$

where $I_{r,r}$ is the matrix of order r whose columns have unit Hamming weight; $H_{r,k}$ is the matrix of size $r \times k$ that contains columns which are orthogonal in the Galois field $GF(4^r)$ to each other, as well as to the columns of the matrix $I_{r,r}$. Therefore, by construction, all columns of the matrix H are mutually orthogonal.

On the basis of the parity-check matrix, the generator matrix can be constructed by concatenating the matrix $I_{k,k}$ of order k whose columns have unit Hamming weight and transposed matrix $H_{r,k}$

$$G = [I_{k,k} \mid -H_{r,k}^T], \tag{3}$$

where T is the transposition symbol.

Consider the example of constructing a Hamming (5,3)-code based on the extension of the extended Galois field $GF(4^2)$. The Galois field $GF(4^2)$ contains 15 nonzero elements, each of which we can represent as a quaternary vector. At the same time, the specified elements form $(q^r - 1)/3$ classes, which contain linearly dependent vectors, in other words, those that can be obtained from each other by multiplying by a constant $a \in \{1,2,3\}$ in the Galois field $GF(4^2)$, i.e., according to the multiplication table (1). For our example, there are $(4^2 - 1)/3 = 5$ classes of linearly independent quaternary vector elements of the Galois field $GF(4^2)$ which are represented by different colors

$$V = \{01,02,03,10,11,12,13,20,21,22,23,30,31,32,33\}. \tag{4}$$

Choosing one vector from each class, we can construct the parity-check matrix H in accordance with (2)

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & 2 & 3 & 0 & 1 \end{bmatrix}, \tag{5}$$

which completely defines the parity-check equations

$$\begin{cases} x_1 + x_2 + x_3 + x_4 = s_1; \\ x_1 + 2x_2 + 3x_3 + x_5 = s_2. \end{cases} \tag{6}$$

where arithmetic operations are performed according to tables (1).

Let us also point out that the columns of the H matrix can be arranged in an arbitrary order, just as any vectors from the equivalent classes (4) can be chosen. In performing these operations, the correcting ability of the code does not change.

Note that decoding of information, as in the case of Hamming binary codes, can be performed on the basis of the syndrome method [8]. The specific value of the syndrome

$S = HC'^T = [s_1 \quad s_2]^T$ coincides with the column of the matrix H, which corresponds to the symbol where the error occurred, which is multiplied by the amplitude of the error. Thus, it becomes possible to correct the error that occurred after calculating the syndrome.

On the basis of the parity-check matrix, a generator matrix can be constructed in accordance with (3)

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 3 \end{bmatrix}, \tag{7}$$

which defines the encoding equations for the parity-check symbols

$$\begin{cases} x_4 = x_1 + x_2 + x_3; \\ x_5 = x_1 + 2x_2 + 3x_3. \end{cases} \tag{8}$$

Consider an example of the operation of the proposed Hamming correction code. Let an information message $A = [0 \quad 1 \quad 2]$ be given, which we will encode with the proposed Hamming code. Let's suppose that an error with a value of amplitude equal to 2 occurred in the second element of the codeword (which corresponds to the second information element), i.e., the error vector is equal to $e = [0 \quad 2 \quad 0 \quad 0 \quad 0]$, while the received codeword will have the form $C' = [0 \quad 3 \quad 2 \quad 3 \quad 3]$.

On the receiving side, we calculate the value of the syndrome, which will be equal to $S = [2 \quad 3]^T$. Since the obtained syndrome corresponds to the second column of the matrix multiplied by a constant $a = 2$, we conclude that the error occurred in the second element of the codeword, while the amplitude of the change was equal to 2. This allows us to reproduce the correct codeword C.

The algorithm for generation of parity-check matrices for quaternary Hamming codes

Note that in the case of using extensions of extended Galois fields, in particular, for the construction of Hamming quaternary codes, there is an urgent need to select linearly independent vectors in the complete quaternary vector code, i.e. to classify it into classes, each of which contains 3 linearly independent vectors. Solving this problem for large values of r can be quite computationally complex, as it involves sorting through a set of $q^r - 1$ elements.

To solve this problem, the proposed algorithm for generating the code of all possible vectors that does not contain their linear combinations can be applied:

Step 1. For the value $r = 1$, this code contains only one codeword $\{1\}$.

Step 2. For a given value of r, the code of linearly independent vectors is constructed as follows based on the code of linearly independent vectors of length $r - 1$.

Step 2.1. Concatenate the symbol "0" to each codeword of the code of linearly independent vectors of length $r - 1$ as the most significant element of the codeword.

Step 2.2. The rest of the codewords of the code of linearly independent vectors are constructed by concatenating the symbol "1" as the most significant element of the codeword to the complete code of quaternary vectors of length $r - 1$.

For example, with the help of the proposed algorithm, we will construct a code of linearly independent vectors for the value $r = 2$

$$\{0 \quad 1\}; \quad \{1 \quad 0\}; \quad \{1 \quad 1\}; \quad \{1 \quad 2\}; \quad \{1 \quad 3\}, \tag{9}$$

on the basis of which the code of linearly independent vectors for the value $r = 3$ can be built

$$\begin{array}{ccccccccccc} \{0 & 0 & 1\}; & \{0 & 1 & 0\}; & \{0 & 1 & 1\}; & \{0 & 1 & 2\}; & \{0 & 1 & 3\}; \\ \{1 & 0 & 0\}; & \{1 & 0 & 1\}; & \{1 & 0 & 2\}; & \{1 & 0 & 3\}; & & & \\ \{1 & 1 & 0\}; & \{1 & 1 & 1\}; & \{1 & 1 & 2\}; & \{1 & 1 & 3\}; & & & \\ \{1 & 2 & 0\}; & \{1 & 2 & 1\}; & \{1 & 2 & 2\}; & \{1 & 2 & 3\}; & & & \\ \{1 & 3 & 0\}; & \{1 & 3 & 1\}; & \{1 & 3 & 2\}; & \{1 & 3 & 3\}, & & & \end{array} \quad (10)$$

and so on.

We note that to build the parity-check matrix of the Hamming code, as its columns the linearly independent vectors of the code of linearly independent vectors can be taken in an unchanged form, or in the form of their linear combinations obtained by multiplying them by some constants $a_i, i = 1, 2, ..., {4^k}/{3} - 1$.

McEliece cryptographic system based on quaternary Hamming codes

The proposed quaternary Hamming codes could be the basis for the McEliece cryptographic system, while giving it specific advantages over existing variants of this cryptographic system based on other codes. Let's consider the algorithms of the McEliece cryptographic system based on quaternary Hamming codes in the mode of transmitting information from party B (Bob) to party A (Alice), accompanying it with specific examples.

The algorithm for generation of key information

Step 1. Alice chooses an (*n*,*k*)-linear code Υ that corrects one error. Then the generator matrix G of size $k \times n$ is calculated for the code Υ.

Step 2. In order to complicate the task of recovering the original code, Alice generates a random non-singular matrix S of size $k \times n$ over the alphabet $\{0,1\}$.

Step 3. Alice generates an arbitrary permutation matrix P of size $n \times n$.

Step 4. Alice computes the matrix $G' = SGP$ of size $k \times n$, which is considered as a public key. A private key is a set $\{S, G, P\}$.

As an example, let's choose the generator matrix (7) synthesized by us in Section 2, and also generate a random non-singular matrix S and a permutation matrix P

$$S = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}; \quad P = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}. \quad (11)$$

We calculate the public key matrix

$$G' = SGP = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 3 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 3 & 0 & 1 \\ 1 & 0 & 2 & 1 & 0 \\ 0 & 1 & 2 & 0 & 1 \end{bmatrix}, \quad (12)$$

for the storage or transmitting of which in the binary form we will need $2kn$ bits, since the elements of this matrix are quaternary.

The algorithm for information encryption

We will describe the encryption algorithm in the form of specific steps.

Step 1. Bob represents his message *m* as sequences of quaternary characters x of length *k*.

Step 2. Bob generates a random vector *e* of length *n* with Hamming weight *t*.

Step 3. Bob calculates the ciphertext as $y = xG' + e$ and transmits it to Alice.

Suppose that after receiving the public key G' from Alice, Bob formed a message $x = \begin{bmatrix} 1 & 2 & 1 \end{bmatrix}$ and also chose an error vector $\begin{bmatrix} 0 & 1 & 0 & 0 & 0 \end{bmatrix}$. Bob can then encrypt his plaintext message

$$y=\begin{bmatrix}1 & 2 & 1\end{bmatrix}\begin{bmatrix}1 & 0 & 3 & 0 & 1\\ 1 & 0 & 2 & 1 & 0\\ 0 & 1 & 2 & 0 & 1\end{bmatrix}+\begin{bmatrix}0 & 1 & 0 & 0 & 0\end{bmatrix}=\begin{bmatrix}3 & 0 & 2 & 2 & 0\end{bmatrix}. \quad (13)$$

After encryption, the open message is transfered to Alice, who performs the following steps to decrypt the message using her private key.

The algorithm for information decryption

Step 1. Alice calculates the inverse matrix P^{-1}.

Step 2. Alice calculates $\hat{y}=yP^{-1}$.

Step 3. Alice uses the Υ code decoding algorithm to obtain from $\hat{y}$ the value of $\hat{x}$.

Step 4. Alice calculates $x=\hat{x}S^{-1}$.

For our example

$$P^{-1}=\begin{bmatrix}0 & 0 & 0 & 1 & 0\\ 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1\\ 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0\end{bmatrix}, \quad (14)$$

while $\hat{y}=\begin{bmatrix}0 & 2 & 0 & 3 & 2\end{bmatrix}$.

Applying the algorithm for quaternary decoding, we see that the syndrome is equal to $[1\ 1]$: due to permutations, the error has moved to the 1st symbol $eP^{-1}=\begin{bmatrix}1 & 0 & 0 & 0 & 0\end{bmatrix}$. Since the obtained syndrome corresponds to the 1-th column of the matrix H, and not to its linear combination, we conclude that the amplitude of the error was 1, i.e., the corrected codeword is $\hat{\hat{y}}=\begin{bmatrix}1 & 2 & 0 & 3 & 2\end{bmatrix}$, while $\hat{x}=\begin{bmatrix}1 & 2 & 0\end{bmatrix}$. We find that $x=[1\ \ 2\ \ 1]$, which corresponds to the original text.

Security of the system

In the case of using binary Hamming codes, as proposed in work [12] for the organization of the McEliece cryptographic system, the number of possible generator matrices G will be determined as $n!$ possible permutations of its rows due to the determined properties of the Hamming code. At the same time, the length of the open key will be kn. On the other hand, in the case of applying the quaternary Hamming code, we can choose each of the columns of the matrix in one of 3 ways from a set of its linear combinations, i.e., we get $(3n)!$ different matrices. At the same time, the length of the open key will be $2kn$.

For example, when using a binary Hamming (63,57)-code, the number of possible generator matrices will be $1.9826\cdot10^{87}$ while 3591 bits are required to store the public key, while a quaternary Hamming (21, 18)-code with the same number of generator matrices will require only 756 bits of the public key, i.e., in 4.75 times less. At the same time, due to the fact that the McEliece cryptographic system is based on Hamming codes in extensions of extended Galois fields it is able to simultaneously process a larger amount of input information, it potentially allows faster algorithmic implementations (compared to binary Hamming codes).

We also note that in the general case, the solution for systems of linear equations in extensions of the extended Galois fields is a more complicated task from a computational point of view, while for larger values of u, the specific Galois field isomorphism can be part of the secret key.

It is considered promising to use the McEliece cryptographic system based on the cascade quaternary Hamming codes to ensure security against the Sidelnikov attack. So, for example, 16 plaintext vectors encrypted by the McEliece cryptographic system based on the Hamming (21,18)-code can be re-encrypted by the McEliece cryptographic system

based on the Hamming (341,336)-code, which should ensure a high complexity of the relationship between the elements of the input and output data.

We note that more detailed security aspects of the proposed modification of the McEliece cryptographic system based on Hamming codes in the extensions of extended Galois fields is considered as subject of futher research.

Conclusions

Let's note the main results of the research performed:

1. New families of Hamming (n,k)-codes in the extensions of extended Galois fields $GF(q^r)$, where $q = 2^u, u = 2,3,\ldots$, are proposed. The properties of these codes as well as their ability to detect errors and correct errors have been established. The features of the application of the syndrome decoding algorithm for the developed families of Hamming codes are established.

2. An asymmetric McEliece cryptographic system based on Hamming codes in the extensions of extended Galois fields is proposed. It is shown that the use of extensions of extended Galois fields allows to provide a larger number of possible generator matrices of the Hamming code (i.e., a larger number of protection levels) with a shorter length of the public key. Thus, in the case of using a quaternary Hamming (21,18)-code instead of a binary Hamming (63,57)-code, with an equal number of possible generator matrices, the length of the public key will decrease by the factor of 4.75 times.

3. The proposed cryptographic system, based on the classical McEliece cryptographic system, is resistant to potential attacks of quantum cryptanalysis, has smaller values of the length of the public key, and therefore can be recommended for practical use in applications that require efficient and secure asymmetric cryptographic algorithms.

References

1. Al-Shabi M.A. A survey on symmetric and asymmetric cryptography algorithms in information security. *International Journal of Scientific and Research Publications (IJSRP)*. 2019. Vol. 9, No. 3. P. 576-589.
2. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley, 1996. 758 p.
3. Mavroeidis V. The impact of quantum computing on present cryptography. International *Journal of Advanced Computer Science and Applications*. 2018. Vol. 9, No. 3. P. 1-10.
4. Shor P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*. 1999. Vol. 41, No. 2. P. 303-332.
5. Washington L.C. Elliptic curves: number theory and cryptography. Chapman and Hall/CRC, 2008. 531 p.
6. Yevseiev S., Korol O., Kots H. Construction of hybrid security systems based on the crypto-code structures and flawed codes. *Eastern-European Journal of Enterprise Technologies*. 2017. Vol. 4, No. 9 (88). P. 4-21.
7. Tsyganenko A.S., Yevseiev S.P. Melnik K.V. McEliece and Niederreiter asymmetric crypto-code constructions in post-quantum cryptography. ITSEC: the 8th Intern. Sci. Conf. Kyiv: NAU, 2018. P. 26-27.
8. Mazurkov M.I. Fundamentals of the theory of information transmission. Odesa: Science and Technology, 2005. 168 p.
9. Yiyi H., Junbiao D. Quaternary checksum, redundancy and Hamming code. Preprint at Researchgate, 2022. P. 1-8.
10. Mazurkov M. I., Konopaka E. A. Families of linear recurrent sequences based on complete sets of isomorphic Galois fields. *Proceedings of universities. Radioelectronics.* 2005. No. 11. P. 58-65.

11. Mazurkov M.I., Sokolov A.V. Nonlinear transformations based on complete classes of isomorphic and automorphic representations of field GF(256). *Radioelectronics and Communications Systems.* 2013. Vol. 56, No. 11. P. 513-521.
12. Kabeya T.C. McEliece's Crypto System based on the Hamming Cyclic Codes. International *Journal of Innovative Science and Research Technology*. 2019. Vol. 4, No 7. P. 293-296.

КРИПТОСИСТЕМА McELIECE НА ОСНОВІ ЧЕТВІРКОВИХ КОДІВ ГЕМІНҐА

Д.А. Ісаков, А.В. Соколов

Національний університет «Одеська політехніка»
Україна, Одеса, 65044, пр-т Шевченка, 1, radiosquid@gmail.com

Застосування сучасних систем захисту інформації у великій мірі базується на асиметричних криптографічних алгоритмах, що дозволяють передавати зашифровану інформацію відкритим каналом зв'язку без необхідності попереднього обміну ключами по додатковому закритому каналу. Сучасні асиметричні криптографічні алгоритми засновані на використанні таких односторонніх функцій як факторизація великих простих чисел та дискретне логарифмування, які вимагають значні обчислювальні затрати для свого застосування, є нестійкими до атак квантового криптоаналізу. Існуючі модифікації цих криптоалгоритмів на основі еліптичних кривих також не позбавлені суттєвих недоліків: багато «вдалих» еліптичних кривих на сьогодні запатентовані, алгоритми на еліптичних кривих часто потребують застосування потужних фізичних генераторів істинно випадкових чисел. Вирішенням зазначених проблем є застосування криптосистеми МакЕліса, яка базується на проблемі декодування повних лінійних кодів. Незважаючи на переважаючу швидкодію даної системи та її стійкість до атак квантового криптоаналізу, такий її недолік, як великі довжини її відкритого ключа, призвів до того, що вона нечасто застосовується на практиці. У даній роботі запропоновано нові сімейства (n,k)-кодів Гемінґа над розширеннями розширених полів та показано, що на основі даних кодів може бути побудована криптосистема МакЕліса, що характеризується значно меншим розміром відкритого ключа при сумірному рівні кількості генераторних матриць коду. Показана можливість застосування каскадних кодів Гемінґа над розширеннями розширених полів, що дозволяє отримати захист від атаки Сідельникова. Запропонована криптосистема може бути рекомендована до практичного використання у застосунках, що потребують великої швидкодії (наприклад, мобільних пристроях, пристроях IoT, вбудовуваних системах), а також значної криптостійкості, у тому числі, захищеності від перспективних квантових атак.

Ключові слова: асиметрична криптографія, криптографічна система МакЕліса, коди Гемінґа, четвіркова логіка.