UDC 004.056.55

CODE-BASED SCHEMES FOR DIGITAL SIGNATURES

Alexandr Kuznetsov[1,2], Anastasia Kiian[1], Ivan Belozertsev[1], Mykola Pastukhov[3], Dmytro Prokopovych-Tkachenko[4]

[1] V. N. Karazin Kharkiv National University, 6 Svobody Sq., Kharkiv, 61022, Ukraine
[2] JSC "Institute of Information Technologies", 12 Bakulin St., Kharkiv, 61166, Ukraine
kuznetsov@karazin.ua, nastyak931@gmail.com, ivanbelozersevv.jw@gmail.com

[3] University of Customs and Finance, 2/4 Volodymyr Vernadsky St., Dnipro, 49000, Ukraine
denart66@gmail.com

[4] University of Customs and Finance, 2/4 Volodymyr Vernadsky St., Dnipro, 49000, Ukraine
me_dnepr@ua.fm

Reviewer: Ivan Gorbenko, Doctor of Sciences (Engineering), Full Professor, Academician of the Academy of Applied Radioelectronics Sciences, V. N. Karazin Kharkiv National University, 4 Svobody Sq., Kharkov, 61022, Ukraine
gorbenkoi@iit.kharkov.ua

Received on May 2018

Abstract. *This article is devoted to the features of construction and use of electronic digital signature schemes based on the use of error-correcting codes, namely the most common scheme, which is based on this approach, CFS and the new proposed scheme. A functioning of these schemes directly depends on used code cryptosystem: the first basically contains principles of Niederreiter code cryptosystem, the second involves use of McEliece cryptosystem, which until recently was considered impossible. Algorithms for generating and verifying signatures according to both schemes, described step by step, are considered in detail. The article studies the efficiency of algorithms in terms of volume of required keys and the length of generated signature, the results of which are presented using analytical ratios and in graphical form for specific examples. The resistance of the considered schemes to classical and quantum cryptanalysis was also analyzed, the latter of which is a actual topic in the era of the rapid development of the sphere of post-quantum cryptography. Both schemes have provable resistance to both types of cryptanalysis, but when using quantum computers it is necessary to significantly increase the key lengths, which is a great shortcoming. It has been revealed that the proposed scheme has an indisputable advantage over the used CFS scheme - protection from specific attacks such as a simultaneous replacement of two signature elements and rapid falsification, by adding an additional element to the generated signature. During the study, the advantages, disadvantages and prospects of using the proposed scheme and the CFS scheme in terms of use of quantum computers are highlighted.*

Keywords: *post-quantum cryptography; digital signature; code-based cryptography; quantum security.*

1 Introduction

In today's increasingly tumultuous world, information is gaining in value. Today, it is perhaps the most expensive resource of mankind. That is why the issue of information security plays an important role and raises serious discussions around it. To date, there is a certain set of proprietary security algorithms that are used during manipulations with information on conventional computers. Despite this, the situation can change radically in the near future, as active work is under way in the quest for the development of a quantum computer [1-6].

A quantum computer is a computing device that works on the basis of the phenomena of quantum confusion and quantum superposition, and allows you to override options and perform complex calculations much faster. For this reason, existing algorithms and ciphers whose security is based on such mathematical problems as factorization of large numbers, discrete logarithms, and others, will lose their security [5].

From this perspective, algorithms designed for the formation and verification of digital signatures also become vulnerable to various types of attacks [3]. This fact will lead to the fact that an digital signature will not guarantee the integrity of the document and reliably confirm the identity of its author. From the above it follows the relevance of the comprehensive study of alternative schemes of digital signature and assessment of their capabilities. One of the most promising areas of research, from the standpoint of post-quantum efficiency, is cryptography, based on error-correcting codes [7-19]. In this work, we will consider two code schemes of a digital signature, we will carry

out their comparative analysis and estimation of possibilities of their application in the post-quantum period.

2 A classic example of a code-based digital signature scheme

A classic example of a digital signature scheme based on error-correcting codes is the CFS scheme, named after the initials of its inventors – Courtois, Finiasz, Sendrier [13].

CFS involves the use of algebraic (n, k, d) code from the class ($n=2^m$, $k=n-mt$, $2t+1$) of non-idle Goppa codes. The formation of the public and private keys of the scheme is in accordance with the principle used in the Niderraiter cryptosystem, which is discussed in detail in the papers [3, 7-11]. Hence, the private keys are matrices X, of size $(n-k)\times n$, and P, of size $n\times n$, which are similar to the Niderraiter scheme defined as a random inverse matrix and a random matrix of permutations respectively, as well as a fast algorithm for decoding an algebraic code. A private key is a matrix $H_X = X \cdot H \cdot P$, where H – the verification $(n-k)\times n$ matrix of the algebraic code and the correcting ability of the code t. The input data for using the CFS is a hash function h, a fast algorithm for decoding an algebraic code and a message (plain text). The hash function is intended to convert a message of arbitrary length. The output of the hash function is a hash value $h(x)$ of bit length $n-k$. A quick algorithm for decoding the algebraic code, that is, having a polynomial complexity, is applied to the syndromic sequence. $s=(s_0, s_1, ..., s_{n-k-1})$. In this case, one of the situations is possible:

- If decoding is successful the vector of errors $e=(e_0, e_1, ..., e_{n-1})$ corresponding to the syndrome will be displayed.
- If decoding is unsuccessful an error message will be displayed.

The signature formation algorithm consists of gradual execution of several steps. Initially, the hashing of the plain text M and the assignment to the counter i of value i=1. The hash value $h(M)$ and counter i are represented as bit sequences, from concatenation of which, the new hash value $h(h(M)\|i)$ is calculated. The latter should be interpreted as a syndromic sequence $s_X=(s_0, s_1, ..., s_{n-k-1})$ calculated for some arbitrary code word and error vector $e=(e_0, e_1, ..., e_{n-1})$. Since it was suggested that $h(h(M)\|i)$ is a syndrome, which is calculated according to the check matrix H of algebraic code, we need to build a vector:

$$s_X^{*T} = X^{-1} \cdot s_X{}^T = X^{-1} \cdot H_X \cdot e^T = H \cdot P \cdot e^T = H \cdot \overline{e}^T.$$

Then we can apply a fast decoding algorithm to find the vector $\overline{e}^T = P \cdot e^T$. If decoding fails, then you need to increment the value of the counter i and perform all actions, starting with the concatenation of the counter and the hash value of the message, until the derived vector $\overline{e}^T = P \cdot e^T$ is deduced, that corresponds to vector s_X^*. When such a vector is found, you need to go to the next step and calculate the value:

$$e^T = P^{-1} \cdot \overline{e}^T = P^{-1} \cdot P \cdot e^T.$$

The final signature for a message consists of two parts: the value of the counter and the vector e, $Y=(e,i)$. Formally, you we write the generated signature as

$$Y=(e,i): H_X \cdot e^T = \left(h(h(M)\|i)\right)^T.$$

In order to verify the authenticity of the signature, it must be ensured that the result of the hashing $h(h(M)\|i)$ is a syndromic sequence that was calculated according to the vector $e=(e_0, e_1, ..., e_{n-1})$, the latter is interpreted as a vector of errors.

A user who wants to verify the authenticity of the signature has an input of an a public key con-

sisting of t a matrix H_X, hash function *h*, the signature itself $Y=(e,i)$ and a message M. In order to verify a signature, you need to calculate the values of two vectors: $(s_X^{'})^T = H_X \cdot e^T$, $(s_X^{''})^T = h(h(M)\|i)$.

A digital signature is considered correct only if these two vectors are the same [3,13].

Therefore, the essence of the CFS scheme is the repeated hashing of a message that is encapsulated with a randomized counter value in order to identify the correct syndromic sequence. The stability of this scheme is based on the complexity of solving the problem of syndromic decoding.

3 An alternative scheme for formation and verification of digital signature

The CFS scheme is the most commonly code-based digital signature scheme. However, this scheme has certain disadvantages. In 2017, an alternative to this scheme was proposed. An alternative to the CFS, unlike the original scheme, is based on the use of the one-sided function of McEliece, which is considered in the works [16-19]. As a result, the private keys of this scheme are the matrixes X and P (in the case of non-binary codes, the matrix D is added), which are an invertible matrix and a permutation matrix, respectively, as well as a fast algorithm for decoding the algebraic code. The public key is a number *t*, which characterizes the corrective ability of algebraic (*n*, *k*, *d*) code from the class of irreducible Goppa codes. For a binary case, the code parameters are related to this relationship: $n = 2^m$, $k = n-mt$, $2t+1$. Also, the component of the public key is the matrix G_x, which is formed according to the rule $G_X = X \cdot H \cdot P \cdot D$, where G is a generating matrix of algebraic code.

When forming a signature, the same hash function *h* as in the CFS scheme is used, which was described in detail earlier, so we will not focus on it. The decoding algorithm is the ability to find the vector of errors $e=(e_0,e_1,...,e_{n-1})$ and the vector $I=(I_0,I_1,...,I_{k-1})$ according to the original code word with errors $c_X^* = (c*_0, c*_1, ..., c*_{n-1})$, taking into account the equation $c_X^* = I \cdot G_X + e$.

When signing a message, the user first has to find the hash code from its content and determine the value of the counter i equal to 1. Then, as in the CFS scheme, the concatenation of the hash value of the message and the counter occurs followed by the hashing of the generated sequence, which results in $h(h(M)\|i)$. $h(h(M)\|i)$ is interpreted as a codeword with errors $c_X^* = (c*_0, c*_1, ..., c*_{n-1})$, which is calculated for some values of the vectors $I=(I_0,I_1,...,I_{k-1})$ and $e=(e_0,e_1,...,e_{n-1})$, provided that $c = IG_X$ and $c_X^* = c+e$ are equal. The next step is to calculate the value of the vector $\bar{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1}$. It is assumed that the value of this vector represents the distorted codeword of the algebraic code no more than in t digits, that is, the distortion does not exceed the correction ability. A similar code word can be decoded using a polynomial complexity algorithm. Therefore, it is assumed that:

$$\begin{aligned}\bar{c}^* &= c_X^* \cdot D^{-1} \cdot P^{-1} = (I \cdot G_X + e) \cdot D^{-1} \cdot P^{-1} = \\ &= (I \cdot X \cdot H \cdot P \cdot D + e) \cdot D^{-1} \cdot P^{-1} = \\ &= I \cdot X \cdot H + e \cdot D^{-1} \cdot P^{-1}.\end{aligned}$$

By applying a polynomial complexity algorithm and decoding the code word. $\bar{c}^* = I' \cdot G + e'$, $e' = e \cdot D^{-1} \cdot P^{-1}$, we can find vector $I' = I \cdot X$. If decoding was successful, then the corresponding values I' and e' will be displayed. If the decoding failed, you need to increment the value of the counter and repeat all steps in the signature formation, starting with the concatenation initially, until the values I' and e' are successfully decoded. After finding such values, the vectors $I = I' X^{-1}$ and $e = e' \cdot D \cdot P$ are calculated.

The signature of a message in this case can be formally defined as

$Y=(I,e,i): IG_X+e=\left(h(h(M)\|i)\right)$ that is, it consists of a counter value i, for which $h(h(M)\|i)$ will be interpreted as a code word with errors a vector of errors e and information vector I. The complexity of calculating vectors I and e using known hash value $h(h(M)\|i)$ for an illegitimate user is a NP-complete task.

To verify the authenticity of the signature, you need to make sure that the result of the hashing $h(h(M)\|i)$ is a codeword with errors, which is calculated using the values of the vectors I and e. For the purpose of verification, it is necessary to calculate the values of two vectors $c_X^*{}' = IG_X + e$ and $c_X^*{}'' = h(h(M)\|i)$.

If the values of these vectors coincide $c_X^*{}' = c_X^*{}''$ and the Hamming weight of the vector e does not exceed the correcting ability of the code $w(e) \le t$, then the signature can be considered true. If at least one of the declared requirements is not fulfilled, the signature is rejected. Therefore, the essence of the CFS schema-alternative is to interpret the hex value of the sequence that came out by combining the value of the counter and the hex value of the message as a codeword with errors. At the same time, the verification procedure is radically different from the original scheme by adding another condition that provides an alternative scheme with advantages over CFS, which will be discussed in the next section.

4 The comparative analysis of schemes for the formation and verification of digital signatures

The lengths comparison of key scheme parameters

The CFS scheme and its alternative are based on two different approaches: the first is to use the function of the Niderraiter scheme, the second one of the McEliece scheme, on which the volumes of key signature data schemes depend directly.

Public Key:

– The CFS public key length is determined by the number of cells in the matrix $H_X = X \cdot H \cdot P$.

$$l_{PB.K.} = (n-k)\cdot n = n^2 - kn = m\cdot t\cdot 2^m.$$

– The length of the public key of the alternative scheme is determined by the number of cells in the matrix $G_X = X \cdot G \cdot P$

$$l_{PB.K.} = k\cdot n = (2^m - m\cdot t)\cdot 2^m.$$

Private Key:

– The length of the private key CFS is determined by the sum of the number of binary cells of the matrix (the size of $(n-k)\times(n-k)$) and the length of n integers in range $0,1,..,n-1$ for determining the matrix P and is calculated:

$$l_{PR.K.} = (n-k)^2 + n\cdot\lceil \log_2 n\rceil = (m\cdot t)^2 + 2^m\cdot m.$$

– The length of the private key of the alternative scheme is determined by the sum of the number of binary cells of the matrix X (the size of $(k\times k)$) and the length of n integers in range $0,1,..,n-1$ for determining the matrix P. This length can be calculated according to [17]:

$$l_{PR.K.} = k^2 + n\cdot\lceil \log_2 n\rceil = (2^m - m\cdot t)^2 + 2^m\cdot m.$$

In order to demonstrate the differences between the alternative scheme and the CFS scheme more clearly, we present a graphic representation (Fig. 1-2). After analyzing of the data, we can conclude that the graph of the private and public keys of the alternative scheme is declining, and the graph of the CFS scheme is increasing. Up to a certain point, the length of the private and public keys of the alternative scheme will exceed the values for the CFS scheme.

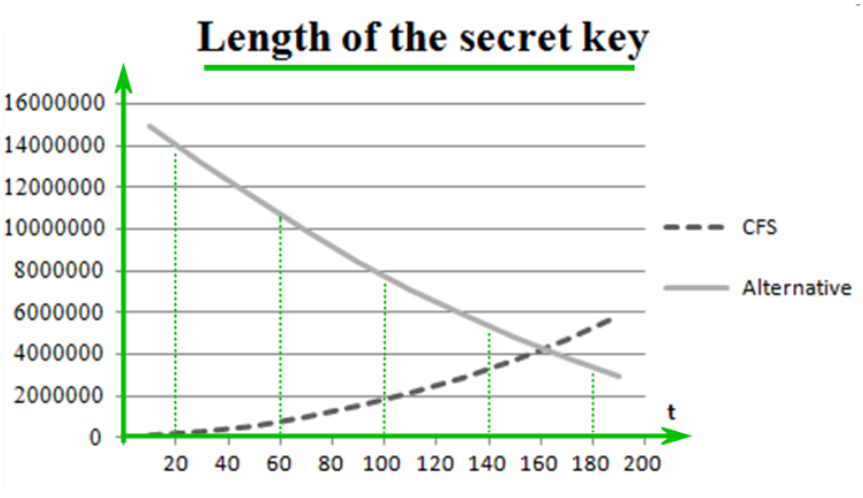

Fig. 1 – Comparison of the length of private keys

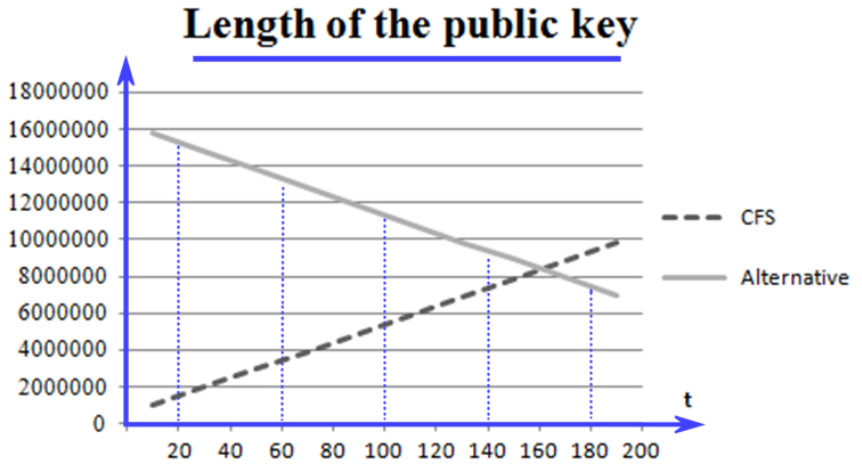

Fig. 2 – Comparison of the length of public keys

The comparison of lengths of signatures, which are formed according to both schemes

According to the CFS scheme, the signature $Y=(e,i)$ contains two components: the binary vector e, which has the length of n, and an integer i. The latter may acquire the values in the range $0,1,..,2^{n-k}-1$. From here, we have that the bit length of the signature is determined according to the expression: $l_{DS}=2\cdot n-k=2^m+m\cdot t$.

Vector e can acquire a limited number of values. The limitation is imposed according to the correcting ability of the code used. The number of possible vectors e is defined as:

$$N_{w(e)\le t}=\sum_{i=0}^{t}C_n^i .$$

Because the vector e corresponds to the condition above, it can be transformed into a break-even sequence $e*$ with bit length of $\lceil \log_2(N_{w(e)\le t})\rceil$. Then we have:

$$l_{DS}*=\left\lceil \log_2\left(\sum_{i=0}^{t}C_n^i\right)\right\rceil+n-k=\left\lceil \log_2\left(\sum_{i=0}^{t}C_{2^m}^i\right)\right\rceil+m\cdot t .$$

Using the expression for the upper bound of Hamming, the expression can be transformed:

$$l_{DS}*\le\left\lceil \log_2\left(2^{n-k}\right)\right\rceil+n-k=2\cdot m\cdot t .$$

In the case of an alternative scheme, the components of the signature become larger $Y=(I,e,i)$: the vector I (the bit length of k), the vector e and an integer i, whose length is determined in the same way as in the CFS scheme. From here, we have the length of the signature $Y=(I,e,i)$ is determined by the expression: $l_{DS}=2\cdot n=2^{m+1}$. If we make a break-even transform of vector e, then this estimate can be rewritten as:

$$l_{DS}*=\left\lceil \log_2\left(\sum_{i=0}^{t}C_n^i\right)\right\rceil+n=\left\lceil \log_2\left(\sum_{i=0}^{t}C_{2^m}^i\right)\right\rceil+2^m.$$

Similarly, to the consideration of CFS, using Hamming's upper boundary we have [20]:

$$l_{DS}*\le\left\lceil \log_2\left(2^{n-k}\right)\right\rceil+n=m\cdot t+2^m.$$

Let us demonstrate the resulting estimates through a graphical representation of an example code with a parameter $n = 12$ (Fig. 3).

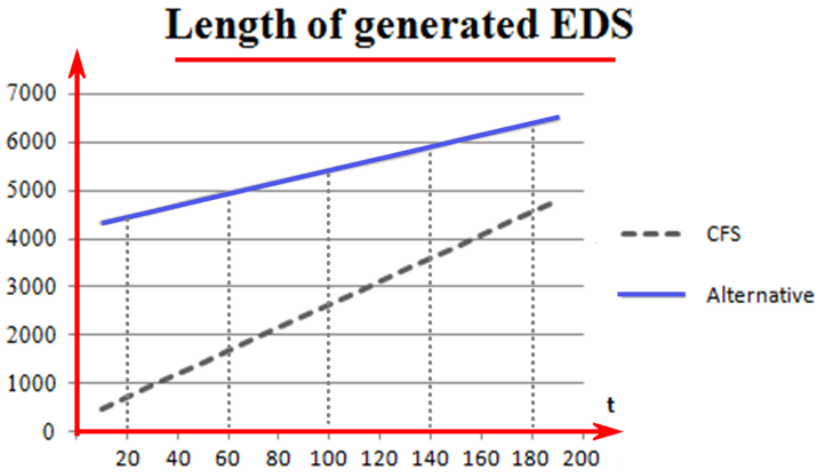

Fig. 3 – Comparison of lengths of signatures

By analyzing the obtained data, we can conclude that the length of the signature formed by the alternative scheme significantly exceeds the length of the signature CFS scheme. In particular, an increase in the length of the signature takes place by adding the vector I.

Cryptographic robustness of the signature schemes

As noted earlier, the CFS scheme is based on the use of a one-way function from the Niderraiter cryptosystem. The robustness of this function can be defined as the number of roofing sets in which it is possible to fix all combinations of t errors without knowledge of the private key [20]:

$$N\ge\frac{C_n^t}{C_{n-k}^t}=\frac{\frac{n!}{t!(n-t)!}}{\frac{(n-k)!}{t!(n-k-t)!}}=\frac{n!(n-k-t)!}{(n-t)!(n-k)!}.$$

In order to form a signature $Y'=(e',i')$ for an altered message M' the attacker needs to implement the decoding of a random code on average *t!* times. Taking into account this fact, the evaluation of digital signature robustness under the CFS scheme can be defined as:

$$N_c\ge t!\frac{C_n^t}{C_{n-k}^t}=t!\frac{n!(n-k-t)!}{(n-t)!(n-k)!}=t!\frac{2^m!(mt-t)!}{(2^m-t)!(mt)!}.$$

In a number of studies that have been carried out, the equivalence of McEliece and Niderraiter cryptosystems has been demonstrated. Hence, we can assume that the robustness of the CFS

schemes and their alternatives is also equivalent.

In the case of the use of quantum cryptanalysis, the estimation of the robustness of both schemes acquires a different character. Using one of the most popular quantum algorithms, Grover's algorithm, it is possible to determine the number of iterations to decode random code, which must be performed $t!$ times: $C^{\frac{2}{2\log n}}$, $C = 1/(1-R)^{1-R}$.

Assume that a quantum algorithm can be used to find the value of a counter i, by checking values (*brute force attack*), which requires an average $\frac{\pi}{4}\sqrt{t!}$ attempts. Therefore, the robustness of digital signature schemes in terms of quantum computers can be defined:

$$N_{PR.K.} \geq \frac{\pi}{4}\sqrt{t!}\left(\frac{1}{(1-R)^{1-R}}\right)^{\frac{n}{2\log n}} = \frac{\pi}{4}\sqrt{t!}\left(\left(1-\frac{k}{n}\right)^{\frac{k}{n}-1}\right)^{\frac{n}{2\log n}} =$$

$$= \frac{\pi}{4}\sqrt{t!}\left(1-\frac{k}{n}\right)^{\frac{k-n}{2\log n}} = \frac{\pi}{4}\sqrt{t!}\left(\frac{m\cdot t}{2^m}\right)^{t/2}.$$

When analyzing an alternative scheme, it is worth noting that it has a significant advantage over CFS, since it is able to provide security against fast signature falsification on the basis of the addition of an arbitrary codeword. An attack of this type with respect to CFS can be organized through the following actions:

- Select an arbitrary codeword from the code (n,k,d), that has a check matrix H_x. In this case the equation $H_x \cdot c^T = 0$ is true. We get a formed signature $Y = (e,i)$.
- Perform a codeword addition:

$$Y = (e+c,i) : H_x \cdot (e+c)^T =$$
$$= H_x \cdot e^T + H_x \cdot c^T = H_x \cdot e^T = (h(h(M)\,||\,\mathrm{i}))^T.$$

Changing the last expression with respect to the alternative scheme, we obtain: $Y = (I, e+c, i) : IG_X + e + c \neq \left(h(h(M)\|i)\right)$. That is, a quick falsification of the signature in this case is impossible. This property is also enhanced by additional testing of Hamming's error vector during the signature verification process. It also protects against other hypothetical attacks, such as simultaneous falsification of two signature elements, etc.

5 Conclusions

In the modern world, digital signature plays an important role and serves as the confirmation of the author's personality, and the integrity of the document. Considering two code-based digital signature schemes, namely CFS and its alternative, one can conclude that both schemes are comparable in length of key parameters, the latter depending on the parameters of the chosen code. The length of the formed signature according to the alternative scheme is slightly larger, but this increase is not critical. It is also worth noting that the robustness of the schemes against classical and quantum cryptanalysis is equivalent, which follows from the estimates equivalence of the robustness of McEliece and Niderraiter schemes on which the work of the considered digital signature algorithms is based. However, the alternative scheme has a significant advantage over the CFS common scheme: it is able to provide protection against specific attacks of fast signature falsification and simultaneous falsification of two signature components.

As the disadvantages of both cryptosystems, it is worth noting the large volumes of key data, which, according to researchers, will need to increase more than three times in the post-quantum period. The ability to reduce the key length while maintaining the robustness of signatures remains a promising area of research.

References

[1] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. Handbook of Applied Cryptography. CRC Press, 1997, 794 p.
[2] N. Ferguson and B. Schneier. Practical Cryptography. John Wiley & Sons, 2003, 432 p.
[3] D. Bernstein, J. Buchmann and E.Dahmen. Post-Quantum Cryptography. Springer-Verlag, Berlin-Heidleberg, 2009, 245 p.
[4] J. Proos and Ch. Zalka. "Shor's discrete logarithm quantum algorithm for elliptic curves". [On-line]: https://arxiv.org/abs/quant-ph/0301141.
[5] D. Deutsch and R. Jozsa. "Rapid solutions of problems by quantum computation". Proceedings of The Royal Society of London A: Mathematical, Physical and Engineering Sciences, Vol. 439, No. 1907. – 1992. pp. 553-558.
[6] P.W. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". Foundations of Computer Science: Conference Publications, 1997, pp. 1484-1509.
[7] Niederreiter, H. "Knapsack-type cryptosystems and algebraic coding theory". Problem Control and Inform Theory, 1986, V. 15. pp. 19-34.
[8] Yu.V. Stasev, A.A. Kuznetsov. "Asymmetric code-theoretical schemes constructed with the use of algebraic geometric codes". Kibernetika i Sistemnyi Analiz, No. 3, pp. 47-57, May-June 2005.
[9] A. Kuznetsov, I. Svatovskij, N. Kiyan and A. Pushkar'ov. "Code-based public-key cryptosystems for the post-quantum period, "2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkov, 2017, pp. 125-130.
[10] A. Kuznetsov, R. Serhiienko and D. Prokopovych-Tkachenko. "Construction of cascade codes in the frequency domain, "2017 4-th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkov, 2017, pp. 131-136.
[11] Yu.V. Stasev, A.A. Kuznetsov. "Asymmetric Code-Theoretical Schemes Constructed with the Use of Algebraic Geometric Codes." Cybernetics and Systems Analysis, Vol. 41, Issue 3, pp. 354-363, May 2005.
[12] M. Finiasz and N. Sendrier. "Security bounds for the design of codebased cryptosystems". In M. Matsui, ed., Advances in Cryptology, ASIACRYPT 2009, Vol. 5912 of Lecture Notes in Computer Science. -Springer Berlin Heidelberg, 2009, pp. 88-105.
[13] N.Courtois, M.Finiasz and N.Sendrier. "How to achieve a McEliece-based digital signature scheme". In Advances in Cryptology - ASIACRYPT 2001, Vol. 2248, pp. 157–174.
[14] M. Finiasz "Parallel-CFS: Strengthening the CFS McEliece-based signature scheme". In Biryukov A., Gong G., Stinson D., eds.: Selected Areas in Cryptography. Vol. 6544 of LNCS., Springer (2010) pp.159-170.
[15] J. Stern "A new identification scheme based on syndrome decoding". In Advances in Cryptology - CRYPTO'93, Vol. 773 of LNCS. Springer Verlag (1994).
[16] R. J. McEliece "A public-key cryptosystem based on algebraic coding theory". DSN Progress Report 42-44, Jet Propulsion Lab., Pasadena, CA, January-February, 1978, pp. 114-116.
[17] V. M. Sidel'nikov "Kriptografiya i teoriya kodirovaniya". Materialy konferentsii «Moskovskii universitet i razvitie kriptografii v Rossii», MGU. – 2002. – 22 p. (in Russian).
[18] S. Sander "Study of McElice cryptosystem". [On-line]: https://courses.cs.ut.ee/MTAT.07.022/2015_spring/uploads/Main/sander-report-s15.pdf.
[19] Li, Y. X., Deng, R.H., Wang, X.M. "On the equivalence of McEliece's and Niederreiter's public-key cryptosystems". [On-line]: https://ieeexplore.ieee.org/document/272496/.
[20] Clark, G.C., Cain, J.B. Error-Correction Coding for Digital Communications. Springer, 1981, 432 p.

Рецензент: Іван Горбенко, д.т.н., проф., академік Академії наук прикладної радіоелектроніки, Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 4, м. Харків, 61022, Україна.
Email: gorbenkoi@iit.kharkov.ua.

Надійшло: Травень 2018.

Автори:

Олександр Кузнецов, д.т.н., проф., академік Академії наук прикладної радіоелектроніки, Харківський національний університет ім. В. Н. Каразіна, майдан Свободи, 6, м. Харків, 61022, Україна; АТ «Інститут інформаційних технологій», вул. Бакуліна, 12, м. Харків, Україна. E-mail: kuznetsov@karazin.ua

Анастасія Киян, студентка, Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 6, м. Харків, 61022, Україна. E-mail: nastyak931@gmail.com

Іван Білозерцев, студент, Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 6, м. Харків, 61022, Україна. E-mail: ivanbelozersevv.jw@gmail.com

Микола Пастухов, к.т.н., доцент, Університет митної справи та фінансів, вул. Володимира Вернадського 2/4, м. Дніпро, 49000, Україна. E-mail: denart66@gmail.com

Дмітро Прокоповіч-Ткаченко, к.т.н., завідувач кафедрою кібербезпеки, Університет митної справи та фінансів, вул. Володимира Вернадського 2/4, м. Дніпро, 49000, Україна. E-mail: me_dnepr@ua.fm

Схеми на основі кодів для цифрових підписів.

Анотація. Стаття присвячена розгляду особливостей побудови і використання схем електронного цифрового підпису, заснованих на використанні кодів, виправляючих помилки, а саме найпоширенішої схеми, яка базується на цьому підході, CFS і нової запропонованої схеми. Функціонування цих схем безпосередньо залежить від використовуваної кодової криптосистеми: перша в своїй основі містить принципи кодової криптосистеме Нідеррайтера, друга передбачає використання криптосистеми Мак-Еліса, що до недавнього моменту вважалося неможливим. Детально розглянуті алгоритми формування та перевірки підпису згідно обох схем, описані покроково. У роботі проведені дослідження ефективності алгоритмів з точки зору обсягу необхідних ключових даних і довжини сформованого підпису, результати якого представлені за допомогою

аналітичних співвідношень і на конкретних прикладах в графічному вигляді. Також було проаналізовано стійкість розглянутих схем до класичного і квантового криптоаналізу, останній з яких є актуальною тематикою в еру стрімкого розвитку сфери пост-квантової криптографії. Розглянуты схеми мають доказову стійкість до обох видів криптоаналізу, однак при використанні квантових комп'ютерів необхідно значно збільшувати довжини ключів, що є вагомим недостакі. Виявлено факт, що запропонована схема має незаперечну перевагу перед використовуваної схемою CFS - захист від специфічних атак таких, як одночасна заміна двох елементів підпису і швидка фальсифікація, за рахунок додавання додаткового елемента в сформований підпис. Протягом дослідження виділені переваги, недоліки і перспективи використання запропонованої схеми і схеми CFS в умовах застосування квантових комп'ютерів.

Ключові слова: постквантова криптографія; цифровий підпис; криптографія на основі кодів; квантова безпека.

Рецензент: Иван Горбенко, д.т.н., проф., академик Академии наук прикладной радиоэлектроники, Харьковский национальный университет имени В. Н. Каразина, пл. Свободы, 4, г. Харьков, 61022, Украина.
Email: gorbenkoi@iit.kharkov.ua.

Поступила: Май 2018.

Авторы:

Александр Кузнецов, д.т.н., проф., академик Академии наук прикладной радиоэлектроники, Харьковский национальный университет имени В. Н. Каразина, пл. Свободы, 6, г. Харьков, 61022, Украина; АО «Институт информационных технологий», ул. Бакулина, 12, Харьков, Украина. E-mail: kuznetsov@karazin.ua

Анастасия Киян, студентка, Харьковский национальный университет имени В. Н. Каразина, пл. Свободы, 6, г. Харьков, 61022, Украина. E-mail: nastyak931@gmail.com

Иван Белозерцев, студент, Харьковский национальный университет имени В. Н. Каразина, пл. Свободы, 6, г. Харьков, 61022, Украина. E-mail: ivanbelozersevv.jw@gmail.com

Николай Пастухов, к.т.н., доцент, Университет таможенного дела и финансов, ул. Владимира Вернадского, 2/4, г. Днепр, 49000, Украина. E-mail: denart66@gmail.com

Дмитрий Прокопови-Ткаченко, к.т.н., заведующий кафедрой кибербезопасности, Университет таможенного дела и финансов, ул. Владимира Вернадского, 2/4, г. Днепр, 49000, Украина. E-mail: me_dnepr@ua.fm

Схемы на основе кодов для цифровых подписей.

Аннотация. Статья посвящена рассмотрению особенностей построения и использования схем электронной цифровой подписи, основанных на использовании кодов, исправлющих ошибки, а именно наиболее распространенной схемы, которая базируется на этом подходе, CFS и новой предложенной схемы. Функционирование данных схем напрямую зависит от используемой кодовой криптосистемы: первая в своей основе содержит принципы кодовой криптосистеме Нидеррайтера, вторая предусматривает использование криптосистемы Мак-Элиса, что до недавнего момента считалось невозможным. Подробно рассмотрены алгоритмы формирования и проверки подписи согласно обоим схемам, описанные пошагово. В работе произведены исследования эффективности алгоритмов с точки зрения объема требуемых ключевых данных и длины формируемой подписи, результаты которого представлены с помощью аналитических соотношений и на конкретных примерах в графическом виде. Также была проанализирована стойкость рассмотренных схем к классическому и квантовому криптоанализу, последний из которых является актуальной тематикой в эру стремительного развития сферы пост-квантовой криптографии. Рассмотренные схемы имеют доказуемую стойкость к обоим видам криптоанализу, однако при использовании квантовых компьютеров необходимо значительно увеличивать длины ключей, что является весомым недостаком. Выявлено факт, что предложенная схема имеет неоспоримое преимущество перед используемой схемой CFS - защита от специфических атак таких, как одновременная подмена двух элементов подписи и быстрая фальсификация, за счет добавления дополнительного элемента в сформированую подпись. В течении исследования выделены достоинства, недостатки и перспективы использования предложенной схемы и схемы CFS в условиях применения квантовых компьютеров.

Ключевые слова: постквантовая криптография; цифровая подпись; криптография на основе кодов; квантовая безопасность.