UDC 004.056.55

CODE BASED FUZZY EXTRACTOR FOR BIOMETRIC KEYS

Alexandr Kuznetsov[1], Anastasia Kiyan[1], Roman Serhiienko[2], Anna Uvarova[3], Dmytro Prokopovych-Tkachenko[4]

[1] V. N. Karazin Kharkiv National University, 6 Svobody Sq., Kharkiv, 61022, Ukraine
kuznetsov@karazin.ua, nastyak931@gmail.com,

[2] National Army Academy named after Hetman Petro Sahaidachnyi, 32 Heroes of Maidan St., Lviv, 79012, Ukraine
romanserg69@gmail.com

[3] Yuzhnoye State Design Office, Dnipro, 3 Krivorozhskaya St., 49008, Ukraine
annet.uvarova@gmail.com

[4] University of Customs and Finance, 2/4 Volodymyr Vernadsky St., Dnipro, 49000, Ukraine
omega2@email.dp.ua

Reviewer: Sergii Kavun, Doctor of Sciences (Economics), Ph.D. (Engineering), Full Prof., Kharkiv University of Technology "STEP", Kharkiv, 61010, Ukraine
kavserg@gmail.com

Received on August 2018

Abstract. *In this paper methods of forming cryptographic keys from biometric images using fuzzy extractors are considered. A new scheme of a fuzzy extractor based on the McEliece cryptosystem is proposed. It is shown that the new design of the fuzzy extractor allows forming cryptographic passwords from biometric images even without the use of non-secret helper string. When using helper string, the proportion of corrected distortions of biometric images increases significantly. In addition, the proposed design relates to a class of post-quantum information security methods, i.e. it is expected to be safely used even for solving cryptanalysis problems with universal quantum computers.*

Keywords: *code based cryptosystem; fuzzy extractor; biometric cryptography; cryptographic keys.*

1 Introduction

Biometric authentication methods [1-12] are an important area of modern research in the field of cyber security. They are widely used in various applications: criminology, e-commerce, copyright protection, electronic document management, and so on.

In recent years, interest in biometric methods has considerably expanded. From traditional biometric systems based on the comparison of biometric images with stored reference copies modern technologies have switched to the formation of cryptographic keys "on the fly." In this case, biometric data no longer requires the storage, transmission, complex and costly means of protection etc., the possibility of their intentional and/or accidental compromise is excluded. All verification, identification and authentication procedures are performed using depersonalized cryptographic keys (*passwords, access codes, PIN-codes*), and the unique biometric personal data remains safe. These formed depersonalized key sequences further will be called "biometric keys".

The next step in the development of such technologies will be the creation of high-quality biometric cryptographic systems in which biometric personal data should be used as a source of unique secret parameters. At the same time, the user will not need to memorize cryptographic keys (*passwords*) and / or use additional devices for their storage, transmission and etc. The biometric cryptosystem is initialized at any time and in any place by extracting "on the fly" the required parameters from the provided biometric images (with possible errors, erasures, etc.) without compromising these images. At the same time it is necessary to provide the maximum range of services and safety guarantees, taking into account the peculiarities of the construction of biometric cryptosystems.

In this paper, we consider methods of forming cryptographic keys from biometric images[1] using fuzzy extractors [3,4].

[1] The term "biometric images (data)" hereinafter refers to sets of biometric characteristics that can be represented in the form of binary vectors that can be compared in the Hamming metric. It is assumed that the different sets of characteristics of the same user differ from each other by no more than 25% (this threshold corresponds to the limiting corrective capabilities of noise immunity codes).

Traditionally, fuzzy extractors, as well as fuzzy containers [2] preceding them, are constructed using the methods of noise immune coding. At the initial stage, biometric data in some sense are "united" with elements of noise-immune codes (for example, codewords or syndrome sequences). For fuzzy extractors an additional helper string is created which "helps" in extracting the secret parameter based on fuzzy biometric set. In the direct use phase noise immune decoding is used, which eliminates the possibility of uncertainty (caused by distortions, erasures, etc.) in user-provided biometric images. If the differences in the sets of characteristics are not large (don't exceed the error-correcting ability of the code), then fuzzy extractors (vaults) allow uniquely to restore the secret parameter (*biometric key*).

In this paper a new scheme of a fuzzy extractor based on the McEliece cryptosystem [13] is proposed. It is shown that the new design allows generation cryptographic passwords from biometric images even without non-secret helper string. When using helper string, the proportion of corrected distortions of biometric images increases significantly. Besides, the proposed design relates to a class of post-quantum information security methods, i.e. it is expected to be safely used even for solving cryptanalysis problems with universal quantum computers.

2 Fuzzy Vault and Fuzzy Extractor

In [1] the forming of a secret key using biometrics is considered, the simplified scheme of which is shown in fig. 1. At the initial stage a secret parameter (key) K is generated, which is encoded by a noise immune code. Biometric user data B is added to the received codeword. The resulting "carrier" $B+c$ is actually a noise-masked biometric secret key. If biometrics B^* which is close to the original data $B^* \approx B$ at the usage stage would be provided, then after subtraction of B decoding will restore the secret key.

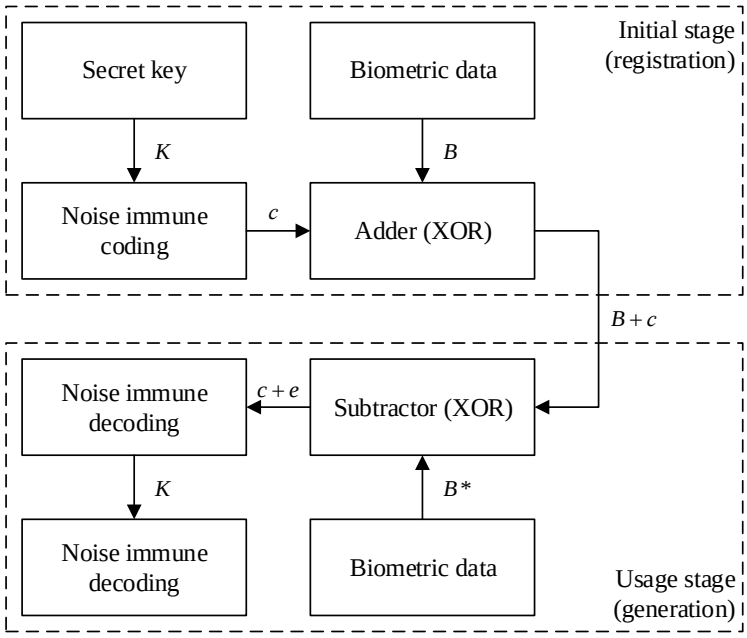

Fig. 1 – Scheme of a biometric key forming

Indeed, after subtraction we obtain: $(B+c)-B^*=c+e$, where $e=B-B^*$ is considered as vector of errors.

If the Hamming weight of the vector e (the number of its non-zero components) does not exceed the corrective capacity of the noise immune code t, then the decoding of the vector $(B+c)-B^*$ will allow to find the vector c, vector e and, as a consequence, the key parameter K.

Obviously, the cryptographic properties of the scheme [1] depend on both the selected noise immune code and method of forming biometric data. The encoded secret parameter K is contained in the "carrier" $B+c$ and, obviously, there are possible statistical attacks that recover the codeword c and the secret key K.

The scheme of the fuzzy storage was first proposed in [2]. It is also based on the use of noise immune codes. The secret parameter is "hidden" in the encoded set of data provided by user. Any user will be able to extract the secret parameter only if his set is close to the original set, and minor differences will be corrected in the process of noise immune decoding. A statistical analysis of a fuzzy vault likely could lead to a possible attack on the stored secret key.

The biometric keys technologies further were developed in [3-12] etc. In particular, in the fundamental papers [3,4] so-called fuzzy extractors where proposed, whose designs are very close to the keys forming schemes from [1]. The main ones are two constructions [3,4]:

- based on code words (Fig. 2);
- based on syndromes (Fig. 3).

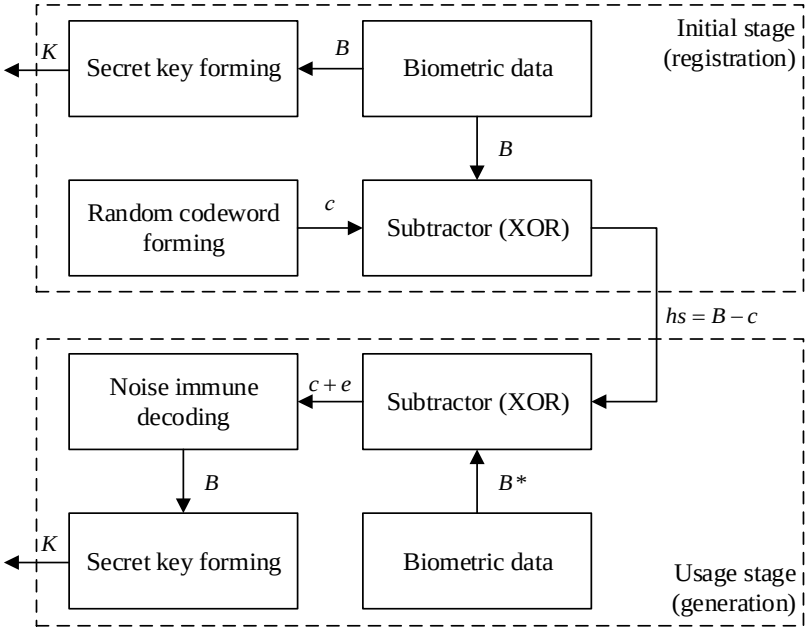

Fig. 2 – Scheme of fuzzy extractor based on codewords

Suppose that a noise immune block $(n,k,d=2t+1)$ code with error-correcting capability t is given. It is assumed that the presence of biometric data B allows the forming of a secret key K and some helper string hs (for this various techniques and techniques are used, for example, Secure Sketches [3,4]).

In the first construction (based on codewords, see Fig. 2) at the initial stage (*registration of the biometric key*) a random codeword c is formed. The open auxiliary line hs is formed by subtracting from the biometric data B the word c:

$$hs = B - c,$$

and by using this open line one can later restore the secret key K.

Indeed, during the usage phase the user provides biometric data B^*, from which the hint hs is subtracted. If $B^* \approx B$, then we have:

$$B^* - hs = B^* - (B - c) = c + e,$$

where $e = B^* - B$, and if Hamming weight of vector e does not exceed t, then decoding the vector $B^* - hs$ allows obtaining vectors c, e and therefore biometric data B:

$$B = c + hs.$$

Proper restoration of biometric data B allows you to generate a secret key K (*as in the registration phase*).

The second scheme (Fig. 3) operates syndrome sequences s that depend solely on the error vector e. To cite one example, for linear block codes given by a check matrix H, the following equalities hold for any codeword c [14,15]:

$$c \cdot H^T = 0,\ s = (c+e) \cdot H^T = e \cdot H^T.$$

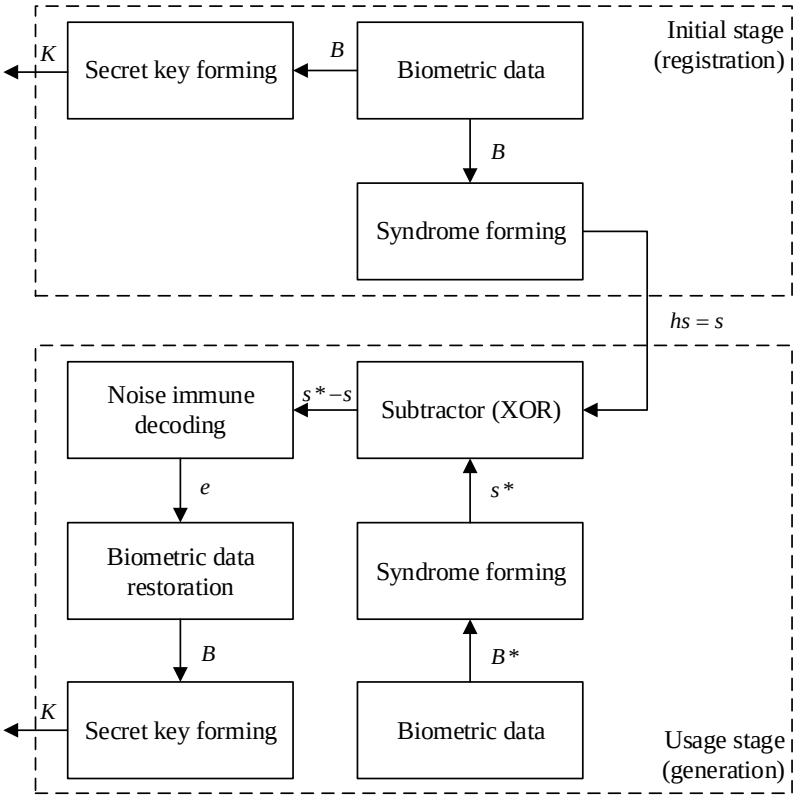

Fig. 3 – Scheme of fuzzy extractor based on syndromes

At the initial stage with use of B a syndrome sequence s is formed, which acts as open auxiliary data. At the stage of usage the user provides biometric data B^* for further syndrome sequence s^* computation. If $B^* \approx B$ then the hint $hs = s$ and the syndrome s^* allows you to restore B and generate the secret key K.

Indeed, if, for example, $s = B \cdot H^T$ and $s^* = B^* \cdot H^T$, then

$$s^* - s = e \cdot H^T,$$

where $e = B^* - B$, and if Hamming weight of vector e does not exceed t, then syndrome decoding of the vector $s^* - s$ allows to obtain e. Proper reconstruction of biometric data $B = B^* - e$ allows generation of secret key K (*as in the registration phase*).

It is obvious that the schemes in fig. 1 and fig. 2 for the binary case (addition and subtraction are realized by the XOR operation) practically coincide. The main difference is that in fig. 1 secret key is randomly generated, and then encoded with a noise immune code. In fig. 2 secret key is formed from biometric data B, which must be uniquely recovered in the event that the user provides the data $B^* \approx B$. However, in both schemes, a common approach is used, consisting in "blending" the biometric data B with the codeword c (randomly generated or encoded key K). This, in our opinion, can cause the main threat of using such biometric keys. If biometric data is transmitted, stored and / or processed in an open manner (*even mixed with codewords, syndromes, etc.*), then statistical attacks aimed at restoring code words c, biometric data B and keys K become possible.

In this paper we propose a new scheme for a fuzzy extractor, in which biometric data is not stored and transmitted in any form. This scheme uses the McEliece cryptosystem in the interpretation of Code-Based Electronic Digital Signature from [16].

3 Proposed scheme of Fuzzy Extractor

At the core of our proposal is the use of the McEliece cryptosystem [13].

McEliece code cryptosystem

McEliece cryptosystem was proposed in 1978 [13] and for 40 years of its existence it did not reveal any significant vulnerabilities. In the case of using Goppa codes [17] with sufficient length and

code distance, it is considered a reliable candidate for post-quantum application, i.e. it is supposed to be safe even if full-scale universal quantum computers are used to solve cryptographic analysis problems [18,19].

The public key in the McEliece scheme is the matrix

$$G_X = X \cdot G \cdot P \cdot D, \quad (1)$$

where G – generating matrix of an algebraic $(n, k, d = 2t+1)$ code over $GF(q)$ (in the original paper [13] it was suggested to use the binary Goppa code [17]), X – a nonsingular matrix $k \times k$ with elements from $GF(q)$, P and D – permutational and diagonal $n \times n$ matrices (for binary codes only the matrix P is used).

Matrices X, P and D in (1) are a secret key that masks the algebraic block code used to match a random code (*general position code*), i.e. the public key G_X is available to the attacker as a randomly formed generating matrix of some linear code for which the fast decoding algorithm is unknown. On the contrary, an authorized user who knows the secret key (matrices X, P and D) can disable the action of the masking matrices and use the fast decoding algorithm for the algebraic code with the generating matrix G. A cryptogram is a vector of length n computed by rule

$$c_X^* = I \cdot G_X + e, \quad (2)$$

where vector

$$c_X = I \cdot G_X$$

is the codeword for the masked code, i.e. c_X belongs to $(n, k, d = 2t+1)$ code with generating matrix G_X, I – k-bit information vector over $GF(q)$, vector e – secret error vector of weight t.

An attacker have to decode c_X^* using known to him matrix G_X. However, the decoding of a random code (with the corresponding parameters n, k, q and $d = 2t+1$) is computationally unattainable. Since attacker doesn't know the matrices X, P and D, he can't recover the matrix G and use the decoding algorithm for polynomial complexity. For an authorized user (*who knows the secret key*) decoding is a polynomially solvable[2]. Indeed, an authorized user, having received a vector c_X^*, constructs a vector

$$\bar{c}^* = c_X^* \cdot D^{-1} \cdot P^{-1}. \quad (3)$$

Further, using an algorithm of polynomial complexity, he decodes a vector $\bar{c}^* = I' \cdot G + e'$, i.e. obtains I', then computes k-bit information vector

$$I = I' X^{-1}. \quad (4)$$

An additional secret parameter that can be used in the case of applying Goppa codes is the Goppa polynomial $G(x)$ [13].

New Code Based Fuzzy Extractor

The proposed scheme of fuzzy extractor allows generation of cryptographic keys even without using non-secret helper string. When using helper string, the proportion of corrected distortions of biometric images significantly increases. A simplified scheme of the proposed fuzzy extractor is shown in fig. 4.

At the initial stage, biometric data[3] B are interpreted as the codeword (2) of the masked code in the McEliece cryptosystem. In accordance with (3) its unmasking accomplished, the resulting vector $\bar{c}^*$ has been decoded. A vector I' is extracted from the decoded codeword, which is also unmasked in accordance with (4). The received information sequence I is interpreted as a secret biometric key K. In the simplest case $K = I$, although a more complex construct of generation K from I is possible, for example, unidirectional hashing: $K = h(I \| i)$, where: $x \| y$ – operation of concatenation of strings x and y; i –additional (service) data that is used to compute the secret key.

[2] For example, the Berlekamp-Massey decoding algorithm contains the number of multiplications of the order of t^2 [14, 15].

[3] It is assumed that at the registration stage the most reliable set of biometric characteristics is formed, represented as binary vectors

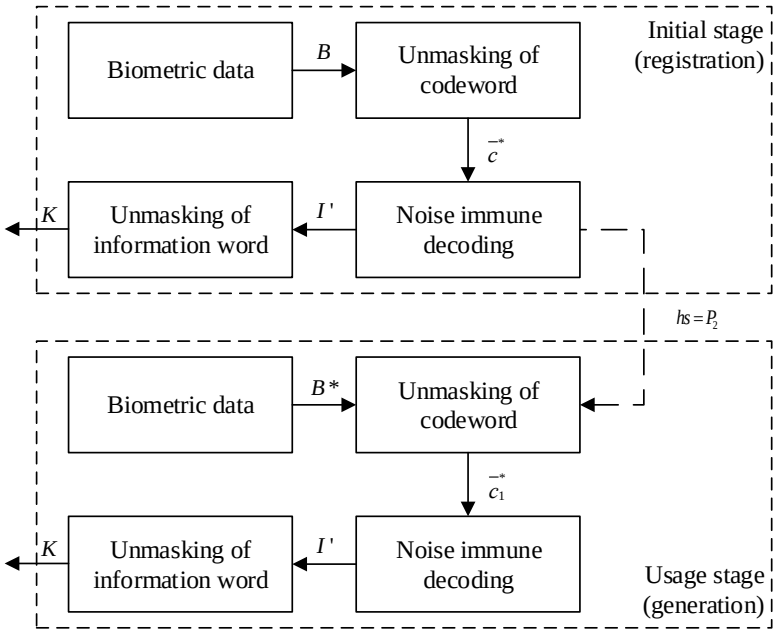

Fig. 4 – The proposed scheme of a fuzzy extractor
(a dashed line corresponds to the possible use of the helper string)

At the usage stage the user provides biometric data B^*, which, like at the registration stage, is interpreted as the codeword (2) of the masked code in the McEliece cryptosystem. In accordance with (3) it become unmasked, the resulting vector (denoted by $\vec{c}_1^*$) is decoded. If $B^* \approx B$ and, in our interpretation,

$$B = I \cdot G_X + e \text{ and } B^* = I \cdot G_X + e^*, \quad (5)$$

where e and e^* – two different vectors with Hamming weight less than t, then the decoding of vectors

$$\vec{c}^* = (I \cdot G_X + e) \cdot D^{-1} \cdot P^{-1} = I' \cdot G + e \cdot D^{-1} \cdot P^{-1}$$

and

$$\vec{c}_1^* = (I \cdot G_X + e^*) \cdot D^{-1} \cdot P^{-1} = I' \cdot G + e^* \cdot D^{-1} \cdot P^{-1}$$

will restore the same vector I'.

After unmasking the vector I' by rule (4), a secret key K is generated (as in the registration phase).

Our method is based on the assumption (5), that all belonging to the same user biometric characteristics have some general information (entropy), which can be notionally set by the vector I. This encoded information is distorted while processing of biometric images (*use of different biometric sensors, interference effects, erasures, etc.*). If we assume that biometric images are distorted by errors whose Hamming weight does not exceed the correcting ability t, then in all cases the secret key will be restored correctly. To reduce the effect of random errors in the registration phase, the most reliable set of biometric characteristics should be formed, for example, by multiple generations with averaging of obtained results.

The efficiency of the proposed fuzzy extractor, as well as other methods considered above, depends on the characteristics of the noise immune code it based on. In fact, False Rejection Rate (FRR) is determined by the probability of erroneous decoding (for case $B^* \approx B$). However, our assumption (5) looks more natural, the proposed extractor corrects various distortions of the same codeword containing biometric entropy. In the schemes [1] and [3,4] differences in the biometric patterns of the same user are corrected, i.e. the basic assumption underlying these constructions has the form where the Hamming weight of the vector must be smaller than t. If we take into account the possibility of multidirectional distortion of biometric images $B - B^*$, then our extractor intuitively appears more reliable.

It should be noted that in the scheme of fig. 4, the helper string is not obliged, i.e. the extractor can work "blindly". From each provided biometric image key data will be extracted and, if (5) is performed, the restored keys will be the same.

However, the additional use of helper string significantly reduces FRR.

Let's write the matrix G in the form of a "union" of two submatrices – a square $k \times k$ matrix G_1 and a rectangular $k \times (n-k)$ matrix G_2:

$$G = G_1 \| G_2 . \tag{6}$$

Then the $\bar{c} = I' \cdot G$ can be written in form:

$$\bar{c} = P_1 \| P_2 , \text{ where } P_1 = I' \cdot G_1 , \; P_2 = I' \cdot G_2 .$$

Using the last identities, we find P_2:

$$P_2 = P_1 \cdot G_1^{-1} \cdot G_2 , \tag{7}$$

where matrix G_1^{-1} is the inverse[4] to matrix G_1.

In fig. 4 the dashed line corresponds to the possible use of P_2 as a helper string (in the stage decoding of $\bar{c}_1^*$). This allows to reduce significantly the influence of errors and thus increase the probability of correct recovery of the vector I' and secret key K (i.e. reduce FRR). Indeed, if the errors (nonzero elements of the vector e) are distributed uniformly throughout the word $\bar{c}^* = I' \cdot G + e'$, then having an undistorted part P_2 of the codeword $I' \cdot G$, you can "ignore" all the errors that occur in the "second" part of the word. This is equivalent to increasing the correcting ability of the code according to the length of the vector P_2, as explained below.

Suppose the errors (non-zero elements of the vector e) occur randomly, equally and independently of each other. Denote by the symbol p the probability of distortion of single symbol of the codeword. Then the probability of distortion of m symbols of the code word of length n:

$$P(m) = C_n^m p^m (1-p)^{n-m} ,$$

where $C_n^m = \dfrac{n!}{m!(n-m)!}$ – binomial coefficient.

The probability of a decoding error (corresponds to FRR in our model without the use of helper string) when using the $(n, k, d = 2t+1)$ code can be written as:

$$FRR = 1 - \sum_{i=0}^{t} P(i) = 1 - \sum_{i=0}^{t} C_n^i p^i (1-p)^{n-i} . \tag{8}$$

When using helper string, errors need to be corrected only at the positions of the vector P_1 and the probability of decoding error (with similar reasoning) takes the form:

$$FRR^* = 1 - \sum_{i=0}^{t} C_k^i p^i (1-p)^{k-i} . \tag{9}$$

In fig. 5 showed the calculated dependences FRR for some (*n*, *k*, *d*) parameters of binary BCH codes: a) (127, 64, 21); b) (255, 115, 43); c) (512, 211, 83).

As follows from the dependencies above, when choosing the appropriate (*n*, *k*, *d)* parameters, the FRR can be very low. For example, when forming a 64-bit key using a binary (127, 64, 21) code and $p = 0,05$ the FRR value for an extractor without helper string does not exceed 10^{-1}. Using of helper string reduces FRR by 2 orders of magnitude. Increasing the length and correcting ability of the code results in a decrease of FRR. For example, for (512, 211, 83)-code even for $p = 0,15$ using helper string allows to form a 211 bit key with FAR no more than 10^{-1}.

[4] To invert the matrix G_1 it is necessary to correctly implement the representation (6): this is not a "union" of the first (any) k columns of the matrix G, but a pseudo-random choice of such k columns from form G which make a nonsingular square matrix G_1.

It should be noted that another important characteristic of biometric passwords – False Acceptance Rate (FAR), – characterizing the probability of incorrect secret key formation by an unauthorized user, increases with growing of code error-correct ability t. With a significant increase of t (due to increased redundancy P_2), the extractor will be able to extract the same key for any given biometric data, i. e. for $B^* \neq B$. For example, if you use a binary code with parameters (511, 112, 239) with a 399-bit hint $hs = P_2$, then even if all 112 bits of the vector P_1 are distorted, the extractor corrects them ($t = 119$) and unambiguously restores the vector I and secret key K. In other words, any user who provided an arbitrary set B^* can correctly recover the key K. From this point of view, when choosing (*n*, *k*, *d*) code parameters, a compromise solution should be chosen between the expected values of FRR and FAR.

Assuming that $k < \frac{n}{2}$ and all users have biometric data equidistant from each other, then FAR (with helper string) can be conditionally evaluated with the following expression:

$$FAR^* = \begin{cases} q^{-k+t}, & k > t; \\ 1, & k \le t, \end{cases} \tag{10}$$

where q – the power of the symbols alphabet over which the noise immune code is constructed (for binary code $q = 2$).

Indeed, in the proposed extractor, a vector I (*or a function of this vector*) of the length k of the code symbols is used as the secret key K. With equidistant code words (biometric images) and equiprobable choices, the probability of matching keys for different users is q^{-k}. The fuzzy extractor is based on noise immune decoding and, in the case of using the helper string, all t errors can be corrected on the block P_1 with the length k of code symbols, i.e. if $k > t$ then probability of coincidence of secret keys for different equiprobably selected biometric images will be equal q^{-k+t}. For $k \le t$ the correcting ability of the code allows to select completely the desired vector for any biometric set, i.e. "skipping the target" is a reliable event. If the helper string is not used, then for each k code characters there are $\frac{t}{n}$ errors which can be corrected in average and the FAR can be estimated as $q^{-k+\frac{t}{n}k}$.

Finally we should note that all the above reasoning, relations and computed values are given for "ideal" conditions, when sets of biometric characteristics are formed in form of binary vectors with random, equally probable (for $p < 0,5$) and independent errors. In real conditions the nature of errors can be significantly different. It is necessary to carry out further studies, including experimental ones, to provide practical recommendations on the direct use of the proposed fuzzy extractor.

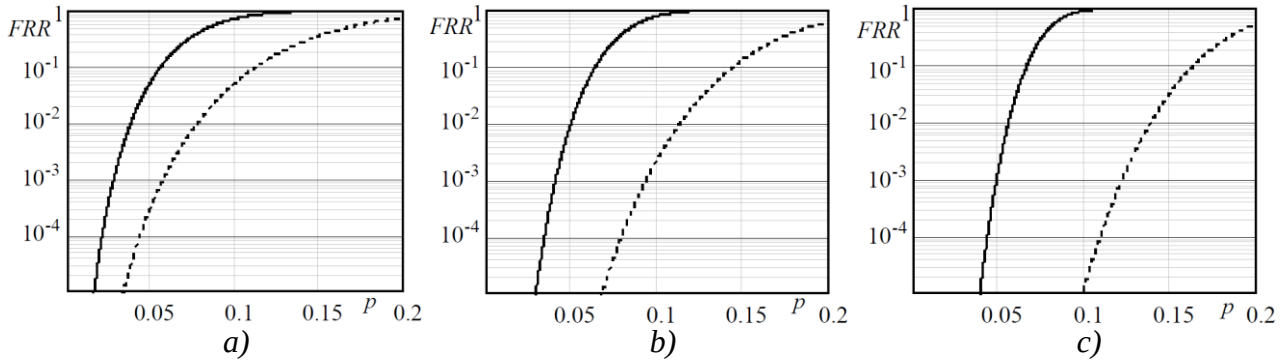

Fig. 5 – Computed dependencies FRR
(solid line – without helper string; dashed line – with helper string)

4 Conclusions

In this paper, a fuzzy extractor based on the McElice cryptosystem is proposed. Our proposal, on the one hand, uses the strengths of this code cryptosystem: cryptographic stability, based on the problem of syndrome decoding; resistance to quantum cryptanalysis methods; relatively high conversion speed (compared to other cryptosystems with a public key). On the other hand, proposed extractor by selecting the necessary (*n, k, d*) parameters of the noise immune code, allows to provide desired small FRRs (*admitting a number of assumptions about the nature of the errors*). The use of hints (*helper strings*) significantly reduces the FRR, but with the increase in the code correcting ability it can increase the FAR due to wrong "correction" of biometric features. The choice of a compromise solution concerning parameters of the code, taking into account the characteristics of the errors that arise, experimental studies of FRR and FAR are promising directions for further work.

References

[1] Hao F., Anderson R., Daugman J. Combining cryptography with biometrics effectively: Technical Report UCAM-CL-TR-640. Cambridge: University of Cambridge Computer Laboratory, 2005. 17 p.
[2] Juels A., Sudan M. A fuzzy vault scheme. Des. Codes Cryptography. 2006. Vol. 38, № 2. pp. 237–257.
[3] Fuzzy extractors: How to generate strong keys from biometrics and other noisy data /Dodis Y., Ostrovsky R., Reyzin L., Smith A. D. SIAM J. Comput. 2008. Vol. 38, № 1. pp. 97–139.
[4] Dodis Ye., Reyzin L., Smith A. Fuzzy Extractors. A Brief Survey of Results from 2004 to 2006. URL: http://www.cs.bu.edu/~reyzin/papers/fuzzysurvey.pdf
[5] Cryptographie key generation from PUF data using efficient fuzzy extractors/ Kang H., Hori Y., Katashita T., Hagiwara M. Iwamura K. 16th International Conference on Advanced Communication Technology. 2014, Pyeongchang. pp. 23–26.
[6] Fuzzy Extractors for Biometric Identification / Li N. and etc. 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS). 2017, Atlanta, GA. pp. 667–677.
[7] Wen Y., Lao Y. Efficient fuzzy extractor implementations for PUF based authentication. 12th International Conference on Malicious and Unwanted Software (MALWARE). 2017, Fajardo. pp.119–125.
[8] Kaur T., Kaur M. Cryptographic key generation from multimodal template using fuzzy extractor. 2017 Tenth International Conference on Contemporary Computing (IC3). 2017, Noida. pp. 1–6.
[9] Gupta N. K. and Kaur M. A robust and secure multitrait based fuzzy extractor. *2017* 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT). 2017, Delhi. pp. 1–6.
[10] LWE-based lossless computational fuzzy extractor for the Internet of Things / Huth C. D. and etc. 2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). 2017, McLean, VA. P. 154.
[11] Securing Systems With Indispensable Entropy: LWE-Based Lossless Computational Fuzzy Extractor for the Internet of Things / Huth C. and etc. IEEE Access. 2017. Vol. 5. pp. 11909–11926.
[12] Eliminating Leakage in Reverse Fuzzy Extractors / Schaller A., Stanko T., Škorić B. and Katzenbeisser S. IEEE Transactions on Information Forensics and Security. 2018. Vol. 13, № 4. pp. 954–964.
[13] McEliece R. J. A public-key cryptosystem based on algebraic coding theory. DSN Progress Report 42-44, Jet Propulsion Lab. 1978, Pasadena, CA. pp. 114–116.
[14] Clark G.C., Cain J.B. Error-Correction Coding for Digital Communications. Springer, 1981. 432 p.
[15] Blahut R. E. Theory and Practice of Error Control Codes. Massachusetts: Addison Wesley Publishing Company Inc., 1983. 500 p.
[16] Code-based electronic digital signature/ Kuznetsov A., Pushkar'ov A., Kiyan N., Kuznetsova T. 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). 2018. Kyiv. pp. 331–336.
[17] Goppa V.D. A New Class of Linear Correcting Codes. Problems Inform. Transmission. 1970. Vol. 6, № 3. pp. 207–212.
[18] Bernstein D., Buchmann J., Dahmen E. Post-Quantum Cryptography. Berlin-Heidleberg: Springer-Verlag, 2009. 245 p.

Рецензент: Сергій Кавун, доктор економічних наук, к.т.н., проф., Харківський технологічний університет "ШАГ", вул. Малом'ясницька, 9/11, м. Харків, 61010, Україна.
E-mail: kavserg@gmail.com

Надійшло: Серпень 2018.

Автори:
Олександр Кузнецов, д.т.н., проф., академік Академії наук прикладної радіоелектроніки, Харківський національний університет імені В.Н. Каразіна, майдан Свободи 6, м. Харків, 61022, 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

Роман Сергієнко, Національна академія сухопутних військ імені гетьмана Петра Сагайдачного, вул. Героїв Майдану 32, м. Львів, 79012, Україна.
E-mail: romanserg69@gmail.com

Анна Уварова, провідний інженер, Конструкторське бюро «Південне» ім. М. К. Янгеля», вул. Криворізька 3, м. Дніпро, 49008, Україна. E-mail: annet.uvarova@gmail.com

Дмитро Прокопович-Ткаченко, к.т.н., завідувач кафедрою кібербезпеки, Університет митниці та фінансів, вул. Володимира Вернадського 2/4, м. Дніпро, 49000, Україна. E-mail: omega2@email.dp.ua

Екстрактор біометричних ключів на кодових криптосистемах.

Анотація. У даній роботі розглядаються методи формування криптографічних ключів з біометричних образів із використанням нечітких екстракторів. Пропонується нова схема нечіткого екстрактора, в основі якої лежить кодова криптосистема Мак-Еліса. Показано, що нова конструкція нечіткого екстрактора дозволяє формувати криптографічні паролі з біометричних образів навіть без використання несекретної підказки (допоміжного рядка). При використанні допоміжної рядка значно зростає частка коректованих спотворень біометричних образів. Крім того, пропонована конструкція відноситься до класу пост-квантових методів захисту інформації, тобто очікується її безпечне використання навіть в умовах застосування універсальних квантових комп'ютерів для вирішення завдань криптоаналізу.

Ключові слова: криптосистема на основі коду; нечіткий екстрактор; біометрична криптографія; криптографічні ключі.

Рецензент: Сергей Кавун, доктор экономических наук, к.т.н., проф., Харьковский технологический университет «ШАГ», ул. Маломясницкая, 9/11, г. Харьков, 61010, Украина.
E-mail: kavserg@gmail.com

Поступила: Август 2018.

Авторы:

Александр Кузнецов, д.т.н., проф., Академик Академии наук прикладной радиоэлектроники, Харьковский национальный университет им. В. Н. Каразина, пл. Свободы 6, г. Харьков, 61022, 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

Роман Сергиенко, Национальная академия сухопутных войск имени гетмана Петра Сагайдачного, ул. Героев Майдана, 32, г. Львов, 79012, Украина. E-mail: romanserg69@gmail.com

Анна Уварова, ведущий инженер, Конструкторское бюро «Южное» им. М. К. Янгеля», г. Днепр, ул. Криворожская 3, 49008, Украина. E-mail: annet.uvarova@gmail.com

Дмитрий Прокопович-Ткаченко, к.т.н., заведующий кафедрой кибербезопасности, Университет таможни и финансов, ул. Владимира Вернадского, 2/4, г. Днепр, 49000, Украина. E-mail: omega2@email.dp.ua

Экстрактор биометрических ключей на кодовых криптосистемах.

Аннотация. В данной работе рассматриваются методы формирования криптографических ключей из биометрических образов с использованием нечетких экстракторов. Предлагается новая схема нечеткого экстрактора, в основе которой лежит кодовая криптосистема Мак-Элиса. Показано, что новая конструкция нечеткого экстрактора позволяет формировать криптографические пароли из биометрических образов даже без использования несекретной подсказки (вспомогательной строки). При использовании вспомогательной строки значительно возрастает доля корректируемых искажений биометрических образов. Кроме того, предлагаемая конструкция относится к классу пост-квантовых методов защиты информации, т.е. ожидается ее безопасное использование даже в условиях применения универсальных квантовых компьютеров для решения задач криптоанализа.

Ключевые слова: криптосистема на основе кода; нечеткий экстрактор; биометрическая криптография; криптографические ключи.