# N,T-LIMENAL SCHEME OF SHAMIR AS THE GENERATION BLOCK OF THE KEY SEQUENCE OF THE BIO CRIPTOGRAPHY IN THE SYSTEM OF MARINE PORTS

***Alexander A. Sukhovey***

*The article proposes an algorithm of a cryptographic key formation based on particular points of a fingerprint using the n,t-limenal scheme of Shamir. The author also describes practical application of the proposed algorithm in the port security system.*

**Keywords:** fingerprint, cryptography, fuzzy data, key generation, key fingerprint, a unique sequence.

Nowadays the close attention has been paying to the creation of algorithm of interaction between the biometrical and cryptographic systems. The new biometrical systems allows to avoid the disadvantages of the classical formulations based on the detachment of particular characteristics and their transformation into biometrical shape stored in the data base. These disadvantages are as follows:

1) The unique biometrical shape in the frame of one system;
2) Limitation in use.

The first disadvantage determines the possibility of pilferage of biometrical shapes and their further use in order to compromise the system. Encryption of the stored data doesn't solve this problem but only increases the time that it takes the penetrator to get the necessary

information. Herewith the hashing is impossible as the biometrical shape is unstable.

The modern use of biometrical systems is reduced to authentication of the user to allow the access to the subject, for example accommodation or computer. The structure of the biometrical shape doesn't allow it to be used in cryptographic systems.

The new trend "biocryptography" made it possible to use biometrical data as a key one for the cryptographic system or the foundation for the generation of closed information. These leads to the use of fingerprints as the pass to the electronic signature. New capabilities eliminate the weak point of the cryptographic system – the protected data base in form of USB-storage mediums, smart-cards, iButton, etc.

Any biometrical system can be divided into several blocks:

1. Hardware ( which realizes the scanning of biometrical materials, for example fingerprints).
2. Preliminary processing (carries the function of image replica of the hardware information in the unified form to identify the elements for the further calculations) [1].
3. Separation of special elements.
4. Creation of the biometrical image or sequence.
5. Practical use (storage of the image in the data base, its comparison, the use of succession in for the cryptographic purposes, etc.)

The development of biocryptography began about 10 years ago but has already put forward two main trends which provide the necessary result i.e. fuzzy extractor and fuzzy vault.

Both trends change the operation process of the biometrical system in $4^{th}$ and $5^{th}$ blocks, what particularly substitute the calculation core of the system. This factor reduces the financial costs for the update of the biometrical systems since the hardware and the equipment comprise the main expanses.

The first trend uses the error control codes. It is base on any method of unique sequence separation from the biometrical systems, as further the key sequence generates accidentally and is blocked by the biometric system.

Let *dis (a,b)* - is the distance between two sequences *a* and *b*, and $l$ - is the length of the necessary unique sequence $U \in \{0,1\}^l$ then the

method of unique sequence in the context of fuzzy extractor scheme will have two functions (user registration and restoration of the closed sequence used for the authentication or further cryptographic transformations) [2]:

1. *Gen(w)=<U,P>*, where *w* - is some biometrical sequence $w \in W$ and *P* - is the relevant open sequence.

2. *Re p(w',P)=U*, where *w'* - is the verifying biometrical sequence $w' \in W$, which satisfies the conditions $dis(w, w') \le t$.

Let *C* - is the error control code with the length *k*, than $C_e : W \to \{0,1\}^k$ is the function for encrypting, a $C_d : \{0,1\}^k \to W$ - decoding function. In this case fuzzy extractor reduces to the following:

1. $P = w \oplus C_e(U)$, where *U* - can be generated accidently;

2. $C_d(w' \oplus P) = U$ in case of $dis(w, w') \le t$, here *t* - is the error-correcting capability of the code. Fuzzy Vault is based on the use of polynomials [3]. This method algorithm includes the following stages:

1) Generation of polynomial, with the coefficient which is the close sequence, and the curve passes through the particular points, for example fingerprints;

2) Then to these particular points we add noise.

Thus, fuzzy vault comprises the points one part of which is the basis for the closed sequence. Restoration of the sequence consists of two stages:

1) The array of points is filtered under the particular points produced from the biometrical material, for example fingerprints;

2) On basis of the rest of points the polynomial which coefficients are the closed sequence is generated.

As the result of calculation error practically the fuzzy vault scheme is supplemented by the additional information such as Helper Data, what improves the accuracy but also leads to the increase of the stored data and the time to restore the close sequence.

The Authors suggest to use *n,t*-threshold circuit of Shamir [4] as the main generation block of the key sequence. Let $D = \{d_{xi}, d_{yi}\}$ - is the multitude of particular points of the preliminary processed biometric image, *p* - is the prime number which specifies the finite field *GF(p)*. Let's build the multinomial under the field *GF(p)* size *n-1:*

$$F(x) = \sum_{i=0}^{n-1} a_i x^i \bmod p \qquad (1)$$

Let $D' \subset D$, than the graph of polynomial passes through the points *D'*, i.e. satisfies the following condition:

$$F(d'_{xi}) = d_{yi} \bmod p \tag{2}$$

Let calculate the coordinates of the ensemble of points *R* so that:

$$\begin{aligned} &|R| < n - t, \\ &R \not\subset D' \end{aligned} \tag{3}$$

Thus, <*R, n, p*> in this system is the open information stored in the data base and coefficients concatenation of polynomial $a_i$ - is the close sequence. To restore the closed sequence it is required to calculate the polynomial coefficient *F(x)*, using the interpolation polynomial of Lagrange. The formula of the polynomial will be as follows:

$$\begin{aligned} &F'(x) = \sum_i l_i(x) y_i, \\ &l_i(x) = \prod_{i \neq j} \frac{x - x_i}{x_i - x_j} \end{aligned} \tag{4}$$

All operation in expression (4) is performed in the finite field *GF(p)*. In addition it is possible to restore the polynomial coefficient only with the missing points *t* in *R*-array, which can be produce only with the again received $D_1 = \{d_{1xi}, d_{1yi}\}$ from the biometrical data:

$$F'(x) = F(x) \Leftrightarrow |D_2| \geq t, D_2 = D \cap D_1 \tag{5}$$

The again received coefficient allows restoring the closed sequence by concatenation. All calculations in the finite field lead to the high accuracy of the system and to the high security.

Let *S* - is the closed sequence, and *H(x)* - is the function of hashing than the scheme of user authentication in the bio cryptographic system, the generation block of the unique sequence which is based on the *n,t*-threshold circuit of Shamir. All these comprise two steps:

1) During registration the following is saved < *R, n, p, H(S)* >.

2) The process of authentication is reduced to the calculation of hash functions from the new sequence *S*.

The security of such system of authentication is based on the impossibility to restore the polynomial from the points the number of which is less than its degree and definition of the term *hash function*

which results in no algorithm of restoration of the original sequence from the value.

Insignificant errors in the closed sequence appeared due to the shift of the particular points of the biometrical data can be eliminated with the correcting errors codes, for example Rid-Solomon code.

The above describe scheme of the key sequence generation with the fuzzy extractor scheme can be used to build bigger security system in the marine port which is the barrier between the foreign community and the state territory. Due to this fact a close attention to the security of such objects must be paid.

The main aspects of security are:

- Authentication of the visitor (personnel, seafarer or a person with temporary pass).
- Electronic documents circulation (sender authentication and security of the circulating information).

Usually all the inspections are undertaken by the hard copies of the document on the control post, i.e. the external boundary of the object, thus both aspects are different systems.

The authors of this paper suggest to integrate the authentication of the user with the system of electronic documents circulation into one unified security system (USS), which is based on the use of biocryptographic methods [1].

Let $U \in \{0,1\}^l$ - is the bit sequence of the length $l$, corresponding to the biometrical information $B$ and which was got by the following way:

$$F : B \rightarrow U \qquad (6)$$

Than the appropriate open sequence $V \in \{0,1\}^k$ is produced by:

$$G : U \rightarrow V \qquad (7)$$

The main conditions to transform $F$ are:

- unidirectionality (it's impossible to get $U$ from $B$);
- accidental (for the same $B$ - $U$ is different during the user registration process in the system; this condition results from the fuzzy extractor principle). To transform $G$ it is necessary to provide one condition of unidirectionality.

Considering that $U$ is the sequence and there is an open key, such approach can be used both for user authentication and the electronic signature system. Such algorithm allows building up the unified security

system of the marine ports enterprises which covers the following aspects:

- the access control management;
- user authentication on his work place;
- encrypting of the key information flows;
- electronic signature security.

Thus the USS will involve the following elements:

- user registration center;
- unified center of certification and authentication (UCCA);
- unified base of the open keys;
- biometrical readers;
- unified network infrastructure (it is assumed that the traffic is secured).

The interaction of the main elements of the system is shown on Figure 1.

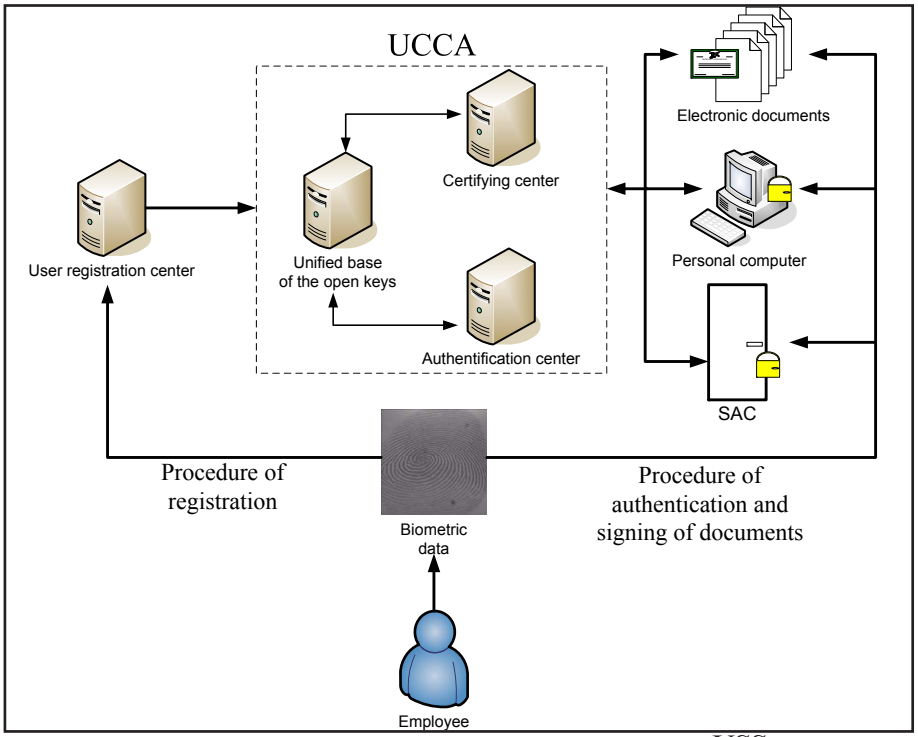


*Figure 1. The interaction of the main elements of the USS*

The registration center has the function of the primary separator of the open key $V$ relying on the biometrical information and transportation of $V$ to the unified key base where the certificate formation of the key

$S_V$ takes place. This further performs the verification of the electronic signature in the Verification Center. The verification procedure of the user and the signature is realized by the Authentication and Verification Centers accordingly.

This scheme of interaction of elements of the USS allows covering all the main aspects of the access to the information and its circulation on the territory of port. Since all the operational information of the USS flows to the UCCA we can change the system structure (see Figure 2) and improve the security function.

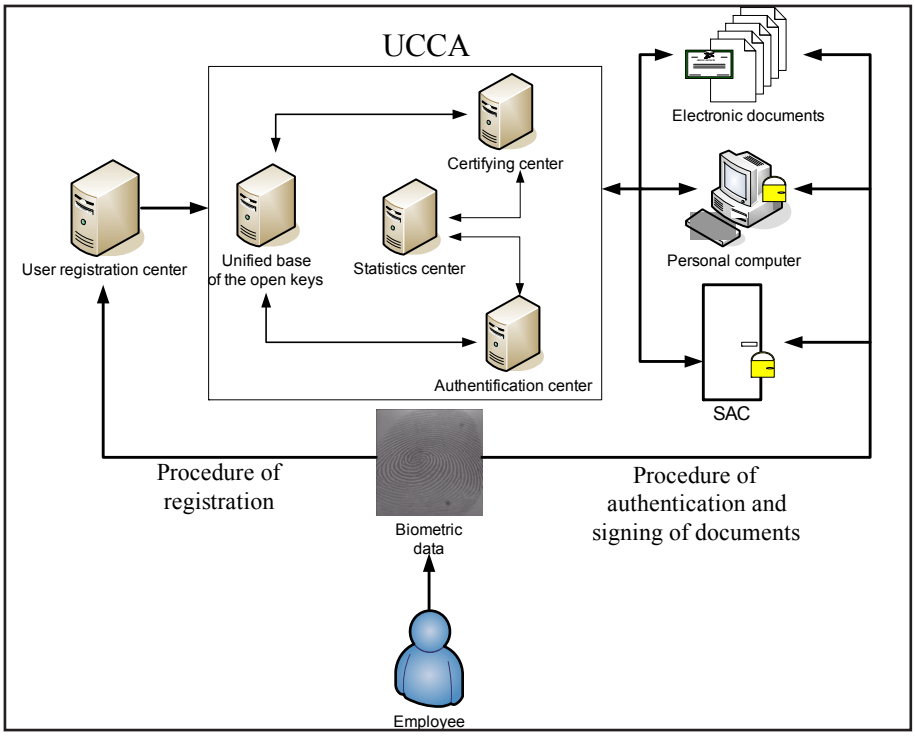


*Figure 2. USS with the Statistics Center*

The statistics Center in the USS allows realizing the authentication of the personnel and the electronic signatures basing on the earlier received information. Herewith the following functions can be blocked for the user:

- Electronic signature without authentication of the user.
- Authentication on the computer if there was no earlier access of the same user from this place.

Such security elements can be realized only by processing the earlier received information. Taking into consideration the big territory of ports the Statistics Center can analyze the user transition time on the port territory what allows to introduce new time intervals $T_{ij}$ for transition from accommodation $i$ to accommodation $j$. Thus if in time $t_i$ user left the accommodation $i$ and is trying to enter accommodation $j$, than the authentication procedure will be as follows:

$$Auth(U) = 1 \Leftrightarrow t_j - t_i \geq T_{ij} \qquad (8)$$

The same way the authentication of the user can be realized on the working station basing on the statistics information.

The organization of the one unified security system on basis of the biocryptographic method enables acquisition of the several advantages:

- Unified personnel management system.
- The information control system integrates into the general security system with the automated systems.
- Possibility of personnel control on the working place, that he or she had passed the authentication control and are at the working place and had passed system access control (SAC).
- No additional storage for SAC;
- No need to use protected key mediums to store closed keys of the users;
- Absence of the ability to compromise the key information when loosing the information storage medium;
- New security capabilities due to the new information from the Statistics Center.

Using the above mentioned approaches during the organization of large security systems which includes the interconnection between different and sometimes not connected elements of security will enable unification of the automated process and create the unified users data base. This will lead to the costs reduction for the server platforms which realize the data storage of different separate systems.

In this case the fingerprint or any other biomaterial can be used by the personnel as the key to the access to the whole company infrastructure.

Taking into account the popularity of the IT in today's information and data storage, the system based on the Statistics Center will improve the security reaction since in such system the security can not only control the movement sensors but also the penetration into the

information data base of the company. Based on the advantages of the describe system biocryptography is becoming a very promising sphere of the information technology industry which allows to join the security elements of the company infrastructure into one unified system with more possibilities of control.

## REFERENCES

1. Гончаров С.М., Суховей А.А. Этапы генерации уникальных ключевых последовательностей на основе папиллярного узора отпечатков пальцев // Доклады Томского государственного университета систем управления и радиоэлектроники: Научный журнал, №1 (21), часть 1 - Томск: Изд-во ТУСУР, 2010. с.97-99. (Russian). [Goncharov S.M., Sukhovey A.A. Etapy generatsii unikalnykh klyuchevykh posledovatelnostey na osnove papillyarnogo uzora otpechatkov paltsev // Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki: Nauchnyy zhurnal, №1 (21), chast 1 - Tomsk: Izd-vo TUSUR, 2010. c.97-99]. Goncharov, S.M., & Sukhovey, A.A. (2010). Stages of unique key sequences generation on the fingerprints papillary pattern basis. *Reports of Tomsk State University of Control Systems and Radio Electronics*, 1(21), part 1, 97-99. Tomsk: TUSUR Publishing House.

2. Суховей А.А., Гончаров С.М. Генерация ключевых последовательностей на основе отпечатков пальцев // Материалы докладов Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых «Научная сессия ТУСУР-2010», часть 3. Томск: Изд-во В-Спектр, 2010. с. 216-219. (Russian). [Sukhovey A.A., Goncharov S.M. Generatsiya klyuchevykh posledovatelnostey na osnove otpechatkov paltsev // Materialy dokladov Vserossiyskoy nauchno-tekhnicheskoy konferentsii studentov, aspirantov i molodykh uchenykh «Nauchnaya sessiya TUSUR-2010», chast 3. Tomsk: Izd-vo V-Spektr, 2010. c.216-219]. Sukhovey , A.A., & Goncharov, S.M. (2010). Generation of key sequences based on fingerprints. *Proceedings from the Conference of Students and Young Scientists "Scientific session TUSUR-2010"*, part 3, 216-219. Tomsk: V-Spectr Public House.

3. Juels, A. ,& Sudan, M. (2002). A Fuzzy Vault Scheme, *Proceedings from International Symposium on Information Theory* (pp. 408). IEEE, Lausanne, Switzerland.

4. Шнайер Б. 3.7. Разделение секрета // Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. - М.: Триумф, 2002. с. 93-96. (Russian). [Shnaider B. 3.7. Razdelenie sekreta // Prikladnaja kriptografija. Protokoly, algoritmy, ishodnyje texty na yazyke Ci. -M.: Triumf, 2002. s.93-96]. Shnaider, B (2002). 3.7. Splitting the secret. *Applied Cryptography. Protocols, Algorithms and Source Code in C* (pp.93-96). Moscow: Triumph.