Spectral Model of the Encryption Key for a Symmetric Cryptosystem Based on Differential Transformations

Olha Hryshchuk [1]

[1] *Korolyov Zhytomyr Military Institute, 22 Mira Avenue, Zhytomyr, 10004, Ukraine*

Abstract

In the transition and post-quantum periods, the problem of cybersecurity is significantly aggravated. The potential compromise of the best symmetric (AES-256) and asymmetric (RSA-240) cryptosystems when an attacker uses quantum computers puts forward a number of security requirements for such systems. Today, a number of approaches are used to solve the problem of increasing cryptographic strength. Classic, which boils down to solving the problem of distributing encryption keys and new, the essence of which is to create promising cryptosystems based on new mathematical principles. The latter approach is based on cognitive cryptography, dynamic chaos theory, constructive, quantum and post-quantum cryptography, DNA algorithms, proxy models of cryptosystems, attribute-based cryptosystems, batch and non-commutative cryptography. The greatest interest from the point of view of security today is integrated cryptography. Thus, in previous works on this topic, it was proposed to create a symmetric cryptosystem based on differential transformations. The principle of functioning of this cryptosystem does not differ from the principles of functioning of classical symmetric cryptosystems. The only difference is that a symmetric cryptosystem based on differential transformations is based on the Fredholm integral equation of the first kind, the encryption key for which is its core. Special requirements for choosing an encryption key for a symmetric cryptosystem based on differential transformations are the requirements regarding its continuity, innate and symmetric. Following these requirements, the article offers a spectral model of the encryption key for the corresponding cryptosystem, which is built on the basis of differential transformations of Academician of the National Academy of Sciences of Ukraine G. E. Pukhov. It is shown that the spectral model of the encryption key for a symmetric cryptosystem on differential transformations is the sum of discret differential spectra for different values of the integer argument. Representation of the encryption key in the form of a spectral model makes it possible to implement encryption and decryption procedures by a symmetric cryptosystem using differential transformations in real time in the future.

Keywords

Encryption key, spectral model, symmetric cryptosystem, differential transformations, cybersecurity, image, T-spectrum, discrete, numeric argument, Fredholm integral equation of the first kind.

1. Introduction

Cybersecurity has now become a cornerstone on the agenda for many countries around the world. The computerization of all spheres of state and civil society activities, as well as the mass access of citizens to information technologies, threatens their use for illegal and terrorist purposes. It is possible that the fact of carrying out a cyberattack by one state against another can be regarded as the beginning of aggression from cyberspace. That is why in the world and Ukraine, scientist's eyes are increasingly focused on cybersecurity issues.

III International Scientific And Practical Conference "Information Security And Information Technologies", September 13–19, 2021, Odesa, Ukraine

EMAIL: Ol.Hry@i.ua

ORCID: 0000-0001-6957-4748

Based on the assessment of the current state of Science and technology, it becomes obvious that in the next 10 years there will be a breakthrough in the use of quantum computers for solving cybersecurity problems [1]. The most pessimistic predictions show that quantum cryptanalysis based on Grover's algorithm will halve the stability of all symmetric cryptographic mechanisms [2–4]. Plans to create a 100-qubit quantum computer by 2024 significantly exacerbate this problem [5, 6].

2. The Latest Studies and Printed Works Analysis

Analysis of recent studies and publications [1, 8–11] and others has shown that a number of new approaches to ensuring the cryptographic stability of symmetric cryptosystems are currently known. In the transition and post-quantum period, the approaches described in [1, 8–13] will also be relevant.

At the same time, there are other alternatives to the established classical approaches. In particular, general approaches to creating a new class of cryptosystems are described in [14, 15], but specific cryptographic mechanisms for their implementation are not given.

In [16], the idea of creating symmetric cryptosystems based on the Fredholm integral equation of the first kind was developed, and in [17] the requirements for choosing an encryption key were formalized. However, the key generation mechanism and its spectral model are not given.

3. Purpose

The purpose of this article is to develop a mechanism for generating an encryption key for a symmetric cryptosystem based on differential transformations and obtain its spectral model.

4. Concept presentation

Based on [18], the encryption key $K(x,s)$ is the core of the Fredholm integral equation of the first kind [16, 17]

$$\int_a^b K(x,s)\, z(s)\, ds = u(x),\ a \le x,\ s \le b,$$

where $z(s)$ – plaintext;

$u(x)$ – cipher.

There are many special features for choosing an encryption key for the Fredholm cryptosystem, which can be applied to the function of the initial wiggle [19]

$$K(x,s) = \sum_{l=1}^{m} g_l(x) q_l(s). \qquad (1)$$

To obtain an analytical spectral model of the encryption key (1), we will use differential transformations of Academician of the National Academy of Sciences of Ukraine G. E. Pukhov [20–23], the use of which for solving cybersecurity problems was first described in the monograph [24].

According to [20–23], differential transformations are transformations of the form

$$X(k) = \underline{x}(k) = \frac{H^k}{k!}\left[\frac{d^k x(t)}{dt^k}\right]_{t=0} \quad \underline{\cdot}$$
$$\underline{\cdot}\ x(t) = \sum_{k=0}^{k=\infty}\left(\frac{t}{H}\right)^k X(k), \qquad (2)$$

where $x(t)$ – the original, which is a continuous, differentiable infinite number of times and bounded together with all its derivatives, function of a real argument t;

$X(k)$ and $\underline{x}(k)$ equivalent notation of the differential image of the original representing a discrete (lattice) function of an integer argument $k =: 0, 1, 2, \ldots$;

H – a scale steel that has the dimension of an argument t and is often chosen equal to the segment $0 \le t \le H$ on which the function is considered $x(t)$;

$\underline{\cdot}$ – a symbol of correspondence between the original $x(t)$ and its differential image $X(k) = \underline{x}(k)$.

To the left of the symbol $\underline{\cdot}$ is a direct transformation that allows you to find the image $X(k)$ behind the original $x(t)$, and to the right is a reverse transformation that allows you to get the original behind the image in the form of a

power series, which is nothing more than an otherwise written Taylor series centered at a point $t = 0$.

Differential images $X(k)$ are called differential T-spectrum, and the values of the T-function $X(k)$ for specific argument k values are called samples.

Using the direct transformation (2) and the general property of the product of functions in the image domain for differential transformations [20–23] for expression (1), we obtain

$$K(x,s) \div K(x,k) \Rightarrow$$
$$\Rightarrow \sum_{l=1}^{m} g_l(x) q_l(s) \div \sum_{l=1}^{m} g_l(x) Q_l(k), \quad (3)$$

where $g_l(x)$ – constant;

$Q_l(k)$ – original image $q_l(s)$, $Q_l(k) = \frac{H_l{}^k}{k!}\left[\frac{d^k q(s)}{ds^k}\right]_{s=0}$.

Let the function $q_l(s)$ belong to a class of power functions, i.e. $q_l(s) = s_l{}^n$.

Then, according to [20–23], its image from the general form $Q_l(k) = \frac{H_l{}^k}{k!}\left[\frac{d^k q(s)}{ds^k}\right]_{s=0}$ will be reduced to an expression

$$Q_l(k) = H_l{}^n \mathfrak{b}(k-n) = \begin{cases} H_l{}^n, k = n, \\ 0, \quad k \neq n. \end{cases}$$

Taking this into account, the right-hand side of expression (3) will have the form

$$K(x,k) = \sum_{l=1}^{m} g_l(x) H_l{}^n \mathfrak{b}(k-n), \quad (4)$$

where $\mathfrak{b}(k-n)$ – displaced "teda", $\mathfrak{b}(k-n) = \begin{cases} 1, k = n, \\ 0, k \neq n. \end{cases}$

We find in general the differential spectra for model (4), substituting sequentially the values of the integer argument $k =: 0, 1, 2, 3$. If, for example $n = 2$, we have:

for $k =: 0$

$$K(x,0) = \sum_{l=1}^{m} g_l(x) H_l{}^2 \mathfrak{b}(0-2) = 0; \quad (5)$$

for $k =: 1$

$$K(x,1) = \sum_{l=1}^{m} g_l(x) H_l{}^2 \mathfrak{b}(1-2) = 0; \quad (6)$$

for $k =: 2$

$$K(x,2) = \sum_{l=1}^{m} g_l(x) H_l{}^2 \mathfrak{b}(2-2) = \sum_{l=1}^{m} g_l(x) H_l{}^2; \quad (7)$$

for $k \geq 3$

$$K(x,k \geq 3) = \sum_{l=1}^{m} g_l(x) H_l{}^2 \mathfrak{b}(3-2) = 0. \quad (8)$$

Thus, the spectral model of the encryption key $K(x,k)$ for a symmetric cryptosystem on differential transformations in general form in the image domain under the accepted conditions is the sum of the discretits found (5)–(8), i.e.

$$K(x,k) = \sum_{l=1}^{m} g_l(x) H_l{}^2. \quad (9)$$

We give examples of constructing a spectral model of the encryption key for a symmetric cryptosystem based on differential transformations based on the initial data given in [25]. So according to [25] the encryption key $K(x,s) = xs$. Then expression (4) is simplified and takes the form

$$K(x,k) = xH\mathfrak{b}(k-1). \quad (10)$$

Changing the value of the integer argument $k =: 0, 1, 2, \ldots$ by analogy with expressions (5)–(8), we obtain the differential spectrum discretits for the desired spectral model.

For $k =: 0$

$$K(x,0) = 0; \quad (11)$$

for $k =: 1$

$$K(x,1) = xH; \quad (12)$$

$$\text{for } k \geq 2$$
$$K\left(x, k \geq 2\right) = 0. \qquad (13)$$

So, for the example given in [25], taking into account the discrete found (11)–(13), the desired spectral model of the encryption key (4) is determined by the expression

$$K\left(x,k\right) = xH,\ m = l.$$

We present a graph of the functions of the encryption key (fig. 1 a) and its T-spectrum (fig. 1 b) for the found model (10).

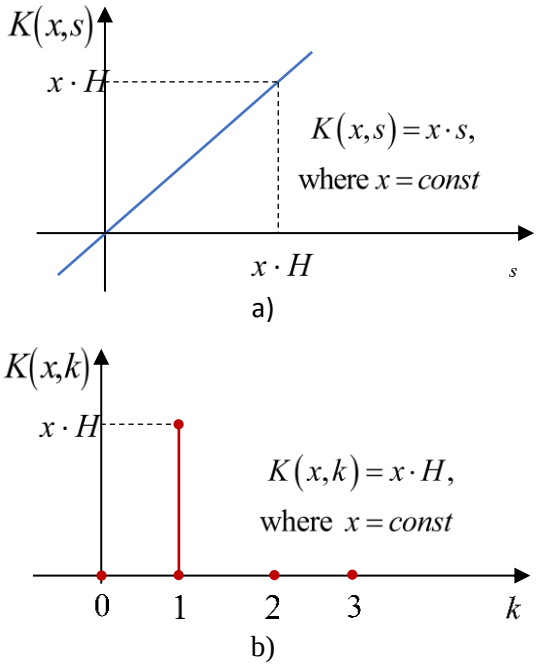

Figure 1: Encryption key function-original (a) and its differential T-spectrum (b) – image

5. Conclusions

In this paper, a mathematical model of the encryption key for a symmetric cryptosystem based on differential transformations is proposed for the first time. The resulting spectral model in the image domain is the sum of discretits for specific argument k values. The model meets the requirements put forward in [19], and its convergence with the results of known studies [25] confirms its adequacy.

The direction of further research will be the formation of a set of possible keys for a symmetric cryptosystem based on differential transformations and obtaining their Spectral models. The main purpose of the resulting model is its use in a symmetric cryptosystem on differential transformations during encryption and decryption in voice message transmission systems (VoIP-traffic).

6. Acknowledgements

I would like to express my gratitude to the staff of the research department of the scientific center of the Korolyov Zhytomyr Military Institute for their support and valuable comments, taking into account which helped to improve the quality of the presentation of the work.

7. References

[1] R. Hryshchuk, Yu. Danik. Osnovy kibernetychnoi bezpeky, (in Ukrainian). Zhytomyr National Agroecological University, Zhytomyr, Ukraine (2016).

[2] I. Hrabar, R. Hryshchuk, K. Molodetska. Bezpekova synerhetyka: kibernetychnyi ta informatsiinyi aspekty, (in Ukrainian). Zhytomyr National Agroecological University, (2019).

[3] B. G. Markaida, X. Larrucea, M. G. Romay Quantum and post-quantum cryptography and cybersecurity: A systematic mapping: Investigación en Ciberseguridad Actas de las VI Jornadas Nacionales (JNIC2021 LIVE) Online 9-10 de junio de 2021 Universidad de Castilla-La Mancha, 2021, pp. 237–244.

[4] K. Kan, M. Une. Recent Trends on Research and Development of Quantum Computers and Standardization of Post-Quantum Cryptography. IMES Discussion Paper Series 21-E-05, Institute for Monetary and Economic Studies, Bank of Japan, No. 2021-E-5, 2021, pp. 1–41.

[5] K. Babber, J. P. Singh. Quantum cryptography and security analysis, Journal of Discrete Mathematical Sciences and Cryptography, 2021, DOI: 10.1080/09720529.2019.1692452.

[6] J.-F. Biasse, B. Pring. A framework for reducing the overhead of the quantum oracle for use with Grover's algorithm with applications to cryptanalysis of SIKE, J. Math. Cryptol. 2021, pp. 143–156, DOI.ORG/10.1515/jmc-2020-0080.

[7] J. Preskill. Quantum computing: Current status and future prospects. Bulletin of the American Physical Society 65 (2020).

[8] Russia sets up lab to create quantum computer [Electronic resource] // huaxia. – 2020. – Resource access mode: http://www.xinhuanet.com/english/2020-11/25/c_139542572.htm.

[9] S. Mitra, B. Jana, S. Bhattacharya, P. Pal, J. Poray. Quantum cryptography: Overview, security issues and future challenges," 2017 4th International Conference on Opto-Electronics and Applied Optics (Optronix), 2017, pp. 1–7, DOI: 10.1109/OPTRONIX.2017.8350006.

[10] A. Ejaz, I. A. Shoukat, U. Iqbal, A. Rauf, A. Kanwal 2021. A secure key dependent dynamic substitution method for symmetric cryptosystems. PeerJ Comput. Sci. 7:e587 DOI 10.7717/peerj-cs.587.

[11] L. Julakidze, Z. Kochladze, T. Kaishauri. New Symmetric Tweakable Block Cipher Bulletin of the Georgian National Academy of Sciences, vol. 15, no. 1, 2021, pp. 13–19.

[12] B. M. Alshammari, R. Guesmi, T. Guesmi, H. Alsaif, A. Alzamil. Implementing a Symmetric Lightweight Cryptosystem in Highly Constrained IoT Devices by Using a Chaotic S-Box. Symmetry 2021, 13, 129. https://doi.org/10.3390/sym13010129.

[13] E. Hernandez-Diaz, H. Perez-Meana, V. Silva-Garcia. Encryption of RGB Images by Means of a Novel Cryptosystem Using Elliptic Curves and Chaos IEEE Latin America Transactions, Vol. 18, NO. 8, August 2020, pp. 1407–14015.

[14] I. Gorbenko, V. Ponomar. Investigation of the possibility of using and the advantages of post-quantum algorithms depending on the conditions of use // Eastern-European Journal of Advanced Technologies. 2017.Vol. 2.No. 9 (86). S. 21–32.

[15] Symmetric block cipher "Kalina" - a new national encryption standard of Ukraine / I. D. Gorbenko et al. // Radio engineering: All-Ukrainian interdepartmental scientific and technical collection - 2015. - Issue. 181. - S. 5 - 22.

[16] G. Bronshpak, I. Gromiko, S. Docenko and E. Perchik, "Kriptografiya novogo pokoleniya Integralnie uravneniya kak alternativa algebraicheskoi metodologiyi", [New generation cryptography: Integral equations as an alternative to algebraic methodology], Prikladnaya elektronika, № 3, pp. 337-349, 2014. DOI: 10.13140/RG.2.1.1973.2645. (In Ukrainian).

[17] I. Gromiko, «Obschaya paradigma zaschiti informacii_ problemi zaschiti informacii v aspektah matematicheskogo modelirovaniya: monografiya», [The general paradigm of information security: problems of information security in aspects of mathematical modeling: a monograph], Harkiv: HNU imeni V.N. Karazina, 2014, p. 216. (In Ukrainian).

[18] R. V. Hryshchuk, O. M. Hryshchuk. A Generalized Model of Fredholm's Cryptosystem. Cybersecurity: education, science, technique, 2019, Vol. 4 (4), pp. 14–23. DOI: 10.28925/2663-4023.2019.4.1423. (In Ukrainian).

[19] O. M. Hryshchuk. Features of the encryption key selection for the Fredholm cryptosystem. Computer Engineering and Cybersecurity: Achievement and Innovation: Materials II All-Ukrainian. nauk.-practical. conf. zdobuvachiv vishoï educate th young pupils, metro Kropyvnytskyi, 25-27 leaf. 2020 p. / Ministry of Education and Science of Ukraine, the State of Science established the “Institute of Modernization for Science of Science”, Central Ukrainian National Technical University; - Kropyvnytskyi: TsNTU, 2020. P. 109-110 p.

[20] G. E. Pukhov, Computational structure for solving differential equations by Taylor transformations, Cybern. Syst. Anal. 14 (1978) 383.

[21] G. E. Pukhov, Expansion formulas for differential transforms, Cybern. Syst. Anal. 17 (1981) 460.

[22] G. E. Pukhov, Differential transforms and circuit theory, Int. J. Circ. Theor. App. 10 (1982) 265. [4] G. E. Pukhov, Differential transforms of functions and equations, in Russian, Naukova Dumka, Kiev, 1980.

[23] G. E. Pukhov, Differential transformations and mathematical modeling of physical processes, in Russian, Naukova Dumka, Kiev, 1986.

[24] R.V. Hryshchuk Theoretical foundations of modeling the processes of attacking information by methods of theories of differential igors and differential revision: monograph / R.V. Grishchuk. - Zhitomir: Ruta, 2010 . - 280 p.

[25] A. M. Wazwaz. The Regularization Method for Fredholm Integral Equations of the First Kind. Comput. Math. Appl. 2011, 61, 2981–2986.