Approach to Constructing Symmetric Cryptographic Systems Ensuring Specified Resilience to Cryptoanalysis over the Long-Term Time Horizon

Sergey Tarasenko, Yuri Ivanov

***Abstract*— The paper presents the results of an analysis of the decrease in cryptographic strength of the most common symmetric ciphers, taking into account the development of cryptanalytic methods. The vector of the threat to the reduction of information confidentiality stored and processed in information systems in the long term has been determined. An approach to constructing hybrid ciphers, based on the symbiosis of a composite cipher and the Vernam cipher, has been proposed to enhance the asymptotic cryptographic strength of symmetric cryptographic systems used for data encryption in information systems, the relevance of stored and processed information in which does not significantly decrease over time. For instance, this is applicable to information systems built on distributed ledger technology (blockchain networks).**

***Tóm tắt*— Bài báo trình bày kết quả phân tích sự suy giảm độ mạnh mật mã của các mật mã đối xứng phổ biến nhất, có tính đến sự phát triển của các phương pháp giải mã. Các vectơ của mối đe dọa làm giảm tính bảo mật thông tin được lưu trữ và xử lý trong hệ thống thông tin về lâu dài đã được xác định. Một cách tiếp cận để xây dựng mật mã lai, dựa trên sự cộng sinh của mật mã tổng hợp và mật mã Vernam, đã được đề xuất để nâng cao sức mạnh mật mã tiệm cận của các hệ thống mật mã đối xứng được sử dụng để mã hóa dữ liệu trong hệ thống thông tin, sự liên quan của thông tin được lưu trữ và xử lý trong đó không giảm đáng kể theo thời gian. Điều này có thể áp dụng cho các hệ thống thông tin được xây dựng trên công nghệ sổ cái phân tán (mạng blockchain).**

This manuscript is received on December 01, 2023. It is commented on December 10, 2023 and is accepted on December 20, 2023 by the first reviewer. It is commented on December 07, 2023 and is accepted on December 15, 2023 by the second reviewer.

***Keywords*— Symmetric ciphers; symmetric cryptosystems; asymptotic cryptographic strength; hybrid cipher; composite cipher; Vernam cipher; cryptanalysis.**

***Từ khóa*— Mật mã đối xứng; hệ thống mật mã đối xứng; độ mạnh mật mã tiệm cận; mật mã lai, mật mã tổng hợp; mật mã Vernam; phân tích mật mã.**

I. INTRODUCTION

As of the present day, a substantial array of diverse symmetric encryption algorithms exists, the resilience of which is currently deemed sufficiently high: Advanced Encryption Standard (*AES*) [1], International Data Encryption Algorithm (*IDEA*) [2], Magma (*GOST* 28147–89) [3], Kuznyechik (*GOST R* 34.12–2015) [4], and so forth.

Nevertheless, for the majority of previously developed algorithms, over time, methods were discovered to reduce their cryptographic resilience by identifying specific algorithmic vulnerabilities (e.g., the resilience of A5 was diminished from 2^{54} to 2^{17} [5]), applying cryptanalysis based on novel principles (e.g., linear and differential cryptanalysis for *DES* [6]), employing keys of insufficient length during encryption (a key length considered acceptable in the 1970s, such as 56 bits, is no longer deemed adequate in contemporary understanding [7]), or uncovering "weak keys" [8].

II. THE VECTOR OF THE THREAT FOR REDUCING INFORMATION CONFIDENTIALITY IN THE LONG TERM

Currently, widely adopted are information systems constructed utilizing distributed ledger technology [9, 10, 11], wherein the deletion or alteration of data is infeasible. There exists no singular central control point (failure point), and a copy of all data is distributed across multiple nodes

within the information system. This characteristic renders such systems potential targets for cryptanalytic attacks in the long term, as malicious entities are relieved of the necessity for prior collection and storage of encrypted information.

Thus, in the current stage of scientific and technical development, considering the escalating computational power of technology, the aforementioned trend of diminishing cryptographic resilience over time, coupled with the existence of information systems wherein a reduction in the confidentiality of stored and processed data is impermissible, underscores the relevance of researching approaches to constructing cryptographic systems that ensure specified resistance to cryptanalysis in the long term.

III. Analysis of the cryptographic resilience of symmetric ciphers

As the majority of existing block ciphers support modes of operation in which they operate as stream ciphers, the resilience information presented in Table 1, expressed in terms of the number of elementary computational operations (e.c.o.), for widely adopted block ciphers is considered indicative of the dynamic changes in the resilience of existing symmetric ciphers, taking into account the development of cryptanalytic methods.

Table 1. Cryptanalysis results of the most common symmetric ciphers

Cipher	**Processing complexity, e.c.o**	**Attack**	**Processing complexity considering the attack, e.c.o**	
RC5	2^{64}	Differential cryptanalysis [12]	2^{44}	
DES	2^{56}	Linear cryptanalysis with chosen-plaintext [13]	2^{39-43}	
3*DES*-168	2^{168}	"Meet-in-the-Middle" attack + chosen-plaintext attack [14]	2^{80}	
GOST 28147–89	2^{256}	Enhanced differential cryptanalysis [15]	2^{179}	
Salsa20-128	2^{128}	Truncated differential cryptanalysis [16]	7 rounds	2^{109}
Salsa20-256	2^{256}	Truncated differential cryptanalysis [16]	8 rounds	2^{250}
CAST-256	2^{256}	Zero-correlation cryptanalysis [17]	$2^{246.9}$	
IDEA	2^{128}	"Meet-in-the-Middle" attack [18]	$2^{126.1}$	
AES-128	2^{128}	"Meet-in-the-Middle" attack [19]	$2^{126.1}$	
AES-192	2^{192}	"Meet-in-the-Middle" attack [19]	$2^{189.7}$	
AES-256	2^{256}	"Meet-in-the-Middle" attack [19]	$2^{254.4}$	
AES-192	2^{192}	Related-key attack [20]	2^{176}	
AES-256	2^{256}	Related-key attack [20]	$2^{99.5}$	
AES-256	2^{256}	Related-key attack [21]	9 rounds	2^{39}
			10 rounds	2^{45}
			11 rounds	2^{70}
GOST R 34.12–2015	2^{256}	"Meet-in-the-Middle" attack [22]	5 rounds	2^{140}

The analysis of applicable methods of cryptanalysis for existing symmetric ciphers has revealed that a reduction in the cryptographic strength of these ciphers over time is possible due to several reasons:

- Imperfections in specific implementations of block and stream ciphers.
- Development of novel cryptanalysis methods, protection against which was not considered during the development of specific ciphers.
- Utilization of a low entropy-to-information ratio, whereby the fundamental operations ensuring cryptographic strength (dispersion and mixing) exhibit a pseudorandom nature and, consequently, are theoretically susceptible to cryptanalysis.

The aforementioned factors contributing to the diminished cryptographic strength of ciphers pose a long-term threat to the confidentiality of information encrypted using these ciphers.

IV. Approach to the development of cryptographic systems ensuring predetermined resilience in the long-term perspective, and the concept of their operation

The enhancement of cryptographic resilience in the long-term temporal perspective can be achieved through the development of a symmetric cryptographic system capable of encrypting information with predetermined resilience without substantial alterations to cryptographic transformation algorithms.

Considering the factors contributing to the reduction in the resilience of symmetric ciphers, a decision has been made regarding the necessity of developing a symmetric cryptographic system utilizing a cipher based on fundamental operations of confusion, diffusion and variable length fractionation. These operations ensure cryptographic resilience of the encrypted information, executed with the utilization of random control data (keys) and based on the Vernam cipher, providing absolute cryptographic resilience under specified requirements.

The concept of the proposed cryptographic system can be described as follows:

1) The Vernam cipher is employed for encrypting the plaintext. Upon exhaustion of the key for the Vernam cipher, a new key is generated using a random number generator (*RNG*). The distinctive feature here lies in the method of key generation. In contrast to stream ciphers, which generate the keystream from the old key, the Vernam cipher, upon key exhaustion, make use of a random number generator to create a new key. This avoidance of generating the keystream from the old key enhances the cryptographic properties and resilience of the system. Subsequently, the generated key is encrypted utilizing a compositional cipher, the fundamental resilience of which is grounded in random fundamental cryptographic operations that resist efficient cryptanalysis methods, with a specified resilience of $O_{CC}(L,t)$ – defined by the equation (1):

$$\lim_{t\to\infty} O_{CC}(L,t) = const, \qquad (1)$$

where L – represents the key length.

2) Since the resilience of a cryptographic system is determined by the element within the system possessing the least resilience, the encryption of plaintext using a key for the Vernam cipher transmitted through its encryption using a compositional cipher will also be carried out with resilience $O_{CC}(L,t)$.

Thus, a combined cipher incorporating the Vernam cipher and a compositional cipher will also exhibit resilience $O_{CC}(L,t)$.

As a compositional cipher, one may consider, for instance, a cipher implemented in accordance with transformations described in works [23, 24].

Figure 1 illustrates the general concept of the operation of the proposed cryptographic system.

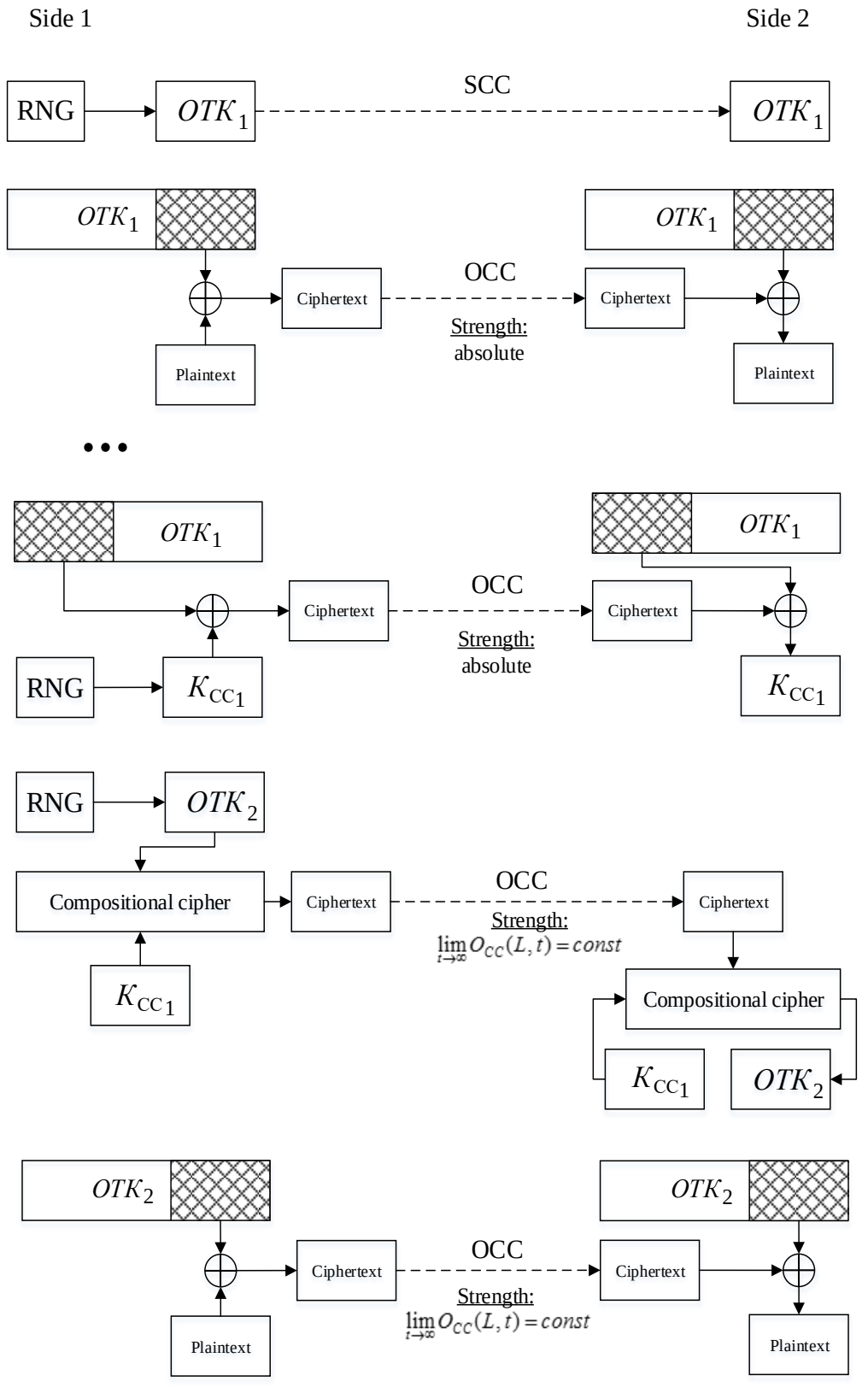

Figure 1. General concept of operation of the proposed cryptographic system

In figure 1: *OCC* – open communication channel, *SCC* – secure communication channel, *OTKi* – *i*-th key for Vernam cipher, K_{CC_i} – *i*-th key for compositional cipher.

V. The methodology for assessing the quality of the developed cryptographic system

As an attributive property for the criterion of suitability G_t for the proposed symmetric cryptographic system (*CS*), the quantity of requisite key exchange sessions over a secure communication channel between parties is adopted. This measure is deemed essential for the uninterrupted operation of the *CS* – defined by the equation (2):

$$G_t : N_{PCS} \le N_{SCS}, \qquad (2)$$

where N_{PCS} – the number of key information transmission sessions required for the proposed cryptosystem, N_{SCS} – the number of key information transfer sessions required for the currently most common symmetric cryptographic systems (N_{SCS} = 1).

Based on the designated purpose of research, the asymptotic strength of the cipher (at time $t \to \infty$) is taken as an attribute property S_t for the criterion of superiority. It is correct to compare the asymptotic strength S_{PC} of the cipher used in the proposed cryptosystem with the asymptotic strength S_{BC} of one of the most common symmetric ciphers at the moment.

Thus, the criterion for the superiority of the developed cryptosystem is determined as follows and defined by the equation (3):

$$S_t : S_{PC} > S_{BC}. \qquad (3)$$

To represent the target function in multiplicative form, indicator functions for criteria are introduced and defined by the equations (4) and (5):

- Suitability G_t:

$$IndF_G\left(N_{PCS}, N_{SCS}\right) = \begin{cases} 1, if\ N_{PCS} \le N_{SCS} \\ 0, else \end{cases}; \qquad (4)$$

- Superiority S_t:

$$IndF_S\left(S_{PC}, S_{BC}\right) = \begin{cases} 1, if\ S_{PC} > S_{BC} \\ 0, else \end{cases}. \qquad (5)$$

To assess the degree of achievement of the goal, the function Λ_s is introduced – defined by the equation (6):

$$\Lambda_s(S_{PC}, S_{BC}) = \frac{S_{PC}}{S_{BC}}. \qquad (6)$$

The value of the objective function defined by the equation (7):

$$\begin{aligned} V : V_p^A \begin{pmatrix} IndF_G\left(N_{PCS}, N_{SCS}\right), \\ IndF_S\left(S_{PC}, S_{BC}\right), \\ \Lambda_S\left(S_{PC}, S_{BC}\right) \end{pmatrix} = \\ = IndF_G\left(N_{PCS}, N_{SCS}\right) \cdot \\ \cdot IndF_S\left(S_{PC}, S_{BC}\right) \cdot \\ \cdot \Lambda_S\left(S_{PC}, S_{BC}\right). \end{aligned} \qquad (7)$$

The cryptosystem is evaluated as effective according to criteria G_t and S_t when the value of its objective function V_{t1} satisfies the condition: $V_{t1} \ge V_{t0} > 1$.

VI. Conclusions

Thus, the approach described in this work provides the capability to construct and assess the quality of symmetric cryptographic systems based on combined ciphers, ensuring resilience against cryptanalysis in the long-term perspective, while adhering to specific requirements imposed on the utilized composite ciphers [24] and the requirements for employing the Vernam cipher [25]. This stands in contrast to block ciphers, the resilience of which may be diminished as t → ∞.

References

[1] Ilia Toli, Alberto Zanoni. An Algebraic Interpretation of AES-128 // Proc. of AES Conference. — 2005. — Vol. 2005. — P. 84—97. — doi:10.1007/11506447_8.

[2] R. Zimmermann, A. Curiger, H. Bonnenberg, H. Kaeslin, N. Felber, and W. Fichtner. A 177Mb/sec VLSI implementation of the

international data encryption algorithm // IEEE Journal of Solid-State Circuits. — March 1994. — T. 29. — C. 303—307.

[3] GOST 28147–89 (RFC 5830).

[4] National Standard of Russian Federation GOST R 34.12–2015 (RFC 7801).

[5] Goldberg, Ian; Wagner, David; Green, Lucky (August 26, 1999). "The (Real-Time) Cryptanalysis of A5/2". David Wagner's page at UC Berkeley Department of Electrical Engineering and Computer Sciences.

[6] Biham, Eli and Shamir, Adi (1991). "Differential Cryptanalysis of DES-like Cryptosystems". Journal of Cryptology. 4 (1): 3–72. doi:10.1007/BF00630563.

[7] Barker, Elaine; Barker, William; Burr, William; Polk, William; Smid, Miles (2005-08-01). "NIST Special Publication 800-57 Part 1 Recommendation for Key Management: General". National Institute of Standards and Technology. Table 4, p. 66. doi:10.6028/NIST.SP.800-57p1.

[8] NIST, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Special Publication 800-67, page 14.

[9] Decree of the Government of the Russian Federation dated 02.09.2021 No. 1471 "On conducting an experiment to test the method of interaction between the depository storing the electronic mortgage and the federal executive body performing the functions of state registration of rights to real estate and transactions with it, using the MasterChain information system based on distributed registry technology."

[10] Official page of the Bank of Russia dedicated to the "digital ruble" [Electronic resource] // URL: https://cbr.ru/fintech/dr (access date: 09/06/2023).

[11] Official page for voting on amendments to the Constitution of the Russian Federation on July 1, 2020 [Electronic resource] // URL: https://www.mos.ru/city/projects/vote2020 (access date: 09/06/2023).

[12] Birykov A., Kushilevitz E. (1998). Improved Cryptoanalysis of RC5. EUROCRYPT 1998.

[13] Junod, Pascal (2001-08-16). On the Complexity of Matsui's Attack. Selected Areas in Cryptography. Lecture Notes in Computer Science. Vol. 2259. Springer, Berlin, Heidelberg. Pp. 199-211. DOI: 10.1007/3-540-45537-X_16. ISBN 978-3540455370.

[14] Barker, Elaine (January 2016). "NIST Special Publication 800-57: Recommendation for Key Management Part 1: General".

[15] Nicolas Courtois. An Improved Differential Attack on full GOST. The New Codebreakers, pp. 282-303. 2016. DOI: 10.1007/978-3-662-49301-4_18.

[16] Zhenqing Shi, Bin Zhang, Dengguo Feng, Wenling Wu (2012). "Improved Key Recovery Attacks on Reduced-Round Salsa20 and ChaCha". Information Security and Cryptology – ICISC 2012. ICISC'12 Proceeding of the 15th International Conference on Information Security and Cryptology. Lecture Notes in Computer Science. Vol. 7839. Pp. 337-351. DOI: 10.1007/978-3-642-37682-5_24. ISBN 978-3-642-37681-8.

[17] Bogdanov, Andrey; Leander, Gregor; Nyberg, Kaisa; Wang, Meiqin (2012). Integral and multidimentional linear distinguishers with correlation zero. Lecure Notes in Computer Science. Vol. 7658. Pp. 244-261. DOI: 10.1007/978-3-642-34961. ISBN: 978-3-642-34960-7.

[18] Dmitry Khovratovich, Gaetan Leurent, Christian Rechberger. Conference: Proceeding of the 31th Annual International conference on Theory and Applications of Cryptographic Techniques, 2012. DOI: 10.1007/978-3-642-29011-4_24.

[19] Andrey Bogdanov, Dmitry Khovratovich, Christian Rechberger. Biclique Cryptoanalysis of the Full AES. Conference: Advances in Cryptology – ASIACRYPT 2011, 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. DOI: 10.1007/978-3-642-25385-0_19. Proceeding.

[20] Alex Birykov, Dmitry Khovratovich, Related-key cryptoanalysis of full AES-192 and AES-256. Advances in Cryptology –ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009. Proceeding. DOI: 10.1007/978-3-642-10366-7_1.

[21] Alex Birykov, Orr Dunkelman; Nathan Keller; Dmitry Khovratovich; Adi Shamir (2009-08-19). "Key Recovery Attacks of Practical Complexity on AES Variants With Up To 10 Rounds".

[22] Riham AlTawy; Amr M. Youssef (2015-04-17). "A Meet in the Miidle Attack on Reduced Round Kuznyechik". IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences. 98 (10): 2194. DOI: 10.1587/transfun.E98.A.2194.

[23] Tarasenko, S.S. "Mathematical model of a cryptographic system for secure information exchange based on the Vernam cipher and ephemeral keys". Zaŝita informacii. Inside: Journal, 2023, No. 4, pp. 62–69. ISSN: 2413-3582.

[24] Tarasenko, S.S. "Justification of strength of a combined cipher based on Vernam cipher and composite cipher". Telecommunications, 2023, Moscow, No. 11, pp. 12–22. ISSN: 1684-2588.

[25] The Venona Translations. The Venona Story. Fort Meade, Maryland: National Security Agency. 2004-01-15. P. 17 th.

ABOUT THE AUTHORS

Tarasenko Sergey

Workplace: Academy of the Federal Guard Service of Russian Federation.

Email: dor7la96@mail.ru

Education: Graduated Academy of the Federal Guard Service of Russian Federation in 2019.

Recent research interests: Information security; Mathematical cryptography; Steganography; Blockchain; Neural networks.

Cơ quan làm việc: Học viện FSO, Liên bang Nga.

Email: dor7la96@mail.ru

Quá trình đào tạo: Tốt nghiệp Học viện FSO vào năm 2019.

Hướng nghiên cứu hiện nay: Bảo mật thông tin; Mật mã toán học; Mật mã; Chuỗi khối; Mạng nơ-ron.

Ivanov Yuri

Workplace: Academy of the Federal Guard Service of Russian Federation.

Email: zhmur@yahoo.com

Education: Graduated Academy of the Federal Agency for Government Communications and Information under the President of the Russian Federation in 2003; Received this PhD degree in Engineering Sciences in Oryol State Technical University in 2008.

Recent research interests: Information security; Cryptography; Distributed control systems.

Cơ quan làm việc: Học viện FSO, Liên bang Nga.

Email: zhmur@yahoo.com

Quá trình đào tạo: Tốt nghiệp Học viện Thông tin và Truyền thông Chính phủ Liên bang Nga vào năm 2003; Tiến sĩ Khoa học kỹ thuật tại Đại học Kỹ thuật Bang Oryol vào năm 2008.

Hướng nghiên cứu hiện nay: Bảo mật thông tin; Mật mã; Hệ thống điều khiển phân tán.