ADVANCES IN CYBER-PHYSICAL SYSTEMS

Vol. 7, No. 1, 2022

FEATURES OF USING LARGE KEYS IN «KALYNA» ALGORITHM

Taras Zaiats, Volodymyr Bilenko, Valerii Hlukhov

Lviv Polytechnic National University, 12, Bandera Str, Lviv, 79013, Ukraine.
Authors' e-mail*: taras.zaiats.mki.2020@lpnu.ua, volodymyr.bilenko.ki.2017@lpnu.ua, valerii.s.hlukhov@lpnu.ua*

https://doi.org/10.23939/acps2021.__.___

Submitted on 10.10.2021

***Abstract*: The information security is playing an increasingly important role nowadays. Therefore, virus can be transmitted through the information in encrypted form. This is also applied to embedded systems. In this regard, the article is assigned to the topic of cryptocurrency protection in embedded systems. The article is focused on the algorithm of symmetric block transformation "Kalyna".**

The algorithm has been developed in cooperation with the State Special Communications Service and leading Ukrainian scientists. The experience and results of international and open national competition of cryptographic algorithms have been taken into account. The algorithm is intended for gradual replacement of the interstate standard DSTU GOST 28147: 2009.

Its differences from other data encryption standards used, both in Ukraine and in the world, have been analyzed. The stability of the "Kalyna" algorithm has been also analyzed using a high-bit key (512 bits) and its speed has been compared with other cryptographic protection algorithms.

***Index Terms*: block cipher, cryptographic information protection, data encryption standard, symmetric block transformation algorithm.**

INTRODUCTION

One of the most important activities in the field of data confidentiality was and remains the data protection by cryptographic methods. Development of cryptographic information protection systems, organization and adjustment of production of domestic protected means and technologies of information processing have become priority areas of activity in the field of information security as a component of national security of our state. Such systems are used in Ukraine, in particular, in the banking sector, public administration, at facilities that are of strategic importance for the economy and security of the state, and so on.

The information security is playing an increasingly important role nowadays. Therefore, virus can be transmitted through the information in encrypted form. This is also applied to embedded systems. In this regard, the article is assigned to the topic of cryptocurrency protection in embedded systems. The article is focused on the algorithm of symmetric block transformation "Kalyna".

The algorithm of symmetric block transformation "Kalyna" is considered in the article. The stability of this cipher, with a block size of 512 bits, is analyzed, and the performance is compared with existing encryption algorithms, such as: AES, GOST 28147-89, "BelT", "Kuznyechik", and the impact of processor and operating system performance on algorithm performance.

ANALYSIS OF RECENT RESEARCH AND PUBLICATIONS

Today, an encryption of symmetric block algorithms (BSC - block symmetric cipher) is the main cryptographic means of ensuring confidentiality in information processing in modern information and telecommunications systems as part of protocols such as TLS [1] or Noise [2], and in the application or system software.

Block ciphers are one of the most common cryptographic primitives. They provide privacy and are also used as design elements to build hash functions, message authentication codes, and more. The importance of BSC is further emphasized by the holding of many international cryptographic competitions, which focused on the development of a block cipher, or its modernization.

At the time of adoption of the standard DSTU 7624: 2014 [3] in Ukraine the following cryptographic algorithms were used: DSTU GOST 28147: 2009 [4] - cryptosystem developed in 1989, which Ukraine inherited from the Soviet Union, in 2009 it was certified as state standard of Ukraine; AES [5] is an algorithm used in general purpose for operating systems and it is included there as a means of encrypting information on disk; RC4 [6] is used to implement SSL / TLS security of web connections [7]; Triple DES [8], which uses [9] the National Bank of Ukraine and for IPsec network traffic protection [10].

The block cipher defined in DSTU GOST 28147: 2009 [4] still provides practical resistance to attacks, but for this algorithm there are effective methods of cryptanalysis [11], the complexity of which is much less than the complexity of the attack by searching all keys, so this standard is derived from actions [12].

Replacing DSTU GOST 28147: 2009 [4] with the international standard AES [5] was not a solution to this problem for Ukraine, as world leaders in the IT industry are gradually abandoning this algorithm.

Thus, in Ukraine there was a significant problem of developing and implementing new modern encryption standards that would allow the creation of effective means of cryptographic data protection.

Taking into account the positive world experience of cryptographic competitions CRYPTREC [13], NESSIE [14], AES [15] and SHA3 [16], the State Service for Special Communications and Data Protection of Ukraine successfully held a national open competition of symmetric block cryptographic algorithms in 2007-2010 [17], which defeated the algorithm "Kalyna" [18], Kharkiv developers of the Institute of Information Technology [19], on the basis of which the national standard of Ukraine was developed [20]. As it has been described above, the new algorithm should provide greater cryptographic transformation speed compared to the AES algorithm [5], as well as have a higher level of stability against AES [5]. In the development it was decided to use an approach involving known and well-researched designs, for the safe use of the algorithm in the context of significant progress in data processing.

The basic parameters of the cipher were chosen based on the analysis of the capabilities of modern search attacks, as well as conflict rules [21], in addition, the developers of cryptographic information security systems were provided with the ability to choose parameters.

The standard symmetric encryption standard DSTU 7624: 2014 [3] defines ten different operating modes that are widely used in accordance with the international standard ISO/IEC 10116:2006 [22]. This is aimed at ensuring the widespread use of DSTU 7624:2014 [3], including the data protection transmitted on computer networks, encryption of hard drives and removable media, electronic documents and key data.

Modes of operation of the cryptographic algorithm defined in the standard DSTU 7624: 2014 [3], their designation, which provides the appropriate mode, are given in Table 2.

The effectiveness of the implementation of systems, tools and protocols for cryptographic data protection in information and telecommunications systems for various purposes can be ensured by the presence of such a number of modes of operation of the algorithm.

The new national encryption standard [3] is flexible and supports the following combinations of block size and key length (Table 3).

The designation of the algorithm operation mode looks like this: "Kalyna-l / k-mode designation-mode parameters" (some modes do not have parameters), where l is the size of the base transformation block, k is the key length.

For example, Kalyna-256/512-CCM-32,128 means the use of an algorithm with a block size of 256 bits, key length – of 512 bits, use in the mode of simulation and tampering, the length of the confidential and public part of the message is always less than 232 bytes, the length of imitation is 128 bit.

The number of iterations of the cryptographic algorithm was chosen so as to provide a sufficient margin of resistance to different types of cryptanalysis and is given in Table 1.

The implementation of the algorithm under optimal conditions involves the use of tables of preliminary calculations that implement both nonlinear and linear transformations (S-block [23] and multiplication by the MDV matrix [24]). Upgrades made in the "Kalyna" cipher allowed leaving only one set of tables, in contrast to the AES cipher [5], which requires two sets.

Table 2

Operating modes

№	Mode name	Marking
1	Simple replacement (basic conversion)	ECB
2	Encryption	CTR
3	Encryption feedback with ciphertext	CFB
4	Production of imitation	CMAC
5	Coupling of cipher blocks	CBC
6	Encryption feedback with cipherprogram	OFB
7	Selective quenching with accelerated production of imitation	GCM, GMAC
8	Production of imitation and encryption	CCM
9	Indexed replacement	XTS
10	Data protection	KW

Table 3

The size of the “Kalyna” block and corresponding possible key length

Block size	Key length
128	128, 256
256	256, 512
512	512

Table 4

Number of the "Kalyna" algorithm encryption iterations [3]

Key length	Number of rounds
128	10
256	14
512	18

During the development of the national standard DSTU 7624: 2014 [3] the assessment of the stability of cryptographic transformation against different types of cryptanalytic attacks was performed [25]. The complexity of the most effective cryptanalytic attacks with a reduced number of cycles (weakened algorithm) and the required number of cycles to ensure stability is given in Table 5 for a cipher with a large block size of 512 bits.

Table 5

The results of the analysis of the stability of the cipher "Kalyna" with a block size of 512 bits [23]

Methods of cryptanalysis	The smallest number of cycles	Indicators of attacks		
		Maximum number of cycles	Complexity eq. op. encrypted	Byte memory
Differential	9	8	2^{490}	
Linear	9	7	$2^{470,4}$	
Integral	7	6	2^{137}	2^{64+5}
Unrealizable differential	6	5	2^{60}	2^{66}
Boomerang	7	6	2^{340}	

After evaluating the stability, we obtained [25] the result that the cryptographic transformation is stable at 9 cycles for a 512-bit block.

In the article [25] the testing of cryptographic transformation speed was aimed at modeling the features of cryptographic protection tools that require high transformation speed such as IP traffic protection and others.

To eliminate the impact of the disk subsystem, all data was stored in random access memory (RAM). To prevent the use of data that is only in the processor's cache, it was decided to allocate a block of 1 GB, which is certainly many times larger than the available cache of any modern processor, which will lead to the need to make appeals to the main RAM. To reduce the impact of CPU context switching, this block of memory has been re-encrypted several times.

Measurement of speed through encryption of the same amount of plaintext (simple replacement mode, ECB) was performed for all combinations of block size and key length of the cipher "Kalyna", AES-128, AES-256, GOST 28147-89 [4], "BelT" (national standard of Belarus) [26] and the code "Kuznyechik" (national standard of Russia) [27] under the same conditions.

The test was performed on a computer running a 64-bit Linux operating system (Ubuntu 12.04) with an Intel Core i5-4670@3.40GHz processor. The results of testing the performance of the software implementation are given in Table 6.

As a result of testing on a 64-bit platform, "Kalyna" is a competitive cipher and shows the following performance results:

- for 128-bit key length, "Kalyna" performance is 3% higher than AES;
- for the 256-bit key length, "Kalyna" performance is 10% slower than AES (for a 128-bit block) and 1% faster (for a 256-bit block);
- "Kalyna" speed at the corresponding key length is higher than GOST 28147-89 2.9 times (for 128-bit block) and 3.2 times (for 256-bit block), and about 2 times higher than the new standards encryption of Belarus and Russia.
- for the 512-bit key length, the "Kalyna" speed is 1386.46 Mbit / s.

Table 6

Speed of block cipher software implementation [25]

№	Intel Core i5-4670@3.40GHz	
	Block cipher	Speed, Mb/s
1	Kalyna-128/128	2611.77
2	Kalyna-128/256	1779.52
3	Kalyna-256/256	2017.97
4	Kalyna-256/512	1560.89
5	Kalyna-512/512	1386.46
6	AES-128	2525.89
7	AES-256	1993.53
8	GOST 28147-89	639.18
9	STB 34.101.31-2011(BelT)	1055.92
10	Kuznyechik [31]	1081.08

It should be noted that the large key length is a feature of the algorithm and, as it can be seen from the test, it is inferior in speed to ciphers with smaller keys, but provides a high margin of resistance to cryptanalytic attacks (Table 5).

The speed of the "Kalyna" cipher is presented in crypto libraries [28] and [29].

In the cross-platform library of cryptographic primitives [28] the performance indicators are presented in Table 7. Measurements were performed for a computer with an Intel Core i7-6700HQ 2.6 GHz processor and with 16 GB of RAM in Windows 10 by encrypting a 16 KB unit during 1 million iterations. The documentation of the crypto library [28] shows the results of speed measurement, which are presented in Table 7 for 64-bit architecture. This cross-platform C ++ library is focused on achieving maximum performance. Performance was measured by encrypting a 130 KB file 1 million times in SHS mode (cipher block coupling mode) on a Xeon E5-1650 v3 processor clocked at 3.50 GHz.

In [29] there are the following results of measuring the speed of the cipher "Kalyna" using the following compilers: VC ++ 2015 (Microsoft Visual Studio 2015); gcc 7.3.0 (GCC); clang 3.7 (LLVM Compiler Infrastructure).

Since the results [28], [29] were presented in MB/s, in order to ease the comparison, they are also listed in cpb (number of cycles per encryption of one byte).

Table 7

Speed implementations of the "Kalyna"-128/128 cipher

Library [29]		Library [30]					
		VC++ 2015		gcc 5.2		clang 3.7	
MB/s	Cpb	MB/s	Cpb	MB/s	Cpb	MB/s	Cpb
128,22	20,2	179	19,5	236	14,8	206	16,9

In [30] the implementation of the cipher "Kalyna" using SIMD instructions SSE-128, AVX-256, AVX-512 is presented. Performance analysis was performed for the Intel Xeon Skylake-SP 2.0 GHz processor, the code is written in C++, the compilers are used from Microsoft Visual Studio 2019 (MSVC) and gcc 7.3.0 (GCC). To reduce the impact of CPU context switching, multiple encryption (100 million iterations) was performed. Cache-resistant implementations with step-by-step execution of cipher operations were evaluated (Table 8, Table 9, Table 10).

Table 8

Step-by-step implementations of the "Kalyna" cipher (SSE-128) [30]

Number of blocks	SSE-128			
	GCC, cpb		MSVC, cpb	
	ENC	DEC	ENC	DEC
1	84,25	107,13	48,75	57,75
2	50,31	77,88	31,75	44,44
4	37,94	61,47	24,00	35,88
8	-	-	-	-
16	-	-	-	-

Table 9

Step-by-step implementations of the "Kalyna" cipher (AVX-256) [30]

Number of blocks	AVX-256			
	GCC, cpb		MSVC, cpb	
	ENC	DEC	ENC	DEC
1	38,13	45,38	35,50	43,88
2	34,75	42,69	24,13	30,94
4	21,59	29,34	15,09	22,50
8	16,42	25,91	10,63	17,19
16	-	-	-	-

Table 10

Step-by-step implementations of the "Kalyna" cipher (AVX-512) [30]

Number of blocks	AVX-512			
	GCC, cpb		MSVC, cpb	
	ENC	DEC	ENC	DEC
1	52,38	74,00	57,25	78,63
2	28,31	43,38	30,00	47,50
4	18,13	24,69	19,72	25,13
8	11,08	16,64	11,73	18,25
16	8,32	15,14	8,78	15,55

From the presented results it follows that the use of AVX-256 technology for the implementation of the code "Kalyna" is justified provided that it is necessary to guarantee resistance to cache attacks. This is especially true for most processors that do not support AVX-512, especially since the transition to AVX-512 in this case does not give a significant increase in performance. SSE-128 technology is significantly inferior to the AVX-256 / AVX-512.

The article [31] describes the features of microcontrollers for the implementation of the cipher "Kalyna", develops the structure of the algorithm on the target platform and approaches to testing the algorithm. On the STM32G071RBT microcontroller, the speed of the algorithm was analyzed, with the size of the executable file 16000 bytes, and the following results were obtained:

- "Kalyna" encryption speed (128, 128) - 3225 bytes/s;
- "Kalyna" decryption speed (128, 128) - 3030 bytes/s;

- "Kalyna" encryption speed (128, 128) - 2693 bytes/s;
- "Kalyna" encryption speed (128, 128) - 2547 bytes/s.

THE PURPOSE OF THE ARTICLE

The aim of the article is to analyze the national standard "Kalyna" and compare it with international encryption algorithms, taking into account the length of the key, and features of the algorithm on different platforms and operating systems.

FORMULATION OF THE PROBLEM

The symmetric block transformation algorithm "Kalyna" is considered in the work. This algorithm was put into operation in 2014, but there is still insufficient information about its properties and the results of comparison with other algorithms in all modes of its operation. This creates difficulties in choosing the algorithm to use. Therefore, this paper analyzes its differences from other data encryption standards used both in Ukraine and in the world. The stability of the "Kalyna" algorithm was analyzed using a high-bit key (512 bits) and its speed was compared with other cryptographic protection algorithms. The influence of CPU and operating system performance on "Kalyna" algorithm performance is also analyzed.

RELEVANCE OF RESEARCH

The role of information technology and the use of computer technology is of importance today. Due to the global spread of computer networks, the issue of reliable information exchange has become relevant, as it must retain all its properties during the process of exchange, processing and storage. That is why one of the most important issues is the data protection in information and communication systems. Users of global and local networks need simple and powerful information security tools that can maintain their confidentiality, integrity and accessibility. Cryptographic protection fully meets these requirements. Modern encryption standards have been developed taking into account the specific features of the environment in which they are used. This raises the urgent question of analyzing modern algorithms with large keys, which are the most resistant to cryptanalysis, or those that have the highest performance and provide a high degree of security of information systems.

Today there is a need to provide real-time encryption of information. Therefore, to solve this problem, there is a need to develop encryption algorithms that would provide speed to implement it, as well as have a margin of resistance to attacks higher than a direct search of key options.

Mass introduction of electronic document management is accompanied by an increase in the use of cryptographic transformations to protect content. This encourages the creation and use of encryption algorithms that are easy to operate and with combinations of block and key sizes ranging from 128 bits to 512 bits.

FEATURES OF USING LARGE KEYS IN THE ALGORITHM "KALYNA"

The platform (Fig. 1) based on a 32-bit ARM MCU core-STM32G071RBT, a PC running a 64-bit Linux operating system (Ubuntu 20.04) with an Interl Core i7-1185G7@3.00GHz processor and a PC running a 64-bit operating system were used for testing Windows 10 with Interl Core I5 6300HQ@2.3GHz processor.

As it can be seen from the diagram below, the system provides communication with a personal computer by converting USB signals into UART telegrams. The firmware will be downloaded from KEIL uVisionIDE using the official ST-Link V2 debugger from STMicroelectronics.

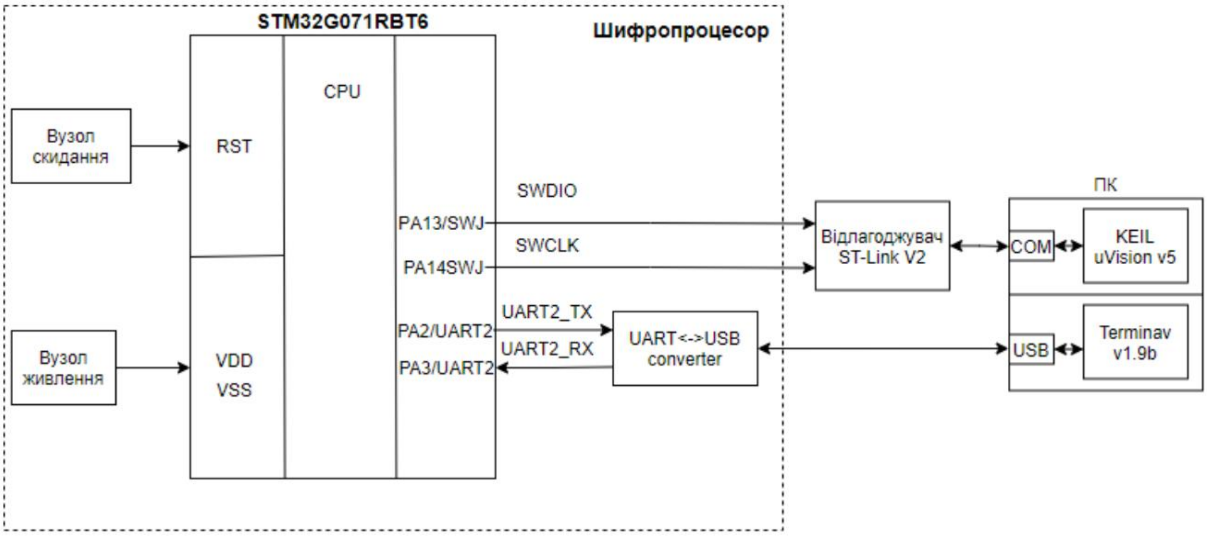

Fig. 1 Functional scheme of microcontroller cell

The procedure was performed for the "Kalyna" algorithm in different block/key configurations with an implemented MDS profile that uses a pre-computed table for multiplication and nonlinear substitution. This version focuses on maximum performance due to a significant increase in code size. The essence of this technique is to combine the operations of SubBytes, ShiftRows and MixColumns into one using pre-calculated tables.

The performance results are presented in megabits per second (Mb/s), see (Table 11).

When comparing the performance of "Kalyna" algorithm (128,128) was the fastest, which is obvious because it involves the use of a block and a key of the smallest value. And "Kalyna" (512, 512) is the slowest due to the large amount of data for processing, but provides the highest data protection (Table 5).

The comparison of processor performance is given in Table 12.

If you compare the data obtained after the tests and the data provided in the article of the developers [25], you can see a slight difference in measurements (Table 11). The main reason for the difference in results was the difference in processor performance, which is given in Table 12. The operating system has little effect on the test results of the software implementation of the block cipher "Kalyna", and therefore it can be ignored.

Testing can be considered correct, as the ratio of the speed of encryption algorithms is preserved.

As it can be seen from Table 11, MCU has the worst performance, but, in contrast to this shortcoming, there are advantages that will help find a place in embedded systems due to the rapid growth of this area, namely:

- Size - 25mm x 45mm;
- Power consumption - ~ 290 mW (at 50 ° C);
- Operating temperature range - from -40 to + 85 ° C;

Due to the described features, microcontrollers are becoming more popular and can compete with traditional software and hardware implementation methods.

Table 11

Comparison of the speed of software implementation of the block cipher "Kalyna"

Modifi-cation	Speed, Mb/s			
	Intel Core i5-4670@ 3.40GHz (Ubuntu 12.04) [25]	Intel Core i7-1185G7@ 3GHz (Ubuntu 20.04)	Intel Core i5-6300HQ@ 2.3GHz (Windows 10)	ARM MCU – STM32 G071RB T
(128,128)	2611.77	2987.4	1898.0	44.3
(128,256)	1779.52	2097.43	1375.29	32.28
(256,256)	2017.97	2588.13	1546.48	35.11
(256, 512)	1560.89	1922.83	1220.11	28.7
(512, 512)	1386.46	1787.14	1065.81	24.9

Table 12

Processor Performance Testing (Benchmark) [32]

Test	Intel Core i5-6300HQ 2.3GHz	Intel Core i5-4670 3.40GHz	Intel Core i7- 1185G7 3GHz
Integer Math, MOps/Sec	12,49	16,58	37,329
Floating Point Math, MOps/Sec	10,605	12,359	21,709
Find Prime Numbers, Million Primes/Sec	24	32	50
Random String Sorting, Thousand Strings/Sec	8	11	14
Data Encryption, Mb/s	1,300	1,278	6,109
Data Compression, Mb/s	62.0	76.6	107.8
Physics, Frames/Sec	385	413	838
Extended Instructions, Matrices/Sec	5,526M	6,365M	7,907M
Single Thread, MOps/Sec	1,791	2,137	2,923
Average CPU Mark	4678	5403	10920

CONCLUSION

The performance of the "Kalyna" block cipher is practically independent of the PC operating system. For a large key, 512-bit long, the average speed of "Kalyna" (including the processors involved) is about 1400 Mb/s.

The use of a specialized microcontroller as a cipher processor allows you to free the CPU from the tasks of cryptographic data protection. When using a microcontroller as a cipher processor, the performance of cryptographic data protection tools substantially lower when switching from PC in about 50 times. However, the advantage of the microcontroller is:

- Size - 25mm x 45mm;
- Power consumption - ~ 290 mW (at 50 ° C);
- Operating temperature range - from -40 to + 85 ° C;

Microcontroller test results of the speed of software implementation of the block cipher "Kalyna":

- "Kalyna" encryption speed (128, 128) is 44.3 Mb/s;
- "Kalyna" encryption speed (128,256) is 32.28 Mb/s;
- "Kalyna" encryption speed (256, 256) is 35.11 Mb/s;
- "Kalyna" encryption speed (256,512) is 28.7 Mb/s;

· "Kalyna" encryption speed (512,512) is 24.9 Mb/s;

To increase productivity, it is worth considering the option of implementing a cryptoprocessor on FPGA.

REFERENCES

[1] Liu, A., Ming, H., and Dharmalingam, B. (2021). "Automatic Verification of SSL/TLS Certificate for IoT Applications", *IEEE Access*, vol. 9, pp. 27038–27050, doi: 10.1109/ACCESS.2019.2961918.

[2] Beaulieu, N. C. and Hu, J. (2006). "A Noise Reduction Amplify-and-Forward Protocol for Distributed Diversity", *IEEE Communications Letters*, vol. 10, no. 11, pp. 787–789, doi: 10.1109/LCOMM.2006.060849.

[3] Informatsiini tekhnolohii. Zakhyst kryptohrafichnykh danykh. Alhorytm symetrychnoho blochnoho peretvorennia, DSTU 7624: 2014, 2015.

[4] DSTU GOST 28147:2009. Systema obrobky informatsii. Zakhyst kryptohrafichnyi. Alhorytm kryptohrafichnoho peretvorennia (GOST 28147-89).

[5] Rhee, M. Y. (2009). "Advanced Encryption Standard and Elliptic Curve Cryptosystems", *Mobile Communication Systems and Security*, vol. 4, no. 4, pp. 341–386, doi: 10.1002/9780470823392.ch9.

[6] Tsunoo, Y., Saito, T. and Suzaki, T. (2007). "A Distinguishing Attack on a Fast Software-Implemented RC4-Like Stream Cipher", *IEEE Transactions on Information Theory*, vol. 53, no. 9, pp. 3250–3255, doi: 10.1109/TIT.2007.903136.

[7] Kim, S., Goo, Y., Kim, M. and Choi, S. (2015). "A method for service identification of SSL/TLS encrypted traffic with the relation of session ID and Server IP", *Asia-Pacific Network Operations and Management Symposium*, vol. 17, pp. 487–490, doi: 10.1109/APNOMS.2015.7275373.

[8] Gong, G and Golomb, S. W. (1999). "Transform domain analysis of DES", *IEEE Transactions on Information Theory*, vol. 45, no. 6, pp. 2065–2073, doi: 10.1109/18.782138.

[9] Verkhovna Rada Ukrainy. (2017). *Shchodo bezpeky rynku platizhnykh kartok v Ukraini*. [online] Available: https://zakon.rada.gov.ua/laws/show/v6378500-06#Text (Accessed: 3 October 2021).

[10] Si, H., Sun, C., Chen, B. and Qiao, H. (2019). "Analysis of Socket Communication Technology Based on Machine Learning Algorithms Under TCP/IP Protocol in Network Laboratory System", *IEEE Access*, vol. 7, pp. 80453–80464, doi: 10.1109/ACCESS.2019.2923052.

[11] Phan, R. and Siddiqi, M. (2006). "A Framework for Describing Block Cipher Cryptanalysis," *IEEE Transactions on Computers*, vol. 55, no. 11, pp. 1402–1409, doi: 10.1109/TC.2006.169.

[12] Uriadovyi portal. (2019). *Derzhspetszviazku vprovadzhuie novi standarty kryptohrafichnoho zakhystu informatsii*. [online] Available: http://old.kmu.gov.ua/kmu/control/uk/publish/article?art_id=247952015&cat_id=248817973 (Accessed: 3 October 2021).

[13] Ma, S. and Guan, J. (2020). "Improved Key Recovery Attacks on Simplified Version of K2 Stream Cipher", *The Computer Journal*, vol. 64, no. 8, pp. 1253–1263, doi: 10.1093/comjnl/bxaa154.

[14] Cassell, B., Szepesi, T., Wong, B. and Brecht, T. (2017). "Nessie: A Decoupled, Client-Driven Key-Value Store Using RDMA", *IEEE Transactions on Parallel and Distributed Systems*, vol. 28, no. 12, pp. 3537–3552, doi: 10.1109/TPDS.2017.2729545.

[15] Zhu, Y., Zhang H. and Bao, Y. (2015). "Novel Self-Body-Biasing and Statistical Design for Near-Threshold Circuits With Ultra Energy-Efficient AES as Case Study," *IEEE Transactions on Very Large Scale Integration Systems*, vol. 23, no. 8, pp. 1390–1401, doi: 10.1109/TVLSI.2014.2342932.

[16] Lee, H., Juvekar, C. S., Kwong, J. and Chandrakasan, A. P. (2017). "A Nonvolatile Flip-Flop-Enabled Cryptographic Wireless Authentication Tag With Per-Query Key Update and Power-Glitch Attack Countermeasures", *IEEE Journal of Solid-State Circuits*, vol. 52, no. 1, pp. 272–283, Jan. 2017, doi: 10.1109/JSSC.2016.2611678.

[17] Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy. (2014). *Oholoshennia pro provedennia vidkrytoho konkursu symetrychnykh blokovykh kryptohrafichnykh alhorytmiv*. [online] Available: https://cip.gov.ua/ua?artid=48383 (Accessed: 3 October 2021).

[18] Horbenko, I. D., Totskyi, O. S. and Kazmina, S. V. (2007). "Perspektyvnyi blokovyi shyfr Kalyna – osnovni polozhennia ta spetsyfikatsiia", *Prykladna radioelektronika*, vol. 2, no. 1, pp. 195–208. [online] Available: http://www.anpre.org.ua/?q=pre20072 (Accessed: 3 October 2021).

[19] Oliynykov, R., Gorbenko, I. and Ruzhentsev, V. (2010). "Results of Ukrainian national public cryptographic competition", *Tatrata Mountains Mathematical Publications*, vol. 5, no. 3, pp. 99–113, doi: 10.2478/v10127-010-0033-6.

[20] Oliynykov, R., Gorbenko, I., Kazymyrov, O., Ruzhentsev, V., Kuznetsov, O., Gorbenko, Y., Dyrda, O., Pushkaryov, A., Mordvinov, R., Kaidalov, D. (2015). "A New Encryption Standard of Ukraine: The Kalyna Block Cipher", *IACR Cryptol*, 97(2), pp.124–141. [online] Available: https://eprint.iacr.org/20 15/650.pdf (Accessed: 3 October 2021).

[21] Zhang, Z., Huang, S., Liu, F. and Mei, S. (2020). "Pattern Analysis of Topological Attacks in Cyber-Physical Power Systems Cascading Outages", *IEEE*, vol. 8, pp. 4257–4267, doi: 10.1109/ACCESS.2020.3006555.

[22] ISO/IEC/IEEE International Standard. (2020). "Systems and software engineering, Software life cycle processes, Part 2: Relation and mapping between ISO/IEC/IEEE 12207:2017 and ISO/IEC 12207:2008", *ISO/IEC/IEEE 1207-2:2020(E)*, vol. 1, no. 2, pp. 1–278, doi: 10.1109/IEEESTD.2020.9238529.

[23] Wikipedia. (2013). *S-blok*. [online] Available: https://ru. wikipedia. org/ wiki/S%D0%B1%D0%BB%D0%BE%D0% BA (%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC% D0%B0%D1%82%D0%B8%D0%BA%D0%B0) (Accessed: 3 October 2021).

[24] Iprop. (2012). *MDV-matrytsia*. [online] Available: https:// ipropua. com / inv/ pdf/f8gte9mbgte9m-claim.pdf (Accessed: 3 October 2021).

[25] Oliinykov, R., Horbenko, I., Kazymyrov, O., Ruzhentsev, V. and Horbenko, Y. (2015). "Pryntsypy pobudovy i osnovni vlastyvosti novoho natsionalnoho standartu blokovoho shyfruania Ukrainy", *Information security, 17(2)*, pp. 142–157, doi: 10.18372/2410-7840.17.8789

[26] Nazeh, A., Wahid, M., Ali, A. and Esparham, B. (2018). "A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention", *Journal of Computer Science Applications and Information Technology*, 3(2), pp: 1–7, doi: 10.15226/2474-9257/3/2/00132

[27] Li, R., Jin, C., Fan, R. and Ashur, T. (2019). "Improved Integral Distinguishers on Compression Function of GOST R Hash Function", *The Computer Journal*, vol. 62, no. 4, pp. 535–544, doi: 10.1093/comjnl/bxy123.

[28] Kovtun, V. and Okhrimenko, A. (2017). *Features of construction of a cross-platform library of cryptographic primitives "Cipher+" v2*. [online] Available: https://cipher.com.ua/media/%D0%9F%D1%80% D0%BE%D0%B4%D1%80%2Bv2.1/Presentation_Cipher_ Plus.pdf (Accessed: 3 October 2021).

[29] Cppcrypto. (2017). *cppcrypto library encryption performance*. [online] Available: http://cppcrypto.sourceforge.net/true&queryText=cppcrypto (Accessed: 3 October 2021).

[30] Sovyn, Y., Khoma, V., Nakonechny, Y., Stakhiv, Y. (2019). "Effective implementation and performance comparison of «Kalyna» and GOST 28147-89 ciphers witch the use of vector extensions SSE, AVX and AVX-512", *Ukrainian Information Security Research Journal*, vol. 21, no. 4, pp. 207–223, doi: 1018372/2410-7840.21.14266

[31] Bilenko, V., Hlukhov. V. (2021). "Implementation Kalyna Algorithm in Microcontroller", *ACPS*. vol. 6, no. 1, pp. 8–13, doi: 10.23939/acps2021.01.008

[32] Kok, C. H., Ong, S. E. (2020). "CPU Utilization Micro-Benchmarking for RealTime Workload Modeling". *IEEE*, 29(1), pp. 1–2, doi: 10.1109/ATS49688.2020.9301524.

Taras Zaiats is a sixth-year student of Computer Engineering Department at Lviv Polytechnic National University. His is interested in topics related to embedded system engineering such as Internet of Things (IoT), Applied Automation Systems, cryptography and steganography.

Volodymyr Bilenko is a fifth-year student of Computer Engineering Department at Lviv Polytechnic National University. He was involved in the development of systems for military purposes with encryption topics. His is interested in topics related to embedded system engineering such as Internet of Things (IoT), Robotics and Applied Automation Systems.

Valerii Hlukhov is a professor of the Department of Computer Engineering Departmentat at Lviv Polytechnic National University, Ukraine. He graduated from Lviv Polytechnic Institute with the engineer degree in Computer Engineering in 1977. In 1991 he obtained his Ph.D. at the Institute of Modeling Problems in Power Engineering of the National Academy of Science of Ukraine. He was recognized for his outstanding contributions into special-purpose computer systems design as a Senior Scientific Researcher in 1995. He was awarded the academic degrees of Doctor of Technical Sciences in 2013 at Lviv Polytechnic National University. He became a Professor of Computer Engineering in 2014. He has scientific, academic and hands-on experience in the field of computer systems research and design proven contribution into IP Cores design methodology and high-performance reconfigurable computer systems design methodology. He is an experienced reseracher in computer data protection, including cryptographic algorithms, cryptographic processors design and implementation. Prof. Hlukhov is an author of more than 100 scientific papers, patents and monographs.