UDC 004.056.55

TESTING THE SPEED OF MODERN STREAM CIPHERS

Ivan Gorbenko[1], Yurii Gorbenko[1], Vladyslav Tymchenko[1], Olena Kachko[2]

[1] V. N. Karazin Kharkiv National University, 6 Svobody Sq., Kharkiv, 61022, Ukraine
gorbenkoi@iit.kharkov.ua, gorbenkou@iit.kharkov.ua, tvlad.tyma@gmail.com

[2] Kharkiv national university of Radio Electronics, 14 Nauky Av., Kharkiv, 61000, Ukraine
iit@iit.com

Reviewer: Vyacheslav Kalashnikov, Doctor of Sciences (Physics and Mathematics), Full Prof., Department of Systems and Industrial Engineering, Campus Monterrey, Monterrey, 64849, Mexico.
kalash@itesm.mx

Received on September 2018

Abstract. *The paper is a continuation of numerous studies of a candidate for encryption national standard of Ukraine, the Strumok new symmetric stream cipher. The result of a study is compare the most famous algorithms of stream cipher, which were presented at various contests, such as eSTREAM, NESSIE and the AES symmetric block cipher in mode of stream about usage CPU time for transformation of one octet data*.

Keywords: *stream cipher; encryption; cycles per byte; synchronous keystream generator; pseudorandom sequence.*

1 Introduction

Strumok is the stream symmetric cipher that presented as a candidate for encryption national standard of Ukraine [1-4]. The cipher designed by a group of scientists in 2015 and it was improve repeatedly. The Strumok has a simple scheme that focuses on a 64-bit computing platform, that enable its become the most fast (over 10 Gbit per sec) [1-4].

The Strumok stream cipher is based on a secret internal state that consist of eighteen 64-bit blocks: 16 blocks of the linear feedback shift register (LFSR) and two blocks of the finite-state machine (FSM). As input data using a secret key of size L_K=256 or 512 bit and an initial vector of size L_{IV}=256 bit.

The closest prototype to the Strumok stream cipher is the SNOW 2.0 cryptographic algorithm that focuses on 32-bit computing systems [5]. It is based on the classical scheme of additive generator [5,6], but unlike the SNOW 2.0 algorithm in the Strumok generator uses an increased internal state with a shift register over 64-bit blocks. Therefore, in one cycle, 64-bit computing systems achieve a higher speed of the formation keystream.

The purpose of this work is obtaining additional results of compare studies speed the Strumok stream cipher and famous cryptographic primitives about usage CPU time for transformation of one octet data at various stages of keystream generation. By comparison, also attached the symmetric block ciphers, such as AES [7,8] and Kalyna [9,10] with usages in stream mode.

2 General Description

AES

Advanced Encryption Standard (AES) is a symmetric block cipher that has a fixed block size of 128 bit, and a key length can take value L_k=128,192 or 256 bit. For a key lengths 128 or 256 bit, the algorithm has 10/14 rounds, according. In 2002, it was declared the encryption standard of United States [7] and later its standardized at the international level in [8].

HC

HC is a stream cipher that designed by Hongjun Wu cryptographer and was first published in 2004. HC-128 was presented at the eSTREAM contest [6], which aimed to create European standards for stream encryption systems.

Rabbit

Rabbit is a high-performance stream encryption algorithm that was first presented at the 10th symposium FSE in 2003. In 2005, it was submitted at the eSTREAM contest [6]. The cipher uses a 128-bit key and a 64-bit initialization vector. It standardized internationally in [5].

Salsa20

Salsa20 is a transformation stream system that developed by Daniel J. Bernstein. The algorithm was presented at the eSTREAM contest [6], where it became the winner contest in the first profile (the stream ciphers for software use with high bandwidth).

SNOW 2.0

SNOW 2.0 is a symmetric stream cipher that developed by Thomas Johansson and Patrik Ekdahl, it's also one of the stream ciphers selected for ISO/IEC 18033-4 [5]. The key size can take 128 or 256 bit, and a 128-bit initialization vector.

Sosemanuk

Sosemank is a stream cipher, developed by a group of French scientists in 2004. In 2008, it became one of the finalists eSTREAM project in the first profile [6]. It's a key length varies between 128 and 256 bit, and use a 128-bit initialization vector.

Trivium

Trivium is a synchronous stream cipher that focuses primarily on hardware implementation, and reasonably efficient software implementation. The cipher was presented at the eSTREAM project and has been selected as part portfolio for low area hardware ciphers [6]. The authors of the cipher are Christophe De Canniere and Bart Prenel. This stream cipher can generate up to 2^{64} bits of output sequence with an 80-bit key and an 80-bit initialization vector. Standardized also as a cipher of lightweight cryptography [11].

3 Software performance of Strumok

The stream encryption of long sequences has the potential advantage over block cryptographic transformations, which is an important benchmark for many applications. Important benchmarks of symmetric stream ciphers are also the speed of encrypting short packages, as well as the time of initialization/generation of key parameters (see in Tables 1-10).

Table 1 – The speed of encryption 1Gb data (*Intel Core i3-5005U 2ГГц*)

Names Of Algorithm	***Speed***	
	Mbps	***Cycles per byte***
Strumok-256	5542	2.88
Strumok-512	5576	2.86
AES-128	1583	10.08
AES-256	1128	14.14
HC-128	7164	2.23
HC-256	2701	5.91
Rabbit	2186	7.3
Salsa20	1598	9.98
SNOW 2.0-128	5177	3.08
SNOW 2.0-256	5095	3.13
Sosemanuk	2925	5.46
Trivium	2387	6.69

To study the performance benchmarks used two computers:

- with an Intel® Core i3-5005U 2 GHz processor (*the memory cache: 128 KB first level and 256 KB second level*), 12 GB of DDR3 1600 MHz RAM and OS Windows® 8.1;

- Intel® Core i9-7980XE 2.60 GHz processor (*the memory cache: 18×32 KB first level and 1024 KB second level*), 64 GB of DDR4 2133 MHz RAM and OS Windows® 10 Pro.

Table 2 – The speed of encryption 1Gb data *(Intel Core i9-7980XE 2.60GHz)*

Names Of Algorithm	***Speed***	
	Mbps	***Cycles per byte***
Strumok-256	10911	1.90
Strumok-512	10850	1.91
AES-128	3228	6.42
AES-256	2295	9.03
HC-128	14676	1.41
HC-256	6286	3.30
Rabbit	4636	4.47
Salsa20	3502	5.92
SNOW 2.0-128	10425	1.99
SNOW 2.0-256	10470	1.98
Sosemanuk	6329	3.28
Trivium	4954	4.19

Table 3 – The results of encryption 50 packages by 1500 bytes *(Intel Core i3-5005U 2ГГц)*

Names Of Algorithm	***Speed***		
	Mbps	***Cycles per byte***	***Cycles per package***
Strumok-256	4580	3.49	5231
Strumok-512	4545	3.50	5250
AES-128	1578	10.13	15194
AES-256	1119	14.25	21368
HC-128	1310	12.18	18275
HC-256	239	66.57	99861
Rabbit	2105	7.59	11378
Salsa20	1578	10.11	15161
SNOW 2.0-128	4687	3.42	5127
SNOW 2.0-256	4580	3.48	5218
Sosemanuk	2830	5.65	8481
Trivium	2197	7.25	10876

Table 4 – The results of encryption 50 packages by 1500 bytes *(Intel Core i9-7980XE 2.60GHz)*

Names Of Algorithm	***Speed***		
	Mbps	***Cycles per byte***	***Cycles per package***
Strumok-256	9231	2.26	3386
Strumok-512	9091	2.26	3387
AES-128	3191	6.47	9710
AES-256	2299	9.03	13545
HC-128	2871	7.21	10819

Continuation of Table 4

HC-256	543	38.21	57318
Rabbit	4255	4.86	7287
Salsa20	3448	6.01	9008
SNOW 2.0-128	9375	2.20	3303
SNOW 2.0-256	9524	2.18	3274
Sosemanuk	7595	2.74	4108
Trivium	4511	4.59	6887

The research was conducted in accordance with the methodology adopted in [6], i.e., the following criteria were used:

- the speed of encryption of long streams;
- the speed of encryption short packages;
- the speed of initialization and key parameters generation.

The results obtained of encryption a long stream (a long 1GB) which carried out for each algorithm on a key, see in Tables 1, 2. From the data in tables, it follows that stream ciphers have an undeniable advantage over blocks when encryption long streams. Among the stream algorithms, HC-128, Strumok-256 and Strumok-512 are the fastest. It should be noted that Intel® Core i9-7980XE 2.60 GHz computing system achieves very high encryption speeds (*over 10 Gbit per sec*), which points to the prospect of using stream ciphers in modern telecommunication systems. At the same time, Strumok-512 is not inferior to the speed of the Strumok-256 version, although it has a much higher supply of stability.

Table 5 – The results of encryption 120 packages by 576 bytes *(Intel Core i3-5005U 2ГГц)*

Names Of Algorithm	***Speed***		
	Mbps	***Cycles per byte***	***Cycles per package***
Strumok-256	3477	4.59	2644
Strumok-512	3456	4.61	5250
AES-128	1562	10.20	5876
AES-256	1103	14.47	21368
HC-128	570	27.95	16099
HC-256	97	164.5	94753
Rabbit	1953	8.15	4696
Salsa20	1612	9.91	5707
SNOW 2.0-128	4189	3.80	2191
SNOW 2.0-256	3711	4.31	2484
Sosemanuk	2850	5.58	3217
Trivium	1920	8.33	4798

Table 6 – The results of encryption 120 packages by 576 bytes *(Intel Core i9-7980XE 2.60GHz)*

Names Of Algorithm	***Speed***		
	Mbps	***Cycles per byte***	***Cycles per package***
Strumok-256	6999	2.96	1702
Strumok-512	7089	2.94	1695

Continuation of Table 6

AES-128	3196	6.48	3732
AES-256	2257	9.18	5288
HC-128	1254	16.53	9520
HC-256	220	94.24	54284
Rabbit	4036	5.13	2957
Salsa20	3392	6.08	3503
SNOW 2.0-128	8378	2.44	1408
SNOW 2.0-256	8507	2.42	1396
Sosemanuk	6356	3.33	1919
Trivium	3921	5.30	3054

By the second criterion, the speed of encryption short packages of different lengths was measured. Each function call includes a separate setup of the initialization vector *IV*. The package lengths (40, 576, and 1500 bytes) were selected to be representative of telecommunication traffic (see Table 3-8) [6].

Analyses the results of the studies presented in Tables 3–8, it should be noted that the advantage the speed of encryption stream algorithms is maintained for packages of lengths hundred or more bytes. For very short packages, the time of internal state initialization begins to play a significant part of the stream algorithms, as expected, are starting to lose. As regards comparing the speed of stream algorithms, the advantage of the SNOW 2.0 and Strumok generators should be noted.

Table 7 – The results of encryption 350 packages by 40 bytes *(Intel Core i3-5005U 2ГГц)*

Names Of Algorithm	***Speed***		
	Mbps	***Cycles per byte***	***Cycles per package***
Strumok-256	543	29.32	1173
Strumok-512	528	30.21	1209
AES-128	1027	15.63	625
AES-256	713	22.38	895
HC-128	42	378.39	15135
HC-256	7	2296.64	91866
Rabbit	682	23.39	936
Salsa20	1009	15.7	628
SNOW 2.0-128	888	17.83	713
SNOW 2.0-256	957	16.67	667
Sosemanuk	756	21.08	843
Trivium	493	32.38	1295

Table 8 – The results of encryption 350 packages by 40 bytes *(Intel Core i9-7980XE 2.60GHz)*

Names Of Algorithm	***Speed***		
	Mbps	***Cycles per byte***	***Cycles per package***
Strumok-256	1120	18.45	738
Strumok-512	1131	18.23	729

Continuation of Table 8

AES-128	2196	9.48	379
AES-256	1600	12.87	515
HC-128	94	219.82	8793
HC-256	16	1326.64	53065
Rabbit	1623	13.04	522
Salsa20	2153	9.70	388
SNOW 2.0-128	2154	9.67	387
SNOW 2.0-256	2154	9.69	388
Sosemanuk	1697	12.28	491
Trivium	1028	20.14	806

The criterion of initialization and generation key parameters separately includes parameters of the establishment of the key and the initialization vector. These two parameters are least critical for displaying the speed of encryption packages, since they are disproportionality small compared to the process of create or update a key. The results benchmarks are shown in the Tables 9, 10.

According to the results of the studies presented in Table 9, 10, the advantage of the Salsa20 cipher should be noted. The HC algorithm, which showed good results the speed, it has the shortest time of installation a key, but the time it takes to initialize the vector is largest. The Strumok algorithm has average values for this criterion.

Table 9 – The speed OF the installation keys and the initialization vectors
(Intel Core i3-5005U 2ГГц)

Names Of Algorithm	**KEY, Cycles per installation**	**IV, Cycles per installation**
Strumok-256	16.07	806.52
Strumok-512	16.16	731.24
AES-128	266.35	0.32
AES-256	423.39	0.32
HC-128	8.07	14701.36
HC-256	133.07	91748.16
Rabbit	475.35	442.69
Salsa20	12.08	1.59
SNOW 2.0-128	16.09	403.21
SNOW 2.0-256	30.21	410.64
Sosemanuk	530.39	496.41
Trivium	22.35	1006.43

Table 10 – The speed OF the installation keys and the initialization vectors
(Intel Core i9-7980XE 2.60GHz)

Names Of Algorithm	**KEY, Cycles per installation**	**IV, Cycles per installation**
Strumok-256	10.24	470.32
Strumok-512	10.24	471.67
AES-128	152.02	0.15

Continuation of Table 10

AES-256	242.14	0.16
HC-128	7.08	8640.58
HC-256	79.44	52514.03
Rabbit	285.73	275.32
Salsa 20	7.69	0.98
SNOW 2.0-128	10.38	238.89
SNOW 2.0-256	19.30	233.66
Sosemanuk	339.99	317.19
Trivium	14.11	617.50

4 Conclusions

The symmetric stream ciphers play an important role in the processes cryptographic protection of information. They have high the speed of cryptographic transformation, especially for the long packages, and are most successfully used when encryption large amounts of input data.

The results obtained of comparative studies have shown that the stream algorithms significantly exceed block ciphers by the speed of encryption the long packages. Among the stream algorithms, the Strumok generator, whose structure is targeted at applications in modern 64-bit computing system, has the advantage of giving it the highest values. In particular, the Intel® Core i9-7980XE 2.60 GHz and OS Windows® 10 Pro have received 14 – 15 Gbps encryption speeds.

When encryption short packages, the computational efficiency of the stream ciphers decreases, and for package lengths of 40 bytes block ciphers become faster. When comparing the stream algorithms, the Strumok generator that stably shows a high encryption speeds, has the advantage.

The study of the initialization time of cryptographic algorithms didn't show the advantage of block or stream algorithms. And although with the increase in the length of the data being processed, the initialization time plays a very small part in the process of encryption, this parameter should also to be given attention. In particular, according to our research, the greatest advantage over the initialization time is the Salsa20 cipher.

Generalizing the results should be noted the Strumok keystream generator, which in most cases showed better results. When implemented on a 64-bit computing platform, it provides enormous the speed of encryption and can be recommended for practical application in the modern information and telecommunication systems.

References

[1] Kuznetsov O., Lutsenko M., Ivanenko D. Strumok stream cipher: Specification and basic properties. 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T). Kharkiv, 2016. pp. 59–62.

[2] The research of modern stream ciphers / Gorbenko I., Kuznetsov A., Lutsenko M., Ivanenko D. 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T). Kharkov, 2017. pp. 207–210.

[3] Strumok keystream generator / Gorbenko I. and etc. 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). 2018. pp. 294–299.

[4] Kuznetsov A., Frolenko V., Eremin E., Zavgorodnia O. Research of cross-platform stream symmetric ciphers implementation. 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). Kyiv, 2018. pp. 300–305.

[5] ISO/IEC 18033-4:2011. Information Technology-Security Techniques-Encryption Algorithms-Part 4: Stream ciphers. URL: http://www.iso.org/iso/home/store/catalogue_ics/ catalogue_detail_ics.htm?csnumber=54532 [Dec., 2012].

[6] The eSTREAM Project. URL: http://www.ecrypt.eu.org/

[7] FIPS-197: Advanced Encryption Standard (AES). NIST, 2001. URL: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[8] ISO/IEC 18033-3:2010. Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers. URL: https://www.iso.org/standard/54531.html

[9] A New Encryption Standard of Ukraine: The Kalyna Block Cipher. URL: https://eprint.iacr.org/2015/650.pdf

[10] DSTU 7624:2014. Information technologies. Cryptographic Data Security. Symmetric block transformation algorithm. URL: http://shop.uas.org.ua/ua/catalogsearch/result/?q=7624 (in Ukrainian).

[11] ISO/IEC 29192-3:2012. Information technology-Security techniques-Lightweight cryptography-Part 3: Stream ciphers. URL: https://www.iso.org/standard/56426.html

Рецензент: В'ячеслав Калашников, д.ф.-м.н., проф., Технологический університет Монтеррея, пр. Еухеніо Гарса Сада 2501, Монтеррей, 64849, Мексика. E-mail: kalash@itesm.mx

Надійшло: Вересень 2018.

Автори:

Іван Горбенко, д.т.н., проф., академік Академії наук прикладної радіоелектроніки, Харківський національний університет ім. В.Н. Каразіна, майдан Свободи 6, м. Харків, 61022, Україна. E-mail: gorbenkoi@iit.kharkov.ua

Юрій Горбенко, к.т.н, Харківський національний університет ім. В.Н. Каразіна, майдан Свободи 6, м. Харків, 61022, Україна. E-mail: gorbenkou@iit.kharkov.ua

Владислав Тімченко, студент факультету комп'ютерних наук, Харківський національний університет ім. В.Н. Каразіна, майдан Свободи 6, м. Харків, 61022, Україна. E-mail: tvlad.tyma@gmail.com

Олена Качко, к.т.н., проф., Харківський національний університет радіоелектроніки (ХНУРЕ), м. Харків, 61000, Україна. E-mail: iit@iit.com.ua

Дослідження швидкості сучасних потокових шифрів.

Анотація. Ця стаття є продовженням численних досліджень кандидата на національний стандарт шифрування України, нового алгоритму симетричного потокового шифрування «Струмок». Результатом дослідження є порівняння найвідоміших алгоритмів потокового шифрування, які були представлені на різних конкурсах, таких як eSTREAM, NESSIE. До порівняння також долучений симетричний блоковий шифр AES в потокових режимах застосування. Оцінювалася складність реалізації алгоритмів за показниками кількості циклів центрального процесора для перетворення одного октету даних.

Ключові слова: потоковий шифр; шифрування; цикли на байт; синхронний генератор ключового потоку; псевдовипадкова послідовність.

Рецензент: Вячеслав Калашников, д.т.н., проф., Технологический университет Монтеррея, пр. Еухенио Гарса Сада 2501, Монтеррей, 64849, Мексика. E-mail: kalash@itesm.mx

Поступила: Сентябрь 2018.

Авторы:

Иван Горбенко, д.т.н., проф., Академик Академии наук прикладной радиоэлектроники, Харьковский национальный университет имени В.Н. Каразина, пл. Свободы 6, г. Харьков, 61022, Украина. E-mail: gorbenkoi@iit.kharkov.ua

Юрий Горбенко, к.т.н. Харьковский национальный университет имени В.Н. Каразина, пл. Свободы 6, г. Харьков, 61022, Украина. E-mail: gorbenkou@iit.kharkov.ua

Владислав Тимченко, студент факультета компьютерных наук, Харьковский национальный университет имени В.Н. Каразина, пл. Свободы 6, г. Харьков 61022, Украина. E-mail: tvlad.tyma@gmail.com

Елена Качко, к.т.н., проф., Харьковский национальный университет радиоэлектроники (ХНУРЭ), г. Харьков, 61000, Украина. E-mail: iit@iit.com.ua

Исследование скорости современных поточных шифров.

Аннотация. Эта статья является продолжением многочисленных исследований кандидата на национальный стандарт шифрования Украины, нового алгоритма симметричного поточного шифрования «Струмок». Результатом исследования является сравнение наиболее известных алгоритмов потокового шифрования, которые были представлены на различных конкурсах, таких как eSTREAM, NESSIE. В сравнение также включен симметричный блочный шифр AES в потоковых режимах применения. Оценивалась сложность реализации алгоритмов по показателям количества циклов центрального процессора для преобразования одного октета данных.

Ключевые слова: потоковый шифр; шифрование; циклы на байт; синхронный генератор ключевого потока; псевдослучайная последовательность.