Analysis of block encryption algorithms being used in devices with restricted amount of technological possibilities

Larissa Cherckesova^{1,}, Olga Safaryan¹, Pavel Razumov¹, Dmitry Medvedev², Veronica Kravchenko¹, Yuriy Ivanov³*

¹Don state technical University, Rostov-on-Don, 1, Gagarin square, Russia

²Don state technical University, Shakhty, Rostov region, 147, Shevchenko str., Russia

³Southern Federal University Taganrog, Taganrog, 44, per. Nekrasovsky, Rostov region, Russia

Abstract. This report is devoted to the comparative analysis of the lightweight NASH block encryption algorithm and the algorithm presented by USA National Security Agency in 2013 – SPECK. Their detailed description is given, the analysis is made. The task of the study is to investigate and analyze cryptographic encryption algorithms used in devices with limited capabilities such as microcontrollers. The study of lightweight encryption algorithms and their application for cybersecurity tasks is necessary to create the latest cryptographic systems aimed at preventing various types of attacks. The study revealed that the NASH block encryption algorithm showed more optimized performance, since the number of rounds of cipher execution is less than that Speck algorithm, which provides greater stability of algorithm with least number of executable rounds.

1 Introduction

The modern world is crowded of various household devices, sensors, recognition mechanisms, intelligent systems and other amenities that are actively involved in the life of the modern society and a specific person.

Every minute people are interacting with automated systems; manage their lives with the help of devices that operate by microcontrollers. In addition, low cost and easy accessibility contributes to wide distribution of micro-controllers market in industrial systems, control systems, as well as in household appliances of the mass-market segment.

Due to the spreading of information technologies in society, their software and hardware complexity increases; as well as the implementation of complex cryptographic transformations, using in those devices, which in the modernized – the world of global cyber wars, viruses and the hunting for information – is actual and very important. Thus, the CIA Director David Petraeus said that the most detailed dossier on any person could be compiled by obtaining data from household appliances connected to the Internet.

Based on the need to protect information, it is possible to implement standard encryption methods on microcontrollers, but this method does not provide the necessary encryption

* Corresponding author: chia2002@inbox.ru

speed. There are so-called "lightweight" encryption algorithms, in which the term "lightweight" does not mean "simple", but rather "low-resource", which more exactly and accurately reflects the essence of this technology.

The urgency of this methodology is due to the conditions of devices functioning, rigid financial limitations, as well as significant restrictions on the memory resources used, computing power, electric feed (supply) and more.

Thus, there are limitations on the energy consumption of the cryptographic algorithms implementation, which is provided by dimension of program code, size of random access memory RAM and the time spent on software execution.

One of the most effective among these kind of cryptographic systems is the SPECK and SIMON algorithms. They developed by NSA (USA) and published in June 2013 shortly before the disclosure of Snowden. This history seriously undermined the reputation of NSA in cryptography development, as its documents have demonstrated that NSA experts weakened consciously the applied cryptographic algorithms. Moreover, on the discussion of ISO meetings, the representatives of USA security refused to motivate the selected constants for matrix permutation algorithms.

All this resulted in the reason why these algorithms were rejected from the official application in the cryptosystems.

These algorithms reflect the idea of an encryption algorithm when a large number of simple transformations are performed. This idea was expressed in letters of the 50-s by Nobel Laureate in Economics John Nash from the NSA.

The purpose of this investigation is comparative analysis of lightweight block encryption algorithm NASH, named after John Nash, and the algorithm presented by the US National Security Agency in 2013 year – SPECK.

2 Scheme of Nash Algorithm

Let us represent the encryption algorithm in the following way. First of all, we need to break the text into half – blocks of bits. In turn, each block is encrypted one after the other rounds on a sequence of round keys that are calculated from the master key by the algorithm of "key extension". Thus, the block of data is forming, which breaks later into two half – blocks – left and right, by bits each.

Further, on round the transformations, caused by the scheme of the encryption round, demonstrated in the figure 1.

Fig. 1. Scheme of the round of encryption.

For round, the equations for the data block encryption (enciphering) are as follows:

As for the last round of block encryption, it is half – blocks and do not change places.

Let us consider in more detail the features of the rounds transformation. The size of the half – block is n , where $n = 16$ or $n = 32$. The block size is 32 or 64 bits, respectively. Moreover, it is proposed also to use the block size of 64 or 128 bits.

Let us note, that in this algorithm there is function of mixing with the round key : M_i – function of adding of two integers by modulo 2^n .

The next stage is shift control functions. It is necessary to interpret the half – block as the values of the Boolean function of n variables. At the output of the algorithm, the first output bit acquires the value of this function on the set of bits from $L(i)$, ..., $R(i)$, where $i=1,..., n$. Alternatively, using equivalent designation as a value M_i , where the numbering of bits from half – block 0 to $n-1$ is applicable.

The equation should be interpreted as vector of Boolean function values of n variables. In this case, the second output bit acquires the value of this function on the set of bits from of the view $2i-1$, where $i=1,..., n$.

Let us consider also the function of round keys generating, the scheme of which is shown in the figure 2.

Let us note, that K_i , where the value of constant is defined as follows. First, the key is divided into n blocks of length n , and the remaining blocks are defined as the values of the square root of the prime numbers (such as root 2, ...). These blocks correspond.

Fig. 2. Scheme of the key generation round.

Further, in the calculation it is necessary to take this constant with the index and sum it by modulo 2 with the number of the round i . As a result, it is necessary to consider as a round key.

3 Lightweight Speck block cipher

Few years after block ciphers publication – SIMON and Speck – practical attacks on any of them did not appear, which can not be said about their pre–properties and advantages, among which the most striking are simplicity and flexibility.

Unlike his sibling and related SIMON algorithm optimized for hardware, the Speck algorithm is used in the framework of program implementation; in particular, in such devices with limited functionality and services, like microcontrollers.

Block encryption algorithm SPECK constitute the ARX cipher, which uses exclusive OR (XOR), addition by modulo, and methods of cyclic shift. It also provides the ability to select the length of the block and the key, based on the values of table 1, depending on the executable task.

In this algorithm, the block is divided into two words, where the key length is multiple of the word length.

Round function is used to calculate the round keys – the number of round is given as the key.

If the key length is equal to the block length, it is possible to use the round function code, which provides the additional flexibility.

Considering the case where the key is longer than the block, it is easy to notice that the key words are used cyclically.

It is worth adding that the most powerful features of this algorithm are the simplicity of its implementation and the small requirement of using memory. It lacks any constants and permutations, and does not use the technology of key bleaching.

4 Comparative Analysis of Lightweight Algorithms

In the course of investigation, significant number of practical tests were carried out. The Tables 1 and 2 for NASH and SPECK block ciphers were presented as the results of experiments have performed, respectively, which display the name of specific particular algorithm, the block sizes in bits, the key length and the number of rounds.

Table 1. Results of the Block Cipher Speck Testing.

Name of algorithm	Block size (in bits)	Key length	Number of rounds
Speck 32/64	32	16*4=64	22
Speck 48/72	48	24*3=72	22
Speck 48/96	48	24*4=96	23
Speck 64/96	64	32*3=96	26
Speck 64/128	64	32*4=128	27
Speck 96/96	96	48*2=96	28
Speck 96/144	96	48*3=144	29
Speck 128/128	128	64*2=128	32
Speck 128/192	128	64*3=192	33
Speck 128/256	128	64*4=256	34

Table 2. Results of the Block Cipher Nash Testing.

Name of algorithm	Block size (in bits)	Key length	Number of rounds
Nash 32/64	32	16*4=64	22
Nash 48/72	48	24*3=72	22
Nash 48/96	48	24*4=96	23
Nash 64/96	64	32*3=96	24
Nash 64/128	64	32*4=128	26
Nash 96/96	96	48*2=96	28
Nash 96/144	96	48*3=144	28
Nash 128/128	128	64*2=128	32
Nash 128/192	128	64*3=192	32
Nash 128/256	128	64*4=256	33

The number of performing rounds in these encryption methods is the most important factor that determines the speed, reliability, cryptographic stability, resistance and durability of specific algorithm. During the testing, the NASH block encryption algorithm demonstrated the more optimized operation, because the number of rounds of the cipher execution is less, than at the SPECK algorithm. In order to increase the execution speed of this algorithm, it is necessary to take advantage of the SPECK algorithm feature, which provides additional

execution flexibility. In order to optimize the execution speed, it is necessary to calculate the round keys beforehand, in advance, which will allow increasing the speed of the algorithm to some extent and, in turn, reduce the number of rounds executed.

5 Conclusion

The increase in the programmatic and technical complexity of the limited possibilities of communication used in today's society contributes to the development of increasingly sophisticated methods of obtaining confidential information, including household appliances and technical devices for everyday use. On the other hand, it is engine for the development and implementation of complex and robust cryptographic algorithms.

One of the most striking examples of this kind of algorithms are lightweight algorithms, in which performs large number of simple transformations, as block ciphers NASH and SPECK. These algorithms possess high cryptographic stability, which is necessary to ensure the protection of information security.

By analyzing these algorithms, the block algorithm of NASH encryption demonstrated more optimized operation, because the number of rounds of this cipher execution is less than at the SPECK algorithm, which provides greater cryptographic stability of the NASH algorithm at the lowest number of executable rounds.

References

1. 2016 *Microcontrollers – and – Processors* [www.nxp.com / products /microcontrollers–and–processors](http://www.nxp.com/products/microcontrollers-and-processors).
2. 2016 *Internet of Things* [http:// www.gemalto.com / iot](http://www.gemalto.com/iot)
3. McKay K, Bassham L, Turan M, Mouha N 2016 *DRAFT NISTIR 8114 Report on Lightweight Cryptography Computer Security Division Information Technology Laboratory NIST* www.nist.gov
4. Dinu D, Le Corre Y, Khovratovich D, Perrin L, Großschädl J, Biryukov A 2015 *Triathlon of Lightweight Block Ciphers for the Internet of Things, Report on Lightweight Cryptography Lightweight Cryptography Workshop 2015, Computer Security Division Information Technology Laboratory NIST* www.nist.gov
5. Mouha N, Mennink B, Van Herrewege A, Watanabe D, Preneel B, Verbauwhede I 2015 *Chaskey: Lightweight MAC Algorithm for Microcontrollers, Lightweight Cryptography Workshop 2015, Cryptography Computer Security Division Information Technology Laboratory NIST* www.nist.gov
6. Tschofenig H, Pegourie J, Gonnard M 2015 *Performance of State-of-the-Art Cryptography on ARM-based Microprocessors* (NIST Lightweight Cryptography Workshop)
7. Beaulieu R, Shors D, Smith J, Treatman–Clark S, Weeks B, Wingers L 2015 *Simon and Speck: Block Ciphers for the Internet of Things* (Fort Meade: National Security Agency)
8. Shannon C 1949 *Bell Systems Techn J* 656-715
9. Nash J 1955 *Letter to NSA* www.nsa.gov/public_info/press_room/2012/nash_exhibit_shtm
10. Beaulieu R, Shors D, Smith J, Treatman–Clark S, Weeks B, Wingers L *The Simon and Speck Families of Lightweight Block Ciphers*