

ՀՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԶԳԱՅԻՆ ԱԿԱԴԵՄԻԱՅԻ ԻՆՖՈՐՄԱՏԻԿԱՅԻ
ԵՎ ԱՎՏՈՄԱՏԱՑՄԱՆ ՊՐՈԲԼԵՄՆԵՐԻ ԻՆՍՏԻՏՈՒՏ

Փեյման Աբդոլահիֆարդ

SAFER ԸՆՏԱՆԻՔԻ ԾԱԾԿԱԳՐԱԿԱՆ ՀԱՄԱԿԱՐԳԵՐԻ
ԼՐԱՅՈՒՑԻՉ ԱՐԴՅՈՒՆՔՆԵՐ

Ե.13.05 «Մաթեմատիկական մոդելավորում, թվային մեթոդներ, ծրագրերի
համալիրներ» մասնագիտությամբ տեխնիկական գիտությունների թեկնածուի
գիտական աստիճանի հայցման ատենախոսության

ԵՐԵՎԱՆ 2013

NATIONAL ACADEMY OF SCIENCES OF ARMENIA
INSTITUTE FOR INFORMATICS AND AUTOMATION PROBLEMS

PEJMAN ABDOLLAHI FARD
FURTHER RESULTS ON SAFER FAMILY OF CIPHERS

AUTHOR'S ABSTRACT

For obtaining candidate in technical sciences in specialty 05.13.05 “Mathematical
modeling, numerical methods and software complexes”

YEREVAN 2013

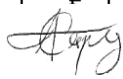
Ատենախոսության թեման հաստատվել է ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում

Գիտական ղեկավար՝ տեխ. գիտ. դոկտոր Գ.Հ.Խաչատրյան

Պաշտոնական ընդդիմախոսներ՝ ֆիզ.մաթ.գիտ.դոկտոր Լ.Հ.Ասլանյան
ֆիզ.մաթ.գիտ.թեկնածու Ս. Ե. Աբրահամյան
Առաջատար կազմակերպություն՝ Հայաստանի պետական
ճարտարագիտական համալսարան

Պաշտպանությունը կայանալու է 2013թ. դեկտեմբերի 10-ին, ժ. 16:00-ին, 037 «Ինֆորմատիկա և հաշվողական համակարգեր» մասնագիտական խորհրդի նիստում, ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտում (հասցեն՝ 0014, Երևան, Պ. Սևակ փ. 1):

Ատենախոսությանը կարելի է ծանոթանալ ինստիտուտի գրադարանում:
Սեղմագիրն առաքված է 2013թ.նոյեմբերի 9-ին.

Մասնագիտական խորհուրդի գիտական քարտուղար,
ֆիզ. մաթ. գիտ. դոկտոր  Հ. Գ. Սարգսյան

The subject of the dissertation has been approved in the institute for informatics and automation of NAS of RA.

Scientific advisor: Doctor of technical science G.H.Khachaturyan

Official reviewers: Doctor of phys. math. sciences L.H.Aslanyan
Candidate of phys. math. sciences S. Abrahamyan


Leading organization: State Engineering University of Armenia

The defense will take place during the meeting of the Specialized Council 037 “Informatics and Computer Systems” at the Institute for Informatics and Automation Problems of NAS of RA on 10 December 2013 at 16:00.

The dissertation is available in the scientific library of IAP.

The synopsis has been distributed at 9 November 2013.

The Scientific Secretary of the Specialized Council 037
Doctor of phys. math. sciences

 H. G. Sarukhanyan

CHARACTERIZATION OF THE THESIS

Actuality of the Subject

Generation of random numbers plays a crucial role in cryptographic applications and many other related areas one of the important problems in cryptographic implementations is a very fast generation of possibly maximum number of different keys from some master key which are not correlated with each other¹. They are paramount in the construction of encryption keys and other cryptographic algorithm parameters². The generalized feedback shift register (GFSR) algorithm suggested by Lewis and Payne is widely used pseudorandom number generator, but has the following several drawbacks discussed in the thesis.

In this thesis, we introduced a mechanism for random number generation based on some operations used in SAFER Family of ciphers. It is shown how some kind of 32-bit shift register can be designed that has a nearly maximum possible period. That design is not based on traditional feedback primitive polynomials but is based on special XOR shift operation using nonlinear operational blocks used in SAFER Family³.

SAFER Family has two nonlinear byte to byte transformation tables which will be used in our design. One table denoted by *EXP* is based on exponentiation function $45^X \square Y \bmod 257$ where X and Y are any numbers between 0 and 255. The second one denoted by *LOG* is based on logarithm function $\log_{45}(X) \square Y \bmod 257$.

¹ Watchman B A and Hill I D . Generating good pseudo-random numbers Computational Statistics and Data Analysis 51 1614–1622, 2006.

² D. Lim. Extracting Secret Keys from Integrated Circuits. Master's thesis, Massachusetts Institute of technology, May 2004.

³ J.Massey, G.Khachatrian, M.Kuregian "Nomination of SAFER+ as a Candidate Algorithm for Advanced Encryption Standard (AES)"- Represented at the first AES conference, Ventura, USA, August20-25, (1998)

$$L(a) = \begin{cases} \log_{45}(a) \bmod 257 & a \neq 0 \\ 128 & a = 0 \end{cases}$$

$$X(a) = (45^a \bmod 257) \bmod 256$$

The presented mechanism can be used for generation's random 128-bit keys (or more) used in symmetric encryption algorithms by combining some of them such shift registers. These new generators are most suitable for simulation of a large distributive system, which requires a number of mutually independent pseudorandom number generators with compact size.

In this dissertation we limit our discussion on generators that imitate uniformly distributed variables. For some generators those conditions can be checked by theoretical analysis, but for most RNGs they are checked by means of empirical tests⁴. Moreover, a good RNG should work efficiently, which means it should be able to produce a large amount of random numbers in a short period of time. For applications like stochastic simulation, stream ciphers, the masking of protocols or online gambling, huge amounts of random numbers are necessary and thus fast RNGs are required.

Objective of Investigations

In this thesis, Pseudo random number generations are studied .The Generalized Feedback Shift Register which are not based on traditional feedback primitive polynomials are investigated.

⁴ James E. Gentle, "Random Number Generation and Monte Carlo Methods", Second Edition, ISBN 0-387-00178-6, 2003, 31)'1998 Springer Science Business Media, Inc.

Methods of Investigation

In the work, we apply methods of Generalized Feedback Shift Register (GFSR). Especially, we use nonlinear function which use in SAFER family of cipher and cycle shift register. Also programming in C++ and matlab environment have been used.

Scientific Novelty

- A new approach of generating random numbers based on the SAFER Family of ciphers is proposed
- Different modifications of the new method are implemented, analyzed and compared with other existing methods
- Random number generators performance characteristics are evaluated for different modifications.

Practical and theoretical significance of the results

The results of the thesis can be used in different application including random number generators, cryptography and simulation.

Publications

The result of the thesis was published in three scientific articles which are listed in “List of Publications”.

Structure and Volume of the Thesis

The dissertation consists of Introduction, three chapters, conclusion and list of references. The number of references is 42. The text of thesis is expounded on 98 pages.

THE MAIN CONTENT OF THE THESIS

Chapter 1 (*Review and Analysis of Basic Methods for Random Number Generation*) In this chapter different pre existing methods for random number generators are analyzed and reviewed. In Chapter 2 (*New Approach for the Random Number Generation Based on SAFER Family of Ciphers*) new mechanisms of generating random number generators based on nonlinear functions of SAFER+ are introduced . It is shown how some kind of 32-bit shift register can be designed that has a nearly maximum possible period. That design is not based on traditional feedback primitive polynomials but is based on special XOR shift operation using nonlinear operational blocks used in SAFER Family. The presented mechanism can be used for generation's random 256-bit keys (or more) used in symmetric encryption algorithms. In chapter 3 (*Experimental Results, Performance Evaluation and Analysis of the New Approach*), the results obtained in chapter 3 are analyzed and evaluated analysis of our model GFSR_BS. Finally, we have **Conclusion** witch summarizes the contributions of this study and suggests future research directions from the results.

Types of Random Number Generators

The first type attempts to capture random events in the real world to create its sequences. It is referred to as a true random number generator, because in normal circumstances it is impossible for anyone to predict the next number in the sequence. The second camp believes that algorithms with unpredictable outputs (assuming no one knows the initial conditions) are sufficient to meet the requirements for randomness (TRNG).

The generators produced through algorithmic techniques are called *pseudo-random generators* (PRNG), because in reality each value is determined based off the system's state, and is not truly random. To gain an understanding of how these generators work, specific examples from both categories will be examined. There are some methods exist for PRNG, but the most important of them are Linear Congruential

Generators, Nonlinear Congruential Generators and Feedback Shift Register Generators. In chapter 2 we define a new mechanism for random number generation based on some operations used in SAFER Family of ciphers.

Chapter 2: New Approach for the Random Number Generation Based on SAFER Family of Ciphers

Generalized Feedback Shift Register (GFSR) generators are a variant of the Tausworthe generators. A GFSR sequence is defined by Lewis and Payne (1973) as a sequence of words, $\{W_i\}$, satisfying the equation

$$W_{k+p} = c_0 W_k \oplus c_1 W_{k+1} \oplus \dots \oplus c_{p-1} W_{k+p-1}$$

for all $k \geq 0$, where $\{c_0, c_1, \dots, c_{p-1}\}$ is some set of zeros and ones with $c_0 = 1$ and \oplus denotes the exclusive-or operator (i.e. bitwise addition modulo 2).

SAFER+ (*Secure And Fast Encryption Routine*)

The cipher **SAFER+** was designed by *Massey* together with *Dr. Gurgen H. Khachaturyan* and *Dr. Melsik K. Kuregian* then both with the National Academy of Sciences Armenia. The earlier ciphers in the SAFER family achieved rapid "diffusion" by exploiting a multidimensional linear transform called the 2-point Pseudo-Hadamard Transform(2-PHT) in which the "shuffling" operation between levels of the 2-PHT operation was the "Hadamard shuffle" or "decimation by two" which is familiar from its use in the usual Fast Fourier Transform. SAFER+ resulted from the realization that even better diffusion could be obtained by judicious choice of the shuffle between levels of the 2-PHT operation. The shuffle chosen for use in SAFER+ was called the "Armenian Shuffle" by Massey in recognition of its development by *Khachatrian* and *Kuregian* and was shown by *Massey* to provide the best possible diffusion among all shuffles for use with the 2-PHT. The name SAFER+ was chosen to reflect the fact

that this cipher was a significant improvement over the previous ciphers in the SAFER family.

GFSR_BS Generator

SAFER Family has two nonlinear byte to byte transformation tables which will be used in our design. One table denoted by *EXP* is based on exponentiation function $45^X \circ Y \bmod 257$ where X and Y are any numbers between 0 and 255. The second one denoted by *LOG* is based on logarithm function $\log_{45}(X) \circ Y \bmod 257$.

As a preliminary step, we describe the *GFSR_BS* algorithm based on nonlinear Operation in SAFER.

Step 1. $B \leftarrow 0$ (0 is seed and can change to another number in 32 Bits).

Step 2. Set B as four Bytes witch called $b3, b2, b1, b0$.

Step 3. Output B as $b3$ and $b0$ with L function AND $b2$ and $b1$ with X function. (X and L functions are described above).

Step 4. $B' \leftarrow (B \gg j1)$. (Notation: symbol (\gg) meaning circular Shift)

Step 5. $B'' \leftarrow (B \gg j2)$

Step 6. $f(B) = B \text{ XOR } B' \text{ XOR } B''$

Step 7. Go to step 2.

In continue we describe *GFSR_BS* algorithm by figures.

We have investigated the following scheme of transformation of 32 bits as 4 blocks witch called B . The first and forth byte of an input combination are processed by using *EXP* function ($X(a)$) and second and third bytes are processed by using *LOG* function ($L(a)$).

In this step we can change primitive number 45 witch used in SAFER cipher with another primitive numbers 257. We called this primitive number Q .After this transformation all 32 bits vector at the output (Figure 1) are shifted 2 times, first 32 bits circular shift J1 bits (Figure 2)

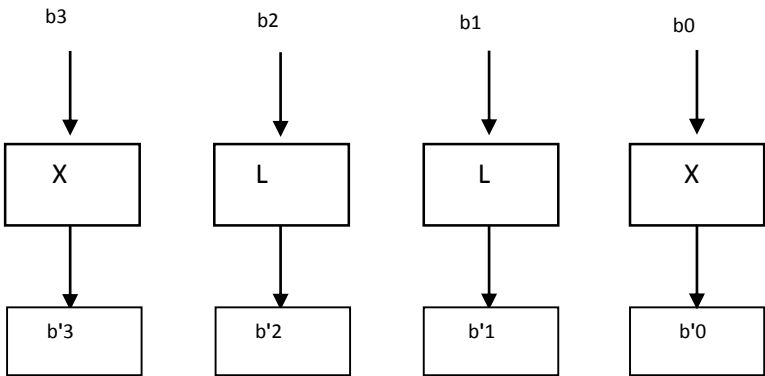


Figure 1: Initial state on GFSR_BS

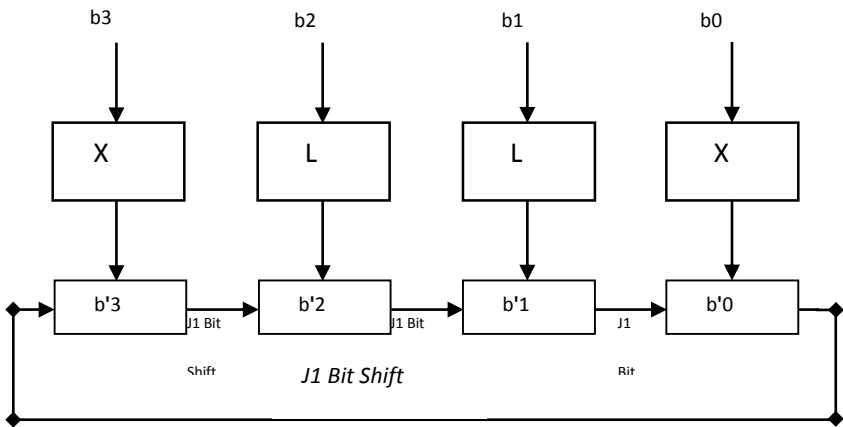


Figure 2: Generate new number

Second circular shift J2 (Figure 3), and then make *XOR* main 32 bits with result of J1 and J2 circular shift. So the schematic of transformation is depicted below.

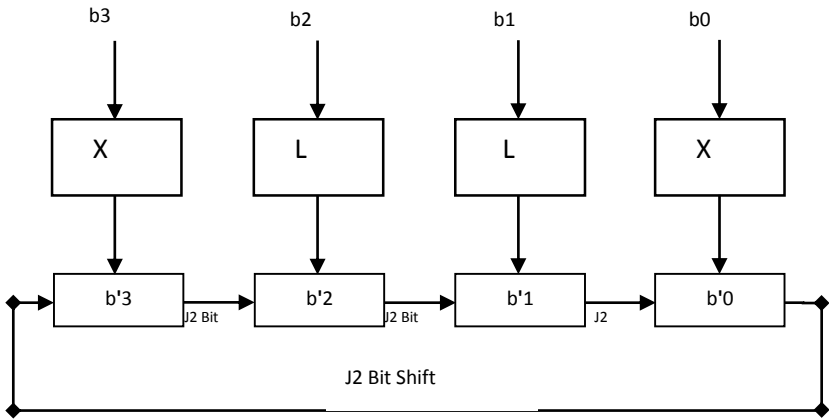


Figure 3.cycle shift in GF2SR_Bs

In Continue, make new B witch is $f(B) = B \text{ XOR } (B \gg j1) \text{ XOR } (B \gg j2)$

After that each of the new bytes goes to the corresponding input and overall transformation is repeated again (Figure 4).

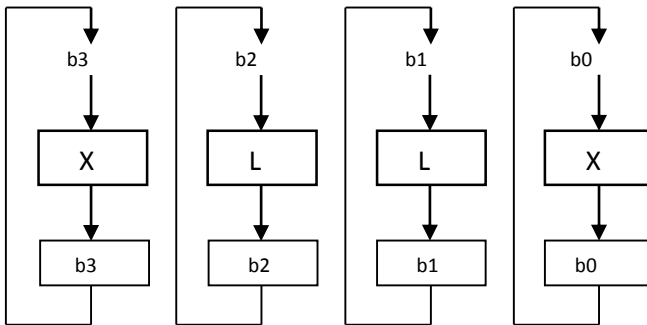


Figure 4: Start Again with New number

Obviously for each initial state there will be some number of different 32 bits generated after which the machine comes back to the initial state. All different 32 bits vectors generated after an initial state will be called to be a cycle.

Chapter 3: Experimental Results, Performance Evaluation and Analysis of the New Approach)

As we discussed in chapter 1, a good random number generator has some properties. In continue we analyze those properties on GFSSR-BS.

Period: The sequence of random numbers must have a long period. All random number generators will repeat the same sequence of numbers eventually, but it is important that the sequence is sufficiently long.

We have written a program to generate all possible cycles with all primitive numbers of 257 (called Q)⁵ and try on different J1 and J2 bits cycle shift, and find out that there is one major cycle that has “almost” all 32-bit combinations, if $q=53$, $J1=9$ and $j2=30$ namely 4294277363 out of $2^{32} = 4294967296$. So this model can generate more than %99.98 numbers in one loop. Quite surprisingly an initial 32 bits state is 0,0,0,0.

We have also investigated the same schematic but with other primitive number of 257 and different bit shifts and different Primitive number; the resulting are show in table 3.1 in dissertation.

⁵ Primitive Numbers of Prime number 257

{3,5,6,7,10,12,14,19,20,24,27,28,33,37,38,39,40,41,43,45,47,48,51,53,54,55,56,63,65,66,69,71,74,75,76,77,78,80,82,83,85,86,87,90,91,93,94,96,97,101,102,103,105,106,107,108,109,110,112,115,119,125,126,127,130,131,132,138,142,145,147,148,149,150,151,152,154,155,156,160,161,163,164,166,167,170,171,172,174,175,177,179,180,181,182,183,186,188,191,192,194,201,202,203,204,206,209,210,212,214,216,217,218,219,220,224,229,230,233,237,238,243,245,247,250,251,252,254};

Reproducible: The sequences should be reproducible. Often it is necessary to test the effect of certain simulation parameters and the exact same sequence of random numbers should be used to run many different simulation runs. It must also be possible to stop a simulation run and then recontinue the same run which means that the state of the RNG must be stored in memory. In GFSR-BS as you see, we can stop and restart in any state. So if use the same initial seed, it generate the same sequences.

Speed of Generation: The RNG must be fast. Large amounts of random numbers are needed in simulations. We Implement GFSR_BS with C++ and run the program on computer with Pentium4, CPU 2.5 MHZ (its normal Computer) and get the speed generation. It's very fast generation. For Example we can generate 20000 random numbers less than 7 second.

Parallelizable: GFSR_BS generator is one of the parallelizable random number generator. As you in section 3.1.1 we can change some parameters witch called Q, J1 and J2 Shift and generate some variable period with these change. We show the result of it in table 3.1 in dissertation.

Distribution: The numbers must have a correct distribution. In simulations, it is important that the sequence of random numbers is uncorrelated (i.e. numbers in the sequence are not related in any way). In numerical integration, it is important that the distribution is flat. A good test is to plot the consecutive sub series as a Scatter plot. We run two visual test on GFSR_BS to test distribution. In continue show the result of them.



show the result of GFSR_BS on 2000 couple

Portability: GFSR_BS is a design concept for RNGs. Thus, specific implementations can be adjusted to any platform and to any specific requirements of the user. The GFSR_BS algorithm does not employ special properties of the hardware or the processor. Consequently, GFSR_BS may be used on arbitrary machines and operating systems.

Implementation of GFSR_BS in C++

Good theoretical work on algorithms is often defeated by a poor computer implementation. This is particularly true of random number generators for two reasons: the overwhelming concern for speed and the inherent ill-conditioning of the problem. The emphasis on speed has often resulted in shortcuts. These shortcuts often accept approximations, which can be disastrous in random number generation. Other shortcuts are very machine-specific, and then often get used in the wrong environment. In dissertation we implement *GFSR_BS* algorithm in C witch show the simple implementation to generate random number very faster than other implementation.

THE MAIN RESULTS OF THE THESIS

In this thesis, several methodologies for random number generator are studied; new algorithms based on GFSR which is not using any polynomial are introduced. We called it GFSR_BS (Generalized Feedback Shift Register Based on SAFER). They can be summarized as follows:

- New approach for generation of random numbers based on nonlinear functions of SAFER family of ciphers is introduced [1].
- Based on this approach several alternative methods of generation of random numbers in presented [1,2].

- Different classes of random numbers obtained are evaluated and analyzed [3].

THE LIST OF PUBLICATIONS

1. G.Khachatrian, M.Kuregian, P.Abdollahi fard,” *Random Number Generator Based on Operation in SAFER Family of Ciphers*”, CSIT, Computer Science and Information Technologies conference, Yerevan, ARMENIA, September 2011
2. G.Khachatrian, P.Abdollahi fard,” *Key Generator Based on Operation in SAFER Family Of Ciphers*”, Australian Journal of Basic and Applied Sciences, 7(6): 34-37, 2013 ISSN: 1991-8178
3. P.Abdollahi fard,” *Generalized Feedback Shift Register Based on Operation in SAFER Family of Ciphers*”, Australian Journal of Basic and Applied Sciences, 2013 ISSN: 1991-8178.

Փեյման Աբդուլահիֆարդ

SAFER ԸՆՏԱՆԻՔԻ ԾԱԾԿԱԳՐԱԿԱՆ ՀԱՄԱԿԱՐԳԵՐԻ ԼՐԱՑՈՒՑԻՉ ԱՐԴՅՈՒՆՔՆԵՐ

Ամփոփագիր

Պատահական թվերի գեներացումը կարևոր դեր է խաղում ծածկագրաբանության և հարակից շատ ոլորտներում: Ծածկագրաբանության կարևորագույն պրոբլեմներից մեկն է հանդիսանում տրված բանալուց գեներացնել հնարավորինս մեծ պարբերություն ունեցող բանալիների հաջորդականություն, որոնք մեկը մյուսի նկատմամբ կորելացված չեն:

Այս աշխատանքում ուսումնասիրվել է պսևդոպատահական թվերի գեներացման գոյություն ունեցող որոշակի ալգորիթմներ, նրանց առանձնահատկությունները, ինչպես նաև առաջարկվել է պսևդոպատահական թվերի գեներացման նոր ալգորիթմ հիմնված SAFER+ ծածկագրական համակարգի ոչ գծային ֆունկցիայի վրա: Առաջարկված ալգորիթմի համար տրվել է որոշակի կարևորագույն գնահատականներ: Առաջարկված ալգորիթմում օգտագործվել է SAFER+ ծածկագրական համակարգի ոչ գծային EXP և LOG ֆունկցիաները սահմանված $(+, \text{mod} 256)$ օղակի վրա վերցրված 45 հիմքով, ինչպես նաև XOR և ցիկլիկ տեղաշարժ գործողությունները:

Ալգորիթմի հակիրճ նկարագրությունը բերված է ստորև:

Քայլ 1. $B \leftarrow 0$ (0 ն սկզբնական արժեքն է և կարող է լինել կամայական 32 բիթ երկարությամբ թիվ).

Քայլ 2. Ֆիքսում ենք B -ն որը 4 բիթանոց թիվ է b_3, b_2, b_1, b_0 .

Քայլ 3. B -ի $b3$ և $b0$ բիթերի վրա կիրառում ենք L ֆունկցիան և $b2$ և $b1$ -ի վրա EXP ֆունկցիան:

Քայլ 4. $B' \leftarrow (B \gg j1)$. ($\gg B$ -ն ցիկլիկ տեղաշարժում ենք $j1$ քայլով)

Քայլ 5. $B'' \leftarrow (B \gg j2) \gg B$ -ն ցիկլիկ տեղաշարժում ենք $j2$ քայլով)

Քայլ 6. $f(B) = B \text{ XOR } B' \text{ XOR } B''$

Քայլ 7. *Անցում քայլ 2-ին.*

Հարկ է նշել, որ տվյալ ալգորիթմի համար առաջարկվել է մի շարք մոդիֆիկացիաներ: Նկարագրված ալգորիթմի համար կատարվել է մի շարք ուսումնասիրություններ և արվել է հետևյալ կարևոր եզրահանգումները: Առաջարկվող ալգորիթմի արդյունքում ստացվում է մեծ պարբերականություն ունեցող չկորելացված թվերի հաջորդականություն, ինչպես նաև առաջարկվող ալգորիթմը արագագործ է ուսումնասիրված մյուս ալգորիթմների նկատմամբ:

Пейман Абдолаифард

Дальнейшие результаты криптосистемы семейства SAFER

РЕЗЮМЕ

Генерация случайных чисел играет важную роль в криптографии и связанных с ней областях. Одной из важнейших проблем криптографии является генерация из ключа последовательности ключей как можно большей периодичности, которые не коррелированы по отношению друг к другу.

В этой работе были изучены некоторые существующие алгоритмы генерации псевдослучайных чисел, их свойства, а также был предложен новый алгоритм генерации псевдослучайных чисел, основанный на нелинейной функции криптографической системы SAFER+. Предложенному алгоритму были даны определенные важнейшие оценки. В предложенном алгоритме были использованы нелинейные функции EXP и LOG криптографической системы SAFER+, определенном на кольце $(+\text{mod } 256)$, взятом с основанием 45, а также действия XOR и циклический сдвиг.

Краткое описание алгоритма приведено ниже.

Шаг 1. $B \leftarrow 0$ (0 - начальное значение и может быть произвольным числом, длиной 32 бит).

Шаг 2. Фиксируем B , которое 4 битовое число b_3, b_2, b_1, b_0 .

Шаг 3. На битах b_3 и b_0 из B применяем функцию L , и на битах b_2 и b_1 функцию EXP .

Шаг 4. $B' \leftarrow (B \gg j_1)$. ($\gg B$ циклически сдвигаем на шаг j_1).

Шаг 5. $B'' \leftarrow (B \gg j_2)$ ($\gg B$ циклически сдвигаем на шаг j_2)

Шаг 6. $f(B) = B \text{ XOR } B' \text{ XOR } B''$

Шаг 7. Переходим к шагу 2.

Необходимо отметить, что для данного алгоритма был предложен ряд модификаций. Для описанного алгоритма был сделан ряд исследований и были даны следующие важнейшие заключения. В результате предложенного алгоритма получается некоррелированная последовательность чисел, имеющая большую периодичность, а также предложенный алгоритм быстрый по сравнению с другими изученными алгоритмами.

