VOL. 12, NO. 6, MARCH 2017 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

NEW METHODS OF PSEUDO-RANDOM SEQUENCES GENERATION BASED ON BLOCKS OF STOCHASTIC TRANSFORMATION

Aleksandr Borisovich Vavrenyuk, Sergey Dmitrievich Dunaev, Michael Aleksandrovich Ivanov, Ekaterina NikolaevnaMartynova, LyubovYuryevna Poplavkova, Andrey AndreyevichSkitev, Nataliya Olegovna Fedorova and Anastasiya Aleksandrovna Chernova
National Research Nuclear University "MEPhI" Kashirskoyeshosse, Moscow, Russian Federation
E-Mail: roctra@mail.ru

ABSTRACT

Stochastic methods are methods that are either directly or indirectly based on the use of unpredictable pseudo-random number generators. In some cases, stochastic methods are the only possible mechanism for the protection of information from an active adversary. We study a new design called "*R'*-box" which can be used as a construction element of cryptographic primitives of hashing, of block and stream encryption, just like its prototype, the *R*-box. Based on the use of *R*-box, we suggest a new way of generating pseudo-random numbers with hidden information, the presence of which does not affect the statistical properties of the output sequence.

Keywords: pseudo-random number generator, pseudo-random sequence, *R*-box, information hiding.

1. INTRODUCTION

The analysis of information security threats and trends in the development of computer technology makes it possible to come to an unambiguous conclusion about the continuously increasing role of stochastic methods of information protection. Stochastic methods are methods that are either directly or indirectly based on the use of unpredictable random number generators (PRNGs). An example of a universal stochastic method of information protection (IP) is a method of introducing uncertainty into the work of tools and objects of protection. PRNGs can help to successfully solve all tasks of IP. Thus, in some cases, stochastic methods are the only possible mechanism for information protection from an active adversary. Cryptographic methods of information protection are a special case of stochastic methods usage.

The term "stochastic" in relation to IP problems has been apparently first applied by Osmolovskiy when building codes to detect and correct errors that occur during the transmission of data via communication channels (Osmolovskiy 1991; Osmolovskiy 2003). Stochastic codes suggested by him have unique properties. Two of them should be singled out: the ability to provide a pre-assigned probability of accurate reception of the information and the possibility of solving two other equally important IP problems in addition to error detection and correction: ensuring confidentiality and integrity of transmitted data.

2. BLOCKS OF STOCHASTIC TRANSFORMATION *R*-BOX

In (Asoskov, *et al*. 2003), a stochastic transformation block is suggested (*R*-box), which can be effectively used to solve various problems related to information security. One of the possible options for building the simplest stochastic transformation block, which was first proposed as a solution to the problem of error correcting coding in (Osmolovskiy1991), and its conventional graphical notation is shown in Figure-1. The key information of the *n*-bit *R*-box is contents of the table $H=\{H(m)\}, m=0,\ldots,(2^n-1)$, with dimension $n\times 2^n$, containing elements $GF(2^n)$, mixed randomly, i.e. $H(m)\in GF(2^n)$. In other words, the table *H* contains the successive states of an *n*-bit PRNG. The transformation result $R_H(A,B)$ of the input *n*-bit binary set *A* depends on the contents of the table *H* and the transformation parameter *B*, which specifies the displacement in the table relative to the cell, containing the value *A*, the following way $R_H(A,B)=H((m_A+B)\bmod 2^n)$, where m_A is the address of the table cell *H*, containing the value *A*, i.e. $H(m_A)=A$. In other words, the result of the work of the *R*-block is reading the content of the table cell *H*, cyclically displaced by *B* positions toward higher addresses relative to the cell containing the value *A*. To ensure the independence of the conversion time from the input data we introduce the additional table $H^{-1}=\{H^{-1}(j)\}$ of dimension $n\times 2^n$ into the *R*-box, at that $\forall j$ = 0, 1, …, (2^n-1) $H^{-1}(j)=m_j$. In other words, the cell with the address *j* in the array H^{-1} stores the address of the cell array *H*, containing the value *j*. Noteworthy are the following facts:

- at $H^{-1}=\{0,1,\ldots,(2^n-1)\}$ and *B*= 0, we obtain a classical *S*-box (substitution box) with the substitution table *H*;
- when recording in each cell the arrays *H* and H^{-1} its own address, we obtain the classical adder modulo 2^n, which means that the *R*-box can be with good reason called a stochastic adder, i.e. an adder with unpredictable results of work, which depends on the way the key table *H* is filled.

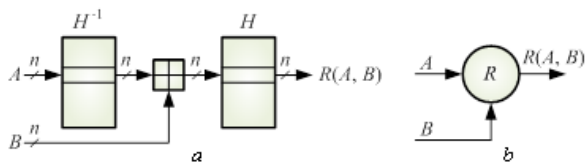


Figure-1. Thelogicof the work of the *R*-block (*a*) and its conventional graphical notation (CGN) (*b*).⊞ –adder modulo 2^n .

3. BLOCKS OF STOCHASTIC TRANSFORMATION *R´*- BOXES

The features of the new block of stochastic transformation include automatic generation of transformation parameters *B* and output digits, equal to one. The equation of work of an *n*-input *R´*- box (Figure 2) can be written as follows:

$$R^{'}(A) = q_0 R_0(A,B) \oplus q_1 R_1(A,B) \oplus ... \oplus q_{(n-1)} R_{(n-1)}(A,B),$$

where *A* – the output of the *n*-bit *R´*- box, *B* – the state of the first *n*-bit linear (LFSR) or nonlinear (NLFSR) generator of the *M*-sequence, changing its state after each contact with the *R´*-box, $R_i(A,B)$ – *ith*bit $R(A,B)$, q_i – *ith*bit of the second *n*-bit linear (LFSR) or nonlinear (RFSR) generator of the *M*-sequence, also changing its state after each contact with the *R´*-box, *i* = 0, 1, …, (*n* – 1). The key information of the *R´*-box concerns the filling of the table of the stochastic transformation $H = \{H(m)\}$, $m = 0,...,(2^n - 1)$,dimension $n \times 2^n$, containing the elements $GF(2^n)$, mixed randomly, i.e. $H\{m\} \in GF(2^m)$.

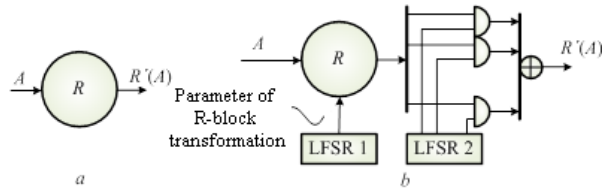


Figure-2. *R´*- box: *a* – CGN; *b* – the structure of the *R´*-box when using LFSR.

4. NEW METHOD OF GENERATING PSEUDO-RANDOM SEQUENCES ON THE BASIS OF*R´*-BOX

In the essence, we offer a method of hiding the *n*-bit binary sequence

$$M_0 M_1 ... M_{N-1}, |M_i| = n, i = 0, 1, \ldots, (N-1),$$

in a pseudo-random sequence (PRS)

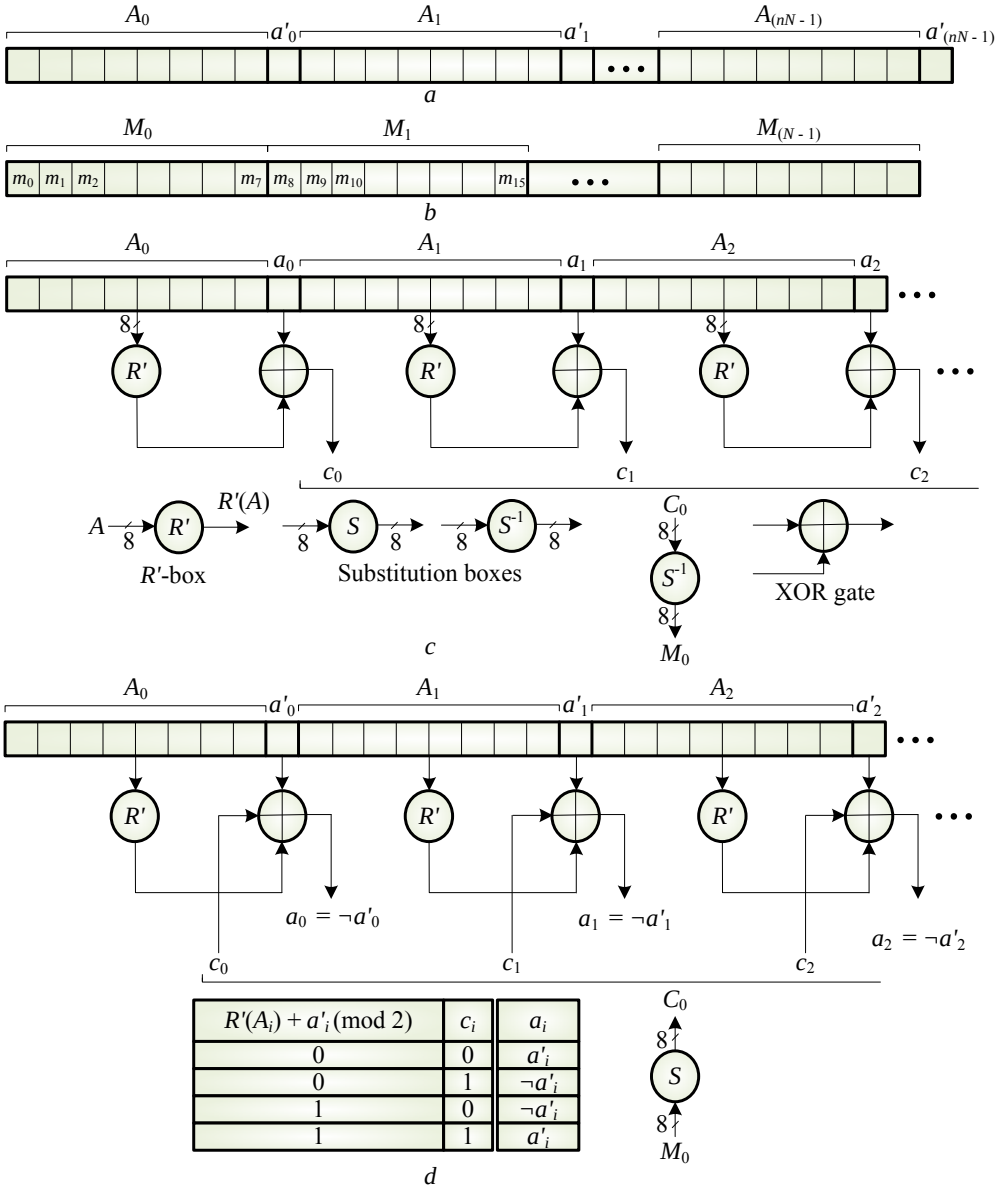
$$A_0 a_0^{'} A_1 a_1^{'} ... A_{(nN-1)} a_{(nN-1)}^{'},$$

$$|A_i| = n, \ |a_i^{'}| = 1, \ i = 0,1,...,(nN-1).$$

The essence of the suggested method is illustrated in Figures 3, 4.

The logic of hiding and extracting consists of the elements XOR, of mutually reverse *n*-bit substitution boxes (S- and S^{-1}-boxes) and blocks of stochastic transformation (R´- boxes). R´- boxes are a modification of R-boxes, considered in (Asoskov, *et al*. 2003).The R´-box has an n-bit informational input A. The input B of the transformation parameter of the inner R-box receives outputs LFSR or NLFSR. The input A R´-box receives the elements $A_i PRS$ during the hiding and extracting of information.

ARPN Journal of Engineering and Applied Sciences



$R'(A_i) + a'_i \pmod 2$	c_i	a_i
0	0	a'_i
0	1	$\neg a'_i$
1	0	$\neg a'_i$
1	1	a'_i

Figure-3. Extracting and hiding information at $n = 8$: a – initial (empty) PRS-container; b –informational sequence; c – extracting information; d – hiding information and the logic of bits calculation a_i.

The algorithm of hiding information:

INPUT: empty PRS-container $A = A_0 A_1 A_2 ... A_{(nN-1)}$, $a' = a'_0 a'_1 a'_2 ... a'_{(nN-1)}$;

initial sequence $M = M_0 M_1 M_2 ... M_{(N-1)}$;

$|A_i| = |M_j| = n, |a'_i| = 1$, S-box, R' -box, $i = 0,1,...,(nN-1)$, $j = 0,1,...,(N-1)$.

1) Calculate $C_0 = (c_0 c_1 c_2 ... c_{(n-1)}) = S(M_0)$, $C_1 = (c_n c_{(n+1)} c_{(n+2)} ... c_{(2n-1)}) = S(M_1)$, $C_2 = (c_{2n} c_{(2n+1)} c_{(2n+2)} ... c_{(3n-1)}) = S(M_2)$, ..., thus forming, $c = c_0 c_1 c_2 ... c_{(nN-1)}$;

2) Calculate $R'(A_0) R'(A_1) ... R'(A_{(nN-1)})$;

3) $i \leftarrow 0$;

4) IF $R'(A_i) + a'_i + c_i \pmod 2 = 1$, $a_i \leftarrow \neg a'_i$, OTHERWISE $a_i \leftarrow a'_i$;

5) IF $i = nN - 1$, OUTPUT, OTHERWISE $i \leftarrow i + 1$ and the jump to the step 4;

OUTPUT: PRS-container $A = A_0 A_1 A_2 ... A_{(nN-1)}$, $a' = a'_0 a'_1 a'_2 ... a'_{(nN-1)}$, containing the sequence *M*.

Algorithm of extracting information:

OUTPUT: PRS-container $A = A_0 A_1 A_2 ... A_{(nN-1)}$, $a' = a'_0 a'_1 a'_2 ... a'_{(nN-1)}$, containing the sequence $M = M_0 M_1 M_2 ... M_{(N-1)}$ $(m = m_0 m_1 m_2 ... m_{(nN-1)})$;

$|A_i| = |M_j| = n$, $|a_i| = |m_i| = 1$, S^{-1}-box, R'-box, $i = 0,1,...,(nN-1)$, $j = 0,1,...,(N-1)$.

1) $i \leftarrow 0$;
2) Calculate $c_i = R'(A_i) + a_i (\mathrm{mod}\, 2)$;
3) IF $i \neq nN-1$, $i \leftarrow i+1$ and the jump to the step 2;
4) Form the sequence $C = C_0 C_1 C_2 ... C_{(N-1)}$ from the sequence obtained $c = c_0 c_1 c_2 ... c_{(nN-1)}$:

$C_0 \leftarrow (c_0 c_1 c_2 ... c_{(n-1)})$, $C_1 \leftarrow (c_n c_{(n+1)} c_{(n+2)} ... c_{(2n-1)})$, $C_2 \leftarrow (c_{2n} c_{(2n+1)} c_{(2n+2)} ... c_{(3n-1)})$, ...;

5) $i \leftarrow 0$;
6) $M_i \leftarrow S^{-1}(C_i)$;
7) IF $i = N-1$, OUTPUT;
8) $i \leftarrow i+1$, jump to the step 6;

OUTPUT: Initial sequence $M = M_0 M_1 M_2 ... M_{(N-1)}$

$((m_0 m_1 m_2 ... m_{(n-1)}) \leftarrow M_0$,
$(m_n m_{(n+1)} m_{(n+2)} ... m_{(2n-1)}) \leftarrow M_1$,
$(m_{2n} m_{(2n+1)} m_{(2n+2)} ... m_{(3n-1)}) \leftarrow M_2$, ...:
$m = m_0 m_1 m_2 ... m_{(nN-1)})$.

5. CONCLUSIONS

A new design of the block of stochastic transformation has been offered. On its basis, we developed a method of generating PRSs with hidden information. The statistical testing of PRSs with hidden information according to the NIST (A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, 2010*;* Chugunkov, *et al*. 2013; Ivanov & Chugunkov2012) technique showed that the presence of hidden information does not affect the statistical properties of the forming sequence of pseudo-random numbers.

The areas of application of the proposed solution: ensuring the privacy of information without encryption; organization of hidden communication channels; opposition to the use of PRNGs for dual purposes.

REFERENCES

Osmolovskiy S.A. 1991. Stokhasticheskiemetodyperedachidannykh [Stochastic Methods of Data Transmission]. Moscow: Radio and Communication.

Osmolovskiy S.A. 2003. Stokhasticheskiemetodyzashchityinformatsii [Stochastic Methods of Information Defense]. Moscow: Radio and Communication.

Asoskov A.V., Ivanov M.A., Mirskiy A.A., Ruzin A.V., Slanin A.V. & Tyutvin A. N. 2003. Potochnyeshifry [Stream Ciphers]. Moscow: Kudits-Obraz.

A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. 2010, April. NIST Special Publications 800-22. Revision 1.a.

Chugunkov I.V., Kutepov S.V. & Shustova L.I. *et al*. 2013. Reducing of Memory Usage in Statistical Research into Pseudorandom Number Generators by Validation Tests. In Proceedings of the Radio-Electronic Devices and Systems for the Infocommunication Technologies (REDS-2013). Moscow, Russia. pp. 148-152.

Ivanov M.A. & Chugunkov I.V. 2012. Kriptograficheskiemetodyzashchityinformatsii v komp'yuternykhsistemakhisetyakh [Cryptographic Methods of Information Defense in the Computer Systems and Networks: Teaching Guide]. Moscow: National Research Nuclear University MEPhI.