Journal of Theoretical and Applied Information Technology
10th May 2016. Vol.87. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

NONLINEAR TRANSFORMATIONS FOR THE CONSTRUCTION OF THE PRIMITIVES OF SYMMETRIC CRYPTORAPHY

MICHAEL ALEKSANDROVICH IVANOV, ALEKSANDR BORISOVICH VAVRENYUK, VIKTOR VALENTINOVICH MAKAROV, ANDREY ANDREYEVICH SKITEV,

National Research Nuclear University MEPhI
(Moscow Engineering Physics Institute),
Kashirskoe sh., 31, Moscow, 115409, Russia

ABSTRACT

Three new stochastic transformations are proposed in the paper. A linear transformation on the basis of a pseudo-random number generator (PRNG), functioning in finite fields and constructed by the Galois scheme, exceeds by its mixing properties the known solution on the basis of PRNG, constructed by the Fibonacci scheme. A nonlinear transformation on the basis of an RFSR (Random Feedback Shift Register) has an efficient software implementation. In the nonlinear multi-round 256-bit transformation, as distinct from known solutions, the entire input block is changed during one round. The considered transformations are directed, first of all, to the construction of crypto-algorithms using multidimensional transformations.

Keywords: *Stochastic Transformation, R-Box, Pseudo-Random Number Generator, 2D Transformation.*

1. INTRODUCTION

The transformations are usually called stochastic, if they involve loading of the input data into the memory of a pseudo-random number generator (PRNG), after which several cycles of its operation are performed. The final state of some of the elements of the generator memory is declared to be the transformation result [1]. The linear and nonlinear stochastic transformations are actively used in constructing the iterated block ciphers, stream ciphers, and cryptographic hash-functions. Analysis of information security threats, trends of development of computer technologies allows to make an unambiguous conclusion about ever-increasing role of stochastic (e.g., cryptographic) methods of information protection. So, in some cases, cryptography is the only mechanism of information protection. The trend in recent years has been the advent of the 2D and 3D stochastic transformation, which confirms the relevance of the chosen topic of research. All, without exception, have appeared in recent years state security standards for encryption, specify the algorithms based on 2D and 3D transformations (block ciphers AES and Kuznechik, the hash function Keccak and Stribog) that allows you to draw the obvious conclusion about the prospects of selected areas of research.

It seems that the term "stochastic", as applied to the problems of information security (IS), was used for the first time by S.A. Osmolovsky in constructing the codes, detecting and correcting the errors which arise in the data transmission over the communication channels [2-3]. The stochastic codes, proposed by him, possess the unique properties, among which two are worth to be mentioned: the capability to provide in advance a given probability of correct reception of information and the ability to solve, besides the task of providing the noise resistance, two no less important IS tasks: ensuring confidentiality and integrity of the transmitted information.

2. METHODS OF RESEARCH

The main objective of the study was the development of the theory of cryptography with the architect-Rami the Square and the Cube, improving the efficiency of stochastic 2D and 3D transformations, including by increasing the scattering and mixing (diffusion and confusion properties, and ease of implementation.

In the work, the methods of the theory of linear sequential circuits [4] and the theory of finite fields [5-6] are used. Statistical testing of multi-round stochastic transformations is carried

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

out by the NIST method [7] using a software package described in [8].

3. LINEAR KEYLESS STOCHASTIC TRANSFORMATION

Consider two examples of linear transformations for the case of a PRNG, functioning in finite fields [1, 5-6, 8]. These transformations can be used for executing the state mixing operation (MixState), which is a part of crypto-algorithms that use multidimensional transformations [8-13].

Let the number of digits M of the input information and the number of digits Q of the PRNG state (the number of memory elements) both equal 128 bits: $|M| = |Q| = 128, Q = (Q_{16} \dots Q_1), Q_i \in GF(2^8), i = 1,\dots,16.$

Since in the sequential PRNG, constructed according to the Fibonacci scheme, only the leading byte of the state is changed during one cycle, whereas the entire state is changed during 16 cycles, the known linear stochastic transformation [10], which forms the transformation result during one cycle, i.e. the new value of the output state Q, will be defined by the following expression:

$$L_1(Q) = R_1^{16}(Q) = R_1^{16}(Q_{16} \| \dots \| Q_1) =$$
$$= (a_{16} \cdot (Q_{16}) + a_{15} \cdot (Q_{15}) + \dots + a_2 \cdot (Q_2) + a_1 \cdot (Q_1) \| Q_{16} \| \dots \| Q_2)^{16} = Q \cdot T_1^{16},$$

where Q is the state row $(Q_{16} \dots Q_1)$, T_1 is a square matrix of the size 16 × 16 of the form

$$\begin{pmatrix} a_{16} & 1 & 0 & \dots & 0 & 0 \\ a_{15} & 0 & 1 & \dots & 0 & 0 \\ a_{14} & 0 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & & \dots & \dots \\ a_3 & 0 & 0 & \dots & 1 & 0 \\ a_2 & 0 & 0 & \dots & 0 & 1 \\ a_1 & 0 & 0 & \dots & 0 & 0 \end{pmatrix},$$

all operations are performed in the field $GF(2^8)$, $a_i \in GF(2^8)$ are the coefficients of the characteristic polynomial $\varphi(x) = a_{16}x^{16} + a_{15}x^{15} + \dots + a_2x^2 + a_1x - 1,$ which is primitive over the field $GF(2^8)$. The operation equations of the basic linear transformation (multiplication of the state row by T_1) have the form:

$$\begin{cases} Q_j = Q_{j-1}, j = 1,\dots,15, \\ Q_{16} = a_{16} \cdot (Q_{16}) + a_{15} \cdot (Q_{15}) + \dots + a_2 \cdot (Q_2) + a_1 \cdot (Q_1). \end{cases}$$

A linear stochastic transformation, providing more intensive dissipation and mixing of information, on the basis of a PRNG, functioning in $GF(2^8)$ and constructed by the Galois scheme, is defined by the following expressions:

$$L_2(Q) = R_2^{16}(Q) = R_2^{16}(Q_{16} \| \dots \| Q_1) =$$
$$= (a_{16} \cdot (Q_1) \| Q_{16} + a_{15} \cdot (Q_1) \| \dots \| Q_2 + a_1 \cdot (Q_1))^{16} = Q \cdot T_2^{16},$$

$$\begin{pmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \\ a_{16} & a_{15} & a_{14} & \dots & a_2 & a_1 \end{pmatrix}.$$

The operation equations of the basic linear transformation (multiplication of the state row by T_2) have the form:

$$\begin{cases} Q_j = Q_{j+1} + a_j \cdot (Q_1), j = 1, \dots,15, \\ Q_{16} = a_{16} \cdot (Q_1). \end{cases}$$

4. *R*-BOX

In [1], a block of stochastic transformation (*R*-box) is proposed, which can be effectively used in solving various problems connected with information security. A scheme of one of the possible simple variants of construction of an *R*-box of stochastic transformation, suggested for the first time for solving the problem of noise-resistant coding in the paper [2], and its conventional graphic representation are shown in Figure 1. The key information of an *n*-bit *R*-box is the filling of the table $H = \{H(m)\}, m = 0,\dots,(2^n - 1),$ of the size $n \times 2^n$, which includes the elements of $GF(2^n)$, which have been 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 result $R_H(A,B)$ of the transformation of the input *n*-bit binary set A depends on the filling of the table H and the transformation parameter B, defining the shift in the table relative to the cell, containing the value A, in the following way $R_H(A,B) = H((m_A + B) \bmod 2^n),$ where m_A is the address of the cell of the table H, containing the code A, i.e. $H(m_A) = A$. In other words, the result of operation of the *R*-box is essentially the reading off of the content of the

Journal of Theoretical and Applied Information Technology
10th May 2016. Vol.87. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

cell of the table *H*, cyclically shifted by *B* positions towards the higher order addresses relative to the cell, containing the code *A*. To provide independence of the transformation time from the initial data, there is introduced into the composition of the *R*-box a table $Addr = \{Addr(j)\}$ of the size $n \times 2^n$, where $\forall j = 0,...,(2^n - 1)\ Addr(j) = m_j$. In other words, the cell with the address *j* in the array *Addr* stores the address of the cell of the array *H*, containing the code *j*. The following facts are noteworthy:

– for $Addr = \{0,1,2, ..., (2^n - 1)\}$ and *B* = 0, we obtain the classical *S*-box (substitution block) with the substitution table *H*;

– when we record into each cell of the arrays *H* and *Addr* its own address, we obtain the classical adder modulo 2^n, and hence, the *R*-box can be rightfully called a *stochastic adder*, i.e. an adder with unpredictable result of operation, depending on the filling of the key table *H*.

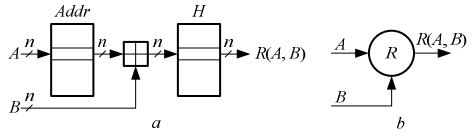

Figure 1. Operation Logic of the R-box (a) and its Conventional Graphic Notation (b).

⊞ is an Adder Modulo 2^n.

R-box can be easily implemented in software. Below we will present an example of the implementation of an 8-bit block of stochastic transformation in Assembler (x86 system of commands, standard Intel notation).

```
;=====================================================
;==== RBox – procedure of stochastic transformation.
;=====================================================
;==== During activation: ===================================
;==== AL is an input byte, AH is a parameter of transformation,
;==== DS is the segment address of the array Addr&H, ==========
;==== BX is a relative address ======================
;==== of the array Addr&H (Figure 2), ===================
;==== CX is the size of the arrays Addr and H (HSize). ====
;==== During return: ================================
;==== AL is the output byte. ========================
;=====================================================
RBox        PROC
            push  bx
            xlat              ; Reading from the table Addr
            add   al, ah      ; AL is the address of the output
; byte in the array H
            add   bx, cx      ; BX is a relative
; address of the array H
            xlat              ; Reading from the table H
            pop   bx
            ret
RBox        ENDP
;=====================================================
```

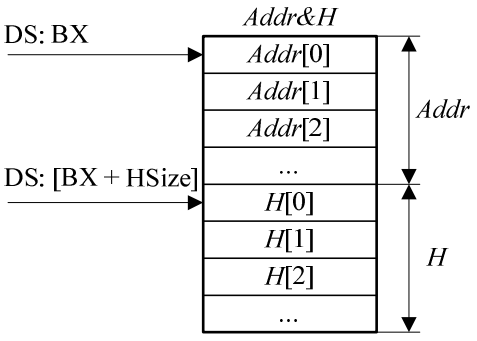

Figure 2. The Array Addr&H.

Journal of Theoretical and Applied Information Technology
10th May 2016. Vol.87. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

R-box can be used for the implementation of synchronize stream encryption. In this case, the original sequence (Plaintext) is delivered to the input *A*; the keystream is delivered to the input *B*, whereas the ciphertext (Ciphertext) is read off from the output $R_H(A,B)$. The only thing that should be taken into account is the necessity to use the transformation R^{-1} (inverse to *R*) on the receiving side.

The second field of application of *R*-boxes is a substitution for the adders modulo 2^n in the modification of the known crypto-algorithm, for example, the stream ciphers PIKE, RC4, and some others. By the way, using *R*-box, it is possible to substitute in two ways the adder modulo 2^n in Figure 1, thus obtaining two kinds of R^2-boxes.

5. NONLINEAR STOCHASTIC TRANSFORMATION

Let us consider an example of nonlinear transformation on the basis of an RFSR (Random Feedback Shift Register), which is obtained after substitution of the adders modulo 2^n by *R*-boxes in the scheme of additive generator [1, 8].

Let the number of digits *M* of the input information and the number of digits *Q* of the state (the number of memory elements) of RFSR equal 128 bits:

$$|M|=|Q|=128,\ Q=(Q_{16}\dots Q_1),\ Q_i\in GF(2^8),\ i=1,\dots,16.$$

A nonlinear stochastic transformation on the basis of RFSR, constructed by the Galois scheme (Figure 3), is defined by the following expressions:

$$F(Q)=f^{16}(Q)=f^{16}(Q_{16}\|\dots\|Q_1).$$

The step transformation has the form:

$$f=R_{16}(Q_1,C_i)\|\,R_{15}(Q_1,Q_{16})\|\dots\|R_1(Q_1,Q_2),\ i=1,\dots,16,$$

where $C=C_1\dots C_i\dots C_{16}$ is the control sequence (possibly, depending on the key).

The operation equations of the basic step-type nonlinear transformation have the form:

$$\begin{cases} Q_j=R_j(Q_1,Q_{j+1}),\ j=1,\dots,15,\\ Q_{16}=R_{16}(Q_1,C_i). \end{cases}$$

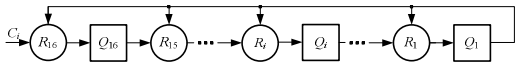

Figure 3. A Scheme of RFSR.

6. NONLINEAR MULTI-ROUND STOCHASTIC TRANSFORMATION

A nonlinear stochastic transformation *E* on the basis of PRNG, constructed by the Galois scheme, is defined by the following expressions:

$$E(Q)=R^n(Q)=R^n(Q_N\|\dots\|Q_1),$$
$$R(Q_N\|\dots\|Q_1)=F[K_{i,N}](Q_1)\|Q_N\oplus F[K_{i,N-1}](Q_1)\|\dots\|Q_3\oplus F[K_{i,2}](Q_1)\|Q_2\oplus F[K_{i,1}](Q_1),$$

where $R(Q)$ is the round transformation, *n* is the number of rounds, $(K_{i,N}\dots K_{i,1})$ is the round key, *i* = 1, …, *n*; $Q=(Q_N\dots Q_1)$ is the state of PRNG, $F[K_{i,2}](\ )$ is a nonlinear function. The operation equations of the basic nonlinear transformation (*i*-th round of $R(Q)$) have the form:

$$\begin{cases} Q_j=Q_{j+1}+F[K_{i,j}](Q_1),\ j=1,\dots,(N-1),\\ Q_N=F[K_{i,N}](Q_1). \end{cases}$$

In Figure 4, an example is shown of such transformation for the case *N* = 2, $|Q_i|=128$. As the nonlinear function *F*, one can use a round transformation, analogous to the one used in the Kuznechik block cipher, specified in the state standard GOST R 34.12-2015 [10]. In addition, as a transformation MixState of mixing the bytes of the state, one can use the above-described linear transformations *L*.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

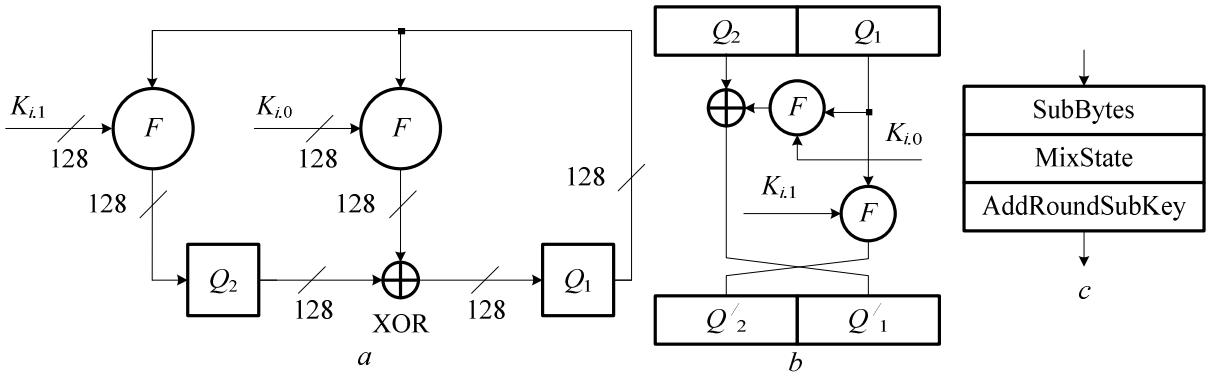

Figure 4 – An Example Of Nonlinear Stochastic Transformation: A − A Scheme Of The I-Th Round, B − An Equivalent Scheme Of The Round, C − An Example Of Construction Of The Transformation F.

7. CONCLUSION

The adoption of the standard AES encryption with a simple and elegant design, has opened a new interesting area of research: cryptographic algorithms based on 2D and 3D transformations, the main feature of which is a high degree of parallelism at the level of elementary transformations. Unlike similar works, the research has been primarily made for multidimensional transformation of the family DOZEN.

Three new stochastic transformations are proposed in the paper:

– a linear one on the basis of a PRNG, constructed by the Galois scheme, exceeding by its mixing properties the known one on the basis of PRNG, constructed by the Fibonacci scheme;

– a nonlinear one on the basis of an RFSR (Random Feedback Shift Register), allowing for effective software implementation;

– a nonlinear multi-round 256-bit transformation, in which, in distinction from the known solutions, the entire input block is transformed during one round.

The solutions, presented in the work, are directed to the construction of crypto-algorithms with the Square and Cube architectures [8, 11]. The multi-round stochastic transformations of the DOZEN family, in which the considered transformations are used, stand all the statistical NIST tests, which allows making conclusion about their statistical security.

REFERENCES:

[1] Asoskov, A.V., A.A. Mirsky, A.N. Tyutvin et al., 2003. Stream Ciphers. Moscow: KUDITS-OBRAZ.

[2] Osmolovsky, S.A., 1991. Stochastic Methods of Data Transmission. Moscow: Radio i Svyaz.

[3] Osmolovsky, S.A., 2003. Stochastic Methods of Information Defense. Moscow: Radio i Svyaz.

[4] Gill, A., 1966. Linear Sequential Circuits. New York: McGraw-Hill Book Company.

[5] Peterson, W.W. and E.J. Weldon, 1971. Error-Correcting Codes (2nd ed.) Cambridge: MIT Press.

[6] Blahut, R.E., 1983. Theory and Practice of Error Control Codes. Reading, MA: Addison-Wesley.

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

[8] Ivanov, M.A. and I.V. Chugunkov, 2012.Cryptographic Methods of Information Defense in the Computer Systems and Networks: Teaching Guide. Moscow: National Research Nuclear University MEPhI.

[9] FIPS 197, Advanced Encryption Standard (AES), 2001. Date Views 12.03.2016 csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[10] GOST R 34.12-2015. Information Technology. Cryptographic Information Defense. Block Ciphers, 2015. Moscow: Standartinform.

[11] Ivanov, M.A., M.M. Rovnyagin, I.V. Chugunkov et al., 2014. Three-Dimensional Data Stochastic Transformation Algorithms for Hybrid Supercomputer Implementation. In Proceedings of 17th IEEE Mediterranean Electrotechnical Conference (MELECON), pp: 451-457.

[12] Nakahara, J., 2008. 3D: A Three-Dimensional Block Cipher. Date Views 21.03.2016 infosci-ence.epfl.ch/record/128649/files/Nak08.pdf.

[13] Bertoni, G., J. Daemen, M. Peeters and G. Van Assche, 2010. Keccak Sponge Function Family. Date Views 21.03.2016 keccak.noekeon.org/Keccak-main-2.1.pdf.