Prospects for the Application of Many-Valued Logic Functions in Cryptography

Chapter *in* Advances in Intelligent Systems and Computing · January 2019

DOI: 10.1007/978-3-319-91008-6_33

2 authors:

Artem Sokolov
National University Odesa Law Academy
66 PUBLICATIONS **164** CITATIONS
SEE PROFILE

Oleg Zhdanov
Siberian State Aerospace University
17 PUBLICATIONS **169** CITATIONS
SEE PROFILE

PROSPECTS FOR THE APPLICATION OF THE VARIABLE BLOCK LENGTH AND MANY-VALUED LOGIC FUNCTIONS IN SYMMETRIC ENCRYPTION ALGORITHMS

Artem Sokolov[1], Oleg Zhdanov[2]

[1]Odessa National Polytechnic University
Shevchenko avenue, 1, Odessa, Ukraine, 65044
[2]Siberian State Aerospace University named after academician Mikhail F. Reshetnev,
Krasnoyarsky Rabochy Av., 31, Krasnoyarsk, Russia 660014
radiosquid@gmail.com

Abstract. The paper considers development of cryptographic methods based on the principles of many-valued logic. The results concerning the construction of block and stream crypto algorithms based on functions of many-valued logic are presented. The synergy of the principles of many-valued logic and the variable fragmentation of the block made it possible to construct an effective block symmetric crypto algorithm. The results of computational experiments confirm its high cryptographic quality and easily scalable number of protection levels. As shown by experiments, the principles of many-valued logic are an excellent basis for the construction of gamma generators (the basis of stream ciphers), which are based on the use of triple sets of ternary bent-sequences. The article outlines the scope of the tasks, the solution of which is necessary for the further development in this direction in cryptography.

Keywords: cryptography, many-valued logic, variable block fragmentation.

1. Introduction

The importance of cryptographic methods in the protection of information is well known. The rapid growth of computer processing power and the new results obtained by researchers in the field of cryptanalysis necessitates the need of further increase of the cryptographic strength of existing cryptographic algorithms, as well as the development of new algorithms.

The purpose of increasing of cryptographic strength is usually achieved by the significant complication of non-linear dependencies between the key and the plaintext and between plaintext and ciphertext (confusion), as well as effective destruction of open-text statistics by cryptographic algorithm (diffusion) [1], which requires corresponding, often significant, computational cost.

A block of plain text has its own structure and more or less inherits the features of texts in natural language. Therefore, working with blocks of the same size in all

rounds cannot guarantee the dispersion of such patterns in the cipher text. To improve the quality of the cryptographic algorithm, we have to either complicate round block operations or increase the number of rounds.
Earlier [2], we proposed an encryption algorithm with dynamic resizing of cryptographic primitives in various rounds.
In other words, it was suggested that the plain text is encrypted using substitution tables of different sizes in different rounds.
Proposed cryptographic algorithm [2] is the combination of substitution and permutation blocks, addition with a round key. The change in the size of the block, according to the authors' intention, should effectively destroy the links between the elements of the plaintext and increase the diffusion.
The results of research of the statistical parameters of this algorithm are presented in [3]. After the fifth round, the statistics of the text differ little from the statistics of the random sequence. In addition, the nonlinearity of the conversion and the correlation characteristics are comparable with those for full-round algorithms, such as GOST 28147-89 and AES after 7 or 8 rounds.
The algorithm is programmed and adapted in [4].
The use of a binary system of representation of data is traditional in modern computing. However, annual conferences held by IEEE confirm the attention of specialists to developments based on non-binary numbering systems. And the analysis of publications allows to draw a conclusion: the main efforts today are concentrated in the field of construction of data processing algorithms based on non-binary logic.
At the moment, the methods of many-valued logic have found their application in many practical information systems for the synthesis of signal constructions, error-correcting and effective codes [5], to ensure data confidentiality.
The application of many-valued logic is obviously best suited for the paradigm of multi-core data processing with is implemented today, and they are of special interest for promising quantum cryptographic algorithms. Thus, in [6] effective algorithms for generating pseudorandom key sequences based on functions of many-valued logic are proposed.
We believe that approach of the concept of variable fragmentation of a block and many-valued logic is one of the best ways in future developing of cryptography. In this paper we present our block symmetric cryptographic algorithm as well as some results in many-valued logic pseudorandom sequence generators based on many-valued perfect algebraic constructions.

2. Block symmetric crypto algorithm based on the principles of many-valued logic and variable block length

As it is known, many modern encryption algorithms use S-boxes and operation of addition modulo with the round key. Wherein the size of the S-box and its quality, that affect the performance of confusion and diffusion, are of importance.
For the most effective organization of the encryption algorithm with dynamic resizing of cryptographic primitives the length of input block of the algorithm must be a composite number. For example, in [7], the plaintext block has the length $L = 120 = 2^3 \cdot 3 \cdot 5$ bits. Partitioning of the plaintext block for the encryption algorithm

may be performed in various ways, such as segments convenient from a computational point of view of the length of $\sigma = 6,8,10,12,15,20,30$ bits, wherein within one procedure the segment size is not changed.

The proposed encryption algorithm involves three basic procedures: Substitution, Permutation and Gamma (adapted to non-binary case).

Successively described, each of these procedures, which are reversible, can therefore be used both in encryption algorithm and in decryption algorithm.

Encryption is performed iteratively, while it is possible to vary the number of rounds. Round transform consists of implementation of Gamma, Substitution or Permutation procedures. The basic version of the encryption algorithm includes five rounds, the first round consists of the Gamma and Permutations procedures, while other rounds include Substitution and Gamma Procedures. The scheme of the proposed encryption algorithm is shown in Fig. 1. We are focusing on the differences of this version of the algorithm:

1. Ternary logic is used;
2. The block size is increased to 240 elementary units, in this case it is trits.

Alphabet: $A = \{0,1,...,q-1\}$, $q > 2$. In this paper we consider in details the case $q = 3$.

Input text: $\{x_i\}$, $i = 0,1,...N-1$. In this paper we consider $N = 240$.

The key is: $K = \{g_i, Q_l, E, a_i\}$, where a_i — variables of splitting which are chosen as different values for each procedure, that are the parts of the encryption round; Q_l — substitution sequences; E — permutation sequence; $\{g_i\}$ — gamma sequence.

Output text: $\{y_i\}$, $i = 0,1,...N-1$.

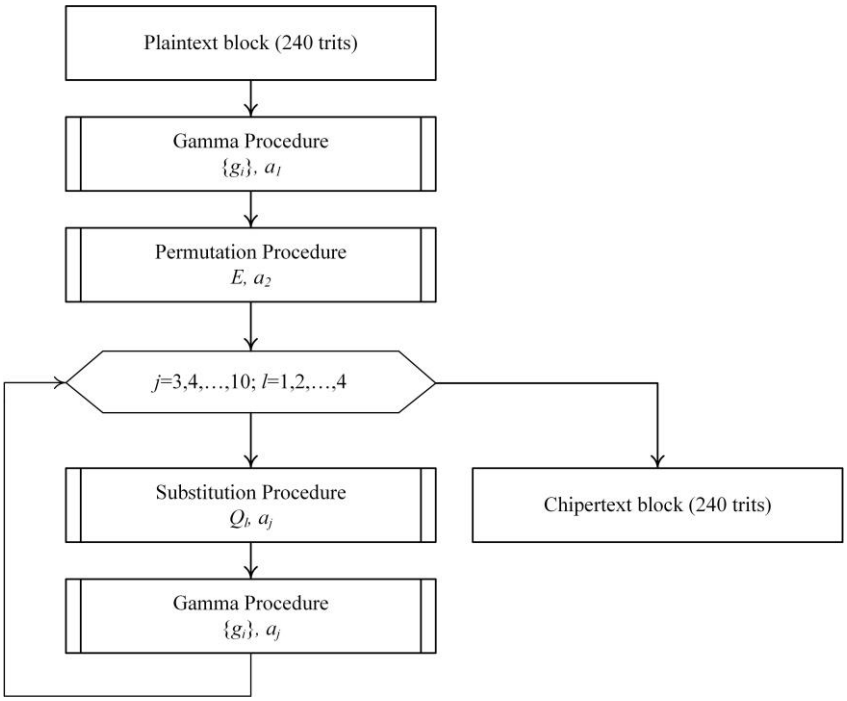


Fig. 1 Proposed encryption algorithm

For the organization of the encryption rounds the values $\{a_i\}$ must be selected from the divisors of the number N, as well as the substitutions Q_1, Q_2, Q_3, Q_4 and permutation E sequences must be determined.

Decryption algorithm is completely similar to the encryption algorithm. More information about this algorithm can be found in [8].

Experiments have shown that the proposed encryption algorithm can be successfully implemented in the modern high-level programming languages, such as MatLab, which allows the encryption / decryption of data on a binary computer. We note in particular that during experiments the encryption was done in a mode of "Electronic Codebook", nonetheless the structure of the original image was completely destroyed, which is a very strong result for a symmetric block cryptographic algorithm.

3. Generation of pseudorandom sequences and stream ciphers based on the principles of many-valued logic

The principles of many-valued logic are an excellent basis for the construction of stream ciphers. The basic components of modern stream ciphers are the generators of pseudo-random key sequences (gamma generator), which in many respects determines their performance and cryptographic strength. In fact, the development of stream cipher today means the development of a high-quality gamma generator,

which, subsequently, with the help of the operation of summation modulo p is added element-wise to the plain text.

The construction of the gamma generator based on the principles of many-valued logic was carried out by using the classical scheme for binary gamma generators, using many-valued LFSR, as well as such highly nonlinear functions of many-valued logic as a bent-sequences.

Definition 1. A ternary sequence $H = [h_0, h_1, \cdots, h_i, \cdots, h_{n-1}]$ of length $N = 3^m, m \in \mathbb{N}$, where the coefficients $h_i \in \pm 1\left\{e^{j0^o}, e^{j2\pi/3}, e^{j4\pi/3}\right\}$, is called a bent sequence, if it has uniform absolute values of the Vilenkin-Chrestensen spectrum, which is representable in the matrix form

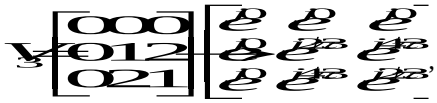
$$\left|\Omega_B(\omega)\right| = \left|H \cdot V_N\right| = const\ ,\ \omega = \overline{0, N-1}\,, \tag{1}$$

where V_N is the Vilenkin-Chrestensen matrix of order N.

We have proposed an efficient method for synthesizing bent-sequences, which are necessary for constructing the gamma generators. The proposed method is based on three constructions for each of which the rules of reproduction have been found. More information about proposed method can be found in [10].

Construction 1.

To construct a bent-sequence of length $N = 9$ in the Vilenkin-Chrestensen basis, we carry out a sequence of concatenations of the rows of the Vilenkin-Chrestensen matrix



(2)

resulting

(3)

In order to verify that the constructed sequence (3) is indeed a bent-sequence, we multiply it by the Vilenkin-Chrestensen matrix of order 9, with the help of the following construction

(4)

As a result, we obtain the spectrum of the sequence (3)

(5)

So, the sequence (3) really satisfies the **Definition 1** and is a bent-sequence in the Vilenkin-Chrestensen basis.

Here are the rules of reproduction:

Rule 1. When the rows of the Vilenkin-Chrestensen matrix are concatenated, their permutation can be performed in $\mu! = 3^L!$ ways.

Rule 2. With respect to each row of the Vilenkin-Chrestensen matrix, a re-coding operation can be applied using all possible rules by adding the number 0, 1 or 2.

By combining *Rule 1* and *Rule 2*, we obtain the first class of bent-sequences in the Vilenkin-Chrestensen basis of the cardinality $J_1 = 6 \cdot 27 = 162$. This class is an analog of the Majorana-McFarland class for binary bent-sequences.

We note that the use of this construction and the reproduction rules for any order of the Vilenkin-Chrestensen matrix determines the possibility of constructing bent-sequences in the Vilenkin-Chrestensen basis of any length $N = 3^{2k}$.

For example, on the basis of the Vilenkin-Chrestensen matrix of order $\mu = 3^2 = 9$ (4), bent-sequences in the Vilenkin-Chrestensen basis of length $N = 81$ can be constructed. Taking into account the rules of reproduction, their number will reach $J_{1,81} = \mu!3^{\mu} = 9! \cdot 3^9 = 7142567040$.

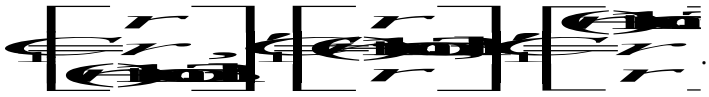
Construction 2.

It is found that the synthesis of bent-sequences of length $N = 9$ in the Vilenkin-Chrestensen basis can be performed on the basis of the following two regular constructions:

(6)

where r is any ternary sequence of length 3, except the rows of the Vilenkin-Chrestensen matrix and their linear combinations. Thus, as the r $29 - 9 = 18$ such sequences can be used.

Obviously, we can rearrange the last line of the construction in three different ways, for example: for the first construction



(7)

Thus, the cardinality of the class is $J_2 = 3 \cdot 2\left(3^3 - 3^2\right) = 6\left(27 - 9\right) = 108$.

Construction 3.

Another construction that allows the synthesis of bent-sequences of length $N = 9$ in the Vilenkin-Chrestensen basis can be written as

(8)

where $\leftarrow$ is the operator of cyclic left shift by the corresponding number of positions; r is any ternary sequence of length 3, except the rows of the Vilenkin-Chrestensen matrix and their linear combinations.

The *Construction 3* can be subjected to all $3! = 6$ possible permutations. Thus, the total cardinality of the third class of bent-sequences in the Vilenkin-Chrestensen basis is $J_3 = 2 \cdot 6 \cdot \left(3^3 - 3^2\right) = 216$.

Combining all three classes of bent-sequences in Vilenkin-Chrestensen basis, we obtain the full class of bent-sequences of cardinality $J = 162 + 108 + 216 = 486$. Previously, such results could only be obtained by a brute force method.

Note that, unlike binary analogs, bent-sequences of many-valued logic exist for lengths $N = 2^k, k \in \mathbb{N}$. Of particular interest is the construction of bent-sequences for odd values of k.

The research carried out in [10] made it possible to classify the complete set of bent-sequences of length $N = 9$ in the Vilenkin-Chrestensen basis, depending on their weight structure into 6 classes

$$\begin{bmatrix} \{144\}(3) & \{522\}(18) \\ \{414\}(3) & \{252\}(18) \\ \{441\}(3) & \{225\}(18) \end{bmatrix} \quad (9)$$

where the numbers in curly brackets indicates, respectively, the number of characters "0", "1" and "2" in the bent-sequence, and the numbers in parentheses indicates the number of bent-sequences having this structure.

Definition 2. A set of three bent-sequences in Vilenkin-Chrestensen basis is called a triple set if the concatenation of their truth tables is symbolically balanced, i.e. number of characters "0" equals to the number of characters "1" and is equal to the number of characters "2".

We propose a gamma generator scheme based on the properties of a complete class of bent-sequences divided into 2 types of triple sets (Fig. 2).

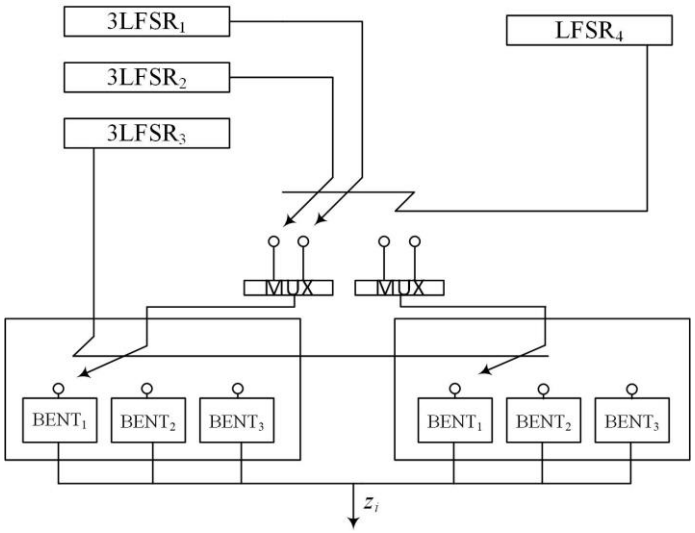


Fig. 2. Gamma generator based on triple sets of bent-sequences

The gamma generator scheme based on triple sets of bent-sequences, shown in Fig. 2 consists of two ternary LFSR that generate input values for a bent-sequence, as well as a single ternary LFSR that selects a 3-bent sequence within the triple set. The circuit contains one binary LFSR, which selects one of the two possible triple sets at each clock cycle.

Researches of the proposed scheme confirmed it's high stochastic and cryptographic quality [10].

4. Conclusion, open problems and directions for further research

The performed research made it possible to establish that the use of the principles of many-valued logic is a promising basis for further development of both block and stream cryptographic algorithms. In this case, the functions of many-valued logic are best suited to modern concepts of multi-core data processing and quantum computing. The task of future research in this direction seems to be important for us.

Despite the positive results obtained in the application of the principles of many-valued logic in cryptography, this question undoubtedly still requires significant attention of the scientific community.

Currently, issues of building of high-quality S-boxes of length $N = p^k$ are poorly covered in the literature. Research of the dynamics of change of parameters of S-boxes with the growth of their length is also an actual problem.

Methods of construction of P-boxes and methods of diagnosis of their cryptographic quality are not available in the literature, not only for many-valued logic, but even for the binary case. Vital for the current state of development of cryptography is the task of creating of a set of criteria for diagnostic of the cryptographic quality of P-boxes and development of effective methods of synthesis of these important cryptographic primitives.

The major problem of many-valued encryption is the development of many-valued schemes of such cryptographic primitives as affine transform blocks, cyclic shifts blocks, as well as perspective controlled F-boxes [11].

On the other hand, the development of gamma generators necessitates research of the already determined perfect algebraic constructions and further search for new perfect algebraic constructions of many-valued logic. Thus, an important problem is the description of the classes of many-valued bent-functions (in particular, of an odd number of variables), the generalization of the definition of perfect binary arrays to the many-valued case, as well as research of many-valued de Bruijn sequences.

Note also the task of developing more efficient methods of representation of binary data for processing in many-valued logic systems, and representation of many-valued logic data in binary form. The development of these methods may be connected to the fundamental researches performed in [12].

The solution to these problems, of course, will not only significantly improve the proposed concept of many-valued logic encryption algorithm with a variable block length, but will lead to a better understanding and the generalization of the theory of binary cryptography and further development of systems of binary data encryption.

Reference

1. Shannon, C.E. (1945) A Mathematical Theory of Cryptography. Bell System Technical Memo. MM 45-110-02.
2. O.N. Zhdanov, A.V. Sokolov (2015), The encryption algorithm with variable block fragmentation [Original text in Russian], Collection of scientific papers on the results of international scientific-practical conference "Problems and achievements in science and technology", Omsk, Russia, Issue 2, P. 153—159.

3. K.O. Zakharova. Research of statistical parameters of the encryption algorithm with different block fragmentation. Materials of the XXI International Scientific and Practical Conference, dedicated to the memory of the general designer of rocket-space systems Academician M.F. Reshetnev, November 8-11, 2017, Krasnoyarsk, part 2, p. 400-401.
4. Mitrashchuk V.V. Protocol of secure data exchange based on encryption algorithm with alternating block fragmentation The youth. Society. Modern science, technology and innovation. 2017. No. 16. P. 299-301.
5. Zhenxian Fang, Ying Liu: Ternary Error Correcting Codes, Chinese Science Abstracts Series A, 1995, P.54.
6. S.O. Gnatyuk, T.O. Zhmurko, V.M. Kinzeryavy, NA Siyilova Method for quality evaluation of trit pseudorandom sequence to cryptographic applications. Information Technology and Security. – 2015. – Vol. 3. – No 2(5). – P. 108-116.
7. O.N. Zhdanov, A.V. Sokolov, The encryption algorithm with variable block fragmentation [Original text in Russian], Collection of scientific papers on the results of international scientific-practical conference "Problems and achievements in science and technology", Omsk, Russia, Issue 2, P. 153—159.
8. O. N. Zhdanov, A.V. Sokolov. Block symmetric cryptographic algorithm based on principles of variable block length and many-valued logic. Far East Journal of Electronics and Communications. Vol. 16. No. 3. P. 573 – 589.
9. Behrooz Parhami Computer Arithmetic: Algorithms and Hardware Designs, New York: Oxford University Press, 2000, 510 p.
10. Mazurkov, M.I., Sokolov, A.V., Barabanov, N.A. (2016). Synthesis method for bent sequences in the Vilenkin-Chrestenson basis. Radioelectronics and Communications Systems, vol. 59, no. 11, pp. 510-517.
11. H.N. Zui, N.A. Moldovyan, R.S. Fakhrutdinov new class of controlled elements f 2/3 for the synthesis of high-speed block ciphers [Original text in Russian], Problems of information security, 2011, N. 1, P. 10—18.
12. A. Stakhov, Brousentsov's ternary principle, Bergman's number system and ternary mirror-symmetrical arithmetic, The Computer Journal, 2002, Vol. 45, No. 2, P. 221–236.