

V. A. Luzhetskii, Dc. Sc. (Eng.), Prof.; A. V. Ostapenko

BLOCK CIPHER ON THE BASE OF PSEUDO-NONDETERMINISTIC SEQUENCE OF CRYPTO PRIMITIVES

There had been suggested a new approach to the realization of block cipher, which is based on the use of pseudo- nondeterministic sequence of cryptoprimitives and decomposition of a message into blocks of different length on each of transfer rounds.

Key words: symmetrical block cipher, cryptography, pseudo-nondeterministic sequence.

Introduction

Constantly increasing requirements to cipher, consideration of modern element base, creation of new types of attacks stipulate for the necessity in development and research of new approaches to building new block ciphers.

According to the realization of ciphering function there had been singled out the block cipher, built on the base of Feistel network [1, 2, 3], alteration of procedures of replacement and globing (SP-networks) [1, 4, 5], structure "Square" [1, 6] and controlled operation [7].

Block ciphers on the base of Feistel networks suffer from a drawback from the point of view of speed and simplicity of operations flow, since only a half of block of input message is been ciphered [8]. Use of table substitutes in a quality manner influences the speed of ciphering, based upon the SP-networks and structure "Square".

The Objective of the work

The objective of the paper is to improve the speed of block ciphering of data, insuring the set level of cryptographic stability by developing block cipher on the base of pseudo- nondeterministic cryptoprimitives.

Task setting

Any block cipher may be described by the following algebraical model:

$$\Sigma = \{\mathbf{M}, \mathbf{K}, \mathbf{C}, \mathbf{E}, \mathbf{D}\},$$

where $\mathbf{M} = \{m_j\}$ – set of open messages ($j = j \dots J$); $\mathbf{K} = \{k_i\}$ – set of keys ($i = i \dots I$); $\mathbf{C} = \{c_j\}$ – set of crypts; $\mathbf{E} = \{E_{ki}\}$ – set of algorithms for encryption; $\mathbf{D} = \{D_{ki}\}$ – set of algorithms for decryption.

Set \mathbf{E} is formed by the reflection of $\mathbf{M} \times \mathbf{K} \rightarrow \mathbf{C}$, and E_{ki} is described by function $F(k_i, m_j)$. Reflection $\mathbf{C} \times \mathbf{K} \rightarrow \mathbf{M}$ forms the set \mathbf{D} of algorithms for decryption D_{ki} . Some decryption algorithms are described by function $F^{-1}(k_i, m_j)$.

Usually, algorithms for encryption and decryption are iterational and consist of sequence R of transformations (rounds) [9]. Each transformation round uses a separate round key k_r , which is received from the general secret key $k \in \mathbf{K}$. Proceeding from this, crypt $c \in \mathbf{C}$ for the open message $m \in \mathbf{M}$ and key k is received as a result of execution of sequence of round transformations:

$$c_r = F(k_r, c_{r-1}), \quad (1)$$

where c_r – enciphered data after the r -th transformation ($c_1 = m, c = c_R, r = \overline{1 \dots R}$); $F(k_r, c_{r-1})$ – function of round transformation.

Correspondingly the open text m for the crypt c and key k is received in the result of transformation:

$$m_r = F^{-1}(k_r, m_{r-1}), \quad (2)$$

where m_r – decrypted data after the r -th transformation ($m_1 = c, m = m_R$).

Algebra of secret system described by K. Shannon [9, 10] describes two methods for combination of secret systems to receive the new secret system.

Method which is called “weighted sum” consists of previous choice of the system T_i with some probability p_i . After the choice is been made, the system T_i , is used in correspondence with its definition. And as this takes place, the new system has a set of reflections, it consists of an aggregate of all sets of reflection, used secret systems with probabilities of their use, which equal the product of probability of choice of these reflections and probability of choice of secret system:

$$S = \sum_{i=1}^n p_i \cdot T_i, \quad \sum_{i=1}^n p_i = 1, \quad (3)$$

where S – combined secret system; T_i – i -th secret system from the set n of secret systems; p_i – Probability of choice of the i -th secret system.

Full key of the system S indicates the system which is used and the key it is used with.

Method “product” consists of the sequent use of secret systems under condition that the system T_{i+1} has the definition area (language space) which may be compared with the definition area (crypt space) of the system T_i , that is:

$$S = \prod_{i=1}^n T_i. \quad (4)$$

And the full key of the system S consists of the keys of all the systems used.

The analysis of the considered approaches to the building block ciphers shows that ciphers on the base of Feistel networks, structure “Square” may be described as the product of secret systems (3) and T_i may be considered as the transformation round.

Block ciphers on the base of controlled operations may be described by the product of systems (3). In each round, in this case there being executed different transformations with fixed sequence but with transient operations parameters. For example, execution of operation of cycle shift to the right by 3 digits in the first round and by 7 digits in the second.

These transformation are described by the same function, but the results of previous transformations and round key is used as an argument.

That is, the algorithm of block ciphers is determined by the size of the key, complexity of the operation performed or number of rounds during the use of simple operations.

To reduce the number of rounds, which means the increase in speed of encryption, using the set of simple operations, we suggest to use non-deterministic sequence of operations (from the point of view of intruder) which is determined by a secret key.

Since the encryption will use special set of the algorithms, in which the sequence of the operations is determined by the key, then in future these algorithms will called pseudo nondeterministic. Such an approach to encryption will encourage the intruder to sort out all possible encryption algorithms.

Idea of building block cipher

Block cipher is suggested to be on the base of using pseudo-nondeterministic algorithms. In general case they consist of a set of functions of transformation F_1, F_2, \dots, F_L and operations which,

using the secret key k form the sequence $a(1), a(2), \dots, a(i)$ [10].

Procedure of encryption of open message m using k consists in application of function F in order, determined by the sequence $a(i)$:

$$c = F_k(m) = F_{a(i)}(\dots(F_{a(2)}(F_{a(1)}(m)))\dots) \quad (5)$$

Thus, encryption algorithm on the base of pseudo-nondeterministic sequences of cryptoprimitives consists of known transformations, which enable to theoretically evaluate the stability of cipher, according to the Kerckoffs's principle, but the order of their use is determined by secret key k and is non-deterministic process from the point of view of cryptanalyst.

The idea of the suggested approach consists in the following: the transformations in each of rounds of elementary transformations (cryptoprimitives), the set and sequences of execution of which is determined by specific set of features which are formed from key information.

From the point of view of secret system of Shannon's, this block cipher may be presented as a combination of "weighted sum" (3) and "product" (4), that is:

$$S = \prod_{i=1}^n (\sum_{j=1}^m p_{ij} \cdot T_{ij}), \sum_{j=1}^m p_{ij} = 1.$$

Proceeding from the above, we suggest the following model of block cipher

$$\Sigma = \{\mathbf{M}, \mathbf{K}, \mathbf{F}_E, \mathbf{F}_D, \mathbf{Q}, \mathbf{P}, \mathbf{C}\}, \quad (6)$$

where $\mathbf{M} = \{m_j\}$ – set of open messages; $\mathbf{K} = \{k_i\}$ – set of keys; $\mathbf{F}_E = \{F_{Eki}\}$ – set of transformation functions for encryption; $\mathbf{F}_D = \{F_{Dki}\}$ – set of transformation functions for decryption; $\mathbf{Q} = \{q_p\}$ – set of factors ($p = 1 \dots P$); $\mathbf{B} = \{b_h\}$ – set of basic operations ($h = 1 \dots H$); $\mathbf{C} = \{c_j\}$ – set of crypts.

The main aspects of the suggested approach is the realization of function of formation of identifiers \mathbf{Q} and realization of choice of basic operations \mathbf{B} .

Identifier $q \in \mathbf{Q}$ is a set of operations \mathbf{B} , which compose the round function F , therefore the transformation on the specific stage of an algorithm will look:

$$P_r = F_q(c_q, k_r)$$

where P_r – round transformation; F_q – function of round transformation is determined by identifier q ; c_q – information which is processed in the current round.

Thus the algorithm of block ciphering \mathbf{A} may be presented by an aggregate of round transformations P_r , function, transformation of which as well as the structure of the data, processed by them, dependent on identifiers q :

$$\mathbf{A} = \{P_1, P_2, \dots, P_R\}.$$

Process of transformation identifiers' formation stipulates for determination of the following identifiers, which are to be singled out on each stage of encryption from the key information (current round subkey k_r):

- Number of subblocks Q_{pb} ;
- Bitwise of the subblock Q_{rb} (bit);
- Function type of round transformation Q_{vp} .

Each of these identifiers is a whole number within a set limits.

The structure of the processed block for the given cipher consists of the specific number of subblocks of variable length. The number of blocks and their length shall be determined by the identifiers Q_{pb} and Q_{rb} . Considering the above, the length of the block N_b :

$$N_b = Q_{pb} \cdot Q_{rb}.$$

Fig. 1 presents the sample of division of the processed information on blocks of variable length

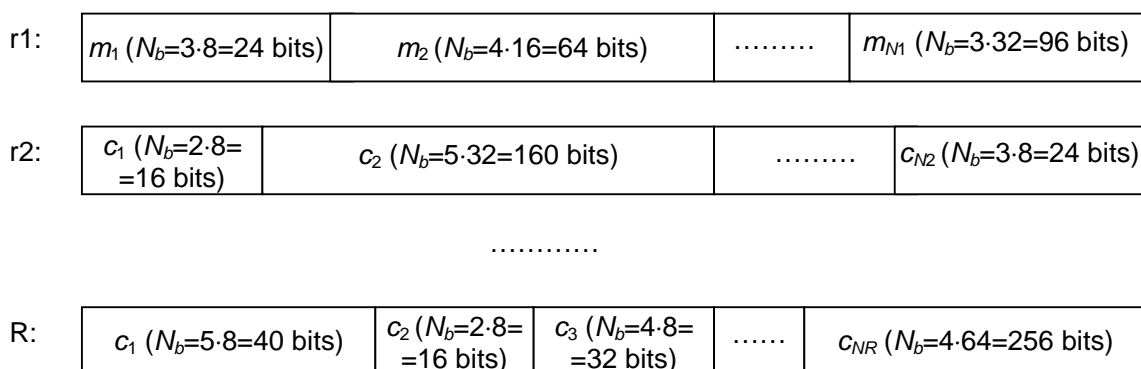


Fig. 1. Scheme of division into blocks of variable length

The peculiarities of the suggested approach stipulate for a big number of possible modifications of algorithms of block ciphering. The selected range of identifier's values enables to build N_m of different algorithms for one round of transformation:

$$N_m = Q_{pb} \cdot Q_{rb} \cdot Q_{vp}.$$



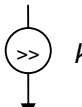
Uncertainty for an intruder in the specific sequence of cryptoprimitives in the specific algorithm of encryption practically disable the previous research of statistic peculiarities of each of them which significantly complicates the task of cryptoanalyses.

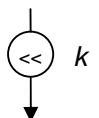
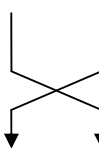
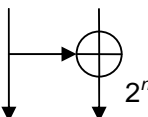
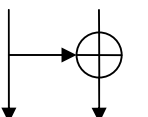
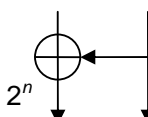
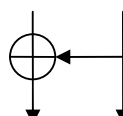
Basic operation for pseudo-nondeterministic block cipher

To build the pseudo-nondeterministic algorithm, the authors suggest a number of basic operations B, consisting of two kinds of operations: one-operand and two-operand. One operand operations are executed on one subblock of data (cyclic shift by k bit inversion, absence of transformation). Two-operand operations are executed on two subblocks of data (addition on module 2, addition on module 2^n , rearrangement of subblock).

Schematic designation of the suggested set of basic operations and their mnemonic description is given in table 1.

Table 1

Basic operations		
Name of operation	Schematic designation	Mnemonic designation
One-operand operations		
Absence of transformation		NOP
Data inversion		NOT
Cycle shift to the right on k bit		LLC

Cycle shift to the left on k bit		RLC
Two-operand operations		
Blocks rearrangement		PR
Two-operand lefthandside operations		
Addition on module 2^n		L^n
Adding on module 2		L^2
Two-operand righthandside operations		
Adding on module 2^n		R^n
Adding on module 2		R^2

The above operations allow to build the big number of cryptoprimitives and their modifications for operation in block cipher.

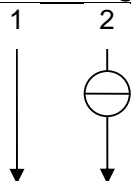
Let's consider the variants of the possible transformations of block cipher using the presented set of basic operations. Let's introduce some designation:

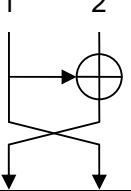
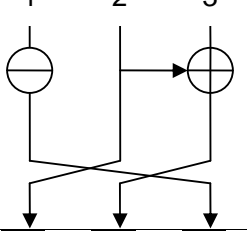
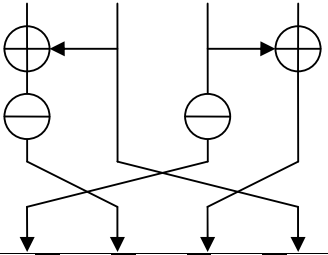
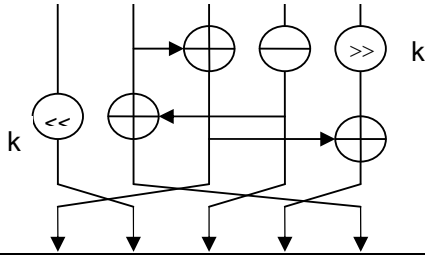
P – transformation; O_a – execution of one-operand operation on subblock a ($a = 1 \dots Q_{pb}$); D_{ab} – execution of two-operand operation on subblocks a and b ($b = 1 \dots Q_{pb}, b \neq a$); PR_{ab} – rearrangement of subblocks a and b ; $||$ – parallel execution of actions; \rightarrow – sequence execution of actions.

Samples of possible transformation for different number of subblocks and their schematic mnemonic description are presented in table 2.

Table 2

Designations of transformations

Schematic designation	Mnemonic designation
	$P = \text{NOP}_1 \text{NOT}_2$

	$P=L_{12}^2 \rightarrow PR_{12}$
	$P=(NOT_1 L_{23}^2) \rightarrow PR (PR_{12} \rightarrow PR_{23})$
	$P=(R_{12}^2 L_{34}^2) \rightarrow$ $\rightarrow (NOT_1 NOP_2 NOT_3 NOP_4) \rightarrow$ $\rightarrow PR(PR_{23} \rightarrow PR_{12} \rightarrow PR_{32})$
	$P=(NOP_1 R_{23}^2 NOT_4 RLC_5) \rightarrow$ $\rightarrow (LLC_1 L_{24}^2 R_{35}^2) \rightarrow$ $\rightarrow PR (PR_{23} \rightarrow PR_{12} \rightarrow PR_{34} \rightarrow PR_{45})$

The formed set of basic operation B is the basic one for round transformations with different structure and the suggested mnemonic description of operations determines their structure.

The use of the suggested idea of block cipher allows to achieve the corresponding level of cryptographic stability of block ciphers with the determined structure, due to the use of pseudo-nondeterministic sequences of cryptoprimitives. This allows to decrease the number of rounds of cipher R and simplify the function of round transformation F , using operations, which are quickly made on modern processors, without the loss of cryptostability. The above allows to achieve the increase in speed of block ciphering.

Conclusions

There had been suggested the new approach to the realization of block cipher, which is based on use of pseudo-nondeterministic sequence of cryptoprimitives and division of message into blocks of variable length on each round of transformation. This allows to complicate the break of the cipher, since it requires sorting out all the possible combinations of basic operations on each of the rounds and all possible variants of message division into blocks and subblocks.

REFERENCES

1. Аграновский А. В. Практическая криптография: алгоритмы и их программирование / А. В. Аграновский, Р. А. Хади. – М.: СОЛОН-Пресс, 2002. – 256 с.
2. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях / М. А. Иванов. – М.: КУДИЦ-ОБРАЗ, 2001. – 346 с.

3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке Си. / Б. Шнайер. – М.: ТРИУМФ, 2003. – 816 с.: ил.
4. Kam J. Structured design of substitution-permutation encryption networks / J. Kam, G. Davida // IEEE Transactions on Computers. – 1979. – Vol. 28, №10. – P. 747.
5. Heys H. Substitution-permutation networks resistant to differential and linear cryptanalysis / H. Heys, S. Tavares // Journal of Cryptology. – 1996. – Vol. 9, №1. – P.1 – 19.
6. Daemen J. The block cipher SQUARE / J. Daemen, V. Rijmen, L. Knudsen // Fast Software Encryption: FSE'97, Israel, January 1997 / Computer Science. Springer – Verlag. – 1997. – Vol. 1267. – P. 149 – 165.
7. Молдовян Н. А. Криптография: от примитивов к синтезу алгоритмов. / Н. А. Молдовян, А. А. Молдовян, М. А. Ефремов. – СПб.: БХВ-Петербург, 2004. – 448 с.
8. Алферов А. П. Основы криптографии / А. П. Алферов, А. Ю. Зубов, А. С. Кузмин. – М.: Гелиос АРВ, 2001. – 479 с.
9. Шеннон К. Работы по теории информации и кибернетики / К. Шеннон – М., 1963. – 829 с.
10. Адигеев М. Г. Введение в криптографию. Ч.1. Основные понятия, задачи и методы криптографии / М. Г. Адигеев. – Ростов-на-Дону: Ростовский гос. ун-т, 2002. – 35 с.

Volodymyr Luzhetskyy – Doctor of Technical Sciences, Professor, Head of the Department for Information Protection.

Alina Ostapenko – post graduate student with the Department for Information Protection.
Vinnitsia National Technical University.