Evaluation of Cryptographic Primitives Security Based on Proximity to the Latin Square

Vladimir V. Palagushin, Anatoly D. Khomonenko
St.Petersburg, Russia
Petersburg State Transport University
vpalagushin@yandex.ru, khomon@mail.ru

Sergey E. Adadurov
JSC "Roszheldorproekt"
Saint Petersburg, Russia
czi_mpc@mail.ru

Abstract—**At the heart of the creation of modern cryptographic systems is the use of cryptographic primitives. This has as its main goal of providing high security created cryptographic primitives and cryptosystem. For the development of cryptographic primitives used various mathematical transformations. To evaluate the security of cryptographic primitives are used very different approaches. The paper proposes a universal approach to the assessment of security of any cryptographic primitives. Cryptographic primitive – algorithms of reversible transformation of the block of the data of the fixed size with use of a set of key parameters of the fixed size is offered. It shown that substitution is a base cryptographic primitive through which it is possible to express all the others. At the heart of the offered approach lies the theorem of C. Shannon that defines perfect secrecy for secret-key systems and shows that they exist. For perfect security receive it is necessary, that the size of a key was not less than size of the converted data and the key was in regular intervals distributed. Matrix representation of similar system is a Latin square – rectangular table, in each line and each column all elements are various. For maximum security of cryptographic primitives defined optimal parameters of the substitutions table. For a number of cryptographic primitives obtained analytical and prognostic assessment of their security based on proximity to the Latin square.**

I. INTRODUCTION

Most a powerful tool of protection of the data stored on memories of computers and passed on telecommunication networks, is the cryptosystems (cryptographic systems of protection of the information).

Protection of the data at use cryptosystem is provided with preservation unknown to the infringer defined component CSPI (a component of algorithm and (or) values of key parameters). Key parameter of quality CSPI is stability to attempts of the infringer to define components cryptosystem unknown to it. Such attempts we will name attacks on cryptosystem, and the parameter characterizing ability to resist by it – security cryptosystem.

Now information encryption algorithms are still actively developed. For example in [1] a modified hill cipher algorithm for encryption of data in data transmission is proposed. Algorithm considers a matrix key and executes a sequence of steps, which generates the sequence. This sequence is represented by m*m matrix. The algorithm takes m*m successive plain text letters represent them in matrix form. The computational over head is much more in public key algorithms.

There is a set of methods of crypto analysis of encryption algorithms. In particular, the most popular statistical techniques are differential, offered by Biham and Shamir [2] and linear, for the first time published Matsui [3].

New methods of crypto analysis and an estimation of their efficiency are actively developed. For example, Aoki in [4] present an algorithm that efficiently evaluates the security of byte-oriented ciphers against linear sum attack; shown the relationship between linear sum attack and higher order differential attack; shown the security of CRYPTON, E2, and RIJNDAEL against linear sum attack using the algorithm.

Rostovtsev and Mahovenko offers the new methods of crypto analysis based on rational and 2-adicheskom continuation of polynoms of Zhegalkin [5]. The method is based on the assumption that the true value of a bit key usually gives a continued increase in the objective function. To it there corresponds the equivalent statement that false value of bit of a key normally conducts to reduction the target Functions.

Currently, the evaluation of cryptosystem security often comes down to expert judgement. The strength of the encryption & Decryption process depends on the strength of sequence generated against crypto analysis. In work [6] some statistical tests like Uniformity tests, Universal tests & Repetition tests are tried on the sequence generated to test the strength of it. In work [7] Software cryptographic protocol for digital signature based on elliptic curves designed and implemented. The protocol encrypts messages, forming a digital signature, message transmission and decoding at the receiver. Resistant cryptographic protocol analyzed by several methods.

To check cryptographic protocols for resistance is widely used in the AVISPA package [8]. The AVISPA package integrates modern approaches to the analysis of protocols, including model checking, tree automata, temporal logic.

Symmetric block ciphers are the most widely used cryptographic primitives. Block ciphers used as basic components in the construction of hash functions, message authentication codes, pseudorandom number generators, as a part of various cryptographic protocols, etc. The article [9] presents an advanced method of finding the number of active substitutions that helps to estimate the security of encryption algorithms against related-key attacks.

We will consider some abstract cryptosystem. Its developers try proving that for given cryptosystem there is no more effective method of crypto analysis, than a method of full search of all possible values of key parameters. Show that similar search with use of modern computer aids will occupy long time and do a conclusion about practical security developed cryptosystem. During studying of algorithm cryptosystem by other experts and as a result science developments can be developed more effective methods of crypto the analysis considered cryptosystem that can essentially lower level of its security.

II. Cryptographic primitives

Now the quantity of the developed algorithms of systems of cryptographic protection of the information totals some hundreds. All of them can be considered as compound − consisting of a set simple components which name cryptographic primitives.

The cryptographic primitive (***CP***) represents algorithm of reversible transformation of the block of the data of the fixed size with use of a set of key parameters of the fixed size.

Now there is no scientifically well-founded data about necessary and sufficient structure, quantity and an order of use CP for synthesis cryptosystem, high security responding the requirement. Basically developers cryptosystem for security increase go by the way of complication of algorithms of cryptographic transformations of the data – increases in quantity used CP, dynamic change of an order of their use, etc. the Given complications lead to increase in time of data processing (reduction of speed of processing).

Security of cryptosystem as a whole added from security making it CP. In the report the universal criterion with which help it is possible qualitatively and quantitatively to estimate security of various types CP is offered.

It is possible to allocate the following basic types CP:

- Substitution;
- Shift;
- Program mathematical transformations.

CP various types can be applied with use of special operating key parameter or without it. In [10] examples of given types CP are in detail considered.

III. Substitution – a base cryptographic primitive

For an estimation of security of various types CP, it is necessary to enter some universal criterion on which it will be possible to compare them among themselves. We will show that *substitution is a base cryptographic primitive* through which it is possible to express all the others.

CP of any type carries out transformation of the block of the data of some fixed size with use of a set of key parameters as fixed size. Therefore any CP can be considered as «a black box» on which input two parameters (the block of the data of a plain text «D» and the block of the data of a key «K») and on an exit the block of the data of text cipher «C» turns out.

The block of the data of a plain text «D» can accept final quantity of values (for example, from 0 to M), and the block of the data of a key «K» also can accept final quantity of values (for example, from 0 to N). We will construct the *substitution table* (*ST*), containing N+1 lines and M+1 columns as follows. We will consistently to sort out and submit on input of CP all values of the block of the data of a plain text «D» and the block of the data of a key «K». Values of the block of the data of text cipher «C» received on exit CP we will place in corresponding elements of ST (the element line number corresponds to value of the block of a key, number of a column of an element corresponds to value of the block of the data of a plain text). Generated thus ST we will name ***equivalent ST*** (for considered CP) as the result of transformation of the block of the data with use CP and use equivalent ST will be identical, as is shown at Fig 1.

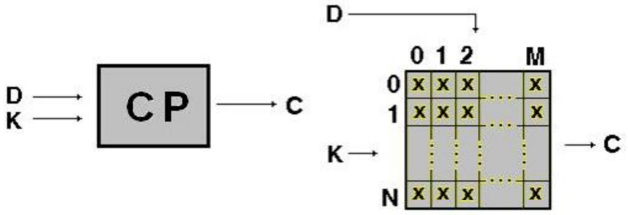

Fig.1. The equivalent substitution table of a CP

Let's consider and compare between themselves equivalent ST for the widest type CP, carrying out program-mathematical data conversions. Among CP the given type it is possible to select CP based only on use of the machine commands supposing reversible transformation of the data, and CP, the realizing specially developed mathematical methods of reversible transformation of the data.

To machine commands, which used at synthesis of cryptographic primitives, concern:

- Commands of integer addition and subtraction (ADD, SUB);
- The addition command on the module 2 (XOR);
- Multiplication and division commands (MUL, DIV, with certain restrictions);
- Commands of cyclic shift (ROL, ROR), and some other.

CP can be formed one or group of the listed commands.

Simple program transformation of the data (without the operating key parameter) set by some set of the machine commands supposing reversible transformation of the data. The example of direct and return program transformation for the block of 1 byte given in the size (register AL) by means of a set from three machine commands shown in the Table I.

At direct transformation each byte of a plain text (is located in register AL) develops with the fixed number cyclically displaced on two categories to the left and develops on the module 2 with the fixed number.

TABLE I. SIMPLE program TRANSFORMATION OF THE DATA

The direct transformation	The reverse transformation
ADD AL, 7 ROL AL, 2 XOR AL, 27	XOR AL, 27 ROR AL, 2 SUB AL, 7

In case of program transformation with operating parameter, machine commands operate not with the fixed numbers, and with values of the operating parameter. The example of direct and reverse program transformation for the block of 1 byte given in the size (register AL) and the operating key parameter (register AH) is shown in the Table II.

TABLE II. PROGRAM TRANSFORMATION OF THE DATA WITH OPERATING KEY PARAMETER

The direct transformation	The reverse transformation
ADD AL, AH ROL AL, 2 XOR AL, AH	XOR AL, AH ROR AL, 2 SUB AL, AH

The result of transformation of each byte of a plain text (is located in register AL) will depend in this case on value of the key parameter placed in register AH.

It is obvious that equivalent ST for all CP without the operating key parameter will represent a vector which quantity of elements will be 2^n , where n – quantity of bits of the processed block. An example of a fragment of equivalent ST for the simple program transformation presented in the Table I, is shown in the Table III.

TABLE III. A FRAGMENT OF THE EQUIVALENT ST FOR SIMPLE PROGRAM TRANSFORMATION

D	00	01	02	03	…	FD	FE	FF
C	07	3B	3F	33	…	0B	0F	03

Equivalent ST for shift with operating parameter and program transformation of the data with operating key parameter will represent the table at which will be 2^n Columns (n – quantity of bits of the processed block), and the quantity of lines is defined by quantity of values which the operating parameter can accept. The fragment of equivalent ST for program transformation with the operating key parameter, presented in Table II, is resulted in Table IV.

In [11] as CP managed control (MC) which realize specially developed mathematical method of reversible transformation of the data are considered.

TABLE IV. A FRAGMENT OF THE EQUIVALENT ST FOR TRANSFORMATION WITH OPERATING PARAMETER

K\D	00	01	02	03	…	FD	FE	FF
00	00	04	08	0C	…	F7	FB	FF
01	05	0A	0D	11	…	FA	FE	01
02	0A	0E	12	16	…	FD	02	06
03	0F	13	17	1B	…	03	07	0B
…	…	…	…	…	…	…	…	…
FD	0A	06	FF	FD	…	16	12	0E
FE	05	01	02	FA	…	11	0D	09
FF	00	FF	FB	F7	…	0C	08	04

In [11] the following classes MC are considered:

- $F_{2/1}$ – Possesses 2 bit input and an exit and a 1-bit operating input;
- $F_{2/2}$ – Possesses 2 bit input and an exit and a 2-bit operating input;
- $F_{3/1}$ – Possesses 3 bit input and an exit and a 1-bit operating input.

On MC input bits of the processed block of the data move, management carried out by means of bits of an operating variable (the operating key parameter), from exit MC bits of the transformed data unit turn out. Target values MC are described in kind Boolean functions from entrance values and values of an operating variable.

In [11] criteria to which should respond Boolean functions for maintenance of the maximum crypto security are resulted and proved.

Let's consider an example of a managed control $F_{2/2}$, resulted in [11], in which target values of Boolean functions (y_1, y_2) depend on values of two bits of the entrance data (x_1, x_2), of two bits of the operating parameter (v_1, v_2):

$$y_1 = v_1x_1 \oplus v_1x_2 \oplus v_2x_1 \oplus v_2x_2 \oplus v_1v_2 \oplus v_2 \oplus x_1 \oplus 1;$$
$$y_2 = v_1x_1 \oplus v_1x_2 \oplus v_2x_1 \oplus v_2x_2 \oplus v_1 \oplus x_2.$$

At direct transformation each two bits of a plain text transformed to two bits of text cipher by calculation of values resulted Boolean functions.

The equivalent table of substitutions for given MC is resulted in the Table V.

TABLE V. THE EQUIVALENT ST FOR AN OPERATING ELEMENT $F_{2/2}$

v_1	v_2	x_1	x_2	x_1	x_2	x_1	x_2	x_1	x_2
		0	0	0	1	1	0	1	1
0	0	1	0	1	1	0	0	0	1
0	1	0	0	1	0	0	1	1	1
1	0	1	1	0	1	1	0	0	0
1	1	1	1	1	0	0	1	0	0
		y_1	y_2	y_1	y_2	y_1	y_2	y_1	y_2

In the main loop (round) of encryption standard GOST 28147-89 [12] there are five cryptographic primitives. Of these only two are cryptographic primitives with operating parameter:

1. Add 32-bit data block with 32-bit block key data modulo 2^{32} .
2. Add two 32-bit data blocks modulo 2.

Standard AES-128 [13] only uses one cryptographic primitive with the Governor of the AddRoundKey() parameter: – add key round (addition modulo 2 all bits of the structure with the appropriate bits key).

Let's define optimum parameters of the table of substitutions from the point of view of achievement of maximum security CP.

IV. Optimum parameters of the table of substitutions

In [14] C. Shannon has theoretically proved existence of the "perfect" cryptographic systems possessing the maximum security to any attempts of crypto analysis. In [14] shown that for reception of "perfect privacy» it is necessary that the size of a key was not less than size of the transformed data and the key was in regular intervals distributed. Matrix representation of similar system is a Latin square, i.e. the rectangular table; in each line and in each column all elements are various.

Example of a fragment of a Latin square for the block of the data and the block of a key in the size In 1 byte it is resulted in the Table VI.

TABLE VI. A fragment of a Latin square

K\D	00	01	02	03	…	FD	FE	FF
00	00	01	02	03	…	FD	FE	FF
01	01	00	03	02	…	FC	FF	FE
02	02	03	00	01	…	FF	FC	FD
03	03	02	01	00	…	FE	FD	FC
…	…	…	…	…	…	…	…	…
FD	FD	FC	FF	FE	…	00	03	02
FE	FE	FF	FC	FD	…	03	00	01
FF	FF	FE	FD	FC	…	02	01	00

Assume the case of random uniformly distributed in the field of key values. Here any value of a byte of plain text when using the replacement table (see table VI – Latin square) can have an equal probability to convert to any other value in the range 0 – 255 (0x00-0hFF) values of block size in one byte. Thus, we provided with the necessary conditions of a perfect cryptosystem.

Thus substitution with operating parameter at which the substitution table is a Latin square provides the maximum security (under condition of the casual in regular intervals distributed key).

The quantity of Latin squares promptly increases with increase in the sizes of elements (the sizes of the block of a key and the data):

- For blocks in the size In 1 bit – 2 Latin squares;
- For blocks in the size In 2 bits – 576 Latin squares;
- For blocks in the size In 3 bits – more $1{,}08*10^{20}$ Latin squares;
- For blocks in the size in 4 bits – more $1*10^{125}$ Latin squares;

The quantity of Latin squares for the block in the size in 1 byte (8 bits) enormously and is not defined now.

V. The approach to estimation of security of a cryptographic primitive

As for any cryptographic primitive is possible to construct the equivalent table of substitutions it is offered to consider as criterion of security CP degree of conformity of its equivalent table of substitutions to a Latin square. If in columns of the equivalent table of substitutions of some CP meet identical elements it speaks about potential weakness corresponding CP. In the Table IV and V such elements are noted by allocation. The degree of compliance can quantified – analyzing the element values of the equivalent ST in each column. The more various elements in each column, the more equivalent ST corresponds to a Latin square.

Let us denote:

$$C = \{c_{i,j}\}, where\ i = 1,...,m; j = 1,...,n;$$
$$m \le n; m = 2^{LK}; n = 2^{L}$$

– equivalent ST for CP, that converts blocks of data using the L bit block key data size in LK bits.

Build matrix $B = \{b_{i,j}\}; where\ i, j = 1,...,n$ – set of matching entries in the columns of the equivalent ST ($b_{i,j} = 1$, if the element is in j-th column of the first or only time and $b_{i,j} = 0$ in other case):

$$b_{i,j} = \begin{cases} 0, & if(m < n \wedge i > m) \vee \begin{pmatrix} \underline{c_{i,j}} \in \{c_{k,j}\}, \\ i = \overline{2,m}, k = \overline{1,i} \end{pmatrix}; \\ 1, & if(i = 1) \vee \begin{pmatrix} \underline{c_{i,j}} \notin \{c_{k,j}\}, \\ i = \overline{2,m}, k = \overline{1,i-1} \end{pmatrix}. \end{cases}$$

Then the formula for determining the number of distinct elements in the columns of the equivalent ST is similar to the following:

$$K = \sum\nolimits_{j=1}^{n} \sum\nolimits_{i=1}^{n} b_{i,j} \ . \qquad (1)$$

The extent to which equivalent ST of cryptographic primitive with operating parameter (that translates data block size L in bits) to the optimal value (the Latin square of order 2^L) in a percentage can be calculated by the formula:

$$S_{Var}^{(L)} = \frac{K * 100}{2^{2L}} \% \ . \qquad (2)$$

If equivalent ST of some CP will correspond to a Latin square, the given indicator will accept value 100.

It is necessary to notice that equivalent ST for operations of integer addition and subtraction which meet often in algorithms various cryptosystem, represent Latin squares. The fragment of equivalent ST for operation of integer addition (ADD command) is resulted in the Table VI.

VI. The calculation experiment

Results of calculation of an offered indicator for some CP are resulted in the Table VII.

The proposed approach can used to evaluate the cryptosystem as a whole. For example, equivalent ST algorithm now in use in the RF cryptographic protection of given GOST 28147-89 [12] in a mode of simple replacement is a vector, at which 2^{64} Elements in the size on 64 bits, as is shown at Fig 2a.

Equivalent ST now in use in the USA of the standard of enciphering AES-128 [13] in a mode of the electronic code book (ElectronicCodeBook) as a vector, at which 2^{128} Elements in the size on 128 bits, as is shown at Fig 2б.

TABLE VII. Degree of conformity of equivalent ST of cryptographic primitives to a Latin square

Cryptographic primitive	**L**	$S_{Var}^{(L)}$
Software convert variable-key parameter		
ADD D,K; SUB D,K	8,16,32	100%
XOR D,K	8,16,32	100%
ROR D,K; ROL D,K	8	3,076%
ROR D,K; ROL D,K	16	0,024%
ROR D,K; ROL D,K	32	$7{,}45*10^{-7}$%
Example at Fig 3.	8	66.9 %
ГОСТ 28147-89		
ADD D2,K	32	100%
XOR D2,D1	32	100%
AES 128		
AddRoundKey() = XOR D,K	128	100%
An example of a source-controlled item		
$F_{2/2}$	2	81,25%

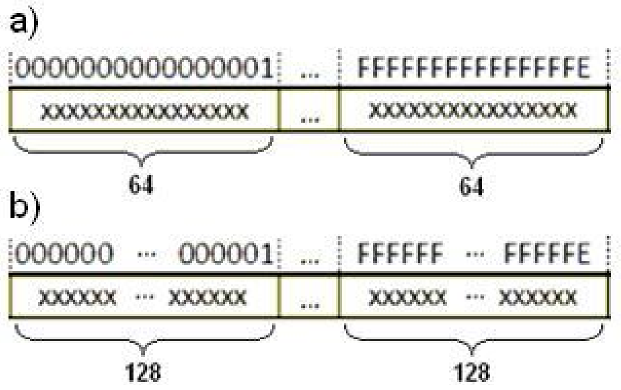

Fig. 2. Equivalent ST a) GOST; b) AES-128

Values of elements of vectors defined by concrete values used in algorithms key parameters. The kind considered equivalent ST does not correspond to a Latin square, therefore it is possible to draw a conclusion that security of GOST 28147-89 in a mode of simple replacement and AES-128 in a mode of the electronic code book, is low. The resulted estimation for low security of GOST 28147-89 proves to be true article [15] data.

VII. Conclusion

The article proposes a single, universal approach, which can be qualitatively and quantitatively assess the security of CP of various types. The given approach allows:

- To estimate security CP and cryptosystem as a whole for developed cryptosystem;
- To provide choice CP with the maximum security at synthesis new cryptosystem that can lead to essential reduction of quantity CP in synthesis of cryptosystem and to increase of speed of data processing at cryptographic transformations.

By working out new cryptosystem it is necessary to aspire to that equivalent TP cryptosystem as a whole corresponded to a Latin square, therefore without fail it is necessary to switch on in structure CP cryptosystem one or the several CP, equivalent ST which corresponds to a Latin square.

Further research should continue in the direction of a balance between the performance of the use of cryptosystem and its security. Thus it is necessary to use model queuing systems and queueing networks, allowing to predict the performance of functioning of information systems taking into account the time spending on information security. See, for example, [16-17].

References

[1] A.V.N. Krishna, Dr. A.Vinaya Babu. A modified hill cipher algorithm for encryption of data in data transmission // *Georgian Electronic Scientific Journal: Computer Science and Telecommunications.* 2007, No. 3 (14). – pp. 78-83.

[2] E. Biham, A. Shamir, Differential cryptanalysis of DES-like cryptosystems // *Advances in Cryptology — CRYPTO '90. LNCS. Springer–Verlag.* 1991. V. 537. pp. 2-21.

[3] M. Matsui, Linear cryptanalysis method for DES cipher // Advances in Cryptology — EUROCRYPT '93. 1994. *LNCS. Springer–Verlag.* V. 765. pp. 386–397.

[4] K. Aoki, Efficient Evaluation of Security against Generalized Interpolation Attack. Howard Heys and Carlisle Adams (Eds.) : *SAC'99, LNCS* 1758, 2000. pp. 135-146.

[5] A.G. Rostovcev, E.B. Mahovenko, Two approaches to the analysis of block ciphers // *Problems of Information Security. Computer Systems* // 2002. № 1. – pp. 49-54. (in Russian).

[6] A.V.N. Krishna, A.Vinaya Babu. Role of Statistical tests in Estimation of the Security of a New Encryption Algorithm // *International Journal of Advancements in Technology (IJoAT)* http://ijict.org/ Vol 1, No 1 (June 2010). pp. 13-25.

[7] S.G. Chekanov. Development, Implementation and Analysis of Cryptographic Protocol for Digital Signatures Based on Elliptic Curves // *Bulletin of the South Ural State University. Series ≪Mathematical Modelling, Programming & Computer Software≫,* 2013, vol. 6, no. 2, pp. 120-127. (in Russian).

[8] AVISPA URL: http://www.avispa-project.org.

[9] D. Kaidalov, R. Oliynykov, O. Kazymyrov. A method for security estimation of the spn-based block cipher against related-key attacks // *Tatra Mt. Math. Publ.* 60. 2014, 25–45.

[10] V.A. Palagushin The analysis of security of cryptographic primitive things. An information technology on railway transportation. *Materials of the fourteenth international scientifically-practical conference «INFOTRANS-2009».* – SPb., 2009. – pp. 185-193 (in Russian).

[11] M. A. Yeremeyev, A.A. Moldovjan, N.F.Moldovjan, Cryptography: from primitive things to synthesis of algorithms. – SPb: - BHV-Petesrburg, 2004. – 446 p.

[12] GOST 28147-89 Systems of processing of the information. Protection cryptographic algorithm of cryptographic transformation: http://citeseer.ist.psu.edu. Algorithm AES: http://www.nist.gov/ae.

[13] C.E. Shannon, Communication Theory of Secrecy Systems. *Bell Systems Technical Journal* 28, 1949, pp. 656-715.

[14] A.G. Rostovcev, E.B.Mahovenko, A.S.Filippov, A.A. Chechulin, On the strength of GOST 28147–89 // *Problems of Information Security. Computer Systems* // 2003. № 2. – pp.75-83.

[15] Yu.I. Ryzhikov, A.D. Khomonenko. Calculations for non-Markovian open networks with flow conversion // *Automatic Control and Computer Sciences.*, 23 (3), 1989, pp.12.

[16] A.D. Khomonenko, S.I. Gindin. Stochastic models for cloud computing performance evaluation. Conference: *Proceedings of the 10th Central and Eastern European Software Engineering Conference in Russia on - CEE-SECR'2014*, October 2014. DOI: 10.1145/2687233.2687256.