საქართველოს მეცნიერებათა ეროვნული აკადემიის მოამბე, ტ. 14, №1, 2021
BULLETIN OF THE GEORGIAN NATIONAL ACADEMY OF SCIENCES, vol. 15, no. 1, 2021

Informatics

New Symmetric Tweakable Block Cipher

Levani Julakidze[*], Zurab Kochladze[**], Tinatin Kaishauri[§]

[*]*Zhiuli Shartava Information Technology Laboratory, Faculty of Informatics and Control Systems, Georgian Technical University, Tbilisi, Georgia*
[**]*Department of Computer Science, Faculty of Exact and Natural Sciences, Ivane Javakhishvili Tbilisi State University, Tbilisi, Georgia*
[§]*Faculty of Informatics and Control Systems, Georgian Technical University, Tbilisi, Georgia*

(Presented by Academy Member Archil Prangishvili)

Modern cryptography is the cornerstone of computer and communications security. Its foundation is based on various concepts of mathematics such as number theory, polynomial algebra, probability theory, etc. In the paper, original method for construction of the new symmetric algorithm is presented and described. In order to obtain the method the appropriate material has been elaborated on: symmetric cryptosystem and tweakable block ciphers. In modern cryptography symmetric block ciphers, which are constructed based upon the principles of the classic cryptography, are irreplaceable while transferring large amounts of confidential information in the open channel. At the same time their capacities are limitless to the extent that it is possible to use them for various cryptographic constructions. General fault of the ciphers is their determination. In order to correct this fault today there are already existing so-called tweakable block ciphers. This direction is the news of the modern cryptography. In our paper the problem of construction of such cipher is overviewed by means of the Hill method. As it is known, Hill algorithm is one of the best methods to achieve diffusion. General attention in the paper is driven to realization of Hill algorithm in the way that, it is fast and presents necessary characteristic of the symmetric algorithm. *© 2021 Bull. Georg. Natl. Acad. Sci.*

Tweakable block cipher, Hill algorithm

As known, because the speed of open-key ciphers is very low, mainly symmetric block algorithms are used for protection of information confidentiality. In some cases, block ciphers substantially differ from each other by the architecture, as well as by the used operations and, often, by the number of rounds, but the result of their operation is always the same. Bit line of n length, the structure of which is determined by open text, using the key of k length, which also represents bit line of k length and using certain operations, after multiple iteration, again transfers into pseudo-random bit line of n length. Actually, mathematically, any block cipher may be presented as the function, depending on two variables

$$E : \{0,1\}^l \times \{0,1\}^k \longrightarrow \{0,1\}^n, \quad (1)$$

where $\{0,1\}^l$ denotes bit line of l length. And the values of k and n depend on specific algorithm of enciphering. Practically, for each fixed $K \in \{0,1\}^k$, K enciphering function represents shifting to $\{0,1\}^n$. As

we know, C. Shannon showed in his fundamental paper, that practically there exists the only theoretically unbreakable cipher of such type (one-time pad), successful operation of which requires fulfillment of the following conditions: the length of key must be equal to the length of the open text, the key must represent absolutely random sequence and the key must be used only once (that is why this cipher was called a one-time pad). Certainly, use of such cipher in everyday practice is very inconvenient. All other symmetric algorithms must be only computationally resistant to crypto-analytic attacks, which means that if the opponent has unlimited possibilities, he can always break such ciphers. However, in practice we do not encounter an opponent with unlimited possibilities, so, from the viewpoint of determination of algorithm security it is important to find quantitative correlations between the cryptoanalyst's possibilities and cipher resistance, which will allow us performing quantitative assessment of safety of symmetric ciphers to crypto-analytic attacks [1].

If the goal of the cryptoanalyst is computation of the key, then the analysis of security of block ciphers may be formulated as the following task: enciphering function $E_k(M)=C$, is given, where $K\in\{0,1\}^k$ is an unknown key. Meanwhile, couples of some q quantity of input and output values $(M_1, C_1),...(M_q, C_q)$ are known to the analyst and he tries to compute the key. In this case, block cipher will be safe, is the best attack, which can be performed by the opponent, requires such great number of q couples and/or time of computing t, which exceeds the cryptoanalyst's possibilities. This is the security towards key computation and shall be measured quantitatively using q and t parameters.

The fact that block cipher will be safe towards attacks in terms of key computation, does not mean that it will be secure in general, as C. Shannon showed in the above-mentioned paper, algorithm may admit leakage of some kind of information about open text. If enciphering algorithm admits leakage of such information, the cryptoanalyst will get a chance to break the algorithm completely after accumulation of sufficient information. Thus, if we want crypto-algorithm to be safe, we shall be able to prove that it is impossible to get any information on open text from ciphertext by computation means, owned by the opponent.

For hiding open text structure, the use of two types of transformation – confusion and diffusion – is the most effective. Confusion is the transformation, which aims at hiding the connection between the key and ciphertext, and diffusion aims at making each symbol of ciphertext dependent on all symbols of open text, which will allow hiding the structure of the open text. As it is impossible to use complex mathematical transformations in symmetric algorithms (it slows down fast operation of algorithm), substitution and transposition operations with multiple iteration are used in modern cryptography to achieve these goals.

Crypto-resistance of block ciphers is also substantially affected by the fact, that by their nature, block ciphers represent the determined system, i.e. one and the same open text always transfers into one and the same ciphertext using one and the same key, making it very easy for the cryptoanalyst to break the cipher.

There are attempts of overcoming of this shortcoming using ciphering regimes (mainly, CBC and CTR regimes, where initialization vector is used, allowing transformation of one and the same open text with one and the same key into different ciphertexts, but often use of one initialization vector is not sufficient to hide the structure of the open text well).

In 2002, the article of M. Liskov, R. Rivest and D. Vagner was published, proposing the idea of using initialization vector not in enciphering mode, but in algorithm itself, besides, not only once, in the beginning, as it happens in enciphering regime, but several times, in equal intervals, at different stages of iteration. It will allow better hiding of structure of open text in ciphertext. Such algorithms were called by the authors tweakable block ciphers [2,3].

The paper considers the possibility of building the new algorithm of this type, which, at the same time, will use famous Hill algorithm modificated by us, allowing very fast performance of diffusive transformation.

Hill Algorithm

In 1929, American mathematician Lester S. Hill, using linear algebra, created *n*-grammic enciphering algorithm, which allows dependence of one output symbol of ciphertext on n number of input symbols. For this purpose, he related the letters of the open text to figures from zero to twenty five, as in many ciphers of classic cryptography. Then he took *n* number of figures and announced them as vectors. To encipher these *n* figures (i.e. *n* number of letters of open text simultaneously), he took square matrix $n \times n$ and multiplied the vector by the matrix with module of twenty six. Again, he obtained the vector with length *n*, which represents ciphertext and each symbol of which depends on *n* symbol of input vector. It was the most important and substantial difference of Hill Algorithm from enciphering methods, existing before. To allow deciphering, the enciphering matrix must have reversed matrix with module twenty six. And sufficient condition for it is that the determinant of enciphering matrix must differ from zero and be inter-simple with the module basis.

E.g., if we want one output symbol of ciphertext to depend on three input symbols, we must take the matrix A:

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

Fig. 1. Matrix A.

So that $A \cdot A^{-1} = E$, where E is a identity matrix. We need to multiply this matrix by three-letter (transferred into numbers) trigram of the open text.

$$M \times A = C.$$

And deciphering will be performed using the formula:

$$\mathrm{C} \times \mathrm{A}^{-1} = \mathrm{M}.$$

Certainly, the bigger the size of enciphering matrix is, the more letters of the open text will participate in computation of one symbol of output ciphertext and the better the open text structure will be hidden in ciphertext, but it is quite complex to use Hill algorithm in the process of manual ciphering, consequently, in this case, the size of enciphering matrix is smaller, making it difficult to achieve the set goal.

At the first stage of development of computer cryptography Hill algorithm was rejected for the reason that multiplication of vector by the matrix is linear operation and if $n \times n$ matrix is used in the algorithm, only resolution of n^2 linear equation is required to break it; nevertheless, in recent years many papers appeared, where various modifications of Hill algorithm are used together with some non-linear operation. It makes it impossible to easily break the algorithm and maintain all positive features of Hill algorithm [4,5].

Modified Hill Algorithm

Our aim is to build new tweakable block enciphering algorithm, where Hill algorithm, modified by us, will be used for hiding the open text structure in efficient way.

In cryptoalgorithm, the 256-bit block is enciphered by 256-bit secret key. After entering in algorithm, the block, subject to enciphering, is represented through 4×4 matrix, which is referred to as the matrix of state (see Fig. 2), where each a_{ij} represents binary byte. The binary line, subject to enciphering, will be written in the matrix from the left to the right, horizontally.

$$M = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix}$$

Fig. 2. Matrix M.

All operations, performed in algorithm on the text, subject to enciphering, are performed on this matrix. In the paper, we touch only one operation, which ensures hiding of the open text structure in ciphertext in an efficient way. This operation may be written mathematically in a very simple way:

$$M \times A (\text{mod} 256),$$

where A represents matrix 4×4, which necessarily has a reversed matrix [6-8].

For further clarification, let us consider the 1st stage of our algorithm in details.

Our Algorithm

Let us assume that we have the following open text: If two wrongs don't make a right, try three. We will take the initial 16 symbols, transfer into ASCII code and represent as matrix A having 4×4 dimensions:

I	f	t	w	o	w	r	o
73	102	116	119	111	119	114	111
n	g	s	d	o	n	‘	t
110	103	115	100	111	110	96	116

73	102	116	119
111	119	114	111
110	103	105	100
111	110	96	116

Fig. 3. Matrix A.

Then we will take the next 16 symbols, which we again transfer into ASCII code and represent as matrix B having 4 × 4 dimensions:

m	a	k	e	a	r	i	g
109	97	107	101	97	114	105	103
h	t	,	t	r	y	t	h
104	116	44	116	114	121	116	104

109	97	107	101
97	114	105	103
104	116	44	116
114	121	116	104

Fig. 4. Matrix B.

N matrix, pre-computed by us:

-1	-2	-2	-2
2	-1	-2	2
1	1	1	2
-1	1	2	-1

Fig. 5. Matrix N.

Matrix A is multiplied by matrix N, as a result of which matrix A_1, having dimensions 4×4 is received. Matrix A_1 is brought by module of 256 and transferred in binary system:

128	-13	4	171
130	-116	-124	133
111	-108	-111	116
89	-120	-114	74

128	243	4	171
130	140	132	133
111	148	145	116
89	136	142	74

128	243	4	171	130	140	132	133
10000000	11110011	00000100	10101011	10000010	10001100	10000100	10000101
111	148	145	116	89	136	142	74
01101111	10010100	10010001	01110100	01011001	10001000	10001110	01001010

Fig. 6. Matrix A_1.

Matrix B is processed using the similar method (see Fig. 4.).

Matrix M, pre-computed by us:

1	1	1	2
-1	-2	-2	-2
2	-1	-2	2
-1	1	2	-1

Fig. 7. Matrix M.

Matrix B is multiplied by matrix M, as a result of which matrix B_1, having dimensions 4×4 is received. Matrix B_1 is brought by module of 256 and transferred in binary system:

125	-91	-97	137
90	-133	-135	73
-40	-56	16	-52
121	-140	-152	114

125	165	159	137
90	123	121	73
216	200	16	204
121	116	104	114

125	165	159	137	90	123	121	73
01111101	10100101	10011111	10001001	01011010	01111011	01111001	01001001
216	200	16	204	121	116	104	114
11011000	11001000	00010000	11001100	01111001	01110100	01101000	01110010

Fig. 8. Matrix B_1.

Deciphering

Deciphering is a reverse process of enciphering with slight difference. Instead of N and M matrices, used in the process of enciphering, we are using the corresponding N^{-1} and M^{-1} matrices, reversed with module of 256. The key, certainly, remains the same.

Reversed N^{-1} matrix of N enciphering matrix, using module of 256:

-1	2	-2	2
-2	-1	-2	-2
1	1	1	2
1	-1	2	-1

Fig. 9. Matrix N^{-1}.

Reversed M^{-1} matrix of enciphering M matrix, using module of 256:

-2	-1	2	2
-2	-2	-1	-2
1	1	1	2
2	1	-1	-1

Fig. 10. Matrix M^{-1}.

Conclusion

We touched only one operation, which ensures efficient hiding of structure of open text in ciphertext. In our case, 129 bits out of 256 bits experienced change, which is a very good result.

ინფორმატიკა

ახალი სიმეტრიული Tweakable ბლოკური შიფრი

ლ. ჯულაყიძე*, ზ. ქოჩლაძე**, თ. კაიშაური§

*საქართველოს ტექნიკური უნივერსიტეტი, ჭიათურის შარტავას სახელობის ინფორმაციული ტექნოლოგიების ლაბორატორია, ინფორმატიკისა და მართვის სისტემების ფაკულტეტი, თბილისი, საქართველო
**ივანე ჯავახიშვილის სახ. თბილისის სახელმწიფო უნივერსიტეტი, კომპიუტერული მეცნიერების დეპარტამენტი, ზუსტ და საბუნებისმეტყველო მეცნიერებათა ფაკულტეტი, თბილისი, საქართველო
§საქართველოს ტექნიკური უნივერსიტეტი, ინფორმატიკისა და მართვის სისტემების ფაკულტეტი, თბილისი, საქართველო

(წარმოდგენილია აკადემიის წევრის ა. ფრანგიშვილის მიერ)

თანამედროვე კრიპტოგრაფია წარმოადგენს ქვაკუთხედს კომპიუტერსა და საკომუნიკაციო უსაფრთხოებას შორის. ის ეფუძნება ისეთ მათემატიკურ ცნებებს როგორიცაა: რიცხვთა თეორია, ალბათობის თეორია, მრავალწევრთა ალგებრა და ა.შ. ნაშრომში წარმოდგენილი და აღწერილია ახალი სიმეტრიული ალგორითმის აგების ორიგინალური მეთოდი. ამ მეთოდის მისაღებად დამუშავებულ იქნა შესაბამისი მასალა, ისეთი როგორებიცაა: სიმეტრიული კრიპტოსისტემა და tweakable ბლოკური შიფრები. თანამედროვე კრიპტოგრაფიაში სიმეტრიული ბლოკური შიფრები, რომლებიც აგებულია კლასიკური კრიპტოგრაფიის პრინციპებზე, შეუცვლელნი არიან ღია არხში დიდი მოცულობის კონფიდენციალური ინფორმაციის გადაცემის დროს. ამავე დროს მათ იმდენად დიდი შესაძლებლობები გააჩნიათ, რომ შესაძლებელია მათი გამოყენება სხვადასხვა კრიპტოგრაფიული კონსტრუქციების ასაგებადაც. ამ შიფრების ძირითადი ნაკლია მათი დეტერმინირებულობა. სწორედ ამ ნაკლის გამოსწორების მიზნით, დღეს უკვე არსებობს ე.წ. tweakable ბლოკური შიფრები. ეს მიმართულება წარმოადგენს თანამედროვე კრიპტოგრაფიის ერთ-ერთ ყველაზე ახალ მიმართულებას. ჩვენს ნაშრომში განხილულია ასეთი შიფრის აგების პრობლემა ჰილის ალგორითმის გამოყენებით. როგორც ცნობილია, ჰილის ალგორითმი წარმოადგენს ერთ-ერთ საუკეთესო მეთოდს დიფუზიის მისაღწევად. ნაშრომში ძირითადი ყურადღება ექცევა ჰილის ალგორითმის რეალიზაციას ისე, რომ ალგორითმი იყოს სწრაფი, რაც წარმოადგენს სიმეტრიული ალგორითმების აუცილებელ თვისებას.

REFERENCES

1. Shanon C. (1948) Communication theory of secrecy systems. *The Bell System Technical Journal*, 27: 379-423, 623-656.
2. Liskov M., Rivest R.L. (2011) Tweakable Block Ciphers. *J. Cryptol*., 24: 588-613.
3. Halevi S., Rogaway P. (2003) A tweakable enciphering mode. *Advances in Cryptology -CRYPTO*. 27, 29: 1-33.
4. Lester S. Hill. (1929) Cryptography in an algebraic alphabet. *The American Mathematical Monthly,* 36, 6: 306-312.
5. Bibhudendra Acharya, Sarojkumar Panigrahy, Saratkumar Patra, Canapsti Panda (2009) Image encryption using advanced Hill cipher algorithm. *International Journal of Recent Trends in Engineering,* 1(1).
6. Julakidze L.E., Qochladze Z.I., Kaishauri T.V. (2015) Designing of a new tweakable block cipher by using the modified Hill's algorithm. *Georgian Engineering News*, 73 (1): 44-49 (in Georgian).
7. Julakidze L.E., Qochladze Z.I., Kaishauri T.V. (2015) The new symmetric tweakable block cipher. *Georgian Engineering News*, 73 (1): 50-56 (in Georgian).
8. Julakidze L.E., Qochladze Z.I., Kaishauri T.V. (2015) A possibility of constructing a new symmetric tweakable block cipher and a method of calculation of Pearsons's correlation coefficient. *Georgian Engineering News*, 76 (4): 39-45 (in Georgian).

Received May, 2020