ახალი Tweakable ბლოკური ალგორითმი

ლევანი ჯულაყიძე[1], ზურაბ ქოჩლაძე[2], თინათინ კაიშაური[1]

[1]საქართველოს ტექნიკური უნივერსიტეტი

[2]ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი

julakidzelevan08@gtu.ge, zurab.kochladze@tsu.ge, t.kaishauri@gtu.ge

რეზიუმე

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.

საკვანძო სიტყვები: კრიპტოგრაფია, ბლოკური შიფრი, მოდიფიცირებული ჰილის ალგორითმი.

1. შესავალი

როგორც ცნობილია, იმის გამო, რომ ღია გასაღებიანი შიფრების სიჩქარე ძალიან დაბალია, ინფორმაციის კონფიდენციალურობის დასაცავად ძირითადად გამოიყენება სიმეტრიული ბლოკური ალგორითმები. ბლოკური შიფრები ზოგჯერ არსებითად განსხვავდება ერთმანეთისაგან როგორც არქიტექტურით, ასევე გამოყენებული ოპერაციებით და ხშირად რაუნდების რაოდენობების მიხედვითაც, მაგრამ მათი მუშაობის შედეგი ყოველთვის ერთი და იგივეა. **n** სიგრძის ბიტური სტრიქონი, რომლის სტრუქტურაც განსაზღვრულია ღია ტექსტით, **k** სიგრძის გასაღების გამოყენებით, რომელიც ასევე წარმოადგენს **k** სიგრძის ბიტურ სტრიქონს და გარკვეული ოპერაციების გამოყენებით, მრავალჯერადი იტერაციის შემდეგ გადადის ისევ **n** სიგრძის ფსევდოშემთხვევით ბიტურ სტრიქონში. ფაქტობრივად, მათემატიკურად ნებისმიერი ბლოკური შიფრი შეიძლება წარმოვიდგინოთ როგორც ორ ცვლადზე დამოკიდებული ფუნქცია

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

სადაც $\{0,1\}^l$ აღნიშნავს l სიგრძის ბიტურ სტრიქონს. **k**-ს და **n**-ს მნიშვნელობები კი დამოკიდებულია დაშიფვრის კონკრეტულ ალგორითმზე.

პრაქტიკულად, თითოეული ფიქსირებული $K \in \{0,1\}^k$-თვის დაშიფვრის ფუნქცია წარმოადგენს გადანაცვლებას $\{0,1\}^n$-ზე. როგორც ვიცით, კ. შენონმა თავის ფუნდამენტურ ნაშრომში აჩვენა, რომ არსებობს ასეთი ტიპის ერთადერთი თეორიულად გაუტეხავი სიმეტრიული შიფრი (ერთჯერადი ბლოკნოტი), რომლის წარმატებული ფუნქციონირებისთვის აუცილებელია შემდეგი პირობების შესრულება: გასაღების სიგრძე უნდა იყოს ღია ტექსტის სიგრძის ტოლი, გასაღები უნდა წარმოადგენდეს აბსოლუტურად შემთხვევით მიმდევრობას და გასაღები უნდა გამოვიყენოთ მხოლოდ ერთხელ (ამიტომ უწოდეს ამ შიფრს ერთჯერადი ბლოკნოტი). ცხადია, რომ ასეთი შიფრის გამოყენება ყოველდღიურ პრაქტიკაში ძალიან მოუხერხებელია. ყველა დანარჩენი სიმეტრიული ალგორითმი კი შეიძლება იყოს მხოლოდ გამოთვლადად მედეგი კრიპტოანალიზური შეტევების მიმართ, რაც იმას ნიშნავს, რომ თუ მოწინააღმდეგეს გააჩნია შემოუსაზღვრავი შესაძლებლობები, მას ყოველთვის შეუძლია გატეხოს ასეთი შიფრები [1].

მაგრამ პრაქტიკაში ჩვენ არ გვხვდება მოწინააღმდეგე შემოუსაზღვრავი შესაძლებლობებით, ამიტომ ალგორითმის უსაფრთხოების დადგენის თვალსაზრისით მნიშვნელოვანია ვიპოვოთ რაოდენობრივი თანაფარდობები კრიპტოანალიტიკოსის შესაძლებლობებსა და შიფრის მედეგობას შორის, რაც მოგვცემს საშუალებას რაოდენობრივად შევაფასოთ სიმეტრიული შიფრების უსაფრთხოება კრიპტოანალიზური შეტევების მიმართ.

თუ კრიპტოანალიტიკოსის მიზანია გამოთვალოს გასაღები, მაშინ ბლოკური შიფრების უსაფრთხოების ანალიზი შეიძლება ჩამოვაყალიბოთ შემდეგი ამოცანის სახით: მოცემულია დაშიფვრის ფუნქცია $E_k(M) = C$, სადაც $K \in \{0,1\}^k$ არის უცნობი გასაღები. ამ დროს კრიპტოანალიტიკოსისათვის ცნობილია შესასვლელი და გამოსასვლელი მნიშვნელობების რაიმე q რაოდენობის წყვილები $(M_1, C_1),...(M_q, C_q)$ და ის ცდილობს გამოთვალოს გასაღები.

ამ შემთხვევაში ბლოკური შიფრი იქნება უსაფრთხო, თუ საუკეთესო შეტევა, რომელიც შეუძლია განახორციელოს მოწინააღმდეგემ მოითხოვს ისეთი დიდი რაოდენობის q წყვილებს ან/და გამოთვლის ისეთ დიდ t დროს, რაც აღემატება კრიპტოანალიტიკოსის შესაძლებლობებს. ეს არის უსაფრთხოება გასაღების გამოთვლის მიმართ და იზომება რაოდენობრივად q და t პარამეტრების საშუალებით.

ღია ტექსტის სტრუქტურის დასამალად ყველაზე ეფექტურია ორი გარდაქმნის - მიმოფანტვის **(confusion)** და დიფუზიის **(diffusion)** გამოყენება. მიმოფანტვა არის გარდაქმნა, რომლის მიზანია დამალოს კავშირი გასაღებსა და შიფროტექსტს შორის, ხოლო დიფუზიის მიზანია გახადოს შიფროტექსტის თითოეული სიმბოლო დამოკიდებული ღია ტექსტის ყველა სიმბოლოზე, რაც მოგვცემს საშუალებას დავმალოთ ღია ტექსტის სტრუქტურა. რადგანაც სიმეტრიულ ალგორითმებში შეუძლებელია გამოვიყენოთ რთული მათემატიკური გარდაქმნები (ეს ამცირებს ალგორითმის სწრაფქმედებას), ამ მიზნების მისაღწევად თანამედროვე სიმეტრიულ კრიპტოგრაფიაში გამოიყენება ჩანაცვლების და გადანაცვლების ოპერაციები მრავალჯერადი იტერაციებით.

ბლოკური შიფრების კრიპტომედეგობაზე არსებით ზეგავლენას ახდენს ის ფაქტიც, რომ თავისი ბუნებით ბლოკური შიფრები დეტერმინირებული სისტემაა, ანუ ერთი და იგივე ღია ტექსტი ერთი და იგივე გასაღების საშუალებით ყოველთვის გადადის ერთსა და იმავე შიფროტექსტში, რაც ძალიან უადვილებს კრიპტოანალიტიკოსს შიფრის გატეხვას.

ამ ნაკლის დაძლევას ცდილობენ დაშიფვრის რეჟიმების (ძირითადად **CBC** და **CTR** რეჟიმების) გამოყენებით, რომლებშიც გამოიყენება ინიციალიზაციის ვექტორი, რაც საშუალებას გვაძლევს ერთი და იგივე ღია ტექსტი ერთი და იგივე გასაღებით გარდავქმნათ

სხვადასხვა შიფროტექსტად, მაგრამ ერთი ინიციალიზაციის ვექტორის გამოყენება ხშირად არ არის საკმარისი ღია ტექსტის სტრუქტურის კარგად დასამალად.

2002 წელს გამოქვეყნდა მ. ლისკოვის, რ. რაივესტის და დ. ვაგნერის სტატია, რომელშიც წამოყენებულია იდეა გამოვიყენოთ ინიციალიზაციის ვექტორი არა დაშიფვრის რეჟიმში, არამედ თვით ალგორითმში, ამასთან არა ერთხელ, დასაწყისში, როგორც ეს ხდება დაშიფვრის რეჟიმში, არამედ რამდენჯერმე, თანაბარი ინტერვალებით იტერაციის სხვადასხვა ეტაპებზე. ეს მოგვცემს საშუალებას უფრო კარგად დავმალოთ ღია ტექსტის სტრუქტურა შიფროტექსტში. ასეთ ალგორითმებს ავტორებმა უწოდეს **tweakable** ბლოკური შიფრები [2-5].

ამ სტატიაში განხილულია, ჩვენს მიერ ერთი ასეთი ტიპის ახალი ალგორითმის აგების შესაძლებლობა. იგი იყენებს ჰილის ცნობილი ალგორითმის მოდიფიკაციას, რომელიც საშუალებას გვაძლევს ძალიან სწრაფად შევასრულოთ დიფუზიური გარდაქმნა.

2. ჰილის მოდიფიცირებული ალგორითმი.

ჩვენი მიზანია ავაგოთ ახალი tweakable ბლოკური დაშიფვრის ალგორითმი, რომელშიც ღია ტექსტის სტრუქტურის ეფექტურად დასამალად გამოვიყენებთ ჩვენს მიერ მოდიფიცირებულ ჰილის ალგორითმს.

კრიპტოალგორითმში ხდება **256** ბიტიანი ბლოკის დაშიფრვა **256** ბიტიანი სიდუმლო გასაღებით. ალგორითმში შესვლის შემდეგ დასაშიფრი ბლოკი წარმოიდგინება **4 × 4**-ზე მატრიცის საშუალებით, რომელსაც უწოდებენ მდგომარეობის მატრიცას (ფიგურა 1), სადაც თითოეული a_{ij} წარმოადგენს ორობით ბაიტს. დასაშიფრი ორობითი სტრიქონი ჩაიწერება მატრიცაში მარცხნიდან მარჯვნივ ჰორიზონტალურად.

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

ფიგ.1. მატრიცა M

ყველა ოპერაცია, რომელიც სრულდება ალგორითმში დასაშიფრ ტექსტზე სრულდება ამ მატრიცაზე. ამ სტატიაში შევეხებით მხოლოდ ერთ ოპერაცის, რომელიც უზრუნველყოფს ღია ტექსტის სტრუქტურის ეფექტურ დამალვას შიფროტექსტში. ეს ოპერაცია მათემატიკურად შეიძლება ჩავწეროთ ძალიან მარტივად:

$$M \times A (mod 256)$$

სადაც **A** წარმოადგენს მატრიცას **4 × 4**-ზე, რომლსაც აუცილებლად გაჩნია შებრუნებული მატრიცა [6-11].

უფრო მეტი თვალსაჩინოებისათვის განვიხილოთ ჩვენი ალგორითმის 1-ლი ეტაპი დეტალურად.

3. ჩვენი ალგორითმი.

ალგორითმის პარამეტრები:

ბლოკის სიგრძე - 256 ბიტი;

გასაღების სიგრძე - 256 ბიტი;

tweak შესასვლელის სიგრძე - 256 ბიტი;

A და **B** მატრიცები - 4×4 განზომილებიანი.

რაუნდში გამოყენებული ოპერაციები:

ბაიტების ჩანაცვლება მათი მულტიპლიკატორული შებრუნებულებით **GF(2^8)** ველში;

4×4 განზომილებიანი მატრიცის გამრავლება მატრიცაზე მოდულით 256;

გასაღებისა და დასაშიფრი ტექსტის შეკრება ოპერაციით **XOR**;

tweak მნიშვნელობის და ტექსტის შეკრება ოპერაციით **XOR**.

როგორც ზემოთ აღვნიშნეთ, ჩვენ შევეხებით მხოლოდ ერთ ოპერაცის, რომელიც უზრუნველყოფს ღია ტექსტის სტრუქტურის ეფექტურ დამალვას შიფროტექსტში.

დავუშვათ მოცემული გვაქვს ღია ტექსტი: **Sakartvelo means land of the Kartvelians.** ვიღებთ საწყის **16** სიმბოლოს, გადაგვყავს **ASCII** კოდში და წარმოვადგენთ **4 × 4** განზომილებიან **A** მატრიცად:

S	a	k	a	r	t	v	e
83	97	107	97	114	116	118	101
l	o	space	m	e	a	n	s
108	111	32	109	101	97	110	115

83	97	107	97
114	116	118	101
108	111	32	109
101	97	110	115

ფიგ.2. მატრიცა A

შემდეგ ვიღებთ მომდევნო **16** სიმბოლოს, რომელიც ასევე გადაგვყავს **ASCII** კოდში და წარმოვადგენთ როგორც **4 × 4** განზომილებიან **B** მატრიცად:

l	a	n	d	space	o	f	space
108	97	110	100	32	111	102	32
t	h	e	space	K	a	r	t
116	104	101	32	75	97	114	116

108	97	110	100
32	111	102	32
116	104	101	32
75	97	114	116

ფიგ. 3. მატრიცა B

ჩვენს მიერ წინასწარ გამოთვლილი **N** მატრიცა:

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

ფიგ.4. მატრიცა N

A მატრიცას ვამრავლებთ **N** მატრიცაზე, რის შედეგადაც მიიღება ისევ **4 × 4** განზომილებიანი A_1 მატრიცა. მიღებული A_1 მატრიცა დაგვყავს **256**-ის მოდულით და გადაგვყავს ორობით სისტემაში:

-73	79	-59	89
-127	129	-140	131
-189	28	-188	-51
-70	100	-56	113

183	79	197	89
129	129	116	131
67	28	68	205
186	100	200	113

183	79	197	89	129	129	116	131
10110111	01001111	11000101	01011001	10000001	10000001	01110100	10000011
67	28	68	205	186	100	200	113
01000011	00011100	01000100	11001101	10111010	01100100	11001000	01110001

ფიგ.5. მატრიცა A_1

ანალოგიური მეთოდით ვმოქმედებთ **B** მატრიცაზე.

ჩვენს მიერ წინასწარ გამოთვლილი **M** მატრიცა:

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

ფიგ.6. მატრიცა M

B მატრიცას ვამრავლებთ **M** მატრიცაზე, რის შედეგადაც მიიღება ისევ **4 × 4** განზომილებიანი B_1 მატრიცა. მიღებული B_1 მატრიცა დაგვყავს **256**-ის მოდულით და გადაგვყავს ორობით სისტემაში:

131	-96	-106	142
93	-260	-330	14
182	-161	-230	194
90	-117	-115	68

131	160	150	142
93	252	182	14
182	95	26	194
90	139	141	68

131	160	150	142	93	252	182	14
10000011	10100000	10010110	10001110	01011101	11111100	10110110	00001110
182	95	26	194	90	139	141	68
10110110	01011111	00011010	11000010	01011010	10001011	10001101	01000100

ფიგ.7. მატრიცა B_1

4. გაშიფვრა

გაშიფვრა დაშიფვრის შებრუნებული პროცესია მცირეოდენი განსხვავებით. დაშიფვრის დროს გამოყენებული **N** და **M** მატრიცის ნაცვლად ვიყენებთ **256**-ის მოდულით შებრუნებულ, შესაბამისად N^{-1} და M^{-1} მატრიცებს. გასაღები რა თქმა უნდა იგივე რჩება [9,10].

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

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

ფიგ.8. მატრიცა N^{-1} **მატრიცა M^{-1}**

5. დასკვნა.

ჩვენ შევეხეთ მხოლოდ ერთ ოპერაციას (ჩვენს მიერ მოდიფიცირებულს), რომელიც უზრუნველყოფს ღია ტექსტის სტრუქტურის ეფექტურ დამალვას შიფროტექსტში. ჩვენ შემთხვევაში **256** ბიტიდან **136** ბიტმა განიცადა ცვლილება, რაც ძალიან კარგი შედეგია. ალგორითმზე გრძელდება მუშაობა და უახლოეს ხანში გვექნება საშუალება მისი სრულყოფილი სახით წარმოდგენის.

გამოყენებული ლიტერატურა:

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. Levani Julakidze, Zurabi Kochladze, Tinatini Kaishauri. New Cryptographic Algorithm. PUBLISHING HOUSE „TECHNICAL UNIVERSITY“, შრომები/Works; (2025), N1(535), ISSN-1512-0996. https://doi.org/10.36073/1512-0996, https://www.isindexing.com, https://shromebi.gtu.ge/storage/archit/162/1(535).pdf.
7. Levani Julakidze, Zurab Kochladze, Tinatin Kaishauri. (2021) New Symmetric Tweakable Block Cipher. *BULLETIN OF THE GEORGIAN NATIONAL ACADEMY OF SCIENCES*. 15 (1): 13-19.
8. L.E. Julakidze, Z.I. Kochladze, T.V. Kaishauri (2017 by Nova Science Publishers, Inc.) New Tweakable Block Cipher. *Computer Science, Technology and Applications. Information and Computer Technology, Modeling and Control. ISBN: 978-1-53612-075-2.* 50: 505-513.
9. 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).
10. 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).
11. 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).

New Tweakable Block Algorithm

Levani Julakidze[1], Zurab Kochladze[2], Tinatin Kaishauri[1]

[1]Georgian Technical University

[2]Ivane Javakhishvili Tbilisi State University

julakidzelevan08@gtu.ge , zurab.kochladze@tsu.ge , t.kaishauri@gtu.geAbstract

Abstract

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.

Keywords: cryptography. block cipher. Modified Hill's Algorithm.