UDC 004
SCOPUS CODE 1701
https://doi.org/10.36073/1512-0996-2025-1-191-198

ახალი კრიპტოგრაფიული ალგორითმი

ლევანი ჯულაყიძე საინფორმაციო ტექნოლოგიების დეპარტამენტი, საქართველოს ტექნიკური უნივერსიტეტი, საქართველო, 0160, თბილისი, მ. კოსტავას 77
E-mail: julakidzelevan08@gtu.ge

ზურაბ ქოჩლაძე კომპიუტერული მეცნიერების დეპარტამენტი, ივ. ჯავახიშვილის სახ. თბილისის სახელმწიფო უნივერსიტეტი, საქართველო, 0128, თბილისი, ი ჭავჭავაძის გამზირი 1
E-mail: zurab.kochladze@tsu.ge

თინათინ კაიშაური საინფრომაციო სისტემები დეპარტამენტი, საქართველოს ტექნიკური უნივერსიტეტი, საქართველო, 0160, თბილისი, მ. კოსტავას 77
E-mail: t.kaishauri@gtu.ge

რეცენზენტები:

ი. ქართველიშვილი, ინფორმატიკისა და მართვის სისტემების ფაკულტეტის პროფესორი
E-mail: s.kartvelishvili@gtu.ge

თ. ასათიანი, ინფორმატიკისა და მართვის სისტემების ფაკულტეტის ასოცირებული პროფესორი
E-mail: t.asatiani@gtu.ge

ანოტაცია. თანამედროვე კრიპტოგრაფია არის ქვაკუთხედი 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, შეუცვლელია ღია არხში დიდი მოცულობის კონფიდენციალური ინფორმაციის გადაცემისას. ამავე დროს მათ იმდენად დიდი შესაძლებლობები აქვთ, რომ შესაძლებელია მათი გამოყენება სხვადასხვა კრიპტოგრაფიული კონსტრუქციის ასაგებადაც. ამ შიფრების ძირითადი ნაკლია მათი დეტერმინირებულობა. სწორედ ამ ნაკლის გამოსწორების მიზნით, დღეს უკვე არსებობს ე.წ. tweakable ბლოკური შიფ-

რები. ეს თანამედროვე კრიპტოგრაფიის ერთ-ერთი ყველაზე ახალი მიმართულებაა. 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 სიმეტრიული ალგორითმების აუცილებელი თვისებაა.

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

შესავალი

როგორც ცნობილია, იმის გამო, რომ ღიაგასაღებიანი შიფრების სიჩქარე ძალიან დაბალია, ინფორმაციის კონფიდენციალურობის დასაცავად ძირითადად გამოიყენება სიმეტრიული ბლოკური ალგორითმები. ბლოკური შიფრები ზოგჯერ არსებითად განსხვავდება ერთმანეთისაგან როგორც არქიტექტურით, ისე 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

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

სადაც $\{0,1\}^l$ აღნიშნავს **l** სიგრძის ბიტურ სტრიქონს. **k**-ს და **n**-ის 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 აქვს შემოუსაზღვრავი შესაძლებლობები, მას ყოველთვის შეუძლია გატეხოს ასეთი შიფრები [1].

მაგრამ პრაქტიკაში ჩვენ არ გვხვდება მოწინააღმდეგე შემოუსაზღვრავი შესაძლებლობებით, ამიტომ ალგორითმის უსაფრთხოების დადგენის თვალსაზ-

რისით მნიშვნელოვანია ვიპოვოთ რაოდენობრივი თანაფარდობები კრიპტოანალიტიკოსის შესაძლებლობებსა და შიფრის მედეგობას შორის, რაც საშუალებას მოგვცემს 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 შესაძლებელობებს. 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. ვინაიდან 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 იმავე გასაღების საშუალებით ყოველთვის გადადის ერთსა და იმავე შიფროტექსტში, რაც ძალიან უადვილებს კრიპტოანალიტიკოსს შიფრის გატეხას.

ამ ნაკლის დაძლევას ცდილობენ დაშიფვრის რეჟიმების (ძირითადად **CBC** და **CTR** რეჟიმების) მეშვეობით, რომლებშიც გამოიყენება ინიციალიზაციის ვექტორი, რაც საშუალებას გვაძლევს ერთი და იგივე ღია ტექსტი ერთი და იმავე 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, თანაც არა ერთხელ, დასაწყისში, როგორც ეს ხდება დაშიფვრის რეჟიმში, არამედ რამდენჯერმე, თანაბარი ინტერვალებით იტერაციის სხვადასხვა ეტაპზე. ეს მოგვცემს საშუალებას უფრო კარგად დავმალოთ ღია ტექსტის სტრუქტურა შიფროტექსტში. ასეთ ალგორითმებს ავტორებმა უწოდეს **tweakable** ბლოკური შიფრები [2,3].

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

ძირითადი ნაწილი

ჰილის მოდიფიცირებული ალგორითმი.

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

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

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

M მატრიცა

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

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

სადაც **A** არის მატრიცა **4 × 4**-ზე, რომლსაც აუცილებლად აქვს შებრუნებული მატრიცა [4-8].

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

ჩვენი ალგორითმი

დავუშვათ, მოცემული გვაქვს ღია ტექსტი: **What is Artificial Intelligence?** ვიღებთ საწყის **16** სიმბოლოს, გადაგვყავს **ASCII** კოდში და წარმოვადგენთ **(4 × 4)** - განზომილებიან **A** მატრიცად:

W	h	a	t	space	i	s	space
87	104	97	116	32	105	115	32
A	r	t	i	f	i	c	i
65	114	116	105	102	105	99	105

87	104	97	116
32	105	115	32
65	114	116	105
102	105	99	105

A მატრიცა

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

a	l	space	I	n	t	e	l
97	108	32	73	110	116	101	108
l	i	g	e	n	c	e	?
108	105	103	101	110	99	101	63

97	108	32	73
110	116	101	108
108	105	103	101
110	99	101	63

B მატრიცა

ჩვენ მიერ წინასწარ გამოთვლილი **N** მატრიცა:

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

N მატრიცა

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:

102	-65	-53	112
261	-22	-95	344
174	-23	-32	225
102	-105	-105	99

102	191	203	112
5	234	161	88
174	233	224	225
102	151	151	99

102	191	203	112	5	234	161	88
01100110	10111111	11001011	01110000	00000101	11101010	10100001	01011000
174	233	224	225	102	151	151	99
10101110	11101001	11100000	11100001	01100110	10010111	10010111	01100011

A_1 მატრიცა

ანალოგიური მეთოდით ვმოქმედებთ **B** მატრიცაზე.

ჩვენ მიერ წინასწარ გამოთვლილია **M** მატრიცა:

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

M მატრიცა

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:

-20	-78	-37	-31
88	-115	-108	82
108	-104	-106	111
150	-126	-164	161

236	178	219	225
88	141	148	82
108	152	150	111
150	130	92	161

236	178	219	225	88	141	148	82
11101100	10110010	11011011	11100001	01011000	10001101	10010100	01010010
108	152	150	111	150	130	92	161
01101100	10011000	10010110	01101111	10010110	10000010	01011100	10100001

B_1 მატრიცა

გაშიფვრა.

გაშიფვრა დაშიფვრის შებრუნებული პროცესია მცირეოდენი განსხვავებით. დაშიფვრისას გამოყენებული **N** და **M** მატრიცების 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

N^{-1} მატრიცა

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

M^{-1} მატრიცა

დასკვნა

ჩვენ შევეხეთ მხოლოდ ერთ ოპერაციას (ჩვენ მიერ მოდიფიცირებულს), რომელიც უზრუნველყოფს ღია ტექსტის სტრუქტურის ეფექტურ დამალვას შიფროტექსტში. ჩვენს შემთხვევაში 256 ბიტიდან 129 ბიტმა განიცადა ცვლილება, რაც ძალიან კარგი შედეგია

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. 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).
9. Julakidze L., Kochladze Z., & Kaishauri T. (2021). New Symmetric Tweakable Block Cipher. BULLETIN OF THE GEORGIAN NATIONAL ACADEMY OF SCIENCES. 15 (1): 13-19.
10. Julakidze L.E., Kochladze Z.I., & Kaishauri T.V. (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.

UDC 004
SCOPUS CODE 1701
https://doi.org/10.36073/1512-0996-2025-1-191-198

New Cryptographic Algorithm

Levani Julakidze Department of information technology, Georgian Technical University, Georgia, 0160, Tbilisi, 77, M. Kostava str.
E-mail: julakidzelevan08@gtu.ge

Zurabi Kochladze Department of Computer Science, Ivane Javakhishvili Tbilisi State University, Georgia, 0128, Tbilisi, 1, Ilia Chavchavadze Avenue
E-mail: zurab.kochladze@tsu.ge

Tinatini Kaishauri Department of iformation system, Georgian Technical University, Georgia, 0160, Tbilisi, 77, M. Kostava str.
E-mail: t.kaishauri@gtu.ge

Reviewers:

I. kartvelishvili, professor, faculty of informatics and control systems, GTU
E-mail: s.kartvelishvili@gtu.ge
T. Asatiani, associate professor, faculty of informatics and control systems, GTU
E-mail: t.asatiani@gtu.ge

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: block cipher; cryptography; modified Hill's Algorithm.

განხილვის თარიღი 15.11.2024
შემოსვლის თარიღი 25.12.2024
ხელმოწერილია დასაბეჭდად 25.03.2025