UDK 004.056.55

BARDOSHLI STATIK S-BOKSLARNI GENERATSIYALASH ALGORITMI

Xudoyqulov Z.T.[1], Rahmatullayev I.R.[2], Boyqo'ziyev I.M.[3]

[1] Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, Toshkent, O'zbekiston
[2] Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Samarqand filiali, Samarqand, O'zbekiston
[3] Renessans ta'lim universiteti, Toshkent, O'zbekiston
ilhom9001@mail.com

Annotatsiya. *Ushbu maqolada dinamik va kalitga bog'liq bo'lgan S-boxlarni generatsiyalash uchun oddiy va innovatsion sxema taklif qilingan bo'lib, mazkur algoritm yordamida generatsiyalangan almashtirish jadvalidan oqimli shifrlash algoritmini kriptotahlil usullariga baholashda foydalanilgan.*

Kalit so'zlar: *Oqimli shifrlash, Blokli shifrlar, S-box, chiziqli trigonometrik transformatsiya, kriptotahlil.*

I. KIRISH

Oqimli shifrlar odatda bir iteratsiyada bit yoki baytni shifrlashni amalga oshirib, kam hisoblash resursi mavjud va ma'lumotlarni uzatishda xatoliklar kuzatilishi mumkin bo'lgan sharoitlarda foydalanish uchun mo'ljallangan. Blokli shifrlar esa ma'lumotlarni o'zgartirishni oldindan belgilangan uzunlikdagi bitlar blokida qayta ishlash orqali amalga oshiradi. Amalga oshirishning qulayligi va joylashtirishning soddaligi tufayli blokli shifrlar odatda axborot xavfsizligi ilovalari uchun keng qo'llaniladi [1, 7-12].

Blokli shifrlar ma'lumotlarni himoyalashda o'rin almashtirish va o'rniga qo'yish deb nomlanuvchi ikkita asosiy akslantirishlar yordamida amalga oshiradi. O'rin almashtirish akslantirishi ma'lumotlar bitlari yoki baytlarini aralashtirishni, o'rniga qo'yish akslantirishi ochiq matn bitlari yoki baytlarini ochiq matnning bir qismi bo'lmagan boshqa bitlar yoki baytlar bilan almashtiradi. Eng mashhur blokli shifrlarda o'rniga qo'yish akslantirishi sifatida bir yoki bir nechta almashtirish jadvallaridan (S-boxlar) foydalaniladi. S-box zamonaviy blokli shifrlarning muhim tarkibiy qismi bo'lib, haqiqiy ma'lumotlarning (ochiq matn) o'zgarishiga katta hissa qo'shadi. S-box ochiq matn va shifrlangan matn o'rtasida chiziqli bo'lmagan aloqani yaratishda muhim rol o'ynab, bu blokli shifrlarning chiziqli bo'lmagan tarkibiy qismi hisoblanadi va chiziqli ishlaydigan, himoyaga kamroq hissa qo'shadigan tegishli blokli shifrning boshqa tarkibiy qismlariga nisbatan kriptotahlilchilar uchun natijaviy shifrlangan matnda ko'proq chalkashliklarni keltirib chiqaradi. Shunday qilib, tuzilmasida S-boxdan foydalanadigan shifrlash algoritmlarining xavfsizligi, kriptotahlillarga qarshi tura olishi tegishli S-boxning kriptografik parametrlariga bevosita bog'liqdir [2, 5, 6].

II. ASOSIY QISM

Shifrlashda ishlatiladigan S-boxslar statik va dinamik ko'rinishda bo'lib, har bir tasodifiy qiymat uchun har doim doimiy qiymatga ega bo'lgan S-box statik

S-box deb nomlanadi. O‘z tarkibida statik S-boxdan foydalanadigan shifrlar ma’lumotlarni yetarli darajada himoya qilmaydi degan farazlar ham mavjud bo‘lib, bu hujumchilarni qandaydir vositalar orqali bunday S-boxlar haqida ma’lumot olish imkoniyatiga egali va oxir-oqibat ochiq matnni tiklashi mumkinligi bilan izohlanadi. Dinamik S-boxlar shifrlash kaliti yordamida yaratilib, belgilangan talablar doirasida ishlab chiqilgan dinamik S-boxlar kriptografik xavfsizlikni kuchaytirish uchun juda katta imkoniyatga ega. Shuning uchun tadqiqotchilar tegishli shifrlash kaliti qiymatlaridan foydalangan holda yaxshi kriptografik xavfsizlikni ta’minlovchi dinamik S-boxlarni qurishning turli usullarini taqdim etganlar. Ushbu usullarda S-boxlarni loyihalashda elliptik egri chiziqlar, chekli maydon, xaotik tizimlar va boshqalar kabi turli xil matematika elementlaridan foydalanilgan. Xaotik dinamik tizimlar tasodifiy o‘xshashligi, ekstremal boshlang‘ich sharoitlarning sezgirligi va davriy emasligi tufayli xavfsiz S-boxlarni yaratish imkoniyatiyatiga ega. Ko‘plab mualliflar [3-6] turli usullarni qo‘llash orqali kuchli S-boxlarni yaratish uchun xaotik tizimlardan foydalangan. Giperxaotik tizimlar oddiy xaotik tizimlarga qaraganda mustahkamroq S-boxlarni qurish imkoniyatiga ega bo‘lib, [4-6] manbalarda mualliflar giperxaotik usullardan foydalangan holda mustahkam dinamik S-boxlarni generatsiyalagan.

Ushbu uslub juda oddiy va innovatsion chiziqli trigonometrik transformatsiyaga (ChTT) asoslanadi. Taklif etilayotgan ChTT dinamik bo‘lib, 8×8 o‘lchamdagi S-boxni generatsiyalash imkonini beradi. S-boxning dastlabki natijalari uning xavfsizligini oshirishning yangi sxemasini qo‘llash orqali yanada yaxshilanadi. Tabiatan dinamik bo‘lib, transformatsiya va ishlashni yaxshilash rejasi generatsiyalashda turli parametrlar o‘zgaruvchilardan foydalanadi va shifrlash kaliti tegishli parametrlarning qiymatlarini ishlatadi. Shifrlash kalitining o‘zgarishi parametrlar qiymatlarida o‘zgarishlarga olib keladi va har safar yangi S-box hosil bo‘lishini ta’minlaydi [13-15].

Taklif etilgan usulning o‘ziga xos xususiyatlari quyidagilardan iborat:

- Dastlabki S-box generatsiyasi uchun oddiy, innovatsion va dinamik chiziqli trigonometrik transformatsiya (ChTT) taklif qilingan. Transformatsiya tabiatan dinamik bo‘lganligi sababli, u parametrlar qiymatlarida ozgina o‘zgarishlar kiritilganda ham juda ko‘p sonli mustahkam S-boxlarni ishlab chiqarish imkoniyatiga ega.
- Innovatsion ChTT tomonidan yaratilgan dastlabki S-boxning chiziqli bo‘lmaganligini, improvizatsiya qilish uchun yangi va dinamik jarayon yordamida ishlab chiqilgan yakuniy S-box kriptotahlilchilar uchun shifrlangan matnda qo‘shimcha chalkashliklarni keltirib chiqarishi mumkinligi.
- Olingan S-box va manbalarda keltirilgan boshqa keng tarqalgan S-boxlarning kriptografik parametrlarini baholash uchun standart S-boxlarni umumiy kriptografik talablarga baholash usuli orqali baholanganligi.

Taklif qilingan yangi algoritmda dinamik chiziqli trigonometrik transformatsiyadan (ChTT) foydalanish orqali n×n o‘lchamli S-box yaratiladi. Ushbu yangi transformatsiya (1) tenglamada berilgan funksiya shaklidagi matematik tavsifga ega.

$$T(z) = \cos((A+B) * X * z + C) \qquad (1)$$

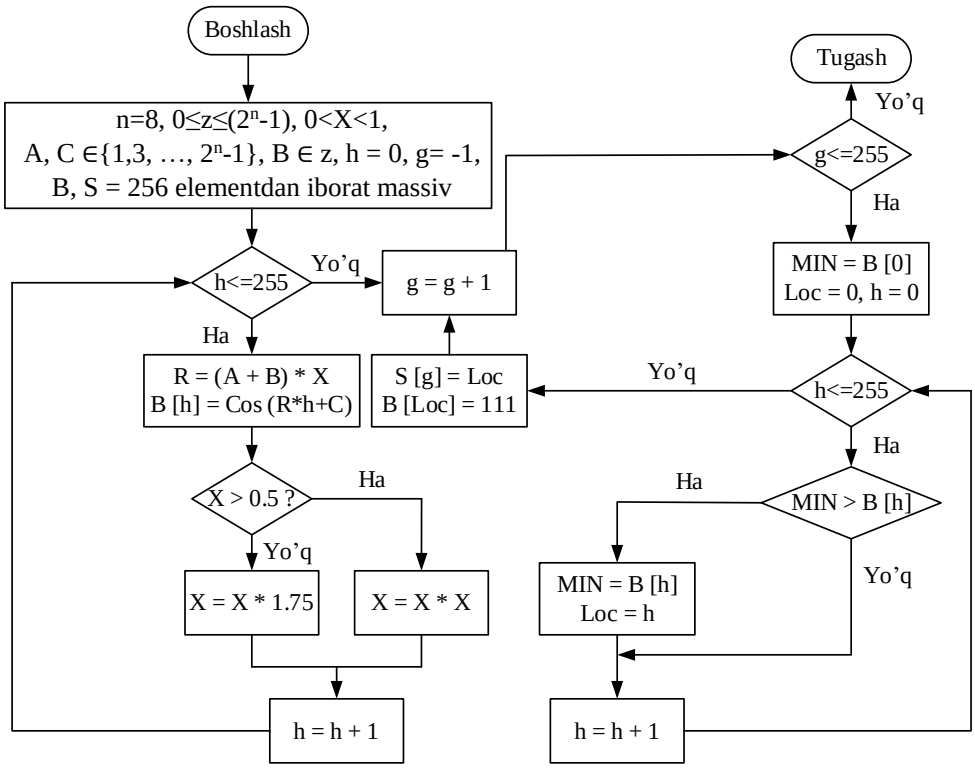
bu yerda, $0 < X < 1$, $0 \le z \le 2^n - 1, B \in Z, A, C = \{1,3,5, \dots, 2^n - 1\}$.

(1) formuladagi A, B, C va X o‘zgaruvchilar qiymatlari bo‘lib, shifrlash kaliti yordamida hosil qilinadi. X o‘zgaruvchisi *double* turga ega va taklif qilingan usul yordamida S-box yaratish uchun 15 ta muhim o‘nlik raqam ko‘rib chiqilgan. Bunday o‘zgaruvchidan foydalangan holda hisoblash float turiga qaraganda biroz sekin. Biroq, bu S-box loyihasiga float tipidagi o‘zgaruvchilar bilan solishtirganda katta kalit maydoni beradi. (1) tenglik yuqorida aytib o‘tilgan parametrlarning turli qiymatlaridan foydalangan holda juda ko‘p kalitga bog‘liq dinamik S-boxlarni (S-box maydoni = $128 \times 256 \times 128 \times 10^{15} \sim 10^{21}$) beradi. $n = 8$ uchun dastlabki n × n o‘lchamli S-box (1) tenglik yordamida o‘rnatiladi. Taklif etilayotgan usul qo‘pol kuch hujumlari imkoniyatlarini kamaytirish orqali yaratilgan S-boxning kriptografik kuchini biroz oshirishga olib kelishi mumkin bo‘lgan ko‘p sonli parametrlarni o‘z ichiga oladi. Biroq, bu taklif qilingan usulning hisoblash vaqtini ortishiga olib keladi. X o‘zgaruvchisi qo‘pol kuch hujumlarini oldini olish uchun o‘z diapazoni bilan shunday imkoniyatni taqdim etib, shu bilan birga hisoblash samaradorligi unchalik ortirmaydi. Quyida taklif qilingan S-boxni generatsiyalash algoritmi (1-algoritm) va uning blok sxemasi (1-rasm) keltirilgan.

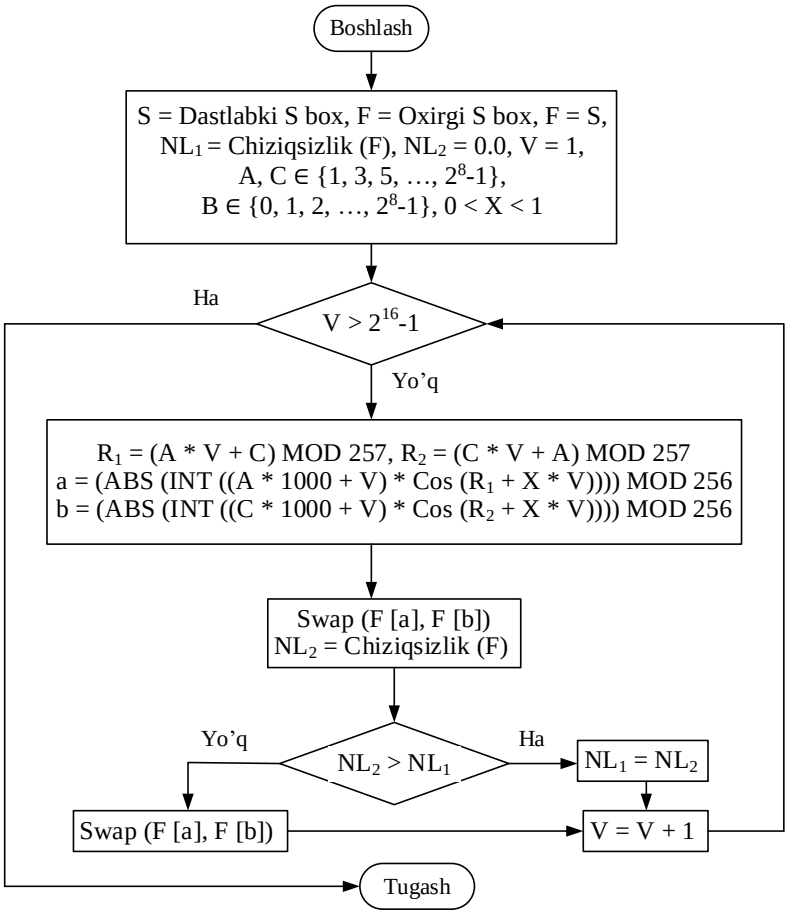
1-algoritm: S-boxni generatsiyalash algoritmi:

Kiruvchi parametrlar:
n = 8 // for n × n o‘lchamli S-box
X // 0 < X < 1
A, C // A, C ∈{1, 3, ..., 2^n - 1}
B //B ∈{0, 1, 2, ..., 2^n - 1}
Chiqish:
S // Dastlabki 8 × 8 o‘lchamdagi S-box
Initsializatsiya:
h ← 0
g ← −1
Loc ← 0
while (h <= 255) do
    R ← (A + B) ∗ X
    B[h] = Cos (R ∗ h + C)
    if (X > 0.5) then
        X = X ∗ X
    else X = X ∗ 1.75
    endif
    h ← h + 1
endwhile
g ← g + 1
while (g <= 255) do
    MIN ← B [0]
    Loc = 0
    h ← 0
    while (h <= 255) do
        if (MIN > B[h])
    then
            MIN = B[h]
            Loc = h
        endif
    h ← h + 1
    endwhile
    S[g] = Loc
    B[Loc] = 111
    g ← g + 1
endwhile
return S

Ushbu bosqich 1-rasmda ko‘rsatilganidek, protsedura bo‘yicha o‘rnatilgan dastlabki S-boxning qiymatlarini aralashtirishga yordam beradi. Tavsiya etilgan usulda ishlashning improvizatsiya rejasi yuqori chiziqli bo‘lmagan xususiyatga ega mustahkam va xavfsiz S-boxlarni generatsiylashda muhim rol o‘ynaydi. Chiziqli bo‘lmagan improvizatsiya rejasi 2-rasmda va 2-algoritmda tasvirlangan. *A, B, C* va *X* o‘zgaruvchilarning qiymatlari shifrlash kaliti tomonidan qo‘llaniladi. Taklif etilgan usul yordamida hosil qilingan 8×8 o‘lchamdagi S-boxga misol 1-jadvalda ko‘rsatilgan.



1-rasm. S-box generatsiya qilish algoritmining blok sxemasi.



2-rasm. Chiziqsiz jarayonning improvizatsiya rejasi.

1-jadval. Taklif qilingan algoritm yordamida generatsiya qilingan S-box

{104, 141, 202, 77, 115, 75, 78, 42, 212, 82, 38, 179, 84, 30, 25, 31, 34, 3, 70, 61, 45, 74, 83, 131, 19, 138, 183, 213, 37, 121, 245, 189, 88, 47, 13, 2, 237, 81, 158, 17, 242, 62, 85, 94, 209, 22, 60, 102, 112, 93, 243, 69, 64, 204, 232, 148, 86, 8, 206, 26, 58, 210, 225, 223, 181, 56, 110, 14, 229, 244, 249, 134, 233, 79, 214, 133, 35, 207, 50, 153, 49, 20, 174, 238, 200, 72, 211, 48, 161, 146, 65, 177, 24, 196, 44, 113, 114, 68, 21, 253, 55, 190, 95, 170, 155, 136, 216, 171, 137, 156, 250, 96, 234, 188, 98, 12, 36, 166, 168, 236, 103, 32, 219, 124, 40, 221, 172, 91, 52, 126, 16, 241, 123, 143, 99, 160, 5, 154, 67, 119, 33, 191, 39, 9, 195, 159, 182, 215, 41, 194, 235, 192, 164, 139, 140, 29, 251, 255, 193, 178, 151, 46, 248, 101, 246, 117, 7, 4, 73, 51, 228, 217, 185, 208, 66, 199, 108, 144, 0, 142, 111, 80, 1, 197, 218, 71, 63, 205, 105, 162, 226, 122, 167, 198, 147, 15, 10, 6, 230, 43, 150, 163, 28, 175, 106, 18, 132, 57, 231, 176, 130, 247, 254, 157, 135, 92, 129, 53, 222, 180, 165, 252, 128, 239, 203, 187, 107, 118, 186, 90, 125, 120, 11, 149, 227, 173, 116, 152, 59, 54, 100, 109, 220, 240, 89, 169, 76, 23, 127, 145, 184, 201, 87, 27, 224, 97}

2-algoritm. Chiziqsiz improvizatsiya rejasi asosida yakuniy S-Box ishlab chiqish algoritmi

Kiruvchi parametrlar:

X // 0 < X< 1

A, C // A, C ∈{1, 3, ..., 2^n- 1}

B //B ∈{0, 1, 2, ..., 2^n- 1}

S // Dastlabki 8 × 8 o'lchamli S-box

Chiqish:

F // Yakuniy 8 × 8 o'lchamli S-box

Initsializatsiya:

V ← 1

F = S

NL1 ← Chiziqsizlik (F)

NL2 ← 0.0

while (V <= 2^{16} – 1) do

R1←(A ∗ V + C) MOD 257

R2←(C ∗ V + A) MOD 257

R3 ← (A ∗ 1000 + V)

R4 ← (C ∗ 1000 + V)

R5 ← (R1 + X ∗ V)

R6 ← (R2 + X ∗ V)

a←ABS(INT(R3 ∗Cos(R5)))MOD 256

b←ABS(INT(R4 ∗Cos(R6)))MOD 256

// INT kasr qiymatidan butun sonni //qaytaradi

// ABS absolyut qiymatni qaytaradi

//F[a] va F[b] ning qiymatlari //almashtiriladi

Temp ← F[a]

F[a] ← F[b]

F[b] ← Temp

NL2 ← Chiziqsizlik (F)

if (NL2> NL1) then

NL1 ← NL2

else

// F[a] va F[b] ning qiymatlari //almashtiriladi

Temp ← F[a]

F[a] ← F[b]

F[b] ← Temp

endif

V ← V + 1

endwhile

return F

III. NATIJALAR TAHLILI

Taklif qilingan algoritm yordamida generatsiya qilingan S-boxlar tahlili.

Ixtiyoriy S-box zaif bo'lishi va kriptotahlilchilarning oson nishoni bo'lishi mumkinligi bois, ularni xavfsizlik talablariga baholash shart hisoblanadi. Har qanday S-boxning kriptografik parametrlarini baholashda tegishli S-box tomonidan bajarilishi kerak bo'lgan turli mezonlardan foydalaniladi. [5] manbada keltirilgan standart baholash mezonlari yordamida taklif qilingan S-boxning umumiy kriptografik parametrlarga tekshirish natijalari 2-6-jadvallarda ko'rsatilgan.

2-jadval. Tarkibiy mantiqiy funksiyalar va chiziqsizlik qiymatlari

Bul funksiyasi	B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8
NL(B)	108	104	108	108	104	108	104	108

3-jadval. Turli S-boxlari uchun chiziqsizlik (NL) qiymatlari

S-box	Chiziqsizlik		
	NL_{Min}	NL_{Max}	$NL_{O‘rt}$
1	**2**	**3**	**4**
Mazkur ish	104	108	106.5
[80]	106	108	106.25
[81]	112	112	112
[82]	106	110	106.5
[83]	112	112	112
[84]	106	108	107
[85]	106	108	106.5
[86]	104	110	106.75
[87]	102	108	105
[88]	100	108	105
[89]	104	108	106.25
[90]	96	110	104
[91]	106	112	109.5
[92]	100	108	104
[93]	98	106	103.5
[94]	106	108	106.5
[95]	104	110	106.25
[96]	104	108	105
[97]	106	110	108.5
[98]	108	110	109.75
[99]	102	110	106.5
[100]	112	112	112
[101]	112	112	112
[102]	110	112	110.25
[103]	104	108	105.5
[104]	104	110	107

4-jadval. Taklif etilgan S-boxning BIC-nochiziqlilik qiymatlari

-	104	106	106	100	108	104	100
104	-	108	104	106	104	108	104
104	104	-	108	104	100	102	106
104	108	104	-	106	104	104	102
106	108	106	104	-	104	106	104
104	104	102	104	104	-	106	104
104	104	104	106	104	108	-	102
104	108	106	104	106	106	108	-

5-jadval. SAC va BIC-NL qiymatlarining qiyosiy bahosi

S-box	SAC	BIC-NL
1	2	3
Mazkur ish	0.496	102.8
[80]	0.5086	102.37
[81]	0.496	102.3
[82]	0.5009	103.93
[83]	0.498	112
[84]	0.493	102.3
[85]	0.499	103.6
[86]	0.509	106.1
[87]	0.503	102.9
[88]	0.500	103.0
[89]	0.501	103.6
[90]	0.493	103.0
[91]	0.507	106.9
[92]	0.497	102.6
[93]	0.496	103.5
[94]	0.501	104.1
[95]	0.503	103.9
[96]	0.506	103.5
[97]	0.500	103.9
[98]	0.5042	110.6
[99]	0.4943	103.35
[100]	0.501	112
[101]	0.495	112
[102]	0.495	104.1
[103]	0.5065	103.57
[104]	0.4993	103.29

6-jadval. Taklif etilgan S-boxning differensial bir xilligi (ayirma matritsa) qiymatlari

8	6	8	10	8	8	10	8	8	8	6	6	8	8	10	8
8	8	6	8	6	10	8	8	8	10	8	6	8	10	8	8
8	6	8	10	8	8	6	8	10	8	10	8	8	6	8	8
8	8	6	8	10	8	8	10	8	8	10	6	8	6	8	8
10	6	8	8	8	10	6	8	6	8	6	10	8	8	10	8
10	6	8	8	8	6	10	6	10	6	8	8	10	8	8	8
8	8	6	10	8	8	6	10	6	8	8	6	10	10	8	8
8	6	8	10	8	10	8	6	10	8	6	10	8	6	8	8
8	8	10	8	8	8	6	8	8	10	6	8	10	8	8	6
8	8	10	8	6	8	8	8	8	10	8	8	6	8	8	8
8	8	8	8	8	10	8	8	6	8	8	8	10	8	8	6
8	8	8	8	10	8	8	8	8	6	8	10	8	8	6	8
8	8	6	8	8	8	10	8	10	8	8	8	8	6	8	8
6	8	8	8	8	10	8	8	8	8	8	10	8	6	8	8
8	8	8	10	8	6	8	8	8	8	8	8	8	6	8	10
10	8	8	8	8	8	6	8	8	10	8	8	6	8	8	8

Tadqiqot doirasida chiziqli bo‘lmagan S-boxlarni generatsiya qilish uchun taklif qilingan innovatsion usullar bo‘yicha ko‘plab tadqiqotlar o‘tkazildi. Ko‘plab S-boxni generatsiyalash usullari uchun har xil xulosalar olish mumkin, masalan, statik almashtirish usuli, statik qaytarilmas polinomdan foydalanish, qo‘zg‘almas nuqtalarning mavjudligi, yuqori hisoblash narxi, va boshqalar. S-boxni qurish uchun mazkur dissertatsiya ishida taklif qilinigan usul oddiy va chiziqli trigonometrik transformatsiyani o‘z ichiga oladi.

3-jadvaldan ko‘rinib turibdiki, taklif qilingan S-boxlar ancha yuqori nochiziqli ko‘rsatkichlarga ega. Taklif qilingan usul yordamida generatsiya qilingan S-boxlar barcha mezonlarga javob bergani bois, boshqa usullarga nisbatan shifrlash jarayonida yuqori chiziqli bo‘lmagan o‘zgartirishni amalga oshirishda ancha samarali ekanligini ko‘rsatadi.

IV. XULOSA

Mazkur maqolada chiziqli trigonometrik transformatsiya yordamida kalitga bog‘liq dinamik S-boxlarni generatsiyalash uchun yangi usul taqdim etildi. Yangi trigonometrik transformatsiya orqali yaratilgan dastlabki S-boxning chiziqli bo‘lmagan bahosini oshiradigan yangi dinamik improvizatsiya rejasi taklif etildi. Transformatsiya va chiziqli bo‘lmagan improvizatsiya rejasi generatsiya qilishda turli xil parametrlardan, shifrlash kalitining tegishli parametrlari qiymatlaridan foydalanadi. Shifrlash kalitining o‘zgarishi parametrlar qiymatlarining o‘zgarishiga olib keladi va har safar yangi chiziqli bo‘lmagan S-box hosil qilanadi. Qiyosiy tahlillar dinamik va xavfsiz S-boxlarni generatsiyalash uchun taklif qilingan sxemaning samaradorligini tasdiqlaydi.

ADABIYOTLAR

[1] *Agren M.* On some symmetric lightweight cryptographic designs. Doctoral Thesis, Department of Electrical and Information Technology, Faculty of Engineering, LTH, Lund University, 2012.

[2] *Manifavas C. et al.* A survey of lightweight stream ciphers for embedded systems //Security and Communication Networks. – 2016. – T. 9. – №. 10. – C. 1226-1246.

[3] *M. M. Lauridsen, C. Rechberger, and L. R. Knudsen,* ‘‘Design and analysis of symmetric primitive,’’ Tech. Univ. Denmark, Lyngby, Denmark, Tech. Rep. 382, 2016.

[4] *E. Tanyildizi and F. Ozkaynak,* ‘‘A new chaotic S-box generation method using parameter optimization of one dimensional chaotic maps’’ IEEE Access, vol. 7, pp. 117829–117838, 2019.

[5] *M. Ahmad, E. Al-Solami, A. M. Alghamdi, and M. A. Yousaf,* ‘‘Bijective S-boxes method using improved chaotic map-based heuristic search and algebraic group structures,’’ IEEE Access, vol. 8, pp. 110397–110411, 2020.

[6] *F. Özkaynak*, ‘‘Construction of robust substitution boxes based on chaotic systems,’’ Neural Comput. Appl., vol. 31, no. 8, pp. 3317–3326, 2019.

[7] *I.R.Rakhmatullaev, I.Boykuziev* “Analysis of cryptanalysis methods applied to stream encryption algorithms” International Conference on Artificial Intelligence, Blockchain, Computing and Security (ICABCS-2023), 2023, India, 1-4 p.

[8] *Khudoykulov Z.T., Rakhmatullayev I.R.,* “Development Of A Software Stream Encryption Algorithm”, Electronic journal of actual problems of modern

science, education and training, january, 2023-1, 51-59.
[9] *Rakhmatullayev I.R., Khudoykulov Z.T.*, "Evaluating Wireless Encryption Algorithms For Devices With Restricted Computing Power", Journal of Automobile Engineering (JAuE), Vol. 13, Issue 1, Jun 2023, 7–12.
[10] *Khudoykulov Z.T., Rakhmatullayev I.R*, "A new key stream encryption algorithm and its cryptanalysis"// Scientific and technical journal Namangan Institute of Engineering and Technology, Volume 8, Issue 1, 2023, 146-157.
[11] *Z.T.Xudoykulov, I.R.Rahmatullayev*, "Yangi oqimli shifrlash algoritmlari va uning kriptotahlili", Milliy standart Ilmiy-texnik jurnali, 2023/2-son, 42-47.
[12] *I.R.Rakhmatullaev*, "Stream encryption algorithims and the basis of their creation", Central asian journal of mathematical theory and computer sciences, Volume 03, Issue 1, 2022, 165-173 p.
[13] *I.R.Rahmatullayev*, "Oqimli shifrlash algoritmlari va ularni vujudga kelish sabablari", International Journal of Theoretical and Applied Issues of Digital Technologies, Vol. 2 No. 2 (2022), 119-128.
[14] *I.R.Rahmatullayev*, "Algebraik kriptotahlil usuli va uning oqimli shifrlash algoritmlariga qo'llanish asoslari", International Journal of Theoretical and Applied Issues of Digital Technologies, Vol. 4 No. 2 (2023), 96-102.
[15] *I.R.Rakhmatullaev*, "Evaluation of new NSA stream encryptt-ion algorithm by integrated cryptanalysis method", VI International Scientific and Practical Conference Recent scientific investigation, July 26-28, 2023 in Oslo, Norway 242-248.

Поступила в редакцию 21.07.2023

Citation: *Xudoyqulov Z.T., Rahmatullayev I.R., Boyqo'ziyev I.M.* (2023). Bardoshli statik S-boxlarni generatsiyalash algoritmi. Raqamli texnologiyalarning nazariy va amaliy masalalari xalqaro jurnali. 3(5). – B. 57-66.

ALGORITHM FOR GENERATING STABLE-STATIC S-BOXES

Xudoykulov Z.T.[1], *Rahmatullaev I.R.*[2], *Boykuziev I.M.*[3]

[1] Tashkent University of information technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan
[2] Samarkand branch of Tashkent University of information technologies named after Muhammad al-Khwarizmi, Samarkand, Uzbekistan
[3] Renaissance University of Education, Tashkent, Uzbekistan
ilhom9001@mail.com

Abstract. *In this paper, a simple and innovative scheme for the generation of dynamic and key-dependent S-boxes is proposed, and the permutation table generated by this algorithm is used to evaluate the stream encryption algorithm with cryptanalysis methods.*

Keywords: *Stream encryption, Block ciphers, S-box, linear trigonometric transformation, cryptanalysis.*

АЛГОРИТМ ГЕНЕРАЦИИ СТАБИЛЬНО-СТАТИЧЕСКИХ S-БЛОКОВ

Худойкулов З.Т.[1], Рахматуллаев И.Р.[2], Бойкузиев И.М.[3]

[1] Ташкентский университет информационных технологий имени Мухаммада ал-Хорезми, Ташкент, Узбекистан
[2] Самаркандский филиал Ташкентского университета информационных технологий имени Мухаммада ал-Хорезми, Самарканд, Узбекистан
[3] Университет Образования Ренессанс, Ташкент, Узбекистан
ilhom9001@mail.com

Аннотация. *В этой статье предлагается простая и инновационная схема генерации динамических и зависимых от ключа S-блоков, а таблица перестановок, сгенерированная этим алгоритмом, используется для оценки алгоритма шифрования потока с помощью методов криптоанализа.*

Ключевые слова: *Потоковое шифрование, Блочные шифры, S-box, линейное тригонометрическое преобразование, криптоанализ.*