UDK 004.056.55

NSA ALGORITMINING AKSLANTIRISHLARI TANLANISHINING XAVFSIZLIK TALABLARINI BAJARILISHIDAGI O‘RNI

Xudoyqulov Z.T.[1], *Rahmatullayev I.R.*[2], *Umurzoqov O.Sh.*[2]
[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
ilhom9001@mail.com

Annotatsiya. *Mazkur maqolada taklif etilgan NSA(New stream algoritm) algoritmi akslantirishlarining tanlanishida xavfsizlik parametrlariga ta’sirini o‘rganish maqsadida tadqiqotlar o‘tkazildi, bunda adabiyotlarda keltirilgan tahlil usullari va ma’lumotlardan foydalanildi. NSA agoritmining chiqish funktsiyasi 64 bitli $a_2(t)$ ni t - raunddan so‘ng chiqish qiymati sifatida taqdim qiladi. Bunda NSA chiqish funksiyasiga kirishdagi kichik o‘zgarishlar qanday ta’sir etishini tekshirish talab etiladi. Chiqish massivi sifatida boshqa har qanday massiv tanlanganda shifrni osongina buzish mumkin bo‘ladi.*

Kalit so‘zlar: *NSA, funksiya, Massiv, tahlil, MDS matritsa, S-box, chiziqsiz.*

I. KIRISH

Yaratilgan har qanday kriptografik algoritmlarga qo‘yiladigan talablardan biri bu algoritm tarkibidagi akslantirishlarning murakkab ifoda va hisoblashlardan holi bo‘lishligi (ya’ni, lo‘ndaligi) bo‘lib, algoritmlar akslantirishlarining kriptografik xususiyatlarini yaqqol tahlil qilinishini, kriptografik samaradorligini, apparat va apparat-dasturiy amalga oshirishni qulayligini ta’minlaydi.

Tahlil jarayonida $\alpha, \beta, \gamma, \delta, \varepsilon$ harflar bilan har bir raundda ikkita F-funksiyaga kirish sifatida beriladgan $a_1(t)$ ning oraliq qiymatlari belgilansin va $Chiqish[t] = a_1(t)$ deb faraz qilinsiz. Bu yerda, bir nechta muhim kuzatuvlarni amalga oshirish mumkin[1].

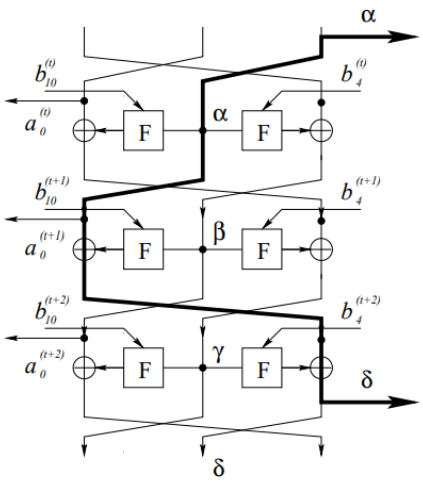
Birinchi kuzatish $a_1(t) = a_0(t+1)$). Bunda tahlilchiga har bir raundda buferni yangilaydigan 64 bitli qiymat ma’lum bo‘ladi. Bu tahlilchiga $\lambda(\cdot)$ – buferni yangilash funksiyasini ramziy ravishda ishga tushirishga va bufer bitlari hamda chiziqli bo‘lmagan p funksiyasiga “qism kalit” sifatida kiradigan bitlar uchun chiziqli tenglamalarni yozishga imkon beradi.

Ikkinchi kuzatish varianti shundan iboratki, $a_1(t)$ qiymat raundning ikkala F-funksiyasiga kirish sifatida ishlatiladi.

Yakuniy kuzatish shundan iboratki, tahlilchi quyidagi tenglamani yozishi mumkin: (1) ifoda.

$$\alpha \oplus \delta = F(\beta, b_{10}^{(t+1)} \lll 19) \oplus F(\gamma, b_4^{(t+2)}). \quad (1)$$

Bu tenglamadagi $\alpha, \beta, \gamma, \delta$ chiqish oqimidagi qiymatlar bo‘lganligi sababli hujumchiga ma’lum bo‘ladi (1-rasm).



1-rasm. Hujum yo‘nalishi.

MDS almashtirishining teskarisini va bayt almashuvi qismlarini M^{-1} bilan va sakkizta S-box qatlamini S bilan belgilanadi [4]. F ning chiziqli qismining teskarisini tenglamaning har ikki tomoniga qo‘llash orqali quyidagi soddalashtirilgan tenglamani hosil qilish mumkin:

$$M^{-1}(\alpha \oplus \delta) = S\left(\beta \oplus \left(b_{10}^{(t+1)} \lll 19\right)\right) \oplus \oplus S\left(\gamma \oplus b_4^{(t+2)}\right). \quad (2)$$

(2) ifoda har bir S-boxning 8 bit qiymatlarida 8 ta mustaqil tenglamaga ajraladi.

Ushbu tenglamadan foydalanishning mumkin bo‘lgan usullaridan biri chiqish oqimida $M^{-1}(\alpha \oplus \delta)$ baytlarining kamida bittasi nolga teng bo‘lgan nuqtalarini izlashdir. Muayyan S-

boxlar uchun bu quyidagi oddiyroq tenglamaga olib keladi:

$$S\left(\beta\oplus\left(b_{10}^{(t+1)} \lll 19\right)\right)\oplus S(\gamma\oplus b_4^{(t+2)}).$$

Mazkur tenglamani yanada soddalashtirish mumkin:

$$\left(b_{10}^{(t+1)} \lll 19\right)\oplus b_4^{(t+2)} = \beta\oplus\gamma. \qquad (3)$$

Bu bufer bitlari uchun 8 bitli chiziqli cheklov bo‘lib, barcha bufer bitlari uchun chiziqli tenglamalar tizimini olishda taxminan 1024/8 = 128 ta shunday tenglamalarni shakllantirish kifoya qiladi. Har bir 64-bitli blokda kamida bitta nol qiymatining paydo bo‘lish ehtimoli $1-(1-1/256)^8 \approx 2^{-5}$.

Shunday qilib, taxminan $25 \cdot 128 = 212$ ta chiqish qiymatlari berilgan bo‘lsa, tahlilchi yechiladigan tenglamalar sistemasini tuzishga va to‘liq 1024-bitli buferni qayta qurishga harakat qiladi [2,4]. Tahlilchi t raunddagi buferni va $a_1^{(t-1)}, a_1^{(t)}, a_1^{(t+1)}$ chiqishlarni bilgan holda, $a^{(t)}$ holat massivlarini quyidagicha tiklashi mumkin:

$$\left(a_0^{(t)}, a_1^{(t)}, a_2^{(t)}\right) = \\ = \left(a_1^{(t-1)}, a_1^{(t)}, F(a_1^{(t)}, b_4^{(t)})\oplus a_1^{(t+1)}\right) \qquad (4)$$

Shifrdagi barcha qadamlar teskari bo‘lganligi sababli, bufer va t nuqtadagi holatni bilish tahlilchiga shifrni oldinga va orqaga ishlatish imkonini beradi. Shifrni orqaga qarab ishga tushirish orqali tahlilchi dastlabki 128 bitli maxfiy kalitni tiklashi mumkin bo‘ladi.

II. ASOSIY QISM

Ushbu hujumning umumiy murakkabligi (taxminan 2^{15} bayt) ma’lum oqimdagi qiymatlar $O(2^{12})$ va 2^{10} ta tenglamalar sistemasini yechish uchun $O(2^{30})$ qadam talab qilinadi. Xuddi shu hujum $Chiqish[t] = a_0(t)$ variant uchun ham ishlaydi.

Mazkur hujumda S-boxning hech qanday xususiyatlaridan foydalanilmagan va shuning uchun S-box noma’lum yoki kalitga bog‘liq bo‘lsa ham ishlashi mumkin. Tahlilchi avval yuqorida tavsiflangan texnikadan foydalangan holda buferni tiklaydi va keyin (3) tenglamadan quyidagi tenglamalar to‘plamini yozish orqali noma’lum S-boxlarni oladi.

$$S(c_1)\oplus S(c_2) = c_3, \qquad (5)$$

bu erda c_1, c_2, c_3 - ma’lum qiymatlar.

Yana bir kuzatuv shundan iboratki “buferni yo‘q qilish” tenglamalaridan NSA ning ushbu variantiga kichikroq ma’lumotlar va vaqt murakkabligi bilan hujum qilishda foydalanilishi mumkin [5]. Bu esa chiziqli tenglamalar sistemasini yechish uchun $O(2^{30})$ operatsiyalarini sarflash shart emasligini ko‘rsatadi.

Tenglamalar quyidagicha ko‘rinishda ifodalanadi (raundlar tartibi $t \geq 48$ va $\lll$ 32 64 bitli massivning chapga 32 bit siklik surilishini bildiradi):

$$a_1^{(t)}\oplus a_1^{(t-48)}\oplus F^{-1}\left(a_1^{(t+1)}\oplus a_2^{(t)}\oplus C_1\right)\oplus F^{-1}\left(a_1^{(t-47)}\oplus a_2^{(t-48)}\oplus C_1\right) = a_1^{(t-6)}\oplus a_1^{(t-1)}\oplus a_1^{(t-14)}\oplus \\ \oplus a_1^{(t-18)}\oplus a_1^{(t-26)}\oplus a_1^{(t-30)}\oplus a_1^{(t-34)}\oplus a_1^{(t-38)}\oplus\left(a_1^{(t-26)} \lll 32\right)\oplus\left(a_1^{(t-42)} \lll 32\right)$$

$$a_1^{(t)}\oplus a_1^{(t-48)}\oplus F^{-1}\left(a_1^{(t-1)}\oplus a_2^{(t+1)}\oplus C_2\right)\oplus F^{-1}\left(a_1^{(t-49)}\oplus a_2^{(t-47)}\oplus C_2\right) = \left(a_1^{(t-12)} \lll 19\right)\oplus \\ \oplus\left(a_1^{(t-16)} \lll 19\right)\oplus\left(a_1^{(t-32)} \lll 19\right)\oplus\left(a_1^{(t-44)} \lll 19\right)\oplus\left(a_1^{(t-16)} \lll 45\right)\oplus\left(a_1^{(t-20)} \lll 45\right)\oplus \\ \oplus\left(a_1^{(t-32)} \lll 45\right)\oplus\left(a_1^{(t-36)} \lll 45\right)$$

Ushbu ikki tenglamaning ikkita muhim xususiyatiga e‘tibor qaratish zarur: har bir tenglamada faqat ikkita a_2 massivi mavjud va ular ikkala tenglamada 48 ta iteratsiya qadamlarini ajratib turadi. Shunday qilib, agar $a_1^{(t)}$ ketma-ketligi ma’lum deb faraz qilinsa, bu tenglamalarni soddaroq akslantirish mumkon bo‘ladi:

$$F^{-1}\left(a_2^{(t)}\oplus C_1'\right)\oplus F^{-1}\left(a_2^{(t-48)}\oplus C_1''\right) = const_1 \quad (6)$$
$$F^{-1}\left(a_2^{(t)}\oplus C_2'\right)\oplus F^{-1}\left(a_2^{(t-48)}\oplus C_2''\right) = const_2 \quad (7)$$

bu yerda, $a_2^{(t)}$ va $a_2^{(t-48)}$ noma’lumdan tashqari barcha miqdorlar ma’lum. Agar $x = M^{-1}(a_2^{(t)})$ va $y = M^{-1}(a_2^{(t-48)})$ kabi belgilash kiritilsa, u holda yuqoridagi (6) va (7) ifodalarni quyidagicha soddalashtirilgan ko‘rinishda yozish mumkin:

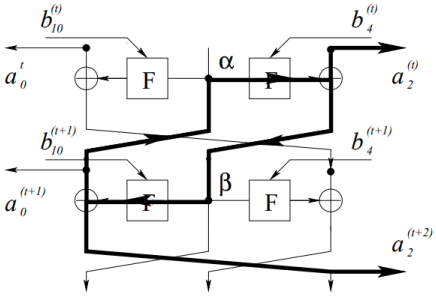
$$S_1(x\oplus C_1')\oplus S_2(y\oplus C_1'') = const_1 \qquad (8)$$

$$S_3(x\oplus C_2')\oplus S_4(y\oplus C_2') = const_2 \qquad (9)$$

Mazkur tenglamalar sistemasini yechish orqali $a_2^{(t)}$ va $a_2^{(t-48)}$ massivlarining to‘liq qiymatini $8 \cdot 2^8 = 2^{11}$ qadamda hosil qilish mumkin. Ushbu jarayonni $t, t+1, \dots, t+7$ uchun sakkiz marta takrorlash orqali $a_2^t, a_2^{t+1}, \dots, a_2^{t+7}$ holat massivlarining qiymatlarini aniqlash mumkin. Bu

esa chiziqli tenglamalar tizimini yechmasdan to‘g‘ridan-to‘g‘ri buferning bitlarini olish imkonini beradi. Ushbu yondashuvning murakkabligi taxminan 2^{14} ta juda oddiy qadamlardan iborat bo‘lib, u taxminan 56 ta chiqish massivi va kam miqdordagi xotiradan foydalanadi (2^{32} baytni egallaydigan (8) va (9) tenglamalar tizimining yechimini saqlaydigan jadval talab qilinadi). Ushbu yondashuvda S-boxes haqidagi bilimlardan va buferni yangilash funktsiyasining maxsus xususiyatlaridan foydalanilib, undan birinchi yondashuvda foydalanilmagan edi.

Endi, buferning bir qismi tahlilchiga ma’lum bo‘lsa, shifrning 192 bitli chiziqli bo‘lmagan holatini tiklashga qaratilgan hujum qanday amalga oshirilishi mumkinligini qarab chiqiladi [6]. Bu hujumni amalga oshirish uchun buferning faqat b_4^t va b_{10}^t qismlarini bilish kifoya. Hujum faqat 3 ta chiqish so‘zlaridan foydalanadi va O(2^{32}) qadam murakkabligiga ega. Avvalgi bo‘limda ko‘rilganidek shifrning chiqishi o‘zgarmaydi, ya’ni, asl chiqish funktsiyasi: $Chiqish[t] = a_2(t)$.



2-rasm. p funksiya sikli

Hujumchi p funksiyada quyidagi siklni ko‘rib chiqishi mumkin (2-rasm):

$$F\left(\alpha, b_4^{(t)}\right) \oplus a_2^{(t)} = \beta \qquad (10)$$

$$F\left(\beta, b_{10}^{(t)}\right) \oplus a_2^{(t+2)} = \alpha \qquad (11)$$

bu yerda $a_2^{(t)}$, $a_2^{(t+2)}$ va $b_4^{(t)}$, $b_{10}^{(t)}$ massivlarning qiymatlari ma‘lum deb qaralsa, (10) va (11) ifodalar bir raundni ifodalovchi o‘zgaruvchilari α va β bo‘lgan chiziqsiz, oddiy tenglamalar sistemasiga aylanadi.

Hosil bo‘lgan sistemani yechish uchun tahlilchi quyidagicha harakat qilishi mumkin:

1. β ning dastlabki to‘rt baytini taxmin qilish (chapdan o‘ngga qarab 0,1,2,3 tartibda belgilangan, $1/2^{32}$ ta ehtimollik bilan).

2. Har bir variant uchun α ning o‘rtadagi to‘rt baytini (2,3,4,5) aniqlash.

3. Ushbu bosqichda $t-$raundda birinchi MDSning kirish va chiqishida ikkita bayt (2- va 3-tartibdagi) ma’lum bo‘ladi. Kirishning dastlabki (0,1 tartibli) ikki baytini quyidagi chiziqli tenglamalar sistemasidan aniqlash mumkin:

$$\begin{cases} x_0 + x_1 = c_0 \\ 3 \cdot x_0 + x_1 = c_1 \end{cases}$$

bu erda, c_0, c_1 kirish va chiqishning 2- va 3-baytlaridan hisoblangan ma’lum qiymatlar. Yangi kirish baytlari x_0, x_1 ni bilgan holda yetishmayotgan chiqish baytlari y_0, y_1 lar hisoblanishi mumkin. Natijada α va β ning ikkita qo‘shimcha baytlari aniqlanadi. MDS matritsasiga ko‘paytirish amalidan keyingi bayt almashinuvi tufayli ikkinchi MDS ning kirish va chiqishida 4- va 5- baytlarini aniqlaydigan va 6- va 7- baytlar uchun tenglamalar sitemasini yechishda foydalaniladigan shunga o‘xshash qoidalar to‘plamini hosil qilish mumkin. Natijada α va β ning qiymatlari to‘liq tiklanadi.

1. Mazkur nuqtada $a_1^{(t)} = \alpha$ ning qiymatini hamda chiqish massivi $a_2^{(t)}$ning qiymatlarini bilish orqali a holat massivlarining 128 bitini aniqlash mumkin. Qolgan 64 bitni esa quyidagicha topish mumkin:

$$a_0^{(t)} = F\left(\alpha, b_4^{(t)}\right) \oplus a_2^{(t+1)}.$$

Ikkita bufer massivi va 3 ta chiqish massivlari hisobga olinsa, O(2^{32}) qadamda 192 bitli $a(t)$ holat massivlarining qiymatlarini to‘liq tiklash mumkinligini ko‘rish mumkin. Agar ushbu hujum, masalan, to‘liq shifrga boshqa hujumning bir qismi sifatida bir necha marta takroran amalga oshirilishi zarur bo‘lsa, uni oldindan hisoblash orqali tezlashtirish mumkin.

Har bir raundda bufer qiymatidagi bitta massivini aralashtirish. NSA da har bir raundda ikkita 64 bitli bufer massivlari aralashtirilishi juda muhim bosqich hisoblanib, faqat bitta 64 bitli massiv chiqish sifatida beriladi. Ushbu bo‘limda har bir raundda faqat bitta massiv aralashtirilganda shifrning to‘liq maxfiy holatini ($a(t)$ holat massivlari va $b(t)$ buferi) tiklaydigan hujum usuli ko‘rib o‘tiladi. Bunda shifr tuzilishining qolgan qismlari o‘zgarishsiz saqlanadi. Ushbu hujumni amalga oshirish murakkabligi O($2^{126.5}$) kalitlarni tanlash murakkabligiga teng, ammo, algoritmda kattaroq uzunlikdagi kalitlardan foydalanilgan holda ham hujumning murakkabligi o‘zgarmagani bois, mazkur murakkablik va kalitlarni to‘liq tanlash usuli o‘rtasidagi bog‘liqlik tasodifiy hisoblanadi. E‘tibor berish joizki, bu hujum 192 bitli holat massivlari qiymatlari hamda 1024 bitli bufer qiymatlarining barcha varaintlarini to‘liq tanlash orqali qidiruvning muqobil variantidan ancha tezroq amalga oshiriladi [7,9].

$b_4^{(t)}$ning ishtirokini hisobga olgan holda, har bir raundning ikkala F-funksiyasini umumiy kalit deb hisoblab, ikkita $b_4^{(t)}$ va $b_4^{(t+1)}$ buferlarning qiymatini taxmin qilish orqali oldingi hujumni qayta ishlatish mumkin va bunda $O(2^{160})$ hisoblash bilan $a^{(t)}$ holat massivlarini tiklash mumkin bo‘ladi [8,10]. Quyida tezroq amalga oshirish mumkin bo‘lgan hujum varianti keltirilgan:

1. t-raundda $a_2^{(t)}$massivning qiymati ma’lum deb faraz qilinsa, chiziqli bo‘lmagan holatning qolgan qismlari $a_0^{(t)}$ va $a_1^{(t)}$ ning qiymatlari taxmin qilish mumkin (mumkin bo‘lgan variantlar soni:128 bit).

2. Quyida keltirilgan tenglama yordamida t-raundda kalit sifatida foydalaniladigan $b_4^{(t)}$ buferning qiymati hisoblanadi:

$$F\left(a_1^{(t)}, b_4^{(t)}\right) \oplus a_0^{(t)} = a_2^{(t+1)},$$

bu yerda kalit deb qaralayotgan $b_4^{(t)}$ dan tashqari $a_1^{(t)}$, $a_0^{(t)}$, $a_2^{(t+1)}$qiymatlar ma’lum deb qaraladi yoki chiqish qiymatidan taxmin qilinadi.

1. Shundan so‘ng, holat massividagi noma’lum $a_1^{(t+1)}$ massivning qiymatini yangi tiklangan kalitdan foydalanib hisoblash quyidagi tenglik yordamida amalga oshiriladi:

$$a_1^{(t+1)} = F\left(a_1^{(t)}, b_4^{(t)}\right) \oplus a_2^{(t)},$$

2. 16 ta bufer qiymatlari to‘liq aniqlangunga qadar 2-qadamga qaytib takror bajariladi. Keyingi raundlardagi holat massivlarini hisoblash uchun ham mazkur jarayon 16 marta takrorlanadi.

III. XULOSA

Qayd etish joizki, har bir bosqichda to‘liq chiziqsiz holatlar va buferning yangilash funktsiyasini $\lambda(\cdot)$ bilgan holda mazkur buferni yangilash funksiyasini ramziy ravishda ishga tushirish mumkin. Ushbu hujumni amalga oshirish uchun qiymati ma’lum bo‘lgan 18 ta chiqish oqimi zarur va $\frac{16}{48} \cdot 2^{128}$ ta kalit tanlash murakkabligiga ega. Mazkur usul yordamida shifrning $1024 + 192$ bitli ichki holatini to‘liq tiklash imkoniyati mavjud, shuningdek, operatsiyalarning o‘zgarmasligidan foydalanib, 128 bit uzunlikdagi asl maxfiy kalitni ham tiklash mumkin.

Quyidagi 1-jadvalda NSA algoritmining chiziqsiz qismlariga qaratilgan hujumlarning umumlashgan yakuniy natijalari keltirilgan:

1-jadval. NSA algoritmining chiziqsiz qismlariga qaratilgan hujumlar

№	Hujum variantlari	Qiymati ma’lum bo‘lgan oqim hajmi	Sarflanadigan vaqt	Tiklanadigan ma’lumotlar miqdori
1.	64 bitli chiqish bilan ifodlangan holat uchun chiqish funksiyasini o‘zgartirish	$O(2^{12})$	$O(2^{30})$	Ichki holatning 192+1024-bit qiymati
2.	S-box qiymatlari ma’lum bo‘lmagan yoki dinamik bo‘lgan hol uchun chiqish funksiyasini o‘zgartirish	56	$O(2^{14})$	Ichki holatning 192+1024-bit qiymati
3.	Chiziqsiz komponentrlarga qaratilgan hujum	3	$O(2^{32})$	$a^{(t)}$ ning 192-bit qiymati
4.	Har bir raundda bitta bufer qiymatini aralashtirish	18	$O(2^{126.4})$	Ichki holatning 192+1024-bit qiymati
5.	To‘liq qidirish	2	$O(2^{128})$	Ichki holatning 192+1024-bit qiymati

Ushbu mumkin bo‘lgan zaif variantlar NSA algoritmining loyihasini tanlash jarayonida aniqlangan hamda loyihaning tanlangan variantida mazkur hujumlarni amalga oshirish imkoniyati mavjud emas. Tanlangan variantdagi NSA algoritmida bufer o‘lchamining katta tanlanganligi va har bir raundda ikkita kalitdan foydalanilganligi sababli yuqorida keltirilgan hujumlarning amaliy samarasi bartaraf etilgan.

ADABIYOTLAR

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

[2] *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.

[3] *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 pages.
[4] *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 pages.
[5] *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 page.
[6] *Z.T.Xudoykulov, I.R.Rahmatullayev*, “Yangi oqimli shifrlash algoritmlari va uning kriptotahlili”, Milliy standart Ilmiy-texnik jurnali, 2023/2-son, 42-47 betlar.
[7] *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.
[8] *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 b.
[9] *I.R.Rahmatullayev*, “Algebraik kripto-tahlil 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 b.
[10] *I.R.Rakhmatullaev*, “Evaluation of new NSA stream encryption algorithm by integrated cryptanalysis method”, VI International Scientific and Practical Conference Recent scientific investigation, July 26-28, 2023 in Oslo, Norway 242-248 p.

Поступила в редакцию 29.09.2023

Citation: *Xudoyqulov Z.T., Rahmatullayev I.R., Umurzoqov O.Sh.* (2023). NSA algoritmining akslantirishlari tanlanishining xavfsizlik talablarini bajarilishidagi o‘rni. Raqamli texnologiyalarning nazariy va amaliy masalalari xalqaro jurnali. 4(6). – B. 97-101.

THE ROLE OF NSA ALGORITHM REFLECTION SELECTION IN MEETING SECURITY REQUIREMENTS

Khudoykulov Z.T.[1], Rakhmatullaev I.R.[2], Umurzakov O.SH.[2]

[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

Abstract. *In order to study the impact of the proposed NSA(New stream algorithm) algorithm reflections on the selection of security parameters, research was carried out, in which analysis methods and data presented in the literature were used. The output function of the NSA algorithm provides the 64-bit $a_2(t)$ as the output value after the t-round. This requires investigating how small changes in input affect the NSA output function. Choosing any other array as the output array is easy to crack.*

Keywords: *NSA, function, Array, analysis, MDS matrix, S-box, non-linear.*

РОЛЬ ВЫБОРА ОТРАЖЕНИЯ АЛГОРИТМА NSA В УДОВЛЕТВОРЕНИИ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ

Худойкулов З.Т.[1], Рахматуллаев И.Р.[2], Умурзаков О.Ш.[2]

[1] Ташкентский университет информационных технологий имени Мухаммада ал-Хорезми, Ташкент, Узбекистан

[2] Самаркандский филиал Ташкентского университета информационных технологий имени Мухаммада ал-Хорезми, Самарканд, Узбекистан

Аннотация. *С целью изучения влияния отражений предложенного алгоритма NSA (Newstream Algorithm) на выбор параметров безопасности было проведено исследование, в котором использованы методы анализа и данные, представленные в литературе. Выходная функция алгоритма NSA предоставляет 64-битное значение $a_2(t)$ в качестве выходного значения после t-раунда. Для этого необходимо изучить, как небольшие изменения входных данных влияют на выходную функцию АНБ. Выбор любого другого массива в качестве выходного массива легко взломать.*

Ключевые слова: *NSA, функция, массив, анализ, матрица MDS, S-box, нелинейный.*