UDK 004.056.55

NSA (NEW STREAM ALGORITHM) SIMMETRIK OQIMLI SHIFRLASH ALGORITMINI KRIPTOTAHLIL USULLARIGA BAHOLASH MEZONLARI

Xudoykulov Z.T.[1], *Boyquziyev I.M.*[1], *Rahmatullayev I.R.*[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@gmail.com

Annotatsiya. *Mazkur maqolada, NSA (New Stream Algorithm) deb nomlangan yangi oqimli shifrlash algoritmi taklif etilgan. Ushbu algoritm 128-bit maxfiy kalit va 128-bit boshlang‘ich vektorlardan foydalanadi va har bir raundda 64-bit chiqish qiymati hosil qiladi. Algoritmning me’moriy va dasturiy amaliyotlar uchun mosligi, qayta sinxronizatsiya hujumi, bog‘langan kalit hujumi va chiqish ketma-ketligining linear korrelyatsiyasi asosida o‘tkazilgan hujum usullariga qarshi xavfsizligi baholanadi. NSA algoritmining tegishli kalit asosidagi hujumlarga va qayta sinxronizatsiya hujumlariga, shuningdek, differentsial va linear kriptotahlil kabi an’anaviy usullarga qarshi qanchalik bardoshli ekanligi batafsil tahlil qilinadi. Tahlil natijalari NSA algoritmi xavfsiz oqimli shifrlash algoritmi ekanligini tasdiqlaydi. Shu bilan birga, algoritmining turli xavf-xatarlarga qarshi turish qobiliyati, jumladan, an’anaviy va zamonaviy tahdidlarga qarshilik ko‘rsatishi muhokama qilinadi. Tahlillar mazkur algoritmni xavfsiz oqimli shifrlash algoritmi ekanligini tasdiqlaydi.*

Kalit so‘zlar: *Linear Feedback Shift Registers (LFSR), chiqish ketma-ketligining tasodifiyligi, qayta sinxronizatsiya hujumi, bog‘langan kalit hujumi, chiziqli kriptotahlil, differensial kriptotahlil, integral kriptotahlil.*

I. KIRISH

Linear Feedback Shift Registers (LFSR) oqimli shifrlash algoritmlarida psevdotasodifiy sonlar generatori sifatida keng qo‘llaniladi [1]. LFSRning asosiy afzalligi shundaki, u juda samarali va ixcham apparat dasturlarini yaratish imkonini beradi, bu esa mobil qurilmalar, IoT qurilmalari va boshqa resurs cheklangan muhitlarda juda foydali hisoblanadi [1,7]. Biroq, LFSRlarning asosiy cheklovlari ularning chiziqli xususiyatlarida yotadi, bu esa ularni xavfsizlik nuqtai nazaridan zaif qiladi, shu sababli, ularni sof shakllarda ishlatish tavsiya etilmaydi. LFSR asosida yaratilgan psevdotasodifiy sonlar generatorlarining xavfsizligini oshirish uchun ko‘plab usullar ishlab chiqilgan bo‘lsa-da, bu generatorlarning dasturiy ta’minotni samarali amalga oshirishdagi muammolari ham bor. LFSRlar asosan apparatda amalga oshirish uchun optimallashtirilgan bo‘lib, ularning ixchamligi va yuqori ish tezligi apparat dasturlarida qo‘llash uchun juda qulaydir.

Dasturiy ta’minotga yo‘naltirilgan oqimli shifrlar haqiqatan ham maxsus dizayn va mezonlarni talab qiladi. Bularning samaradorligi va xavfsizligini baholash uchun ko‘plab metodologiyalar va vositalar mavjud, lekin ularni to‘g‘ri qo‘llash va tushunish muhim ahamiyatga ega. Tasodifiylikdan og‘ishlarni tekshirish, ayniqsa, dasturiy ta’minotda amalga oshiriladigan oqimli shifrlarning xavfsizligini baholashda juda muhimdir [2,5,7].

Tasodifiylikni tekshirish uchun turli statistik test to‘plamlari mavjud. Bular orasida eng mashhuri NIST (National Institute of Standards and Technology) tomonidan ishlab chiqilgan testlar to‘plamidir. NIST SP 800-22 hisobotida taqdim etilgan testlar to‘plami, psevdotasodifiy va tasodifiy sonlar ketma-ketliklarining sifatini baholash uchun keng qo‘llaniladi. Bu testlar ketma-ketlikning chiziqli bo‘lmaganligi, muvozanati, periodi va boshqa xususiyatlarini tekshirish imkonini beradi.

Oqimli shifrlarni dasturiy ta’minotda qo‘llashda ularning kriptografik mustahkamligini baholash uchun turli xil kriptografik tahlillar mavjud. Bu tahlillar oqimli shifrlar uchun ma’lum bo‘lgan hujumlarga qarshi ularning qanchalik bardoshli ekanligini aniqlashga qaratilgan. Masalan, xorijiy kalit hujumi (related-key attack), vaqtiga bog‘liq hujumi (timing attack), va boshqalar.

Algoritmning xavfsizlik darajasini baholashda, ayniqsa oqimli shifrlash algoritmlarida, qayta sinxronizatsiya hujumlari va tegishli kalit hujumlariga qarshi bardoshliligi juda muhimdir. Bu hujum turlari algoritmning zaif joylarini aniqlash va ularni bartaraf etish uchun zarur bo‘lgan xavfsizlik choralari haqida tushuncha beradi.

Qayta sinxronizatsiya hujumlari, odatda, shifrlash algoritmi boshlang‘ich holatga qaytarilganda (masalan, initsializatsiya vektori orqali) amalga oshiriladi. Hujumchi bu jarayonni manipulyatsiya qilish orqali algoritmning ichki holatini aniqlashga harakat qiladi. Buning uchun hujumchi turli xil initsializatsiya vektorlari bilan ma’lumotlarni shifrlab, natijalarni taqqoslaydi. Bu usul yordamida hujumchi algoritmning ichki ishlash mexanizmini ochib, kalitni yoki shifrlangan ma’lumotni aniqlay oladi.

Chiqish ketma-ketligining chiziqli korrelyatsiyasini hisoblash, shifrlash algoritmlarining xavfsizligini baholashda muhim qadamdir. Bu, algoritm tomonidan yaratilgan ketma-ketlikning bashorat qilinish qiyinligi va tasodifiyligining kuchini aniqlaydi. Agar chiqish ketma-ketligining chiziqli korrelyatsiyasi past bo‘lsa, bu ketma-ketlikning yuqori darajada tasodifiy ekanligini va shu tariqa xavfsiz ekanligini ko'rsatadi. Bunday tahlil natijasida algoritmning shifrlash va xabar autentifikatsiyasini ta’minlash uchun ishonchli va samarali kriptografik vosita ekanligi aniqlanadi [10,11].

Chiqish ketma-ketligining chiziqli korrelyatsiyasi, ma’lum bir ketma-ketlikning boshqa ketma-ketliklar bilan qanchalik yaqin bog‘liqligini o‘lchaydi. Kriptografik kontekstda, bu o‘lchov ketma-ketlikning boshqa ketma-ketliklar bilan chiziqli bog‘liqligining darajasini ko‘rsatadi. Agar bu bog‘liqlik juda past bo‘lsa, demak algoritm kuchli tasodifiy chiqishlar yaratadi, bu esa xavfsizlik uchun juda muhimdir.

Yangicha yondashuv asosida yangi oqimli shifrlash algoritmlarini ishlab chiqish, bugungi kiber xavfsizlik muhitida dolzarb tadqiqot yo‘nalishlaridan biri hisoblanadi.

II. ASOSIY QISM

Algoritmning xavfsizligi ichki holat va chiqish bitlari o‘rtasidagi munosabatlarga juda bog‘liq ekanligi, kalitni to‘liq tanlash hujumi yoki oqimli shifrlash algoritmlariga qarshi boshqa strategiyalar orqali amalga oshiriladigan hujumlar ushbu munosabatlardan foydalanib, algoritmdan zaif joylarni topishga harakat qiladi. Bunday hujumlar, hujumchiga algoritmning ichki holatini aniqlash va shu orqali kalitni yoki shifrlangan matnni ochish imkonini beradi.

Tahlilchi tomonidan kirish va chiqish bitlari o‘rtasida yoki faqat chiqish bitlari o‘rtasida og‘ishlarni kuzatish imkoniyati, oqimli shifrlash algoritmlarining xavfsizligi uchun muhim ahamiyatga ega. Bunday og‘ishlar, hattoki ichki holat to‘g‘risida to‘liq ma’lumotga ega bo‘lmasa ham, hujumchiga foydali bo‘lishi mumkin. Bu falsafa asosida, xavfsiz psevdotasodifiy sonlar generatorining (PRNG) chiqish ketma-ketligini oldindan taxmin qilish imkonsiz bo‘lishi uchun, generatorning ichki holati va uning chiqish ketma-ketligi o‘rtasidagi munosabatlar diqqat bilan ko‘rib chiqilishi kerak. Yuqorida tilga olingan munosabatlar quyidagi uchta asosiy holatga bo‘linishi mumkin:

1. *Linearity (Chiziqli Munosabatlar)*. Chiziqli munosabatlar, PTSGning chiqish ketma-ketligida aniq bir chiziqli bog‘liqlik mavjudligini bildiradi. Bu, hujumchiga algoritmning kelajakdagi qiymatlarini prognoz qilish imkonini berishi mumkin, chunki chiziqli tenglamalar oson yechim topishi mumkin. Chiziqli munosabatlardan qochish uchun, chiziqli bo‘lmagan transformatsiyalardan va aralashtirish mekanizmlaridan foydalanish kerak.

2. *Predictability (Bashorat Qilinish)*. Bashorat qilinish, PTSGning kelajakdagi chiqishlari haqida oldindan ma’lumot olish imkoniyatini anglatadi, bu esa odatda ichki holatning yoki chiqish ketma-ketligining biron bir xususiyati tufayli yuzaga keladi. Bu xavfi minimallashtirish uchun, generatorning ichki holatini tez-tez va prognoz qilinmaydigan tarzda o‘zgartirish, shuningdek, chiziqli bo‘lmagan va murakkab matematik operatsiyalardan foydalanish tavsiya etiladi.

3. *Correlation (Korrelyatsiya Munosabatlari)*. Korrelyatsiya munosabatlari, PTSGning chiqish ketma-ketligidagi qiymatlar o‘rtasida aniq bir statistik bog‘liqlikning mavjudligini bildiradi. Agar bu bog‘liqliklar aniqlansa, ular hujumchiga generatorning ichki holati haqida qo'shimcha ma'lumot taqdim etishi mumkin. Korrelyatsiyadan qochish uchun, chiziqli bo‘lmagan operatsiyalarni, shuningdek, ichki holatning diversifikatsiyasini va kengaytirilgan tasodifiylikni ta’minlaydigan usullardan foydalanish kerak.

Boshqa tomondan, kalitlarni to‘liq qidirish haqiqiy kalitni topish uchun o‘rtacha 2^{127} ta hisoblashni talab qiladi. Agar amalga oshirigan hujumda o‘rtacha 2^{127} ta kalitni tanlash uchun sarflanadigan resursdan kamroq resurs sarf qilinsa, hujum samarali deb hisoblanadi [4].

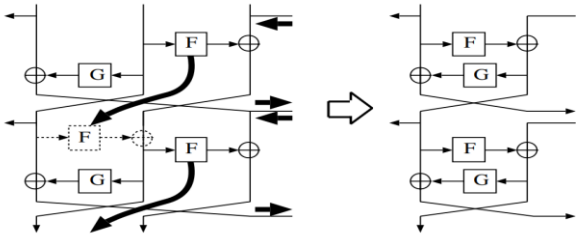
Chiziqli yaqinlashuvning faol S-qutilari sonini AS bilan belgilanadi. Taklif qilingan NSA algritmining S-boxining maksimal chiziqlilik ehtimoli 2^{-6} ni tashkil qiladi, shuning uchun AS<22 bilan chiziqli yaqinlashish bo‘lmasa, algoritmning chiqish ketma-ketligining chiziqliligi yetarlicha kichik deb taxmin qilish mumkin. Ushbu usulni taklif qilingan NSA algoritmiga qo‘llash natijasida quyidagi teorema o‘rnatildi:

Teorema. NSA algoritmining chiziqli approksimatsiyasi AS ≥ 22 ni tashkil qiladi.

Quyida ushbu teoremaning isboti keltiriladi. Chiqish birliklaridan tashkil topgan chiziqli yaqinlashishni qurish quyidagi tarzda ikki bosqichga bo‘linadi:

1. p ning chiziqli yaqinlashishlarini qurish.
2. Buferni o‘z ichiga olgan yo‘lni qidirish.

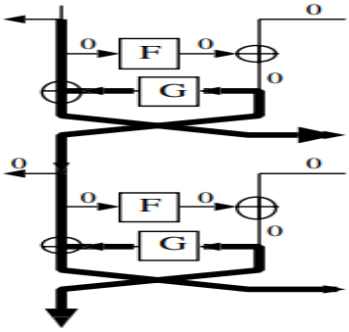
***p* ning chiziqli yaqinlashishlarini tuzish**. Baholashni boshlashdan oldin tahlil qilish osonroq bo‘lishi uchun p ning ekvivalent variantlari tanlanadi. 1-rasmda transformatsiyaning o‘zgartirilgan variantlari keltirilgan. Chap tomondagi F-funksiya G bilan belgilangan; Bu belgilashlardan faqat qulaylik uchun foydalaniladi. Birinchidan, F keyingi bosqichda chap tomonga o‘tkazilishi mumkin. Keyinchalik, chiqish birligiga mos keladigan niqob barcha qiymatlarni qabul qilishi mumkin, shuning uchun biz bu qismni ikkita maskaga, chiqish maskasi kirish maskasiga ajratiladi. Ushbu transformatsiya umumiy ma’noda ekvivalent emas, lekin maska shablonlari transformatsiya bilan o‘zgarmasligi ma’nosida ekvivalentdir. Shundan so‘ng biz keraksiz bog‘lanishlarni olib tashlaymiz. 1-rasmning o‘ng tomonida p funksiyning o‘zgartirilgan varianti tasvirlangan. Keyinchalik “p” o‘zgartirilgan p ni bildiradi. E’tibor bering, bog‘lamlar soni ikkiga kamayadi va F- va G - funksiyalarining chiqish maskalari to‘g‘ridan-to‘g‘ri tahlilchi tanlashi mumkin bo‘lgan “kirish” va “chiqish” maskalaridan keladi.



1-rasm. p funksiyning o‘zgartirilgan variant.

1-rasmda p ning ba’zi muhim yo‘llari ko‘rsatilgan. Faqat u erda ko‘rsatilgan beshta yo‘l faol S-boxlar soni beshdan ortiq ekanligini ta’minlaydi. M matritsaning tarmoq raqami $min_{x\neq 0}(w_H(x) + w_H(M_x))$ bilan aniqlanadi, bu erda $w_H(x)$ x ning bayt bo‘yicha Xemming og‘irligini bildiradi [1]. Chiziqli transformatsiyaning tarmoq raqami blokli shifrning diffuziya xususiyatlari uchun muhim xususiyatdir.

Ammo PTSG uchun M matritsasining tarmoqlari soni bir nechta faol F-funktsiyalarni o‘z ichiga olsa ham, chiziqli yaqinlashish uchun faol S-boxlari sonining pastki chegarasini kafolatlamaydi. Bu xususiyat blokli shifrlarning xossasidan keskin farq qiladi.



2-rasm. p funksiyaning chiziqli approksimatsiyalari.

NSA algoritmining chiziqli yo‘li. Keyinchalik, faqat chiqish bitlaridan iborat chiziqli taxminiylikni beruvchi buferni o‘z ichiga olgan yo‘l qidiriladi. PTSGlar uchun tahlilchi istalgan sonli raundlarni kuzatishi mumkin. Shunday qilib, har qanday raundning chiqishi bilan chiziqli yaqinlashuvni qurish mumkin. Bundan tashqari, ba’zi chiziqli yaqinlashishlar oraliq p-funksiyalarni o‘tkazib yuborishi mumkin, bu ko‘proq raundlarni kuzatish va og‘ishni oshirish imkoniyati mavjudligini anglatadi. Bu xususiyat barcha yo‘llarni qidirishni qiyinlashtiradi.

Yo‘lning birinchi va oxirgi raundlarini t_b va t_o deb belgilash mumkin. a holatidan b buferiga XOR qilingan ma’lumotlarga qo‘llaniladigan niqob $\Gamma(D)(t)$ sifatida belgilanadi. Bundan tashqari, faol F −funksiyani 1, nolga yaqin F −funksiyani 0 deb belgilab olish mumkin. Masalan, F −funksiya faol bo‘lsa, lekin t −davrda G −funksiya faol bo‘lmasa, bu holat $\Gamma(a)^{(t)} = (1,0)$ deb belgilanadi.

Birinchidan, biz yo‘lning birinchi va oxirgi bosqichiga alohida e’tibor berish zarur. Buferning barcha birliklari va ularning holati uchun kirish maskasining qiymati birinchi raundda nolga teng va faqat $Chiqish[t_b]$ chiqish birligining maskasi faol. Faqat ikkita yo‘l, 4-rasmdagi a) va c) holatlar bu shartni qondiradi. Oxirgi raund a) holat bilan bir xil, shuning uchun t_o raunddagi mumkin bo‘lgan yo‘llar faqat a) va b) holatlar sifatida ko‘rsatilgan.

Keyingi qadamda, buferning p ga ta‘sirini ko‘rib chiqiladi. $\Gamma(D)^{(t)}$ ning qiymati t_b raundda

$t_b + 4$ raundgacha 0 ga teng, chunki birinchi raund uchun barcha kirish maskalari 0 ga teng. Shuningdek, buferdan G funksiyasiga kirish maskasi faol bo‘lishi kerak, shuning uchun $\Gamma(D)^{(t_b+5)}$ faol. Xuddi shunday, $\Gamma(D)^{(t)}$ ning qiymati $t_o - 5 \le t \le t_o$ raundlarda 0 ga teng va $t_o - 5$ - raundda faoldir.

Agar $(\Gamma(a)^{(t_b+i)}, \Gamma(a)^{(t_b+i+1)}) = ((0,0),(1,1))$ bo‘lgan i $(1 \le i \le 4)$ raundlar bo‘lsa yo‘l a) yoki c) toifadagi faolroq F −funksiyalarni o‘z ichiga oladi, shuning uchun AS ≥ 25 bo‘ladi. Demak, faqat i 1 dan 4 gacha bo‘lgan barcha qiymatlari uchun $\Gamma(a)^{(t_b+i)} = 0$ bo‘lgan holatni ko‘rib chiqish zarur. Xuddi shunday oxirgi raund oldidagi maska i ning 1 dan 6 gacha qiymatlarning barchasi uchun $\Gamma(a)^{(t_o-i)} = 0$ bo‘lishi kerak. Bu shartga ko‘ra $\Gamma(a)^{(t_b+5)} \neq 0$. Bundan tashqari, $\Gamma(a)^{(t_b+5)}$ va $\Gamma(a)^{(t_o-6)}$ faol va $\Gamma(a)^{(t_o-6)}$ ning qiymati 0 ga teng. Demak, $t_o - t_b$ raundlar soni 14 dan katta bo‘lishi kerak. Ushbu natijalar va $\Gamma(a)^{(t_o-6)}$ ning faol ekanligi $\Gamma(a)^{(t_o-6)} \neq (0,0)$ yoki $\Gamma(a)^{(t_o-7)} \neq (0,0)$ ekanligini ko‘rsatadi. Shuning uchun bu holatda AS ≥ 22 ekanligi kelib chiqadi.

Qayta sinxronizatsiya va bog‘langan kalit hujumi. Qayta sinxronlash hujumi [2,6] PTSGlarga qarshi eng samarali hujum hisoblanadi, shuning uchun NSA algoritmini ham mazkur usul bilan baholash maqsadga muvofiq. Qayta sinxronizatsiya hujumi nafaqat maxfiy kalitga, balki umumiy parametrga ega bo‘lgan asosiy oqimli shifrlash algoritmi generatorlariga qarshi ishlatilishi mumkin. Agar algoritmni ishga tushirish juda oddiy bo‘lsa, bu samarali hujumdir. Maxfiy kalit o‘zgarmas holda o‘rnatilgan (fiksirlangan) degan faraz ostida, tahlilchi birinchi navbatda umumiy parametrlar va tegishli natijalar o‘rtasidagi bog‘liqlikni qidiradi. Agar bog‘liqlik ehtimoli yuqori bo‘lsa, u maxfiy kalit haqidagi ma‘lumotlarni taxmin qilish uchun ishlatilishi mumkin. Masalan, blokli shifrlarining sanagich rejimida chiziqli kriptotahlil qayta sinxronizatsiya hujumining bir turi hisoblanadi. Bog‘langan kalit hujumiga qarshi xavfsizlikni baholash dastlabki vektorlarni maxfiy kalitlar bilan almashtirish orqali qayta sinxronizatsiyaga o‘xshaydi.

NSA ning kirish va chiqishlari o‘rtasidagi munosabatni baholash uchun differensial va chiziqli xarakteristikalar hamda integral kriptotahlil [3] variantlari tanlandi. Ushbu xususiyatlardan foydalangan holda blokli shifrlarga qarshi hujumlar differensial kriptoanaliz [4] va chiziqli kriptoanaliz [5] deb nomlanadi. NSA algoritmining generatorining dizayni, ayniqsa uning p funksiyasi blokli shifrlash dizayniga juda o‘xshaydi. Bu shuni ko‘rsatadiki, yuqoridagi ikkita statistik xususiyat initsializatsiya vektori I va mos keladigan ichki holat o‘rtasidagi munosabatlarni baholash uchun juda mos keladi.

***p* ning takrorlanishining maksimal differensial va chiziqli xarakteristikalari**. Bufer va chiqish massivlariga XORni e‘tiborga olmasdan faqat p ning iteratsiyasini ko‘rib chiqiladi va uning differensial va chiziqli xususiyatlari baholanadi. Ushbu baholash usullarini blokli shifrlarga nisbatan ham xuddi shunday qo‘llash mumkin. 1 – jadvalda har bir hujum uchun a holat massivlarining barcha qismlarida faol F −funksiyalarining minimal soni ko‘rsatilgan.

1-jadval. p ning chiziqli va differensial yo‘llari uchun aktiv F − funksiyalarning soni.

Raund raqami	…	11	12	13	14	15	16	17	18	19	20	21	22	23
Differensial	…	10	12	12	12	14	16	16	16	18	20	20	20	22
Chiziqli	…	10	12	12	13	14	16	16	17	18	20	20	21	22

Qayta sinxronlash hujumiga bardoshlilik: 1-jadvalda initsializatsiya vektori I va p ning t −iteratsiyasidagi $a(t)$ holat massivlari o‘rtasidagi bog‘liqlik ko‘rsatilgan. Bu p ning 23 dan ortiq iteratsiyasi 2^{-128}dan yuqori ehtimollik bilan differentsial va chiziqli xususiyatlarga ega emasligini anglatadi.

NSA algoritmini ishga tushirishda initsializatsiya vektori I o‘rnatilgandan so‘ng faqat p funksiya 16 marta bajariladi. Keyinchalik, T funksiyaning tarkibida p funksiya yana 16 marta bajariladi. Biroq, bufer b a holatning differensial va chiziqli xarakteristikalariga faqat 9-iteratsiyadan so‘ng, ya’ni I o‘rnatilgandan keyin 22 iteratsiyadan keyin ta’sir qiladi. Shuning uchun, yuqoridagi xususiyatlar tufayli $t > 0$ iteratsiyadan keyin og‘ishni kuzatish qiyin degan xulosa berish mumkin [5].

Boshqa tomondan, 1-jadvalda I initsializatsiya vektori va 0-raundda mos keladigan b buferining ba’zi birliklari o‘rtasida qandaydir bog‘liqlik borligi ko‘rsatilgan. Biroq, differensial xarakteristika chiqish ketma-ketligidan iborat va buferda ikkitadan ortiq bufer birliklari mavjud. Mazkur birliklar o‘rtasidagi bog‘liqlik kuzatish va keraklicha natijaga erishish uchun juda kichik hisoblanadi. Shuning uchun tahlilchi bu korrelyatsiyadan foydalanishi imkonsiz hisoblanadi. Chiziqli kriptotahlil uchun ham shu xususiyatlar o‘rinli [1].

Bog‘langan kalit hujumi: Kalitlar va mos keladigan chiqishlar o'rtasidagi korrelyatsiyani kuzatish birinchi aralashtirish bosqichi tufayli initsializatsiya vektori va mos keladigan natijalar o‘rtasidagi korrelyatsiyadan ko'ra qiyinroq. Shunday qilib, differensial va chiziqli kriptoanaliz yordamida hech qanday xavfsizlik kamchiligi topilmadi.

Integral kriptotahlil. Yuqori baytga yo‘naltirilgan tuzilma tufayli Integral kriptotahlil hujumining ba’zi variantlarini [3] NSA algoritmiga nisbatan qo‘llab ko‘rish mumkin. Integral kriptotahlil hozirda SPN tuzilmasi bo‘lgan blokli shifrlarga (masalan, Rijndael, AES, Kuznechik kabi) qarshi eng muvaffaqiyatli hujumdir.

Blok shifriga qarshi Integral kriptotahlil bu tanlangan ochiq matnli hujum bo‘lib, bunda tahlilchi bir-biriga bog‘liq bo‘lgan bir nechta ochiq matn bloklarini tanlaydi, ularning har biri odatda faqat bir yoki ikki bayti bilan farqlanadi. Agar bayt barcha qiymatlarga ega bo‘lsa, ushbu tanlangan ochiq matnlarni aktiv to‘plam deyiladi va Λ deb belgilanadi. Agar to‘plamda farq qiluvchi bayt yoki ikki baytning barcha variantlari mavjud bo‘lsa bu to‘plam to‘liq tanlangan to‘plam deyiladi. Chiziqli bo‘lmagan funksiyaning kirishidagi to‘liq tanlanganlik tufayli, tahlilchi oraliq qiymatlarni ma‘lum darajada boshqarishini kutishi mumkin. Tahlilchi to‘liq tanlangan ochiq matn bloklari tufayli shifrlangan matn tomondan boshqariladigan oraliq qiymatni qisman aniqlaydi. Agar tahlilchi shifrlash kalitini qisman aniqlay olsa, mumkin bo‘lgan kalit variantlari ichidan haqiqiy va haqiqiy bo‘lmagan kalitlarni ajrata oladi [9].

Oqimli shifrlash algortimlarida tahlilchi ushbu hujumni o‘tkazish uchun kalit yoki initsializatsiya vektori qiymatlarining boshqa qiymatini tanlashga harakat qilishi kerak. Shuning uchun Integral kriptotahlilning hujumi bog‘langan kalit hujumi yoki tanlangan initsializatsiya vektori hujumiga keltirilishi kerak.

Bog‘langan kalit hujumi: Dastlab hujum modeli aniqlanishi zarur. Tahlilchi kalit qiymatini bilmaydi deb taxmin qilinadi. To‘liq tanlanganlik xususiyatini olish uchun tahlilchi bir qator kalitlarni ishga tushirishi zarur, tanlangan kalitlar faqat kalit qiymatining bir qismidagina farqlanadi. Ushbu mulohaza bo‘yicha kalitlarga bog‘liq bo‘lgan qismlarga e’tibor qaratiladi, bu yerda kalitlar bir bayt yoki ikki bayti bilan farqlanadi. Soxta tasodifiy sonlar ketma-ketligi chiqmagun-cha tajovuzkor hech narsani kuzata olmaydi. Tahlilchi bir qator iteratsiyalar orasida chiqish ketma-ketligida biron bir xususiyatni topishi mumkinligini tekshirish zarur [12].

To‘liq tanlangan kalitlar to‘plami buferni ishga tushirish paytida to‘plam to‘liq tanlanganlik xususiyati kiritiladi. Oraliq so‘zning xususiyatini shunday belgilaymizki, har bir raundda to‘plamning tegishli bayt qismi boshqa qiymatga ega bo‘ladi. Ishga tushirish uchun qiymati doimiy bo‘lgan ya’ni to‘plamning passiv elementlarini O bilan belgilanadi. Shuningdek, biz Φ bilan belgilangan eng zaif “balanslashgan” xususiyatini kiritiladi, ya’ni barcha to‘plamning tegishli elementining barcha qiymatlari bo‘yicha XOR yig‘indisi nolga teng. Agar to‘plamning elementi aktiv ham, passiv ham, balanslashgan ham bo‘lmasa, ya’ni boshqarib bo‘lmaydigan bo‘lsa, $*$ belgisi bilan belgilanadi. Agar uchlik (A, B, C) so‘zi A, B, C so‘zlari uchun Λ, O va Φ xossalariga ega bo‘lsa, u holda $(A, B, C) \xrightarrow{p} \Lambda, O, \Phi$ kabi, yoki $A \xrightarrow{p} \Lambda, B \xrightarrow{p} O, C \xrightarrow{p} \Phi$ kabi belgilanadi.

Shubhasiz, to‘yinganlikni kiritish uchun eng samarali element boshqa elementlarga oxirgi ta‘sir qiladigan so‘zdir. Shu sababli, $a_0, a_1, a_2 \xrightarrow{p} (\Lambda, O, O)$ holatlarini tahlil qilish zarur. $t-$ raundning chiqishi (a_0^t, a_1^t, a_2^t) bilan belgilanadi. To‘plam xususiyatlarining o‘zgarishi natijalari 2-jadvalda keltirilgan.

2-jadval. Oraliq qiymatlarda to‘plam elementlarning xususiyatlarining o‘zgarishi.

Oraliq qiymatlar	Elementlarning xususiyatlari
(a_0^0, a_1^0, a_2^0)	(Λ, O, O)
(a_0^1, a_1^1, a_2^1)	(O, O, Λ)
(a_0^2, a_1^2, a_2^2)	(O, Λ, O)
(a_0^3, a_1^3, a_2^3)	$(\Lambda, \Lambda, \Lambda)$
(a_0^4, a_1^4, a_2^4)	(Λ, Φ, Φ)
(a_0^5, a_1^5, a_2^5)	$(\Phi, *, *)$
$(a_0^{6+}, a_1^{6+}, a_2^{6+})$	$(*, *, *)$

Demak, bufer b_i ning boshlang'ich qiymatlari i indeksiga qarab quyidagi xususiyatlarga ega bo‘ladi:

$$b_i \xrightarrow{p} \begin{cases} O : i = 15,14 \\ \Lambda : i = 13,12 \\ \Phi : i = 11 \\ * : i = 10,9,8, \dots, 0 \end{cases} \quad (1)$$

E'tibor berish zarurki, (1) dagi xususiyatlar tahlilchi b_{11} gacha bo'lgan oraliq qiymatlarni nazorat qila oladi degani emas. Aslida, b_{11} boshqa bufer qiymatlari va bitta F −funksiyani baholash bilan ifodalanishi mumkin (chiziqli bo'lmagan bufer munosabatlari haqida yuqorida ta'kidlab o'tilgan). Biroq, initsializatsiya vektori kiritilgandan keyingi iteratsiyalardagi tasodifiylik tufayli, bu xususiyat chiqish ketma-ketligi ishlab chiqulgunga qadar bartaraf etiladi. Shuning uchun Integral kriptotahlil usuliga asoslangan tegishli kalit hujumi ham NSA algoritmiga nisbatan hech qanday xavf tug'dirmaydi deb hisoblash mumkin [6].

Qayta sinxronlash hujumi: Ushbu hujum yuqoridagi kalitlarni tanlashga asoslangan kriptotahlilga qaraganda amaliyroq bo'lishi mumkin. Biroq, Initsializatsiya vektori 16 iteratsiya aralashtirish tugamagunga qadar buferga hech qanday qiymat kiritmaydi. Yuqorida ko'rsatilgan boshqariladigan raundlar sonini hisobga olgan holda, 16 iteratsiya aralashtirish initsializatsiya vektorining tanlangan to'plam-laridagi to'liq tanlanganlik xususiyatini bartaraf qilish uchun yetarli.

III. XULOSA

Mazkur ishda Yangi taklif qilingan NSA (New Stream Algorithm) oqimli shifrlash algoritmi, uning noyob xususiyatlari va kuchli xavfsizlik mezonlari bilan, hozirgi va kelajakdagi kriptografik ehtiyojlarni qondirish potentsialiga ega. NSA (New Stream Algorithm) algoritmining bufer o'lchamining katta tanlanganligi va har bir raundda ikkita kalitdan foydalanilganligi kabi xususiyatlar, uning kriptotahlillarga bardosh-liligini ancha oshiradi. Bu xususiyatlar algoritmini turli xavf-xatarlarga qarshi yanada mustahkam qiladi. Ammo, kiber tahdidlar doimiy rivojlanib borishi bilan, NSA algoritmining xavfsizligini doimiy ravishda baholab turish va kerak bo'lganda uni yangilash muhimdir.

ADABIYOTLAR

[1] *J. Daemen*, "Cipher and hash function design strategies based on linear and differential cryptanalysis," Doctoral Dissertation, March 1995, K. U. Leuven

[2] *Rakhmatullaevich R. I., Mardano-kulovich I. B.* Analysis of cryptanalysis methods applied to stream encryption algorithms //Artificial Intelligence, Blockchain, Computing and Security Volume 1. – CRC Press, 2024. – С. 393-401.

[3] *Rahmatullayev I. R.* Oqimli shifrlash algoritmlari va ularni vujudga kelish sabablari //International Journal of Theoretical and Applied Issues of Digital Technologies. – 2022. – Т. 2. – №. 2. – С. 119-128.

[4] *Raxmatullayebich R. I.* Stream encryption algorithms and the basis of their creation //central asian journal of mathematical theory and computer sciences. – 2022. – т. 3. – №. 12. – с. 165-173.

[5] *Rahmatullayev I.* A new key stream encryption algorithm and its cryptanalysis: The new stream encryption algorithm (NSA-New Stream Algorithm) is proposed in this work. The input parameters are considered a 128-bit secret key and 128-bit initialization vectors in the new algorithm. A 64-bit line is generated in each round as the output value. The architecture of the algorithm is particularly suitable for efficient hardware implementations, together with this, this algorithm is also suitable for software implementation ... //Scientific and Technical Journal of Namangan Institute of Engineering and Technology. – 2023. – Т. 8. – №. 1. – С. 146-157.

[6] *Rakhmatullaev I.* Self-synchronizing (asynchronous) Stream Encryption Algorithms //Scientific Collection «InterConf». – 2023. – №. 164. – С. 249-254.

[7] *S. Fluhrer, M. Shamir*, "Weaknesses in the Key Scheduling Algorithm of RC4," Selected in Areas in Cryptography, SAC 2001, Springer-Verlag, LNCS 2259, pp. 1– 24, 2001.

[8] *A. Clark, J. Golic, W. Millan, L. Penna, L. Simpson*, "The LILI-128 Keystream Generator," NESSIE project submission, 2000, http://www.cryptonessie.org

[9] *S. Fluhrer*, "Cryptanalysis of the SEAL 3.0 Pseudorandom Function Family," Fast Software Encryption, FSE 2001, Proceedings, pp. 142–151, 2001.

[10] *Khudoykulov Z. T., Rakhmatullaev I. R., Umurzakov O. S. H.* NSA algoritmining akslantirishlari tanlanishining xavfsizlik talablarini bajarilishidagi o 'rni //International Journal of Theoretical and Applied Issues of Digital Technologies. – 2023. – Т. 6. – №. 4. – С. 97-101.

[11] *P. Rogaway, D. Coppersmith*, "A Software-Optimized Encryption Algorithm," Journal fo Cryptography, Vol. 11, No. 4, pp. 273–287, 1998.

[12] *Rahmatullayev I.R.* Algebraik kriptotahlil usuli va uning oqimli shifrlash algoritmlariga qo'llanish asoslari: Algebraic Cryptanalysis Method and

Basics of its Application to Stream Encryption Algorithm //International Journal of Theoretical and Applied Issues of Digital Technologies. – 2023. – Т. 4. – №. 2. – С. 96-102.

Поступила в редакцию 17.01.2024

Citation: *Xudoykulov, Z., Boyquziyev, I., & Rahmatullayev, I.* (2024). NSA (New Stream Algorithm) simmetrik oqimli shifrlash algoritmini kriptotahlil usullariga baholash mezonlari. Международный Журнал Теоретических и Прикладных Вопросов Цифровых Технологий, 7(1), 66–72. https://doi.org/10.62132/ijdt.v7i1.165

RESULTS OF ASSESSMENT OF NSA (NEW STREAM ALGORITHM) SYMMETRICAL STREAM ENCRYPTION ALGORITHM BY CRYPTOANALYSIS METHODS

Khudoykulov Z.T.[1], Boykuziev I.M.[1], Rakhmatullaev I.R.[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

Ilhom9001@gmail.com

Abstract. *In this paper, a new stream encryption algorithm called NSA (New Stream Algorithm) is proposed. This algorithm uses a 128-bit secret key and 128-bit seed vectors and produces a 64-bit output value in each round. The suitability of the algorithm for architectural and software implementations, security against resynchronization attack, linked key attack and linear correlation of output sequence attacks are evaluated. The robustness of the NSA algorithm against relevant key-based attacks and resynchronization attacks, as well as traditional methods such as differential and linear cryptanalysis, is analyzed in detail. The analysis results confirm that the NSA algorithm is a secure stream encryption algorithm. At the same time, the ability of the algorithm to resist various threats, including resistance to traditional and modern threats, is discussed. Analysis confirms that this algorithm is a secure stream encryption algorithm.*

Keywords: *Linear Feedback Shift Registers (LFSR), output sequence randomization, resynchronization attack, related key attack, linear cryptoanalysis, differential cryptoanalysis, integral cryptoanalysis.*

РЕЗУЛЬТАТЫ ОЦЕНКИ АЛГОРИТМА СИММЕТРИЧНОГО ПОТОКОВОГО ШИФРОВАНИЯ NSA (NEW STREAM ALGORITHM) МЕТОДАМИ КРИПТОАНАЛИЗА

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

Ilhom9001@gmail.com

Аннотация. *В статье предлагается новый алгоритм шифрования потока, называемый NSA (New Stream Algorithm). Этот алгоритм использует 128-битный секретный ключ и 128-битные начальные векторы и выдает 64-битное выходное значение в каждом раунде. Оцениваются пригодность алгоритма для архитектурной и программной реализации, защищенность от атак ресинхронизации, атак со связанными ключами и линейной корреляции атак на выходную последовательность. Подробно анализируется устойчивость алгоритма АНБ против соответствующих атак на основе ключей и атак ресинхронизации, а также традиционных методов, таких как дифференциальный и линейный криптоанализ. Результаты анализа подтверждают, что алгоритм АНБ является алгоритмом шифрования безопасного потока. При этом обсуждается способность алгоритма противостоять различным угрозам, в том числе устойчивости к традиционным и современным угрозам. Анализ подтверждает, что этот алгоритм является алгоритмом шифрования безопасного потока*.

Ключевые слова: *Linear Feedback Shift Registers (LFSR), случайность последовательности выходных данных, атака повторной синхронизации, атака привязанного ключа, линейный криптоанализ, дифференциальный криптоанализ, интегральный криптоанализ*.