UO‘K 004.056.55

A5/1 OQIMLI SHIFRLASH ALGORITMINI BARDOSHLILIGINI BAHOLASHNING YANGI YONDASHUVLARI

[+] *Rahmatullayev I.R.*[1,2], *Abduraximov B.F.*[3]

[1] Raqamli texnologiyalar va sun’iy intellektni rivojlantirish ilmiy-tadqiqot instituti, Toshkent, O‘zbekiston
[2] Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Samarqand filiali, Samarqand, O‘zbekiston
[2] Mirzo Ulug‘bek nomidagi O‘zbekiston milliy universiteti, Toshkent, O‘zbekiston

[+] ilhom9001@gmail.com

Annotatsiya. Ushbu maqolada A5/1 oqimli shifrlash algoritmining zaif tomonlari tahlil qilinib, unga hujum qilish uchun ikkita yangi yondashuv taklif etilgan. Birinchi usul majority bitlarning bog‘liqligini tahlil qilish orqali registrlarning qiymatlarini tiklashga asoslangan bo‘lsa, ikkinchi usul registrlarning boshlang‘ich qiymatlarini teskari hisoblashga qaratilgan. Tadqiqot natijalari shuni ko‘rsatadiki, A5/1 algoritmi zaifliklarga ega bo‘lib, ularni ekspluatatsiya qilish orqali registrlarning boshlang‘ich holatini tiklash yoki kalit oqimini oldindan hisoblash mumkin. Ushbu maqola A5/1 algoritmini chuqur kriptotahlil qilish, yangi hujum usullarini ishlab chiqish va algoritmning xavfsizlik darajasini baholash imkoniyatlarini o‘rganishga qaratilgan.

Kalit so‘zlar: A5/1, oqimli shifrlash, kriptotahlil, majority biti, LFSR, kalit oqimi, teskari hisoblash, GSM xavfsizligi, shifrlash algoritmlari, zaiflik tahlili.

1 KIRISH

Kriptografiya – bu ma’lumotlarni shifrlash va himoyalash bilan shug‘ullanuvchi fan sohasi bo‘lib, u axborot xavfsizligini ta’minlashda muhim o‘rin tutadi. Zamonaviy aloqa tizimlarida, xususan, GSM tarmoqlarida foydalaniladigan shifrlash algoritmlaridan biri A5/1 hisoblanadi. Ushbu algoritm oqimli shifrlash usuliga asoslangan bo‘lib, mobil aloqada uzatiladigan ma’lumotlarni shifrlash uchun ishlab chiqilgan [1].

A5/1 algoritmi GSM tarmoqlarida xavfsizlikni ta’minlash maqsadida ishlab chiqilgan bo‘lsa ham, uning tahlili va zaif tomonlari ko‘plab tadqiqotlarning asosiy mavzusiga aylangan. Ushbu maqolada A5/1 algoritmining ishlash prinsiplari, uning zaifliklari hamda algoritmga hujum qilish uchun taklif etilgan yangi yondashuvlar tahlil qilinadi [2].

Maqolaning asosiy maqsadi – A5/1 algoritmiga nisbatan amalga oshirilishi mumkin bo‘lgan hujum usullarini chuqur o‘rganish va ularning samaradorligini baholashdir. Bunda ikkita usul taklif etiladi: majority bitlarning bog‘liqligini tahlil qilish orqali registrlarning qiymatlarini tiklashga asoslangan usul va teskari aloqa bitlaridan foydalangan holda registrlarning boshlang‘ich qiymatlarini teskari hisoblash usuli.

Maqolada ushbu yondashuvlarning har biri alohida tahlil qilinib, ularning afzalliklari va kamchiliklari muhokama qilinadi. Natijada, A5/1 algoritmining zaif tomonlarini aniqlash va yanada samarali tahlil usullarini taklif etish imkoniyatlari o‘rganiladi.

2 ADABIYOTLAR TAHLILI

A5/1 oqimli shifrlash algoritmi bo‘yicha olib borilgan tadqiqotlar kriptografiya va axborot xavfsizligi sohalarida muhim mavzulardan biri hisoblanadi. Ushbu algoritm GSM tarmoqlarida ma’lumotlarni shifrlash uchun ishlab chiqilgan bo‘lib, uning zaifliklari va hujum usullari bo‘yicha turli tadqiqotlar amalga oshirilgan [3].

Dastlabki tadqiqotlar A5/1 algoritmining matematik modeli va uning kriptotahlilga nisbatan chidamliligini baholashga qaratilgan. Biryukov va Shamir (2000) A5/1 algoritmining zaif tomonlarini ochib beruvchi ilk ishlardan birini taqdim etdi [4]. Ushbu tadqiqotda algoritmning ichki mexanizmlaridan foydalangan holda samarali hujum usuli taklif qilindi, natijada A5/1 algoritmi real vaqt rejimida buzilishi mumkinligi isbotlandi. Keyinchalik Ekdahl va Johansson (2003) A5/1 algoritmining statistik

xususiyatlarini tahlil qilib, uning zaif nuqtalarini aniqlashga imkon beradigan yangi hujum metodlarini ilgari surdi [5].

Shuningdek, Golic (1997) tomonidan olib borilgan tadqiqotlar A5/1 algoritmining chiziqli tahlil metodlari yordamida zaif tomonlarini aniqlashga asoslangan edi [6]. Tadqiqotda LFSR registrlari orasidagi bog‘liqlik va ularning tahlil qilinishi mumkin bo‘lgan strukturasi ko‘rib chiqilgan.

A5/1 algoritmi uchta LFSR (Linear Feedback Shift Register) asosida ishlaydi va ularning boshqarilishi majority bit mexanizmi orqali amalga oshiriladi. Maximov va Biryukov (2005) ushbu mexanizmni atroflicha o‘rganib, uning zaif tomonlarini ekspluatatsiya qilish orqali algoritmga nisbatan samarali hujumlarni amalga oshirish mumkinligini isbotladi [7]. Ular tomonidan taklif qilingan tahlil usuli yordamida kalit oqimi bitlarini qayta tiklash va algoritmni teskari hisoblash imkoniyati o‘rganildi.

Bundan tashqari, Hell, Johansson va Meier (2007) tadqiqotlari majority bit mexanizmining tasodifiylik darajasini baholab, uni zaiflashtirish uchun optimal strategiyalarni ishlab chiqishga qaratilgan edi [8].

A5/1 algoritmiga qarshi qo‘llaniladigan hujum usullari orasida tashqi xotira hujumlari (TMTO - Time-Memory Trade-Off), ko‘pchilik ovoz mexanizmiga asoslangan hujumlar, va teskari aloqa bitlarini tahlil qilish orqali registrlarni tiklash kabi yondashuvlar keng qo‘llanilgan.

Barkan, Biham va Keller (2006) tomonidan olib borilgan tadqiqotda A5/1 algoritmining zaif tomonlarini ekspluatatsiya qilish uchun TMTO usuli ishlatildi va real sharoitda algoritmni buzish mumkinligi isbotlandi. Ushbu yondashuv kriptotahlilda sezilarli yutuqlarga olib keldi va A5/1 algoritmining muhim zaifliklarini ochib berdi [9].

Shuningdek, Nohl, Meier va Preneel (2010) A5/1 algoritmini buzish uchun precomputed rainbow table (oldindan hisoblangan kalitlar to‘plami) usulini taklif qilib, bu orqali algoritmni real vaqt rejimida tezkor tahlil qilish imkoniyatini ko‘rsatdi [10].

Ko‘plab tadqiqotchilar A5/1 algoritmining zaif tomonlarini bartaraf etish va uni kuchaytirish bo‘yicha izlanishlar olib borgan. Kumar va Varshney (2018) tomonidan taklif etilgan yondashuvda A5/1 algoritmini mustahkamlash uchun qo‘shimcha kriptografik mexanizmlar va hash-funktsiyalar bilan kombinatsiyalangan himoya usullari taklif qilindi [11].

Jakobsen va Knudsen (2015) esa A5/1 algoritmini takomillashtirish uchun LFSR registrlarini o‘zgartirish va qo‘shimcha kiritish mexanizmlarini qo‘llash orqali xavfsizlikni oshirish imkoniyatlarini o‘rganib chiqdi [12].

A5/1 algoritmi bo‘yicha olib borilgan tadqiqotlar natijalaridan kelib chiqib, uning zaif tomonlarini aniqlash va ularni bartaraf etish bo‘yicha turli yondashuvlar taklif etilgan. Biroq, zamonaviy hisoblash quvvatlarining o‘sishi bilan birgalikda, ushbu algoritmga nisbatan hujumlarning samaradorligi oshib bormoqda.

Maqolada ko‘rib chiqilgan majority bit tahlili va teskari aloqa bitlariga asoslangan hujum usullari ilgari olib borilgan tadqiqotlar bilan bog‘liq bo‘lib, ular algoritmning zaif tomonlarini yanada chuqurroq o‘rganish imkonini beradi. Shu sababli, kelajak tadqiqotlarida ushbu yondashuvlar asosida real sharoitlarda sinovlar o‘tkazish va ularning samaradorligini oshirish yo‘nalishida izlanishlar olib borish maqsadga muvofiq bo‘ladi.

3 METODOLOGIYA

A5/1 algoritmi GSM (Global System for Mobile Communications) tarmog‘ida ma’lumotlarni shifrlash uchun ishlab chiqilgan. A5/1 oqimli shifrlash algoritmi bo‘lib, u uzatiladigan ma'lumotlarni bit-by-bit shaklida shifrlaydi.

Algoritmda uchta o‘zaro bog‘liq bo‘lmagan chiziqli teskari bog‘liqli registrlardan (LFSR - Linear Feedback Shift Registers) foydalaniladi. Ular quyidagilar:

19-bitli LFSR (R1);
22-bitli LFSR (R2);
23-bitli LFSR (R3).

Algoritm boshlang‘ich kalit (64-bit) va kadr raqami (22-bit) bilan ishga tushadi, bu esa har bir kadr uchun alohida kalit oqim (keystream) hosil qilinishini ta’minlaydi.

Uchta LFSR "ko‘pchilik ovoz" (majority vote) qoidasi yordamida boshqariladi. Bu sinxronizatsiyani kuchaytirish va xavfsizlikni oshirishga yordam beradi.

LFSRlar o‘zaro ko‘pchilik ovoz usuli (majority vote mechanism) yordamida sinxronlashadi.

Majority bit (ko‘pchilik biti) tushunchasi A5/1 algoritmida uchta LFSR (Linear Feedback Shift Register) o‘rtasida sinxronizatsiyani boshqarish uchun ishlatiladi. Ushbu mexanizm yordamida qaysi registrlar keyingi bosqichda harakat qilishini aniqlash mumkin.

A5/1 algoritmidagi uchta registrdan har birining bitta muhim biti mavjud bo‘lib, ular "ko‘pchilik ovoz berish" qoidasi bo‘yicha baholanadi. Ushbu bitlar quyidagilar:

- $R1$: 8-pozitsiyadagi bit (majority biti uchun mas'ul);
- $R2$: 10-pozitsiyadagi bit (majority biti uchun mas'ul);
- $R3$: 10-pozitsiyadagi bit (majority biti uchun mas'ul).

Bu bitlar majority bitni aniqlashda asosiy rol o'ynaydi.

Uchta registrning majority bitni aniqlashda foydalaniladigan major bitlari qiymatlari ichida ko'pchilik bit qaysiligi (masalan, 0 yoki 1) asosiy natijani beradi.

Agar ikkita yoki undan ortiq registr major biti bitta qiymatga ega bo'lsa, ushbu qiymat majority bit bo'ladi.

Majority bit A5/1 algoritmida registrlarni harakatga keltirish uchun ishlatiladi:

Agar biror registrning major biti majority biti bilan bir xil bo'lsa, u holda ushbu registr keyingi bosqichda harakat qiladi (ya'ni, shift operatsiyasi bajariladi).

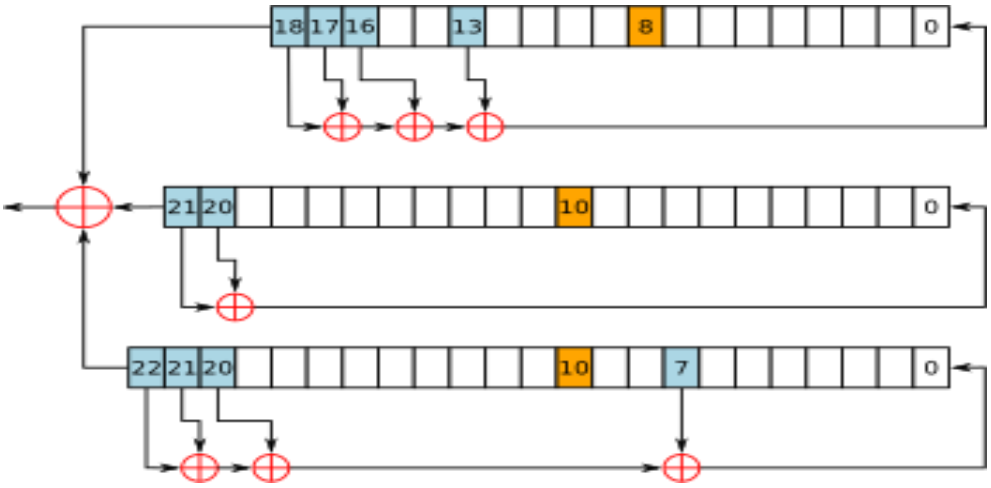
Agar registrning major biti majority biti bilan mos kelmasa, u holda registr harakatsiz qoladi.

Bu mexanizm algoritmga bir oz noaniqlik kiritib, hujumchilar uchun qiyinchiliklar tug'diradi. Shu bilan birga, bu mexanizm algoritmni chiziqlilikdan biroz uzoqlashtiradi, ammo zamonaviy hujum usullari bunday zaiflikni ham tahlil qilishga qodir.

Major bitlari majoriy bitga teng bo'lgan registrlar surilgandan keyin LFSRlarning chiqish bitlari XOR amali orqali birlashtiriladi va kalit oqimi (key stream) hosil qilinadi.

Hosil bo'lgan kalit oqimi ma'lumotlar oqimi bilan XOR amalini bajarib, shifrlangan ma'lumotlar oqimini hosil qiladi.

Algoritmning asosiy afzalligi sifatida ishlash tezligi yuqoriligi va kam resurs talab qilishi hisoblanadi, bu esa GSM qurilmalarida foydalanish uchun qulaylik yaratadi.



1-rasm. A5/1 shifrlash algoritmining ishlash sxemasi

A5/1 algoritmida kalit oqimining har bitini hosil qilishda quyidagi 4 ta holatdan biri bo'lishi mumkin:

$$\begin{gathered} R1 \text{ va } R2 \text{ suriladi, } R3 \text{ surilmaydi: } R1[17]\oplus R2[20]\oplus R3[22] = K[i]; \\ R1 \text{ va } R3 \text{ suriladi, } R2 \text{ surilmaydi: } R1[17]\oplus R2[21]\oplus R3[21] = K[i]; \\ R2 \text{ va } R3 \text{ suriladi, } R1 \text{ surilmaydi: } R1[18]\oplus R2[20]\oplus R3[21] = K[i]; \\ R1, R2 \text{ va } R3 \text{ suriladi: } R1[17]\oplus R2[20]\oplus R3[21] = K[i]. \end{gathered} \quad (1)$$

Kalit oqimi biti $K[i] = 0$ bo'lgan holat uchun:

$$\begin{gathered} 0\oplus 0\oplus 0 = 0; \\ 0\oplus 1\oplus 1 = 0; \\ 1\oplus 0\oplus 1 = 0; \\ 1\oplus 1\oplus 0 = 0. \end{gathered} \quad (2)$$

Kalit oqimi biti $K[i] = 1$ bo'lgan holat uchun:

$$\begin{gathered} 0\oplus 0\oplus 1 = 1; \\ 0\oplus 1\oplus 0 = 1; \\ 1\oplus 0\oplus 0 = 1; \\ 1\oplus 1\oplus 1 = 1. \end{gathered} \quad (3)$$

K=01111110011001001001100001011111001001111011110111… hosil qilingan kalit oqimi bo'lsa $K[0] = 0$ holat uchun (2) ifodaga ko'ra quyidagi variantlardan biri bo'lishi mumkin:

$$\begin{gathered} R1\ va\ R2\ suriladi, R3\ surilmaydi: R1[17]=0, R2[20]=0, R3[22]=0; \\ R1\ va\ R3\ suriladi, R2\ surilmaydi: R1[17]=0, R2[21]=1, R3[21]=1; \\ R2\ va\ R3\ suriladi, R1\ surilmaydi: R1[18]=1, R2[20]=0, R3[21]=1; \\ R1, R2\ va\ R3\ suriladi: R1[17]=1, R2[20]=1, R3[21]=0. \end{gathered} \quad (4)$$

$K[1]=1$ holat uchun (3) ifodaga ko‘ra quyidagi variantlardan biri bo‘lishi mumkin:

$$\begin{gathered} R1\ va\ R2\ suriladi, R3\ surilmaydi: R1[17]=0, R2[20]=0, R3[22]=1; \\ R1\ va\ R3\ suriladi, R2\ surilmaydi: R1[17]=0, R2[21]=1, R3[21]=0; \\ R2\ va\ R3\ suriladi, R1\ surilmaydi: R1[18]=1, R2[20]=0, R3[21]=0; \\ R1, R2\ va\ R3\ suriladi: R1[17]=1, R2[20]=1, R3[21]=1. \end{gathered} \quad (5)$$

$R1$ va $R2$ suriladi, $R3$ surilmaydi: $R1[17]=0, R2[20]=0, R3[22]=0$ va $R1$ va $R2$ suriladi, $R3$ surilmaydi: $R1[17]=0, R2[20]=0, R3[22]=1$ holatlar uchun $R1[8]=R2[10]\neq R3[10]$ bo‘ladi.

$R1$ va $R3$ suriladi, $R2$ surilmaydi: $R1[17]=0, R2[21]=1, R3[21]=1$ va $R1$ va $R3$ suriladi, $R2$ surilmaydi: $R1[17]=0, R2[21]=1, R3[21]=0$ holatlar uchun $R1[8]=R3[10]\neq R2[10]$ bo‘ladi.

$R2$ va $R3$ suriladi, $R1$ surilmaydi: $R1[18]=1, R2[20]=0, R3[21]=1$ va $R2$ va $R3$ suriladi, $R1$ surilmaydi: $R1[18]=1, R2[20]=0, R3[21]=0$ holatlar uchun $R2[10]=R3[10]\neq R1[8]$ bo‘ladi.

$R1$, $R2$ va $R3$ suriladi: $R1[17]=1, R2[20]=1, R3[21]=0$ va $R1$, $R2$ va $R3$ suriladi: $R1[17]=1, R2[20]=1, R3[21]=1$ holatlar uchun $R1[8]=R2[10]=R3[10]$ bo‘ladi.

4 NATIJALAR TAHLILI

Yuqoridagilardan kelib chiqib A5/1 oqimli shifrlash algoritmi uchun quyida ketiriladigan tahlil usullarini amalga oshirish algoritmlari samarali bo‘ladi.

Algoritm 1.

1. $K[0], K[1]$, ... kalit oqimi qiymatlarini tartiblashtirish;
2. 4), 5) va (6) ifodalarning bajarilishini rekursiv tarzda ifodalash;
3. Har bir iteratsiya uchun $R1[8], R2[10], R3[10]$ major bitlarining bog‘ligini kuzatish;
4. Yuqoridagi 2- va 3- qadamlarni $R1[8], R2[10], R3[10]$ bitlarini mazkur major bitlarining kalit oqimini hisoblashda ishtirok etuvchi $R1[17], R1[18], R2[20], R2[21], R3[21], R3[22]$ registr o‘rniga kelguncha davom ettirish;
5. Navbatdagi iteratsiyadagi mos kalit biti uchun (4) va (5) ifodalarning bajarilishini tekshirish va mos iteratsiyadagi $R1[17], R1[18], R2[20], R2[21], R3[21], R3[22]$ registrlarning qiymatlarini aniqlash;
6. Keyingi iteratsiyalar uchun ham shu qadamlarni takrorlash.

Algoritm 2.

1. $R1$ registrning $R1[18], R1[17], R1[16], R1[13]$ teskari aloqani ta’minlash bitlari va R1[8] major biti, $R2$ registrning $R2[21], R2[20]$ teskari aloqani ta’minlash bitlari va R2[10] major biti, $R3$ registrning $R3[22], R3[21], R3[20], R3[7]$ teskari aloqani ta’minlash bitlari va R3[10] major biti, jami 13 bit to‘liq tanlash usuli bilan tanlanadi;
2. Tanlangan registr bitlari yordamida kalit oqimining tegishli bitlarini hisoblash amalga oshiriladi;
3. Tanlangan registr bitlarining 2-qadamda hisoblash shartlarini qanoatlantirgan variantlari qoldiriladi;
4. 2-3-qadamlardagi hisoblash natijalaridan major bitlarining qiymatlariga mos ravishda suriladigan registrlarni teskari aloqa bitlari yordamida surish va surilgan registrlar uchun mos bitlarni yangisi bilan almashtirish, bunda yarim bitlar uchun to‘liq tanlash amalga oshiriladi.
5. 2-4-qadamlar teskari aloqa registrlari yordamida registrlarning surilgan qiymatlari registrlarning major bitlariga yetib kelguncha davom ettiriladi.
6. Keyingi har bir iteratsiyada regitrlarning mos qiymatlarini aniqlash amalga oshiriladi.

1-algoritmning maqsadi A5/1 algoritmining majority bitlarining ta’sirini tahlil qilib, registrlarning muhim bitlarini aniqlash va kalit oqimi bitlari bilan bog‘liq bog‘lanishlarni ochish hisoblanadi. Quyida har bir qadamni tahlili keltirilgan.

1. Kalit oqimi bitlarini tartiblashtirish. Kalit oqimi K[0], K[1], ... bitlari tartibga solinadi, ya’ni tahlil qilish uchun ketma-ketlik hosil qilinadi.

Bu qadam keyingi bosqichlarda kalit oqimi bitlari va registrlarning o‘zaro bog‘liqligini tahlil qilishga yordam beradi.

2. Rekursiv ifodalash. A5/1 algoritmining ishlash qoidalariga muvofiq (4), (5) va (6) bosqichlarning rekursiv tarzda bajarilishini o‘rnatish nazarda tutilgan.

Bu majority mexanizmining har iteratsiyadagi ta’sirini hisoblashni osonlashtiradi.

3. $R1[8], R2[10], R3[10]$ bitlarining major bitlar bilan bog‘liqligini kuzatish. $R1[8], R2[10], R3[10]$ - bu har bir registrning majority mexanizmi uchun tanlangan trigger bitlari. Ularning kalit oqimi bitlaridagi roli va qanday ta’sir qilishini kuzatish mumkin.

4. 2- va 3-qadamlarni davom ettirish. Registrlarning muhim bitlari ($R1[17], R1[18], R2[20], R2[21], R3[21], R3[22]$) aniqlanguncha 2- va 3-qadamlarni takrorlash.

Maqsad: ushbu bitlarning ta’siri va ularning qiymatlari kalit oqimi bitlari bilan qanday bog‘liqligini ochish.

5. Mos iteratsiyadagi registr bitlarini aniqlash. Yangi kalit oqimi biti hosil bo‘lishida qaysi registr bitlari ishtirok etayotganini tekshirish. (4) va (5) ifodalar bajarilishi bilan ushbu registr bitlarining qiymatlarini topish va keyingi bosqichlar uchun asos yaratish.

6. Keyingi iteratsiyalar uchun shu qadamlarni takrorlash. Har bir iteratsiya uchun ushbu jarayonni davom ettirish orqali butun kalit oqimi bitlari ketma-ketligi bo‘yicha registrlarning o‘zgarishini kuzatish.

Bu registrlarning boshlang‘ich holatini qayta tiklash yoki kriptotahlil qilish imkoniyatini yaratadi.

1-algoritmning afzalliklari: majority bitlarning ta’siri batafsil o‘rganiladi – bu keyinchalik registr bitlarining orqaga hisoblanishini amalga oshirish imkonini beradi; rekursiv bog‘lanishlarni tahlil qilish orqali A5/1 ichki mexanizmlarini chuqurroq o‘rganish; kalit oqimi bitlari orqali registrlarning muhim bitlarini qayta tiklash imkoniyati paydo bo‘lishi mumkin;

Hamda kamchiliklari va mumkin bo‘lgan qiyinchiliklar: rekursiv hisoblash hajmi oshib ketishi mumkin – agar uzun keystream bilan ishlansa, bu ko‘p resurs talab qilishi mumkin; majority mexanizmi tasodifiy bo‘lib, u registrlarning qaysi biri surilishini har safar o‘zgartirib yuborishi natijasida aniqlash qiyinlashishi mumkin; raqobatbardosh usullar (masalan, XOR-linear analiz yoki diferencial analiz) bilan solishtirganda praktikaga joriy qilish qiyin bo‘lishi mumkin.

2-algoritmning esa A5/1 registrlarini to‘liq tanlash (brute-force) usuli orqali tahlil qilish va teskari hisoblash imkoniyatini berishi bilan farqlanadi. Har bir qadamni batafsil tahlil qilamiz:

1. Registrlarning muhim bitlarini to‘liq tanlash:

R1: $R1[18], R1[17], R1[16], R1[13]$ (teskari aloqa) va $R1[8]$ (major bit);

R2: $R2[21], R2[20]$ (teskari aloqa) va $R2[10]$ (major bit);

R3: $R3[22], R3[21], R3[20], R3[7]$ (teskari aloqa) va $R3[10]$ (major bit);

Jami 13 ta bit tanlab olinadi va barcha mumkin bo‘lgan qiymatlar sinab ko‘riladi (brute-force approach).

2. Kalit oqimi bitlarini hisoblash. Tanlangan bitlar asosida keystream bitlari hosil qilinadi. Ushbu bosqich A5/1 algoritmidagi teskari aloqa bitlarining keystreamga ta’sirini aniqlashga yordam beradi.

3. Faqat mos keluvchi variantlarni tanlab qoldirish. Hamma kombinatsiyalar tekshirilmaydi, faqat teskari aloqa va major bitlariga mos keladigan natijalar qoldiriladi. Bu tahlil hajmini kamaytirishga yordam beradi va tezlikni oshiradi.

4. Registrlarni teskari aloqa bitlari orqali qayta tiklash. Mos bitlarni yangilab borish orqali registrlarning harakatini orqaga qaytarish. Yarim bitlarni to‘liq tanlash (half-bit selection) orqali variantlarni tekshirish. Registrlar major bitlarga yetib kelguncha bu jarayon davom etadi.

5. Har bir iteratsiyada registrlarning qiymatlarini aniqlash. Keyingi iteratsiyalarda registrlarning yangi qiymatlari hisoblab chiqiladi. Shu yo‘l bilan boshlang‘ich holatni tiklash yoki kalitni qayta tiklashga erishiladi.

Afzalliklari: to‘liq tanlash (brute-force) usuli orqali registrlarni tahlil qilish imkoniyati mavjud; har bir iteratsiyada registrlarning harakatini kuzatib borish va teskari hisoblashni amalga oshirish mumkin; A5/1 algoritmiga chuqurroq kriptotahlil qilish uchun moslashuvchanlik mavjud.

Kamchiliklari va mumkin bo‘lgan qiyinchiliklar: Brute-force usuli juda ko‘p kombinatsiyalarni sinovdan o‘tkazishni talab qilishi mumkin; real vaqtli hujum uchun bu usul ancha resurs talab qilishi mumkin; majority mexanizmi tasodifiy bo‘lib, uni teskari hisoblash har doim ham oson emas.

5 XULOSA

Ushbu maqolada A5/1 oqimli shifrlash algoritmi tahlil qilinib, unga hujum qilish uchun ikkita yangi usul taklif etildi. Birinchi yondashuv majority bitlarning bog‘liqligini tahlil qilish orqali registrlarning qiymatlarini tiklashga asoslangan bo‘lsa, ikkinchi yondashuv registrlarning boshlang‘ich qiymatlarini teskari hisoblashga qaratilgan.

Tahlil natijalari shuni ko‘rsatdiki, A5/1 algoritmining zaif tomonlari mavjud bo‘lib, ularni ekspluatatsiya qilish orqali registrlarning boshlang‘ich holatini tiklash yoki kalit oqimini oldindan hisoblash mumkin. Ayniqsa, majority bitlarning roli va teskari aloqa mexanizmlarining zaifliklari ushbu algoritmning kriptotahlilga moyilligini oshiradi.

Taklif etilgan usullar turli tahlil strategiyalarini birlashtirgan holda, A5/1 algoritmining xavfsizlik darajasini baholash imkoniyatini beradi. Kelajak tadqiqotlari uchun ushbu yondashuvlar real sharoitlarda sinovdan o‘tkazilib, ularning samaradorligini oshirish yo‘nalishlari ishlab chiqilishi mumkin.

Tadqiqotdan kelib chiqib, A5/1 algoritmining mustahkamligini oshirish uchun yanada murakkab shifrlash usullarini qo‘llash zarurati kelib chiqadi. Ushbu yondashuvlarni amaliy sinovlardan o‘tkazish va ularning samaradorligini baholash kelajak tadqiqotlar uchun muhim yo‘nalish hisoblanadi.

ADABIYOTLAR

[1] *Rakhmatullaevich R. I., Mardanokulovich I. B.* Analysis of cryptanalysis methods applied to stream encryption algorithms //Artificial Intelligence, Blockchain, Computing and Security Volume 1. – CRC Press, 2023. – C. 393-401.
[2] *Xudoykulov Z. T., Rahmatullayev I. R.* Yangi oqimli shifrlash algoritmlari va uning kriptotahlili //Milliy standart Ilmiy-texnik jurnali. – 2023. – C. 42-47.
[3] *Turakulovich X. Z., Rahmatullayevich R. I.* Mavjud oqimli shifrlash algoritmlarining qiyosiy tahlili //Al-Farg’oniy avlodlari. – 2024. – T. 1. – №. 1. – C. 129-134.
[4] *Biryukov, A., & Shamir, A.* (2000). “Cryptanalysis of the A5/1 GSM Stream Cipher.” Proceedings of Fast Software Encryption, Springer, pp. 1-17.
[5] *Ekdahl, P., & Johansson, T.* (2003). “A New Attack on A5/1.” Proceedings of Selected Areas in Cryptography (SAC), Springer, pp. 239-255.
[6] *Golic, J. D.* (1997). "Cryptanalysis of Alleged A5 Stream Cipher." Advances in Cryptology – EUROCRYPT '97, Springer, pp. 239-255.
[7] *Maximov, A., & Biryukov, A.* (2005). "Two Efficient Attacks on A5/1." Proceedings of Selected Areas in Cryptography (SAC), Springer, pp. 1-18.
[8] *Hell, M., Johansson, T., & Meier, W.* (2007). "Grain: A Stream Cipher for Constrained Environments." International Journal of Information Security, 6(3), pp. 235-244.
[9] *Barkan, E., Biham, E., & Keller, N.* (2006). "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication." Advances in Cryptology – CRYPTO 2003, Springer, pp. 600-616.
[10] *Nohl, K., Meier, W., & Preneel, B.* (2010). "Reverse-Engineering A5/1." Proceedings of USENIX Security Symposium, pp. 1-16.
[11] *Kumar, S., & Varshney, S.* (2018). "Enhancing A5/1 Algorithm Security using Hybrid Cryptographic Mechanism." International Journal of Information Security Science, 7(1), pp. 12-22.
[12] *Jakobsen, T., & Knudsen, L.* (2015). "Enhancing LFSR-Based Stream Ciphers." Journal of Cryptographic Engineering, 5(2), pp. 65-78.

Поступила в редакцию 30.01.2025

Citation: *Rahmatullayev I.R, Abduraximov B.F.* (2025). A5/1 oqimli shifrlash algoritmini bardoshliligini baholashning yangi yondashuvlari. Raqamli texnologiyalarning nazariy va amaliy masalalari xalqaro jurnali. 8(1). – B. 122-128. https://doi.org/10.62132/ijdt.v8i1.240.

NEW APPROACHES TO ASSESSING THE RESILIENCE OF THE A5/1 STREAM CIPHER ALGORITHM

[+] *Rakhmatullaev I.R.*[1,2], *Abdurakhimov B.F.*[3]
[1] Digital technologies and artificial intelligence develomment research institute, Tashkent, Uzbekistan
[2] Samarkand branch of Tashkent University of Information Technologies named after Muhammad Al-Khwarizmi, Samarkand, Uzbekistan
[3] National University of Uzbekistan named after Mirzo Ulugbek, Tashkent, Uzbekistan

[+] ilhom9001@gmail.com

Abstract. This article analyzes the vulnerabilities of the A5/1 stream cipher algorithm and proposes two new approaches to attack it. The first method is based on reconstructing the values of registers by analyzing the dependencies of majority bits, while the second method focuses on reverse-calculating the initial values of registers. Research results indicate that the A5/1 algorithm has weaknesses that can be exploited to recover the initial state of registers or predict the key stream in advance. This article aims to explore the possibilities for in-depth

cryptanalysis of the A5/1 algorithm, develop new attack methods, and assess the algorithm's security level.

Keywords: A5/1, stream cipher, cryptanalysis, majority bit, LFSR, key stream, reverse calculation, GSM security, encryption algorithms, vulnerability analysis.

НОВЫЕ ПОДХОДЫ К ОЦЕНКЕ УСТОЙЧИВОСТИ АЛГОРИТМА ПОТОКОВОГО ШИФРОВАНИЯ A5/1

[+] *Рахматуллаев И.Р.*[1,2], *Абдурахимов Б.Ф.*[3]

[1] НИИ развития цифровых технологий и искусственного интеллекта, Ташкент, Узбекистан
[2] Самаркандский филиал Ташкентского университета информационных технологий имени Мухаммада ал-Хоразмий, Самарканд, Узбекистан
[3] Национальный университет Узбекистана имени Мирзо Улугбека, Ташкент, Узбекистан

[+] ilhom9001@gmail.com

Аннотация. В данной статье проанализированы уязвимости алгоритма потокового шифрования A5/1 и предложены два новых подхода для атаки на него. Первый метод основан на восстановлении значений регистров путем анализа зависимости majority-битов, а второй метод направлен на обратное вычисление начальных значений регистров. Результаты исследования показывают, что алгоритм A5/1 имеет уязвимости, эксплуатация которых позволяет восстановить исходное состояние регистров или предварительно рассчитать поток ключей. Данная статья направлена на глубокий криптоанализ алгоритма A5/1, разработку новых методов атаки и оценку уровня безопасности алгоритма.

Ключевые слова: A5/1, поточное шифрование, криптоанализ, majority-бит, LFSR, поток ключей, обратное вычисление, безопасность GSM, алгоритмы шифрования, анализ уязвимостей.