UDK 004.415

ALGEBRAIK KRIPTOTAHLIL USULI VA UNING OQIMLI SHIFRLASH ALGORITMLARIGA QO‘LLANISH ASOSLARI

Rahmatullayev I.R.[1]

[1] Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Samarqand filiali, Samarqand, O‘zbekiston

Ilhom9001@mail.com

Annotatsiya. *Mazkur ishda oqimli shifrlash algoritmlarini algebraik kriptotahlil usullari orqali baholash jarayonlari tahlil qilingan. Tahlil qilingan algoritmni NIST statistik testlari yordamida tasodifiylik bo‘yicha baholash natijalari olingan. Generatsiya qilish tezligi bo‘yicha olingan natijalar parametrlari solishtirilgan.*

Kalit so‘zlar: *Algebraik krtiptotahlil, NIST, NSA, Gryobner, MutantXL, Kuznechik, SAT.*

I. KIRISH

Axborot nazariyasi asoschisi hisoblangan Klod Elvud Shennon ishida «Bardoshli shifrlash algoritmini ochish uchun, ko‘p o‘zgaruvchili tenglamalar sistemasini yechish talab etiladi» – degan g‘oyani ilgari surgan [1]. Algebraik kriptotahlil usulining bugungi kundagi rivojlanishi ushbu g‘oyani tasdiqlamoqda. Bugungi kunga qadar algebraik kriptotahlil usulining bir nechta variantlari taklif etilgan va bir qancha rivojlanish bosqichlarini boshdan kechirgan [2].

Algebraik kriptotahlil usulining asosiy murakkabligi, algoritmni ifodalash mumkin bo‘lgan barcha tenglamalardan iborat sistemani shakllantirish (1-bosqich) va uni yechish (2-bosqich) qiyinchiligi bilan baholanadi. Tenglamalar sistemasini shakllantirishda algoritmning algebraik strukturasiga asoslaniladi. Kriptotahlil jarayonining 2-bosqichi samarali o‘tishi uchun, shifrni ifodalovchi minimal past darajadagi hadlardan (termlardan) iborat bo‘lgan tenglamalarni hosil qilish talab etiladi.

II. ASOSIY QISM

Uzluksiz shifrlarni baholashda asosan “Algebraik kriptotahlil (bazaviy usul)” va “Tezkor algebraik kriptotahlil (takomillashgan usul)” nomlarini olgan usullar keng qo‘llaniladi. Uzluksiz shifrlarga nisbatan *Algebraik kriptotahlil (bazaviy usul)* jarayonida generator orqali hosil bo‘luvchi gamma ketma-ketliklarini registrning dastlabki maxfiy qiymati bilan bog‘lovchi algebraik tenglamalar sistemasi shakllaniriladi. Tenglamalar sistemasini yechimi esa, maxfiy kalit hisoblanadi.

Oqimni shifrlash shunchaki oddiy matn bitlari soxta tasodifiy ketma-ketlik bitlari bilan modul 2 qo‘shilganligidadir. **Foyda uchun** oqim shifrlarida naslchilik xatolari yo‘q, oddiy bajarilish va yuqori shifrlash tezligi mavjud **Kamchilik** sinxronizatsiya ma’lumotlarini xabar sarlavhasi oldidan uzatish zarurati bo‘lib, uni har qanday xabarni shifrlashdan oldin olish kerak. Buning sababi shundaki, agar ikkita xil xabar bir xil kalit yordamida shifrlangan bo‘lsa, unda ushbu xabarlarni shifrlash uchun bir xil soxta tasodifiy ketma-ketlikdan foydalanish kerak. Ushbu holat tizimning kriptografik quvvatiga xavfli tahdid tug‘dirishi mumkin va shuning uchun qo‘shimcha ravishda tasodifiy tanlangan xabar kaliti ko‘pincha ishlatiladi, u xabar boshida uzatiladi va shifrlash kalitini o‘zgartirish uchun

ishlatiladi. Natijada, turli xil xabarlar turli xil ketma-ketliklar yordamida shifrlanadi. Oqim shifrlari harbiy tizimlarda va ular bilan chambarchas bog‘liq bo‘lgan boshqa tizimlarda ma’lumotlarni va raqamli nutq signallarini shifrlash uchun keng qo‘llaniladi. Yaqin vaqtgacha bunday dasturlar ustunlik qilar edi va bu usul shifrlash. Bu, xususan, yaxshi shifrlash ketma - ketliklarining generatorlarini qurish va amalga oshirishning nisbatan soddaligi bilan bog‘liq. Ammo asosiy omil, albatta, oqim shifrida xatolar tarqalishining yo‘qligi. Taktik aloqa tarmoqlarida ma’lumotlar va ovozli xabarlarni uzatish uchun nisbatan past sifatli kanallardan foydalanilganligi sababli, yuqori darajadagi xatolar tezligini oshiradigan har qanday kriptografik tizim qo‘llanilmaydi. Bunday holatlarda xatolarni tarqatmaydigan kriptosistemadan foydalanish juda muhimdir.Shu bilan birga, xatolarni ko‘paytirish ham ijobiy rivojlanish bo‘lishi mumkin. Aytaylik, masalan, shifrlangan ma’lumotlar xato ehtimoli juda past bo‘lgan kanal orqali uzatilishi kerak (masalan, 10 5) va ma’lumotlar mutlaqo aniq qabul qilinishi juda muhimdir. Bu kompyuter tarmoqlari uchun odatiy holat bo‘lib, unda bir oz xato halokatli bo‘lishi mumkin va shuning uchun aloqa kanali juda ishonchli bo‘lishi kerak. Bunday vaziyatda bitta xato 100 yoki 1000 ta xato kabi xavflidir. Ammo 100 yoki 1000 ta xatolarni bitta xatoga qaraganda osonroq topish mumkin. Shuning uchun, bu holda xatolarning ko‘payishi endi shifrning noqulayligi bo‘lmaydi.

Aytaylik, filtrlovchi generatorga asoslangan uzluksiz shifrda foydalanilgan registr uzunligi n ga teng bo‘lib, filtirlovchi funksiya – f, teskari bog‘lanishni ta’minlovchi funksiya – L, hamda registrning dastlabki qiymati – $K=k_1||k_2||k_3||...||k_n$ bo‘lsin. Ushbu holda, har bir chiquvchi zi – gamma qiymatga ko‘ra quyidagicha tengamalar sistemasini shakllantirish mumkin:

$$\begin{aligned} &f(K)=z_0\\ &f(L(K))=z_1\\ &f(L(L(K)))=z_2\\ &f(L(L(L(K))))=z_3\\ &\cdots\cdots\cdots\cdots \end{aligned} \qquad (1)$$

(1) - tenglamalar sistemasidagi shakllantiriluvchi tenglamalar soni registr uzunligiga va kriptotahlilchi qo‘lidagi gamma uzunligiga bog‘liq bo‘ladi. Hosil bo‘lgan tenglamalarning algebraik chiziqsizlik darajalari esa, algoritmning algebraik strukturasiga (algebraik modeliga) bog‘liq bo‘ladi [3].

Tezkor algebraik kriptotahlil (takomillashgan usul) usuli bazaviy algebraik kriptotahlil usulining qisman takomillashgan varianti hisoblanib, uni yuqori algebraik bardoshlikka ega bo‘lgan uzluksiz shifrlarga ham ayrim hollarda qo‘llash imkoni mavjud bo‘ladi.

Algebraik kriptotahlil usullari bugungi kunga qadar turli uzluksiz shifrlarga qo‘llanilgan va tegishli baholash natijalari olingan. Quyidagi 1-rasmda ushbu kriptotahlil usuli qo‘llanilgan algoritmlar keltirilgan [4].

Ma’lumki, tenglamalar sistemasini yechish qiyinchiligi ushbu tenglamalarning algebraik chiziqsizlik darajalariga va chiziqsiz bog‘liqsiz tenglamalar soniga uzviy bog‘liq. Shunga ko‘ra, algebraik kriptotahlil jarayonlarida algebraik chiziqsizlik darajalari past bo‘lgan tengamalar sistemasini qurish va uni yechishning optimal yo‘llari qidiriladi.

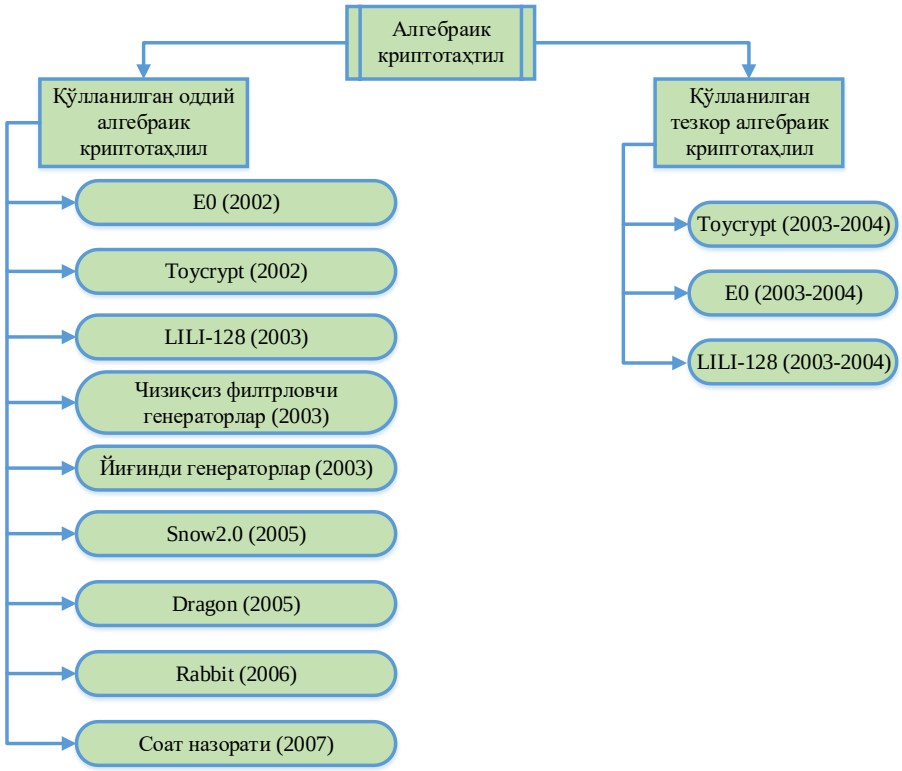
Chekli maydonda aniqlangan chiziqsiz tenglamalar sistemasini yechishga qaratilgan bugungi kundagi mavjud usullar (algoritmlar)ni quyidagi asosiy to‘rtta yo‘nalishga bo‘lish mumkin:

1. Gryobner bazisini qurish asosidagi algoritmlar (masalan: Buxberger, F4, F5, F5C, G2V va GVW);

2. SAT (SAT-solvers) – hisoblagichlaridan foydalanish asosidagi algoritmlar;

3. Moslashtirish va briktirish algoritmlari;

4. Chiziqlilashtirish asosidagi algoritmlar (masalan: XL, XL', XL2, XLF, XSL, FXL, XFL, WXL, HXL, ElimLim, MutantXL va MXL2).



1-rasm. Algebraik kriptotahlil usuli qo‘llanilgan uzluksiz shifrlar.

Tenglamalar sistemasini ifodalovchi “Minimal soddalashgan Gryobner ideal bazisini qurish” bilan bog‘liq bo‘lgan usullar, tenglamalar sistemasini yechishning klassik yo‘nalishi hisoblanadi [5]. Qurilgan bazis sistema tenglamalarini ifoda etadi hamda ushbu bazisga kiruvchi so‘ngi tenglama faqatgina bitta noma’lumga bog‘liq bo‘ladi. Sistemani yechish, dastlab bir noma’lumli tenglamani yechish hamda uning topilgan yechimini Gryobner bazisini tashkil etuvchi qolgan tenglamalarga qo‘yish va shu tariqa barcha noma’lumlarni aniqlash orqali amalga oshiriladi.

Tenglamalar sistemasini yechishning yana bir usulllaridan biri, “KNF ning bajarilish masalasi”ni (SATisfiability problem) yechishga qaratilgan algoritmlardan foydalanish hisoblanadi [6]. Ma’lumki, tenglamalar sistemasining yechish masalasini KNF ning bajarilish masalasiga keltirish mumkin. Ya’ni, noma’lumlarning qanday qiymatlarida sistema tenglamalarini ifodalovchi barcha bul funksiyalarning konyuktiv normal formasi bir vaqtda rost qiymatni beradi? Ko‘plab adabiyotlarda ushbu masalani yechishga qaratilgan algoritmlar (dasturlar) “SAT-solvers”, “SAT Competition”, “SAT Race” deb ham yuritiladi va mazkur turdagi algoritmlar bugungi kunda ham faol rivojlanib kelmoqda.

“Moslashtirish” va “Briktirish” algoritmlari orqali tenglamalar sistemasini yechish ushbu yo‘nalishdagi yana bir usul hisoblanadi [7]. Sistemani yechish jarayonida dastlab tenglamalar sistema-

sining har bir tashkil etuvchi tenglamalari kompleks (ya’ni, tenglamani ifodalovchi ma’lumotlar jamlanmasi)lar to‘plami orqali ifodalanadi, so‘ng ushbu komleks-lar ustida tegishli amallar bajarib noma’lumlar qiymati aniqlanadi.

Tenglamalar sistemasini yechishning yana bir tarixiy va keng tarqalgan usuli, bu – “Chiziqlilashtirish”dir [8]. Chiziqlilash-tirish (L, **L**inearization) usulining mo-xiyati tenglamalar sistemasi tarkibidagi barcha chiziqsiz o‘zgaruvchilarni (hadlarni) yangi chiziqli o‘zgaruvchi bilan almashtirish va shu tariqa hosil qilingan chiziqli tenglamalar sistemasini yechish-dan iborat. Bugungi kunga kelib, tenglamalar sistemasini yechishning chiziqlilashtirish asosidagi bir nechta zamonaviy usullari ishlab chiqilgan va bugungi kunda ham mazkur yo‘nalishdagi tadqiqot ishlari davom etmoqda. Chiziqlilashtirishga asoslangan zamona-viy usullardan biri sifatida XL (e**X**tended **L**inearization – kengaytirib-chiziqlilash-tirish) usulini keltirsh mumkin.

XL – usuli mashhur kriptotahlilchi Nicolas Courtois va Alexander Klimov, Jacques Patarin, Adi Shamir lar tomonidan 2000 yilda taklif etilgan [8,3]. Aynan ushbu usulning paydo bo‘lishi algebraik kriptotahlilning jadal rivoj-lanishiga katta turtki bo‘ldi.

Mazkur usulning umumiy moxiyati, berilgan chiziqsiz tenglamalar sistema-sidagi tenglamalar sonini oshirish hamda chiziqsiz o‘zgaruvchilarni yangi chiziqli o‘zgaruvchilar bilan almashtirish va shu tariqa hosil bo‘lgan chiziqli tenglamalar sistemasini yechishga qaratilgan. XL usuli ishlab chiqilganidan so‘ng, bugungi kunga qadar mazkur usulni bir nechta takomillashgan variantlari (XL', XL2, XLF, XSL, FXL, XFL, WXL, HXL, ElimLim, MutantXL va MXL2) taklif etildi. Olib borilgan tahlil natijalari shuni ko‘rsatadiki, tenglamalar sistemasini yechishning chiziqlilashtirishga asos-langan MutantXL usuli, bugungi kunda eng zamonaviy usullardan biri sifatida e’tirof etiladi.

MutantXL – usuli Szintay Din g‘oyasi asosida [9] ishda taklif etilgan bo‘lib, past darajadagi yangi tenglamalarni hosil qilish orqali tenglamalar sistemasini kengaytirishga qaratilgan. Aytaylik, $P(x)$ – chekli maydonda aniqlangan chiziqsiz tenglamalar to‘plami, D – ushbu tenglamalarning eng yuqori darajasi bo‘lib, $P(x)=0$ sistemani yechish masalasi qaralayotgan bo‘lsin. $P(x)=0$ boshlang‘ich tenglamalar sistemasiga Gauss almash-tirishini (to‘g‘ri-yurish) qo‘llab, yangi tenglamalar sistemasini hosil qilish orqali darajasi D-1 ga teng bo‘lgan tenglamaga ega bo‘lish mumkin. Ushbu topilgan tenglama umumiy tenglamalar sistemasi uchun mutant tenglama (tenglamalar) hisoblanadi.

Tenglamalarni kengaytirish jarayonida mutant tenglamalariga tegishli birxadlar ko‘paytiriladi. Ko‘paytirish natijasida hosil qilingan tenglamalarni boshlang‘ich tenglamalar sistemasiga biriktirish orqali yangi tenglamalar sistemasi hosil bo‘ladi. Mazkur sistema esa, boshlang‘ich teng-lamalar sistemasi bilan bir xil darajadagi, ammo unga nisbatan ko‘p sondagi erkli tenglamalar sistemasiga ega bo‘lishi mumkin. MutantXL usulining samara-dorligi ham aynan shu orqali namoyon bo‘ladi. Ko‘p o‘zgaruvchili ko‘phad-lardan iborat tenglamalar sistemasi uchun har doim ham mutant topilmasligi mumkin. Agar mutant topilmasa ushbu tenglamalar sistemasini yechish XL usuliga asoslanadi.

Olib borilgan tahlil natijalariga ko‘ra, filtrlovchi generatorlarga asoslangan uzluksiz shifrlarga nisbatan annigilyator (nollovchi ko‘pxad)lar asosidagi algeb-raik kriptotahlil usuli keng qo‘llaniladi.

1-jadval. NSA algoritmida foydalanilgan Kuznechik shifrlash algoritmining S-boxining umumiy kriptografik talablar bo‘yicha xarakteristikasi.

NSA (Kuznechik)	S – блок							
	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
Balanslashganlik	+	+	+	+	+	+	+	+
Regulyarlik	+							
deg (f)	7	7	7	7	7	7	7	7
N (f)	104	106	116	104	110	106	102	104
N (φ)	100							
$CI(f)$	0	0	0	0	0	0	0	0
$SAC(f)$*	-	-	-	-	-	-	-	+
$PC(f)$*	0	0	0	0	0	0	0	1
$AI(S)$	3							
$BIC(S)$	0							

Mazkur jadvalda mazkur *S*-blokga nisbatan tenglamalarni shakllantirish usullari o‘rganilgan, shu usullarda shakllantirilgan algebraik tenglamalarning parametrlari quyidagi jadvalda keltrilgan:

2-jadval. Kuznechik shifrlash algoritmining S akslantirishini ifodalovchi algebraik tenglamalar sistemasining parametrlari.

	DEG	NS	7-darajali TS	6- darajali TS	5- darajali TS	3- darajali TS
1-usul	7	860	354	10	1	
2- usul	7	860	360	5	-	
3- usul	3	697	-	-	-	441

MDS akslantirishiga nisbatan tenglamalarni shakllantirish esa [10-11] ishda keltirilgan usul yordamida amalga oshiriladi. Bunda chiziqli tenglamalar hosil bo‘ladi. Quyida mazkur akslantirishdan chiquvchi bir bitni ifodalovchi tenglamaning ko‘rinishi keltirilgan:

$$y_0 = x_2 \oplus x_3 \oplus x_5 \oplus x_7$$

Shuningdek algoritmda foydalanilgan siklik surish amaliga nisbatan ham chiziqli algebraik tenglamalar hosil qilinadi.

$$y_0 = x_{19}$$
$$y_1 = x_{20}$$
$$y_2 = x_{21}$$
$$\dots$$
$$y_i = x_{(i+19)\ mod\ 64}$$
$$\dots$$
$$y_{63} = x_{18}$$

Yuqoridagi ko‘rib o‘tilgan akslantirishlarning algebraik xarakteristikalaridan shuni xulosa qilish mumkinki, algebraik kriptotahlil jarayonida tenglamalarning darajasiga faqat $S-blok$ akslantrishi ta’sir o‘tkazadi.

Har bir akslantirishga algebraik tenglamalar shakllantirilgandan so‘ng ularni bog‘lab bir raund uchun tenglamalar shakllantiriladi.

NSA algoritmining sxemasidan ko‘rish mumkinki dastlabki a holat massivlaridan faqat a_1 massivi F akslantirishidan o‘tadi.

III. XULOSA

Mazkur ishda ishlab chiqilgan NSA oqimli shifrlash algoritmi algebraik kriptotahlil usullariga bardoshliligi baholandi.

Mazkur usulning umumiy mohiyati, berilgan chiziqsiz tenglamalar sistemasidagi tenglamalar sonini oshirish hamda chiziqsiz o‘zgaruvchilarni yangi chiziqli o‘zgaruvchilar bilan almashtirish va shu tariqa hosil bo‘lgan chiziqli tenglamalar sistemasini yechishga qaratilgan. XL usuli ishlab chiqilganidan so‘ng, bugungi kunga qadar mazkur usulni bir nechta takomillashgan variantlari (XL', XL2, XLF, XSL, FXL, XFL, WXL, HXL, ElimLim, MutantXL va MXL2) taklif etildi. Olib borilgan tahlil natijalari shuni ko‘rsatadiki, tenglamalar sistemasini yechishning chiziqlilashtirishga asoslangan *MutantXL* usuli, bugungi kunda eng yuqori natijadorlikka erishish mumkinligi ko‘rsatib o‘tildi.

ADABIYOTLAR

[1] *Шеннон К.* Теория связи в секретных системах // В кн. Работы по теории информации и кибернетике. – М., ИЛ, 1963.

[2] *Kazymyrov O., Raddum H.* Binary Decisions Diagrams for Algebraic Attacks. Winter School in Information Security Finse, Norway, 2014.–p. 60.

[3] *Martin V.* Algebraic Attack on Stream Ciphers. Master’s Thesis, Bratislava, 2007.

[4] *Sattar B. S, Rafeef M. H.* A study of Algebraic Attack and proposed developed clock control stream cipher. Journal of Babylon University//Pure and Applied Sciences// No.(2)// Vol.(22): 2014.

[5] *Buchberger B.* Grobner-Bases: An Algorithmic Method in Polynomial Ideal Theory. Reidel Publishing Company, Dodrecht - Boston - Lancaster, 1985. Pp. 184-232.

[6] *Abdel A.K., Amr Y.M.* Applications of SAT Solvers to AES key Recovery from Decayed Key Schedule Images // Cryptology ePrint Archive. 2010. Vol. 324.

[7] *Raddum F., Semaev I.* New technique for Solving Sparse Equation Systems //Cryptology ePrint Archive. 2006. Vol. 475.

[8] *Courtois N., Klimov A., Patarin J., Shamir A.* Efficient algorithms for solving overdefined systems of multivariate polynomial equations // EUROCRYPT, 2000. – P. 392–407.

[9] *Ding J., Buchmann J., Mohamed M., Mohamed W. and Weinmann R.* MutantXL. In Proceedings of the 1st international conference on Symbolic Computation and Cryptography (SCC08), pp. 16 – 22.

[10] *Boyquziyev I.M.,* “Kriptotahlil usullarining Kuznechik shifrlash algoritmiga nisbatan qo‘llanilishi”. Fizika-matematika fanlari bo‘yicha falsafa doktori (PhD) darajasini olish uchun yozilgan dissertatsiya. 2022, 64-75 betlar.

[11] *Бойқузиев И.М.* Кузнечик шифрлаш стандартининг S ва L акслантиришлари учун чизиқли тенгламалар тузиш муаммоси ва ечими // Муҳаммад ал-Хоразмий авлодлари илмий-амалий ва ахборот-таҳлилий журнал, 2021, № 2(16), 58-62 бет. (05.00.00 №10)

Поступила в редакцию 13.04.2023

Citation: *Rahmatullayev I.R.* (2023). Algebraik kriptotahlil usuli va uning oqimli shifrlash algoritmlariga qo‘llanish asoslari. Raqamli texnologiyalarning nazariy va amaliy masalalari xalqaro jurnali. 2(4). – B. 96-102.

ALGEBRAIC CRYPTANALYSIS METHOD AND BASICS OF ITS APPLICATION TO STREAM ENCRYPTION ALGORITHM

Rahmatullaev I.R.[1]

[1] Samarkand branch of Tashkent university of information technologies named after Muhammad al-Khwarizmi, Samarkand, Uzbekistan

Ilhom9001@mail.com

Abstract. *In this work, the processes of evaluation of stream encryption algorithms by algebraic cryptanalysis methods are analyzed. The results of randomness evaluation of the analyzed algorithm using NIST statistical tests were obtained. The parameters of the results obtained by the speed of generation are compared.*

Keywords: *Algebraic cryptanalysis, NIST, NSA, Groebner, MutantXL, Kuznechik, SAT.*

МЕТОД АЛГЕБРАИЧЕСКОГО КРИПТОАНАЛИЗА И ОСНОВЫ ЕГО ПРИМЕНЕНИЯ К АЛГОРИТМАМ ПОТОКОВОГО ШИФРОВАНИЯ

Рахматуллаев И.Р.[1]

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

Ilhom9001@mail.com

Аннотация. *В данной работе анализируются процессы оценки алгоритмов потокового шифрования методами алгебраического криптоанализа. Получены результаты оценки случайности анализируемого алгоритма с помощью статистических тестов NIST. Сравниваются параметры полученных результатов по скорости генерации.*

Ключевые слова: а*лгебраический криптоанализ, NIST, NSA, Groebner, MutantXL, Кузнечик, SAT.*