MA’LUMOTLARNI SHIFRLASH ALGORITMI AKSLANTIRISHLARINING ALGEBRAIK XUSUSIYATLARI TAHLILI

Rahmatullayev Ilhom Raxmatullayevich[1,4], Abduraximov Baxtiyor Fayziyevich[2,3], Boykuziyev Ilhom Mardonakulovich[2,3] , Kholliyev Bakhriddin Yakubovich[5]

[1]Raqamli texnologiyalar va sun’iy intellektni rivojlantirish ilmiy-tadqiqot instituti doktoranti, Ilhom9001@gmail.com
[2]Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiylari universiteti, salyut2017@gmail.com
[3]Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti, a_bakhtiyor@mail.ru
[4]Sharof Rashidov nomidagi Samarqand Davlat universiteti
[5]EMU universiteti, xolliyevb45@gmail.com

K E Y W O R D S

Algebraik kriptotahlil, O‘zDSt 1105:2009, Simmetrik blokli shifrlash algoritmi, Chiziqli akslantirishlar, Chiziqsiz akslantirishlar, Algebraik tenglamalar sistemasi, Shifrlash kaliti, Kriptografik xavfsizlik, Algebraik xususiyatlar, Dekompatsiyalash usuli.

A B S T R A C T

Mazkur maqolada O‘zDSt 1105:2009 algoritmida ishlatilgan akslantirishlarning algebraik xususiyatlari tahlil qilinadi. Tadqiqotda algebraik kriptotahlil usuli asosida O‘zDSt 1105:2009 algoritmi komponentlarining algebraik tenglamalar orqali ifodalanishi, ularning xususiyatlari va samaradorlik tahlili amalga oshirilgan. Shuningdek, algoritm komponentlari uchun ishlab chiqilgan tenglamalar sistemalari va ularni tahlil qilish usullari ko'rib chiqilgan. Bu usullar orqali algoritmning maxfiy kalitiga oid ma'lumotlarni aniqlash imkoniyati tahlil qilingan. Tadqiqot natijalari algebraik kriptotahlilning samaradorligini oshirishga qaratilgan tavsiyalarni o‘z ichiga oladi.

KIRISH.

Kriptografik tizimlarning xavfsizligi ulardan foydalaniladigan shifrlash algoritmlarining matematik asoslariga bog‘liq. Algebraik kriptotahlil usuli aynan shunday matematik asoslarga tayanadi va bu usulda shifrlash algoritmini algebraik tenglamalar sistemasi orqali ifodalash va ushbu sistemani yechish orqali algoritmning maxfiy kalitini aniqlash maqsad qilib qo‘yiladi. O‘zDSt 1105:2009 algoritmi – bu axborotni kriptografik muhofaza qilishga mo‘ljallangan simmetrik blokli shifrlash algoritmi bo‘lib, unda foydalanilgan akslantirishlarning algebraik xususiyatlarini o'rganish dolzarb hisoblanadi.

Ushbu maqolada algebraik kriptotahlil usulining asosiy bosqichlari, jumladan, shifrlash algoritmini dekompozitsiyalash, algebraik tenglamalar sistemalarini shakllantirish va ularni samarali yechish usullari tahlil qilinadi. Shu bilan birga, maqolada O‘zDSt 1105:2009 algoritmi uchun ishlab chiqilgan algebraik tenglamalar va ularning matematik xususiyatlariga oid tahlil natijalari keltiriladi.

Simmetrik blokli shifrlash algoritmlariga nisbatan *Algebraik kriptotahlil* usulining asosiy mohiyati, shifrlash algoritmini (chiziqsiz akslantirishlarni) ifodalovchi chekli maydonda aniqlangan *algebraik tenglamalar sistemasini tuzish* (1-bosqich) va ushbu *tenglamalar sistemasini yechish* (2-bosqich) orqali shifrlash kalitini aniqlashdan iboratdir. Ushbu kriptotahlil usuli ochiq va shifr matn asosidagi hujum turiga mansub bo‘lib, kriptotahlil o‘tkazish uchun kriptotahlilchiga bir juft ochiq va shifr matn juftliklarining ma’lum bo‘lishi yetarlidir [5].

Axborot nazariyasi asoschisi bo‘lgan Klod Elvud Shennon «Bardoshli shifrlash algoritmini ochish uchun, ko‘p o‘zgaruvchili tenglamalar sistemasini yechish talab etiladi» – ma’nosidagi g‘oyani taklif etadi. Aynan ushbu g‘oyaga asoslangan algebraik kriptotahlil usulining bugungi kundagi rivojlanishi uning taklifini tasdiqlamoqda [1].

© I.R. Rahmatullayev, B.F. Abduraximov, I.M. Boykuziyev, B.Ya. Kholliyev

Algebraik kriptotahlil usulining asosiy qiyinchiligi, mumkin bo'lgan barcha tenglamalar sistemasini qurish va uni yechish bilan baholanadi [1-15].

METODOLOGIYA

Algebraik kriptotahlil usulining dastlabki bosqichi, shifrlash algoritmini ifodalovchi algebraik tenglamalar sistemasini tuzish hisoblanadi. Ushbu sistema elementlari «Algebraik tenglama» bo'lib, u quyidagicha ta'riflanadi.

Ta'rif. Algebraik tenglama deb, quyidagi:

$$f(x_1,x_2,x_3,\ldots,x_n) = 0 \qquad (1)$$

ko'rinishidagi tenglamaga aytiladi. Bu yerda, f – noma'lum x_1, x_2, $x_3,\ldots$, x_n o'zgaruvchilardan iborat bo'lgan ko'phad [14].

Odatda f ko'phad koeffitsientlari biror F maydondan olinadi va shunga ko'ra (1) ifoda F maydonda aniqlangan algebraik tenglama deb yuritiladi. Algebraik tenglama darajasi f ko'phad darajasini anglatadi. Masalan, quyidagi:

$$y^4 + \frac{xy}{2} + y^2z^5 + x^3 - xy^2 + \sqrt{3}x^2 - \sin 1 = 0$$

tenglama haqiqiy sonlar maydonida aniqlangan, 3 o'zgaruvchili (noma'lum), 7-darajali (ya'ni chiziqsiz) algebraik tenglama hisoblanadi.

Algebraik tenglamalar sistemasini tuzishda qaralayotgan shifrlash algoritmi chiziqsiz akslantirishining algebraik strukturasiga asoslaniladi. Kriptotahlil jarayonining 2-bosqichi samarali o'tishi uchun, akslantirishni algebraik ifodalovchi minimal darajadagi hadlardan (termlardan) iborat bo'lgan maksimal sondagi tenglamalarni hosil qilish talab etiladi [11, 14]. Ya'ni, ushbu tenglamalar sistemasi qaralayotgan akslantirishni to'liq ifodalashi zarur.

Ma'lumki shifrlash algoritmlarida chiziqli va chiziqsiz akslantirishlardan foydalaniladi. Tenglamalar dastlab chiziqsiz akslantirishlarga nisbatan ishlab chiqilib keyinchalik ularni chiziqli akslantirishlarga nisbatan moslashtirish qulay hisoblanadi [8].

Shifrlash algoritmlari tarkibida chiziqsiz akslantirishlardan foydalanilishi, mazkur akslantirishlarni p=1 ehtimollik bilan bajariluvchi chiziqli tenglamalar sifatida ifoda etish imkoniyatini bermaydi. Shuning uchun ham bu turdagi akslantirishlarga nisbatan tenglamalar sistemasini shakllantirishda ikki (yoki undan ko'p) noma'lum ko'paytmasidan iborat bo'lgan birhadlarni ham ko'rish, ya'ni chiziqsiz tenglamalar orqali ifodalash talab etiladi. Tenglamalar sistemasini tuzishda, ushbu birhadlarni (ya'ni tenglamalarni) mumkin bo'lgan barcha kombinasiyalarini ko'rib chiqish kerak bo'ladi.

Tuzilgan barcha kombinasiyadagi tenglamalarning aksariyati noto'g'ri tenglama bo'lib, ularning berilgan akslantirishga muvofiqligini, ya'ni to'g'ri tenglama ekanligini tekshirish uchun akslantirishning chinlik jadvalini (tekshiruv jadvali) tuzib chiqish kerak bo'ladi.

Shunga muvofiq, akslantirishni ifodalovchi tenglamalarni aniqlashning bugungi kunda mavjud bo'lgan usullaridan biri mumkin bo'lgan barcha tenglamalarni ko'rib chiqish (to'liq tanlov) usulidir. Ushbu usulning aniqligi yuqori, biroq akslantirishga kiruvchi va chiquvchi bitlar hajmining ortishi bilan hisoblash amallari soni ham ortib boradi. Masalan, kirish va chiqish o'lchami s bit bo'lgan S – blok akslantirishi uchun 2^t ta tenglama tuzish mumkin. t – tenglamada ishtirok etuvchi birhadlar soni bo'lib, u quyidagi (2) formula orqali hisoblanadi:

$$t = \binom{2s}{2} + 2s + 1 \qquad (2)$$

Ya'ni, $2s$ – S blokka kiruvchi va chiquvchi bitlar soni, $\binom{2s}{2}$ – S blokga kiruvchi va chiquvchi bitlarning mumkin bo'lgan barcha ko'paytmalari soni va 1 ta η – koeffitsient.

Masalan, 4x4 o'lchamli S blok uchun 2-darajali to'g'ri tenglamalarni hosil qilishda (2) ifodaga ko'ra 2^{37} ta tenglamani ko'rib chiqish kerak

© I.R. Rahmatullayev, B.F. Abduraximov, I.M. Boykuziyev, B.Ya. Kholliyev

bo‘ladi [23,29,32,]. Mazkur hisoblashlar sonining yuqoriligi esa, tenglamalar sistemasini tuzishning samarali usulidan foydalanishni taqozo etadi.

Avvalgi bobda keltirilgan ma’lumotlarga asosan, algebraik kriptotahlil usuli quyidagi ikki bosqichni o‘z ichiga oladi [4]:

1. Shifrlash algoritmini ifodalovchi minimal darajali birxadlar (term)dan tashkil topgan maksimal sondagi tenglamalarni shakllantirish.
2. Tenglamalar sistemasini yechish.

Tenglamalar sistemasini yechish shifrlash algoritmida foydalanilgan maxfiy kalit (yoki ayrim bitlarini) qiymatini aniqlashga olib keladi.

O‘z navbatida, shifrlash algoritmini tenglamalar sistemasi orqali ifodalash quyidagi qism qadamlar asosida amalga oshiriladi [9]:

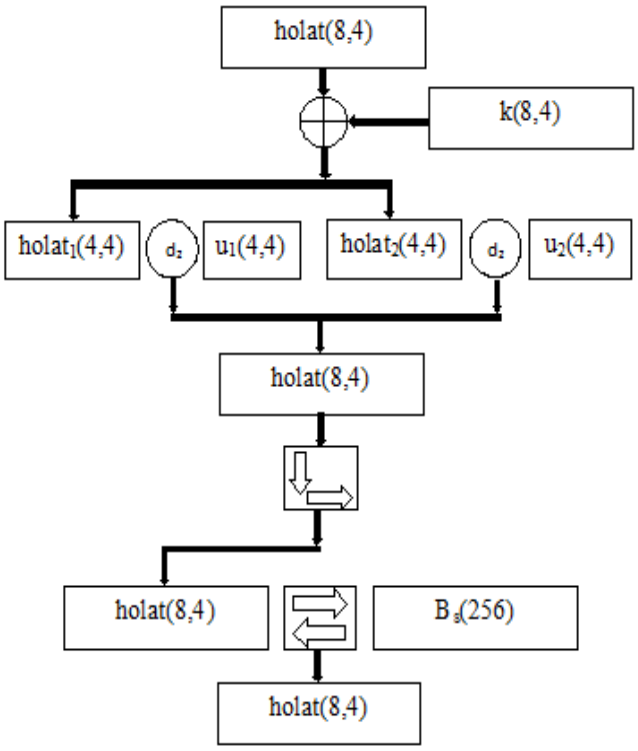
1. *shifrlash algoritmini dekompozitsiyalash;* ya’ni, shifrlash algoritmining tashkil etuvchilarini imkon qadar kichik va alohida elementlar (chiziqli, chiziqsiz va boshqa akslantirishlar)ga ajratish.
2. *har bir elementni algebraik ifodalash;*
3. *har bir elementning kirishi va chiqishini boshqa elementlar hamda kalit, ochiq matn va shifr matn bitlari bilan bog‘lash.*

NATIJALAR VA MUHOKAMA

O’zDSt 1105:2009 shifrlash algoritmiga algebraik kriptotahlil usulini qo‘llashda ham yuqoridagi masalalarni alohida ko‘rib o‘tish lozim.

Shifrlash algoritmini **dekompozitsiyalash** jarayonida ochiq matn bitlarini shifr matn bitlari bilan bog‘lovchi eng qisqa yo‘l hamda ushbu yo‘lda joylashgan va o‘zaro mustaqil ishlaydigan har bir akslantirish alohida elementlarga ajratiladi.

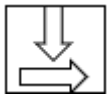
O’zDSt 1105:2009 algoritmini dekompozitsiyalashda uning quyidagi bir raundlik strukturasiga tayanish mumkin (1-rasm).

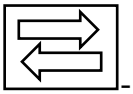


1-rasm. O’zDSt 1105:2009 algoritmining bir raundlik dekompozitsion sxemasi

 - akslantirish 2 modul bilan qo‘shish (Qo’shBosqichKalit) amali, ushbu akslantirishni shartli ravishda *X* bilan belgilaymiz.

 - akslantirish diamatritsaviy ko‘paytirish (Aralash) amali, ushbu akslantirishni shartli ravishda *A* bilan belgilaymiz.

 - akslantirish ustun va satr bo‘yicha surish (Sur) amali, ushbu akslantirishni shartli ravishda *S* bilan belgilaymiz.

 - akslantirish bayt bo‘yicha chiziqsiz almashtirish (BaytAlmash) amali, ushbu akslantirishni shartli ravishda *B* bilan belgilaymiz.

Mazkur sxemaga ko‘ra, O’zDSt 1105:2009 algoritmining har bir raundida foydalanilgan

© I.R. Rahmatullayev, B.F. Abduraximov, I.M. Boykuziyev, B.Ya. Kholliyev

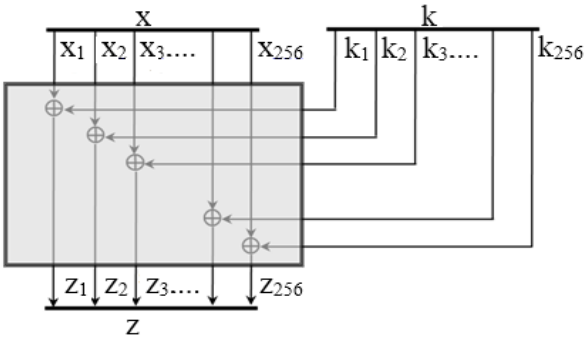
akslantirishlarni 4 tur (*X, A, S, B* - funktsiyalar) ga ajratish mumkin.

Qism elementlarga ajratishda shifrlash algoritmida foydalanilgan chiziqsiz akslantirishlar muhim ahamiyat kasb etadi. Chunki, aynan ushbu turdagi akslantirish o'lchami katta bo'lsa, ularni ifodalovchi tenglamalar sistemasini qurish ko'plab hisoblashlarni talab etadi. Shuning uchun, ajratilgan har bir elementning kirish va chiqish o'lchami imkon qadar kichik bo'lishi lozim.

Ajratilgan elementlarni algebraik ko'rinishda ifodalash jarayonida har bir element algebraik tenglamalar sistemasi ko'rinishida shakllantiriladi. YA'ni, har bir akslantirish uchun, ularni kirishi va chiqishini bog'lovchi tenglamalar sistemasi hosil qilinadi. Bir turga mansub bo'lgan akslantirishlar uchun tenglamalar sistemasini hosil qilish bir xil tarzda amalga oshiriladi. Tuzilgan tenglamalar sistemasi faqat noma'lumlari bilan farqlanadi.

O'zDSt 1105:2009 algoritmi uchun hosil qilingan qism elementlarni algebraik ifodalashda *X, A, S, B* – funktsiyalarni ko'rib o'tish etarli.

***z=X(x,k)* - funkiya** – umumiy uzunligi 256 bit bo'lgan, har bir elementi baytlardan tashkil topgan (8,4) o'lchamli ikkita matritsa elementlarini mos ravishda 2 modul bo'yicha qo'shish ($\oplus$) jarayonini amalga oshiradi (2-rasm).

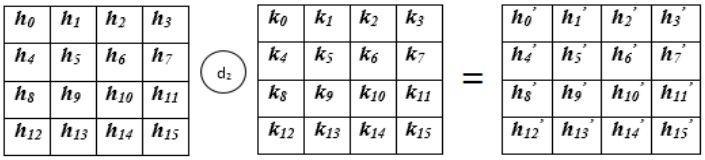


2-rasm. X(x,k) – funktsiya sxemasi.

Demak, ushbu akslantirish uchun quyidagicha tenglamalar sistemasini qurish mumkin (3):

$$\begin{cases} z_1 = x_1 \oplus k_1 \\ z_2 = x_2 \oplus k_2 \\ z_3 = x_3 \oplus k_3 \\ \dots\dots\dots \\ z_{255} = x_{255} \oplus k_{255} \\ z_{256} = x_{256} \oplus k_{256} \end{cases} \quad (3)$$

y=A(x) - funkiya – umumiy uzunligi 128 bit bo'lgan, har bir elementi baytlardan tashkil topgan (4,4) o'lchamli ikkita matritsa ustida diamatritsaviy ko'paytirishni amalga oshiradi (1-jadval, 3-rasm).



3-rasm. Diamatritsaviy ko'paytirish amali.

1-jadval.

Aralash akslantirishida foydalanilgan diamatritsaviy ko'paytirish formulasi.

h'[0,0]	$h'_0=h_0(k_0+k_4+k_8+k_{12})-h_5k_4-h_{10}k_8-h_{15}k_{12} \pmod p$
h'[1,1]	$h'_5=h_5(k_1+k_5+k_9+k_{13})-h_0k_1-h_{10}k_9-h_{15}k_{13} \pmod p$
h'[2,2]	$h'_{10}=h_{10}(k_2+k_6+k_{10}+k_{14})-h_0k_2-h_5k_6-h_{15}k_{14} \pmod p$
h'[3,3]	$h'_{15}=h_{15}(k_3+k_7+k_{11}+k_{15})-h_0k_3-h_5k_7-h_{10}k_{11} \pmod p$
h'[0,1]	$h'_1=h_1(k_1+k_5+k_9+k_{13})+(h_0+h_4+h_8+h_{12})k_1-h_2k_9-h_3k_{13} \pmod p$
h'[0,2]	$h'_2=h_2(k_2+k_6+k_{10}+k_{14})+(h_0+h_4+h_8+h_{12})k_2-h_1k_6-h_3k_{14} \pmod p$
h'[0,3]	$h'_3=h_3(k_3+k_7+k_{11}+k_{15})+(h_0+h_4+h_8+h_{12})k_3-h_1k_7-h_2k_{11} \pmod p$
h'[1,0]	$h'_4=h_4(k_0+k_4+k_8+k_{12})+(h_1+h_5+h_9+h_{13})k_4-h_6k_8-h_7k_{12} \pmod p$
h'[1,2]	$h'_6=h_6(k_2+k_6+k_{10}+k_{14})+(h_1+h_5+h_9+h_{13})k_6-h_4k_2-h_7k_{14} \pmod p$
h'[1,3]	$h'_7=h_7(k_3+k_7+k_{11}+k_{15})+(h_1+h_5+h_9+h_{13})k_7-h_4k_3-h_6k_{11} \pmod p$
h'[2,0]	$h'_8=h_8(k_0+k_4+k_8+k_{12})+(h_2+h_6+h_{10}+h_{14})k_8-h_6k_4-h_{11}k_{12} \pmod p$
h'[2,1]	$h'_9=h_9(k_1+k_5+k_9+k_{13})+(h_2+h_6+h_{10}+h_{14})k_9-h_8k_1-h_{11}k_{13} \pmod p$

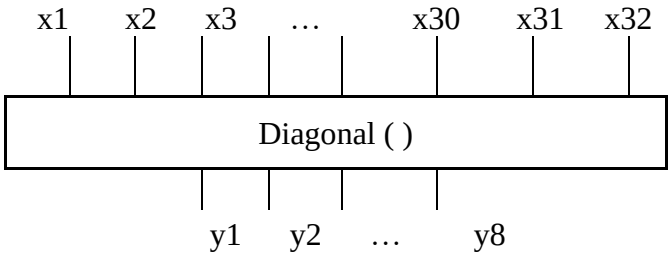
(cc) BY

$h'[2,3]$	$h'_{11}=h_{11}(k_3+k_7+k_{11}+k_{15})+(h_2+h_6+h_{10}+h_{14})k_{11}-h_8k_3-h_9k_7 (mod\ p)$
$h'[3,0]$	$h'_{12}=h_{12}(k_0+k_4+k_8+k_{12})+(h_3+h_7+h_{11}+h_{15})k_{12}-h_{13}k_4-h_{14}k_8 (mod\ p)$
$h'[3,1]$	$h'_{13}=h_{13}(k_1+k_5+k_9+k_{13})+(h_3+h_7+h_{11}+h_{15})k_{13}-h_{12}k_1-h_{14}k_9 (mod\ p)$
$h'[3,2]$	$h'_{14}=h_{14}(k_2+k_6+k_{10}+k_{14})+(h_3+h_7+h_{11}+h_{15})k_{14}-h_{12}k_2-h_{13}k_6 (mod\ p)$

ЮQoridagi 1-jadvaldan ko‘rinadiki *Aralash*() akslantirishida chiqishdagi $h'[4,4]$ matritsaning diagonal elementlarini hosil qilishda kirishdagi $h[4,4]$ matritsaning 4 ta elementi, nodiagonal elementlarini hosil qilishda esa 7 ta elementi ishtirok etadi.

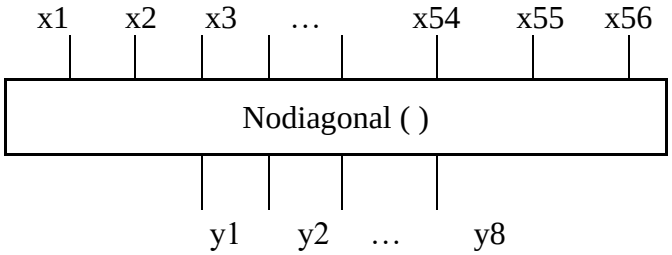
Akslantirishning bu xususiyati uni ikkita mustaqil akslantirish sifatida o‘rganishni talab etadi. Shu sababli, bu akslantirishlarni shartli ravishda diagonal akslantirish va nodiagonal akslantirish deb nomlangan ikkita akslantirish sifatida o‘rganish maqsadga muvofiq.

Diagonal akslantirish bu natijaviy matritsaning diagonal elementlarini hosil qilish uchun foydalaniladigan 32 bit kirishga 8 bit chiqishga ega bo‘lgan akslantirish:



4-rasm. Diagonal akslantirishining sxemasi.

Nodiagonal akslantirish esa natijaviy matritsaning nodiagonal elementlarini hosil qilish uchun foydalaniladigan 56 bit kirishga 8 bit chiqishga ega bo‘lgan akslantirish.



5-rasm. Nodiagonal akslantirishining sxemasi

Ma’lumki, ushbu 32x8 va 56x8 akslantirishlariga nisbatan bul tenglamalarini tuzish uchun hisoblash texnikasi imkoniyati etmaydi. Shuning uchun bu akslantirishlarning algebraik xususiyatini o‘rganish uchun ularning kichraytirilgan variantlariga nisbatan diamatritsaviy ko‘paytirish amali xususiyatlarini saqlagan holda tenglamalar tuzish jarayoni amalga oshirildi.

Shunga ko‘ra, diagonal akslantirishi uchun 8x2, 12x3 va 16x4 o‘lchamdagi, nodiagonal akslantirishi uchun esa 14x2 va 21x3 o‘lchamdagi variantlarga nisbatan tenglamalar tuzildi va ushbu tenglamalar xususiyatlari o‘rganildi (2-jadval).

Algoritmning o‘quv varianti uchun tanlangan ushbu:

$$K_s = \begin{pmatrix} 1 & 1 & 2 & 1 \\ 3 & 1 & 3 & 3 \\ 1 & 3 & 1 & 1 \\ 1 & 3 & 0 & 1 \end{pmatrix}$$

diamatritsa uchun tenglamalar quyidagi ko‘rinishda hosil bo‘ldi:

2-jadval.

8x2, 12x3 va 16x4, 14x2 va 21x3 o‘lchamli diamatritsali ko’paytirish akslantirishi uchun shakllantirilgan tenglamalar

8x2 K_s
$\mathbf{y_1}=x_2+x_3+x_4x_6+x_4x_8+x_5+x_6x_8+x_6+x_7+x_8$. deg=2
$\mathbf{y_2}=x_4+x_6+x_8$. deg=1
12x3 K_s
$\mathbf{y_1}=x_2+x_3+x_4+x_6+x_7+x_9+x_{10}+x_{11}+x_{12}+x_3x_5+x_3x_6x_9+x_3x_6x_{12}+x_3x_8+x_3x_9x_{12}+x_3x_9+x_3x_{11}+x_3x_{12}+x_5x_6x_9+x_5x_6x_{12}+x_5x_8+x_5x_9x_{12}+x_5x_9+x_5x_{11}+x_5x_{12}+x_6x_8x_9+x_6x_8x_{12}+x_6x_9x_{11}+x_6x_9+x_6x_{11}x_{12}+x_6x_{12}+x_8x_9x_{12}+x_8x_9+x_8x_{11}+x_8x_{12}+x_8+x_9x_{11}x_{12}+x_9x_{11}+x_9x_{12}+x_{11}x_{12}$. deg=3
$\mathbf{y_2}=x_3+x_5+x_8+x_9+x_{11}+x_{12}+x_6x_9+x_6x_{12}+x_9x_{12}$. deg=2
$\mathbf{y_3}=x_6+x_9+x_{12}$. deg=1
16x4 K_s
$\mathbf{y_1}=x_2+x_3x_4x_7+x_3x_4x_8x_{12}+x_3x_4x_8x_{16}+x_3x_4x_{11}+x_3x_4x_{12}x_{16}+x_3x_4x_{12}+x_3x_4x_{15}+x_3x_4x_{16}+x_3x_4+x_3x_6+x_3x_7x_8x_{12}+x_3x_7x_8x_{16}+x_3x_7x_{11}+x_3x_7x_{12}x_{16}+x_3x_7x_{12}+x_3x_7$

(cc) BY

$x_{15}+x_3x_7x_{16}+x_3x_8x_{11}x_{12}+x_3x_8x_{11}x_{16}+x_3x_8x_{12}x_{15}+x_3x_8x_{12}+x_3x_8x_{15}x_{16}+x_3x_8x_{16}+x_3x_8+x_3x_{10}+x_3x_{11}x_{12}x_{16}+x_3x_{11}x_{12}+x_3x_{11}x_{15}+x_3x_{11}x_{16}+x_3x_{11}+x_3x_{12}x_{15}x_{16}+x_3x_{12}x_{15}+x_3x_{12}x_{16}+x_3x_{12}+x_3x_{14}+x_3x_{15}x_{16}+x_3x_{15}+x_3x_{16}+x_3+x_4x_6x_7+x_4x_6x_8x_{12}+x_4x_6x_8x_{16}+x_4x_6x_{11}+x_4x_6x_{12}x_{16}+x_4x_6x_{12}+x_4x_6x_{15}+x_4x_6x_{16}+x_4x_6+x_4x_7x_8x_{11}x_{12}+x_4x_7x_8x_{11}x_{16}+x_4x_7x_8x_{12}x_{15}+x_4x_7x_8x_{15}x_{16}+x_4x_7x_8+x_4x_7x_{10}+x_4x_7x_{11}x_{12}x_{16}+x_4x_7x_{11}x_{12}+x_4x_7x_{11}x_{15}+x_4x_7x_{11}x_{16}+x_4x_7x_{12}x_{15}x_{16}+x_4x_7x_{12}x_{15}+x_4x_7x_{14}+x_4x_7x_{15}x_{16}+x_4x_7+x_4x_8x_{10}x_{12}+x_4x_8x_{10}x_{16}+x_4x_8x_{11}x_{12}x_{15}+x_4x_8x_{11}x_{12}+x_4x_8x_{11}x_{15}x_{16}+x_4x_8x_{11}x_{16}+x_4x_8x_{11}+x_4x_8x_{12}x_{14}+x_4x_8x_{12}x_{15}+x_4x_8x_{12}x_{16}+x_4x_8x_{12}+x_4x_8x_{14}x_{16}+x_4x_8x_{15}x_{16}+x_4x_8x_{15}+x_4x_8x_{16}+x_4x_8+x_4x_{10}x_{11}+x_4x_{10}x_{12}x_{16}+x_4x_{10}x_{12}+x_4x_{10}x_{15}+x_4x_{10}x_{16}+x_4x_{10}+x_4x_{11}x_{12}x_{15}x_{16}+x_4x_{11}x_{12}x_{15}+x_4x_{11}x_{12}x_{16}+x_4x_{11}x_{12}+x_4x_{11}x_{14}+x_4x_{11}x_{15}x_{16}+x_4x_{11}x_{15}+x_4x_{11}x_{16}+x_4x_{11}+x_4x_{12}x_{14}x_{16}+x_4x_{12}x_{14}+x_4x_{12}x_{15}x_{16}+x_4x_{12}x_{15}+x_4x_{12}x_{16}+x_4x_{12}+x_4x_{14}x_{15}+x_4x_{14}x_{16}+x_4x_{14}+x_4x_{15}x_{16}+x_4x_{15}+x_4x_{16}+x_5+x_6x_7x_8x_{12}+x_6x_7x_8x_{16}+x_6x_7x_{11}+x_6x_7x_{12}x_{16}+x_6x_7x_{12}+x_6x_7x_{15}+x_6x_7x_{16}+x_6x_8x_{11}x_{12}+x_6x_8x_{11}x_{16}+x_6x_8x_{12}x_{15}+x_6x_8x_{12}+x_6x_8x_{15}x_{16}+x_6x_8x_{16}+x_6x_8+x_6x_{10}+x_6x_{11}x_{12}x_{16}+x_6x_{11}x_{12}+x_6x_{11}x_{15}+x_6x_{11}x_{16}+x_6x_{11}+x_6x_{12}x_{15}x_{16}+x_6x_{12}x_{15}+x_6x_{12}x_{16}+x_6x_{12}+x_6x_{14}+x_6x_{15}x_{16}+x_6x_{15}+x_6x_{16}+x_7x_8x_{10}x_{12}+x_7x_8x_{10}x_{16}+x_7x_8x_{11}x_{12}x_{15}+x_7x_8x_{11}x_{15}x_{16}+x_7x_8x_{11}+x_7x_8x_{12}x_{14}+x_7x_8x_{12}x_{16}+x_7x_8x_{12}+x_7x_8x_{14}x_{16}+x_7x_8x_{15}+x_7x_8x_{16}+x_7x_{10}x_{11}+x_7x_{10}x_{12}x_{16}+x_7x_{10}x_{12}+x_7x_{10}x_{15}+x_7x_{10}x_{16}+x_7x_{11}x_{12}x_{15}x_{16}+x_7x_{11}x_{12}x_{15}+x_7x_{11}x_{14}+x_7x_{11}x_{15}x_{16}+x_7x_{11}+x_7x_{12}x_{14}x_{16}+x_7x_{12}x_{14}+x_7x_{12}x_{16}+x_7x_{12}+x_7x_{14}x_{15}+x_7x_{14}x_{16}+x_7x_{15}+x_7x_{16}+x_7+x_8x_{10}x_{11}x_{12}+x_8x_{10}x_{11}x_{16}+x_8x_{10}x_{12}x_{15}+x_8x_{10}x_{12}+x_8x_{10}x_{15}x_{16}+x_8x_{10}x_{16}+x_8x_{10}+x_8x_{11}x_{12}x_{14}+x_8x_{11}x_{12}x_{15}+x_8x_{11}x_{12}x_{16}+x_8x_{11}x_{12}+x_8x_{11}x_{14}x_{16}+x_8x_{11}x_{15}x_{16}+x_8x_{11}x_{15}+x_8x_{11}x_{16}+x_8x_{11}+x_8x_{12}x_{14}x_{15}+x_8x_{12}x_{14}+x_8x_{12}x_{15}x_{16}+x_8x_{12}x_{15}+x_8x_{12}x_{16}+x_8x_{12}+x_8x_{14}x_{15}x_{16}+x_8x_{14}x_{16}+x_8x_{14}+x_8x_{15}x_{16}+x_8x_{15}+x_8x_{16}+x_8+x_9+x_{10}x_{11}x_{12}x_{16}+x_{10}x_{11}x_{12}+x_{10}x_{11}x_{15}+x_{10}x_{11}x_{16}+x_{10}x_{11}+x_{10}x_{12}x_{15}x_{16}+x_{10}x_{12}x_{15}+x_{10}x_{12}x_{16}+x_{10}x_{12}+x_{10}x_{14}+x_{10}x_{15}x_{16}+x_{10}x_{15}+x_{10}x_{16}+x_{10}+x_{11}x_{12}x_{14}x_{16}+x_{11}x_{12}x_{14}+x_{11}x_{12}x_{15}x_{16}+x_{11}x_{12}x_{15}+x_{11}x_{12}x_{16}+x_{11}x_{12}+x_{11}x_{14}x_{15}+x_{11}x_{14}x_{16}+x_{11}x_{14}+x_{11}x_{15}x_{16}+x_{11}x_{15}+x_{11}x_{16}+x_{11}+x_{12}x_{14}x_{15}x_{16}+x_{12}x_{14}x_{15}+x_{12}x_{14}x_{16}+x_{12}x_{14}+x_{12}x_{15}x_{16}+x_{12}x_{15}+x_{12}x_{16}+x_{12}+x_{13}+x_{14}x_{15}x_{16}+x_{14}x_{15}+x_{14}x_{16}+x_{14}+x_{15}x_{16}+x_{15}+x_{16}$. deg=5

y_2=$x_3+x_4x_7+x_4x_8x_{12}+x_4x_8x_{16}+x_4x_{11}+x_4x_{12}x_{16}+x_4x_{12}+x_4x_{15}+x_4x_{16}+x_4+x_6+x_7x_8x_{12}+x_7x_8x_{16}+x_7x_{11}+x_7x_{12}x_{16}+x_7x_{12}+x_7x_{15}+x_7x_{16}+x_8x_{11}x_{12}+x_8x_{11}x_{16}+x_8x_{12}x_{15}+x_8x_{12}+x_8x_{15}x_{16}+x_8x_{16}+x_8+x_{10}+x_{11}x_{12}x_{16}+x_{11}x_{12}+x_{11}x_{15}+x_{11}x_{16}+x_{11}+x_{12}x_{15}x_{16}+x_{12}x_{15}+x_{12}x_{16}+x_{12}+x_{14}+x_{15}x_{16}+x_{15}+x_{16}$. deg=3

y_3=$x_4+x_7+x_8x_{12}+x_8x_{16}+x_{11}+x_{12}x_{16}+x_{12}+x_{15}+x_{16}$. deg=2

y_4=$x_8+x_{12}+x_{16}$. deg=1

Diagonal akslantirish uchun 8x2, 12x3, 16x4 variantlarda bir qancha diamatritsalar yordamida eksperimentlar o‘tkazildi. Har xil diamatritsalar uchun tuzilgan tenglamalarni tahlil qilgan holda юqoridagi barcha o‘lchamdagi diagonal akslantirishi uchun quyidagilarni xulosa qilish mumkin:

- akslantirishdan chiqishdagi eng kichik bitni (kichik razryad, ya’ni y_n) ifodalovchi tenglama uchun deg=1 o‘rinli, mos kalit biti qiymatiga bog‘liq ravishda kirish biti ishtirok etadi;

Misol uchun, $k_0=01$, $k_4=01$, $k_8=01$, $k_{12}=11$ bo‘lgan holda $h'_0=2\cdot h_0-1\cdot h_5-1\cdot h_{10}-3\cdot h_{15}(mod4)$ ko‘rinishdagi formula hosil bo‘lib, chiqishdagi eng kichik bitni ifodalovchi tenglama quyidagicha shakllanadi: $y2+x4+x6+x8=0$.

- akslantirishdan chiqishdagi y_{n-1} bitni ifodalovchi tenglama uchun deg=2 o‘rinli, ushbu bitning tenglamasida kirishning mos va o‘zidan kichik razryaddagi bitlarining ishtirok etishi kalitning mos razryadi va o‘zidan kichik razryaddagi biti qiymatiga bog‘liq;

Misol uchun, $k_0=01$, $k_4=01$, $k_8=10$, $k_{12}=01$ bo‘lgan holda $h'_0=1\cdot h_0-1\cdot h_5-2\cdot h_{10}-1\cdot h_{15}(mod4)$ formula hosil bo‘lib, y_{n-1} bitni ifodalovchi tenglama quyidagicha shakllanadi: $y1+x1+x2x4+x2x8+x3+x4x8+x4+x6+x7+x8=0$.

- har bir razryaddagi bitni ifodalovchi tenglamada kirishning shu va undan kichik razryaddagi bitlari va ularning kombinatsiyasining ishtirok etishi kalitning mos bitlari qiymatiga bog‘liq;
- o‘rganilgan diagonal akslantirish formulasida qatnashgan oxirgi uchta ayirma qiymatlarning barchasi uchun bir xil qonuniyat o‘rinlidir, bu esa ushbu uchta qiymatning bir yoki ikkitasini fiksirlagan holda tenglamalarni shakllantirib ushbu tenglamalardagi fiksirlanmagan qiymatlar uchun mavjud xususiyatlarni fiksirlangan

(cc) BY

qiymatlar uchun ham ko‘chirish mumkinligini anglatadi.

Tajribalar natijasida olingan ushbu xulosalar 32x8 o‘lchamli akslantirish uchun ham maxsus dasturiy ta’minot yordamida tenglamalarni shakllantirish imkoniyatini beradi (3-jadval).

3-jadval.

32x8 o‘lchamli diamatritsali ko’paytirish akslantirishi uchun shakllantirilgan tenglamalar

14x2 K_s
$\mathbf{y_1}=x_8+x_9+x_{10}+x_{12}$. deg=1
$\mathbf{y_2}=x_{10}$. deg=1
21x3 K_s
$\mathbf{y_1}=x_1+x_2x_3x_9+x_2x_3x_{12}+x_2x_3x_{15}+x_2x_3x_{18}+x_2x_3x_{21}+x_2x_8+x_2x_9x_{12}+x_2x_9x_{15}+x_2x_9x_{18}+x_2x_9x_{21}+x_2x_{11}+x_2x_{12}x_{15}+x_2x_{12}x_{18}+x_2x_{12}x_{21}+x_2x_{12}+x_2x_{14}+x_2x_{15}x_{18}+x_2x_{15}x_{21}+x_2x_{17}+x_2x_{18}x_{21}+x_2x_{20}+x_3x_8x_9+x_3x_8x_{12}+x_3x_8x_{15}+x_3x_8x_{18}+x_3x_8x_{21}+x_3x_9x_{11}+x_3x_9x_{12}x_{15}+x_3x_9x_{12}x_{18}+x_3x_9x_{12}x_{21}+x_3x_9x_{12}+x_3x_9x_{14}+x_3x_9x_{15}x_{18}+x_3x_9x_{15}x_{21}+x_3x_9x_{17}+x_3x_9x_{18}x_{21}+x_3x_9x_{20}+x_3x_{11}x_{12}+x_3x_{11}x_{15}+x_3x_{11}x_{18}+x_3x_{11}x_{21}+x_3x_{12}x_{14}+x_3x_{12}x_{15}x_{18}+x_3x_{12}x_{15}x_{21}+x_3x_{12}x_{15}+x_3x_{12}x_{17}+x_3x_{12}x_{18}x_{21}+x_3x_{12}x_{18}+x_3x_{12}x_{20}+x_3x_{12}x_{21}+x_3x_{12}+x_3x_{14}x_{15}+x_3x_{14}x_{18}+x_3x_{14}x_{21}+x_3x_{15}x_{17}+x_3x_{15}x_{18}x_{21}+x_3x_{15}x_{20}+x_3x_{17}x_{18}+x_3x_{17}x_{21}+x_3x_{18}x_{20}+x_3x_{20}x_{21}+x_7+x_8x_9x_{12}+x_8x_9x_{15}+x_8x_9x_{18}+x_8x_9x_{21}+x_8x_{11}+x_8x_{12}x_{15}+x_8x_{12}x_{18}+x_8x_{12}x_{21}+x_8x_{12}+x_8x_{14}+x_8x_{15}x_{18}+x_8x_{15}x_{21}+x_8x_{17}+x_8x_{18}x_{21}+x_8x_{20}+x_9x_{11}x_{12}+x_9x_{11}x_{15}+x_9x_{11}x_{18}+x_9x_{11}x_{21}+x_9x_{12}x_{14}+x_9x_{12}x_{15}x_{18}+x_9x_{12}x_{15}x_{21}+x_9x_{12}x_{15}+x_9x_{12}x_{17}+x_9x_{12}x_{18}x_{21}+x_9x_{12}x_{18}+x_9x_{12}x_{20}+x_9x_{12}x_{21}+x_9x_{12}+x_9x_{14}x_{15}+x_9x_{14}x_{18}+x_9x_{14}x_{21}+x_9x_{15}x_{17}+x_9x_{15}x_{18}x_{21}+x_9x_{15}x_{20}+x_9x_{17}x_{18}+x_9x_{17}x_{21}+x_9x_{18}x_{20}+x_9x_{20}x_{21}+x_9+x_{10}+x_{11}x_{12}x_{15}+x_{11}x_{12}x_{18}+x_{11}x_{12}x_{21}+x_{11}x_{12}+x_{11}x_{14}+x_{11}x_{15}x_{18}+x_{11}x_{15}x_{21}+x_{11}x_{17}+x_{11}x_{18}x_{21}+x_{11}x_{20}+x_{11}+x_{12}x_{14}x_{15}+x_{12}x_{14}x_{18}+x_{12}x_{14}x_{21}+x_{12}x_{14}+x_{12}x_{15}x_{17}+x_{12}x_{15}x_{18}x_{21}+x_{12}x_{15}x_{18}+x_{12}x_{15}x_{20}+x_{12}x_{15}x_{21}+x_{12}x_{15}+x_{12}x_{17}x_{18}+x_{12}x_{17}x_{21}+x_{12}x_{17}+x_{12}x_{18}x_{20}+x_{12}x_{18}x_{21}+x_{12}x_{18}+x_{12}x_{20}x_{21}+x_{12}x_{20}+x_{12}x_{21}+x_{13}+x_{14}x_{15}x_{18}+x_{14}x_{15}x_{21}+x_{14}x_{17}+x_{14}x_{18}x_{21}+x_{14}x_{20}+x_{15}x_{17}x_{18}+x_{15}x_{17}x_{21}+x_{15}x_{18}x_{20}+x_{15}x_{20}x_{21}+x_{16}+x_{17}x_{18}x_{21}+x_{17}x_{20}+x_{18}x_{20}x_{21}+x_{19}$. deg=4
$\mathbf{y_2}=x_2+x_3x_9+x_3x_{12}+x_3x_{15}+x_3x_{18}+x_3x_{21}+x_8+x_9x_{12}+x_9x_{15}+x_9x_{18}+x_9x_{21}+x_{11}+x_{12}x_{15}+x_{12}x_{18}+x_{12}x_{21}+x_{12}+x_{14}+x_{15}x_{18}+x_{15}x_{21}+x_{17}+x_{18}x_{21}+x_{20}$. deg=2
$\mathbf{y_3}=x_3+x_9+x_{12}+x_{15}+x_{18}+x_{21}$. deg=1

Nodiagonal akslantirishni ifodalovchi formulalarda qatnashgan $(h_i+h_j+h_k+h_l)k_n$ ko‘rinishdagi ifodalarda yig‘indini 4 bayt kirib 1 bayt chiquvchi akslantirish sifatida ifodalab $-h_mk_t$ ko‘rinishga keltirish mumkin. Shundan so‘ng bu ko‘rinishdagi akslantirishga ham diagonal akslantirish uchun xos bo‘lgan xossalar o‘rinlidir.

Shuningdek, ushbu akslantirishlar uchun tuzilgan tenglamalarni tahlil qilish jarayonida, umumiy holda quyidagicha qonuniyat o‘rinli ekanligi ham aniqlandi.

Diamatritsa elementlari $k_0=01$, $k_4=01$, $k_8=01$, $k_{12}=10$ bo‘lgan hol uchun $h’_0$ hosil qilish formulasi quyidagicha ko‘rinishga ega: $h’_0=1h_0-1h_5-1h_{10}-2h_{15}(mod4)$. Ushbu formulani quyidagi:

$$h’_0=1h_0+3h_5+3h_{10}+2h_{15}(mod4)$$
$$=h_0+h_5+h_5+h_5+h_{10}+h_{10}+h_{10}+h_{15}+h_{15}(mod4)(*)$$

ko‘rinishda ifodalashimiz mumkin. $h’_0$ natijaviy qiymatning eng kichik bitini ifodalovchi tenglamada kirish bitlarining oxirgi bitlari qatnashishi ushbu kirish biti юqoridagi yig‘indida toq yoki juft marta qatnashishiga bog‘liq. YA’ni, chiqish bitini ifodalovchi tenglamada (*) yig‘indida toq marta qatnashgan kirish qiymatlarning oxirgi bitlari qatnashadi. Bizning hol uchun $y2+x2+x4+x6=0$ o‘rinli. Ushbu tenglamada x8 – bit qatnashmaydi, chunki юqoridagi (*) yig‘indida h_{15} qiymat 2 marta qatnashgan.

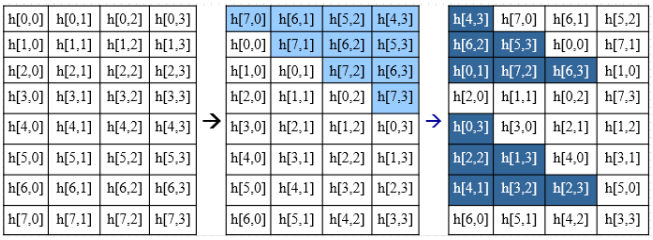
Katta razryad uchun tuzilgan tenglamalar uchun esa quyidagi qonuniyat o‘rinli: (*) Yig‘indida toq marta qatnashgan qiymatlarning mos bitlari, (*) yig‘indida bir martadan ortiq qatnashgan qiymatlarning oxirgi bitlari va toq marta qatnashgan qiymatlarning oxirgi bitlari o‘zaro kombinatsiyalari (ko‘paytmalari) yig‘indisi natijaviy tenglamani hosil qiladi. Bizning hol uchun: $y1+x1+x2x4+x2x6+x3+x4x6+x4+x5+x6+x8=0$ o‘rinli.

Ushbu qonuniyat har bir razryadni qo‘shish o‘zidan oldingi kichik razryadlarni qo‘shish natijasiga bog‘liq bo‘lgan sonlarni qo‘shish qoidasiga asoslangan.

© I.R. Rahmatullayev, B.F. Abduraximov, I.M. Boykuziyev, B.Ya. Kholliyev

Bu qonuniyat 12x3, 14x2, 16x4, 21x3 variantlar uchun ham o‘rinli ekanligi tajribalar yordamida aniqlandi.

Shundan kelib chiqib xulosa qilish mumkinki ushbu qonuniyat 32x8 va 56x8 variantlar uchun ham o‘rinlidir.

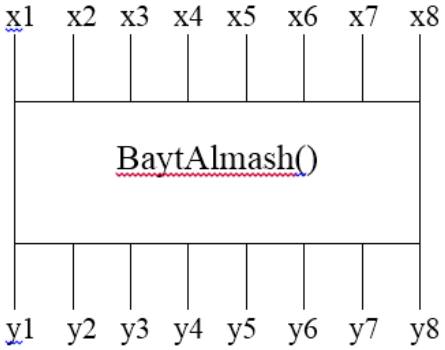


6-rasm. S(x) – funktsiya sxemasi.

Demak, ushbu akslantirish uchun quyidagi tenglamalar sistemasini qurish mumkin (4):

$$\begin{cases} y_1 = x_{153} \\ y_2 = x_{154} \\ y_3 = x_{155} \\ \dots\ \dots\ \dots \\ y_{129} = x_{25} \\ y_{130} = x_{26} \\ y_{131} = x_{27} \\ \dots\ \dots\ \dots \\ y_{256} = x_{128} \end{cases} \qquad (4)$$

***y=B(x)* - funksiya** – o‘lchami 8x8 bit bo‘lgan BaytAlmash() akslantirishini amalga oshiradi (BaytAlmash() jadvali o‘zgaruvchan bo‘lib, maxfiy kalit yordamida hisoblanadi) (7-rasm) .



7-rasm. B(x) – funktsiya sxemasi.

***y=S(x)* - funksiya** – umumiy uzunligi 256 bit bo‘lgan, har bir elementi baytlardan tashkil topgan (8,4) o‘lchamli matritsa elementlarini ustun bo‘yicha pastga va satr bo‘yicha o‘ngga surishni amalga oshiradi (6-rasm).

Ushbu akslantirishga nisbatan to‘g‘ri (shifrlash) yo‘nalishda, teskari (deshifrlash) yo‘nalishda va aralash (darajasi pasaytirilgan) algebraik tenglamalarni qurish mumkin, ya’ni:

1. $y_i = F(x_1, x_2, \dots, x_8)\ ,\ i = 1,2,\dots,8$
2. $x_i = F(y_1, y_2, \dots, y_8)\ ,\ i = 1,2,\dots,8$
3. $F(x_1, x_2, \dots, x_8, y_1, y_2, \dots, y_8) = 0$

1 – ko‘rinishdagi to‘g‘ri (shifrlash) yo‘nalishda tuzilgan tenglamalar sistemasi akslantirishdan chiquvchi bitlarni akslantirishga kiruvchi bitlar orqali ifodalovchi tenglamalardan iborat bo‘ladi. 2 – ko‘rinishdagi teskari (deshifrlash) yo‘nalishda tuzilgan tenglamalar sistemasi akslantirishga kiruvchi bitlarni akslantirishdan chiquvchi bitlar orqali ifodalovchi tenglamalardan iborat bo‘ladi. Agar BaytAlmash() jadvali regulyarlik shartini qanoatlantirsa 1 – va 2 – ko‘rinishdagi tenglamalar sistemasining maksimal darajasi deg=7 ga teng bo‘ladi.

XULOSA

O‘zDSt 1105:2009 algoritmida foydalanilgan akslantirishlarning algebraik xususiyatlarini o'rganish natijasida quyidagi asosiy xulosalar chiqarildi:

–algoritm komponentlari algebraik tenglamalar sistemasi shaklida ifodalanib, ularni yechish imkoni mavjud bo‘lsa shifrlash kaliti haqidagi ma‘lumotlarni aniqlash mumkin.

–tenglamalar sistemasini shakllantirishda algoritmning barcha akslantirish elementlari, ayniqsa, chiziqsiz akslantirishlar asosiy rol o‘ynaydi. Ushbu elementlarning algebraik tahlili hisoblashlarning murakkabligini oshiradi.

–tadqiqot natijalariga ko'ra, algebraik kriptotahlil usuli yordamida O‘zDSt 1105:2009

(cc) BY © I.R. Rahmatullayev, B.F. Abduraximov, I.M. Boykuziyev, B.Ya. Kholliyev

algoritmining xavfsizlik darajasi baholanib, uning mustahkamligi haqida xulosa qilish mumkin.

Mazkur tadqiqot algebraik kriptotahlil usulining amaliyotda qo'llanilishini rivojlantirishga va shifrlash algoritmlarini baholashda yangi yondashuvlarni taklif etishga hissa qo'shadi.

FOYDALANILGAN ADABIYOTLAR

1. **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.
2. **Alekseychuk A. N. and Kovalchuk L. V.**: Towards a Theory of Security Evaluation for GOST-like Ciphers against Differential and Linear Cryptanalysis, Preprint 9 Sep 2011.
3. **Babenko L., Ishchukova E.**: Differential analysis of GOST encryption algorithm, In SIN 2010, pp. 149-157, ACM, 2010.
4. **Buchberger B.** Grobner-Bases**:** An Algorithmic Method in Polynomial Ideal Theory. Reidel Publishing Company, Dodrecht - Boston - Lancaster, 1985. Pp. 184-232.
5. **Courtois N.** Algebraic Complexity Reduction and Cryptanalysis of GOST. Preprint, 12 November 2011.
6. **Courtois N. and Misztal M.** First Differential Attack on Full 32-Round GOST*. in ICICS'11, pp. 216-227, Springer LNCS 7043, 2011.
7. **Courtois N., Gregory V. Bard:** Algebraic Cryptanalysis of the Data Encryption Standard. IMA Int. Conf. 2007: 152-169
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. **Courtois N.**: Low Complexity Key Recovery Attacks on GOST Block Cipher, In Cryptologia, Volume 37, Issue 1, pp. 1-10, 2013.
10. **Ferguson, N., Schroeppel, R. and Whiting, D.** (2001) A Simple Algebraic Representation of Rijndael. Proceedings of Selected Areas in Cryptography, Springer-Verlag, New York, 103-111. http://dx.doi.org/10.1007/3-540-45537-X_8
11. **Fleischmann E., Gorski M., Huhne J., and Lucks S.** KR Attack on full GOST Block Cipher with Zero Time and Memory. Published as ISO/IEC JTC 1/SC27 N8229. 2009.
12. **Harris N.** Algebraic cryptanalysis of AES: an overview. 2010.
13. **Haruki S. and Toshinobu K.:** Differential Cryptanalysis of Reduced Rounds of GOST. In SAC 2000, Selected Areas in Cryptography, Douglas R. Stinson and Stafford E. Tavares, editors, LNCS 2012, pp. 315-323, Springer, 2000.
14. **Jintai Ding, Johannes Buchmann, Mohamed Saied Emam Mohamed, Wael Said Abdelmageed Mohamed, and Ralf-Philipp Weinmann**. MutantXL. In Proceedings of the 1st international conference on Symbolic Computation and Cryptography (SCC08), pages 16 – 22, http://www.cdc.informatik.tu–darmstadt.de/reports/reports/MutantXL Algorithm.pdf, Beijing, China, April 2008. LMIB.
15. **Kelsey J., Schneier B. and Wagner D.** "Key Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES", Advances in Cryptology – CRYPTO '96, volume 1109 of Lecture Notes of Computer Science, Springer-Verlag, 1996, pp. 237-251.
16. **Kleiman E.** The XL and XSL attacks on Baby Rijndael // Ms. Thesis. Iowa SU, USA, 2005.

© I.R. Rahmatullayev, B.F. Abduraximov, I.M. Boykuziyev, B.Ya. Kholliyev