KONFERENSIYALAR UZ
ANJUMANLAR PLATFORMASI

O‘ZBEKISTON – 2030: INNOVATSIYA, FAN VA TA’LIM ISTIQBOLLARI

II RESPUBLIKA ILMIY-AMALIY KONFERENSIYA MATERIALLARI

IYUN, 2025-YIL

O‘ZBEKISTON 2030

KONFERENSIYALAR UZ
ANJUMANLAR PLATFORMASI

O‘ZBEKISTON — 2030: INNOVATSIYA, FAN VA TA’LIM ISTIQBOLLARI

II RESPUBLIKA ILMIY-AMALIY KONFERENSIYASI MATERIALLARI

2025-yil, iyun

TOSHKENT-2025

ISBN 978-9910-09-204-6

O‘ZBEKISTON – 2030: INNOVATSIYA, FAN VA TA’LIM ISTIQBOLLARI. II Respublika ilmiy-amaliy konferensiyasi materiallari. – Toshkent: Scienceproblems team, 2025. – 138 bet.

Elektron nashr: https://konferensiyalar.uz/uzbekistan-2030

Konferensiya tashkilotchisi: “Scienceproblems Team” MChJ

Konferensiya o‘tkazilgan sana: 2025-yil, 23-iyun

Mas’ul muharrir:
Isanova Feruza Tulqinovna

Annotatsiya
Mazkur nashrda “O‘zbekiston — 2030: innovatsiya, fan va ta’lim istiqbollari” nomli II Respublika ilmiy-amaliy konferensiyasi doirasida taqdim etilgan ilmiy maqolalar to‘plami jamlangan. Unda O‘zbekistonning turli oliy ta’lim va ilmiy-tadqiqot muassasalari, tarmoq tashkilotlari, mustaqil tadqiqotchilar tomonidan taqdim etilgan ijtimoiy-gumanitar, iqtisodiyot, huquq, biologiya, tibbiyot va boshqa sohalarga oid maqolalar kiritilgan. Maqolalarda ilm-fanning zamonaviy yo‘nalishlari, innovatsion texnologiyalar, ta’lim islohotlari hamda barqaror taraqqiyotga oid masalalar muhokama qilingan. To‘plam akademik izlanishlar, amaliy tajribalar va ilmiy xulosalarni birlashtirgan holda, fanlararo integratsiyani chuqurlashtirish va ilmiy hamkorlikni kuchaytirishga xizmat qiladi.

Kalit so‘zlar: ilmiy-amaliy konferensiya, innovatsiya, fan va ta’lim, O‘zbekiston 2030, barqaror rivojlanish, ilmiy izlanishlar, fanlararo integratsiya, ilmiy hamkorlik, texnologik taraqqiyot, zamonaviy ta’lim.

ISBN 978-9910-09-204-6

MUNDARIJA

GEOGRAFIYA FANLARI

YURIDIK FANLAR

PEDAGOGIKA FANLARI

ZAMONAVIY SIMMETRIK SHIFRLASH ALGORITMLARINI CHIZIQLI KRIPTOTHLILI

Tursunov Otabek Odiljon o‘g‘li
Muahammad al-Xorazmiy nomidagi TATU,
Kriptologiya kafedrasi kata o‘qituvchisi

Shakarov Muhiddin Abdug‘affot o‘g‘li
Muahammad al-Xorazmiy nomidagi TATU Nurafshon filiali,
O‘quv uslubiy boshqarma boshlig‘i

Annotatsiya. Ushbu ishda zamonaviy kriptografik tizimlar xavfsizligini baholashda muhim bo‘lgan chiziqli kriptotahlil usuli asosida simmetrik shifrlash algoritmlarining zaif tomonlarini aniqlashdagi roli yoritilgan. Shuningdek, chiziqli kriptotahlilning mohiyati, matematik asosi va ishlash algoritmi haqida tushuncha berilgan. DES simmetrik shifrlash algoritmiga nisbatan chiziqli tahlil usullarini qo‘llash orqali ularning zaiflik darajalari o‘rganilgan.

Kalit so‘zlar: Simmetrik shifrlash, chiziqli kriptotahlil, kriptobardoshlilik, DES algoritmi, matematik tahlil.

LINEAR CRYPTANALYSIS OF MODERN SYMMETRIC ENCRYPTION ALGORITHMS

Tursunov Otabek Odiljon o‘g‘li
Senior Lecturer, Department of Cryptology,
Muhammad al-Khwarizmi Tashkent University
of Information Technologies

Shakarov Muhiddin Abdug‘affot o‘g‘li
Head of the Educational and Methodological Department,
Nurafshon Branch of Muhammad al-Khwarizmi
Tashkent University of Information Technologies

Abstract. This work highlights the role of linear cryptanalysis in identifying weaknesses of symmetric encryption algorithms, which is important in assessing the security of modern cryptographic systems. It also provides an understanding of the essence, mathematical basis, and working algorithm of linear cryptanalysis. The levels of vulnerability of the DES symmetric encryption algorithm are studied using linear analysis methods.

Key words: Symmetric encryption, linear cryptanalysis, cryptresistance, DES algorithm, mathematical analysis.

DOI: https://doi.org/10.47390/978-9910-09-204-6/uzb-03

Kirish

Zamonaviy chiziqli kriptoanaliz usuli Yaponiyalik kriptograf M.Matsui tomonidan 1993-yilda DES shifrlash algoritmiga qarshi hujum turi sifatida ishlab chiqilgan.

Ushbu kriptoanaliz usulining mohiyati tanlab olingan ochiq matn M va mavjud shifrmatn C larning bitlarini XOR amali yordamida qo‘shish va natijada kalit bitlarini aniqlashdan iborat:

$$M[i_1, i_2, \dots . i_n) \oplus C[j_1, j_2, \dots . j_n] = K[k_1, k_2, \dots . k_n],$$

bu yerda $M[i_1, i_2, \dots . i_n) = M[i_1) \oplus M[i_2) \oplus \dots . M[i_n)$

$S[i_1, i_2, \dots . i_n) = S[i_1) \oplus S[i_2) \oplus \dots . S[i_n)$

$K[i_1, i_2, \dots . i_n) = K[i_1) \oplus K[i_2) \oplus \dots . K[i_n)$

Natijada yuqoridagi tenglikdan eng yaqin chiziqli approksimatsiyani aniqlash, ya’ni tahlil qilinayotgan algoritm akslantirishlari xossalaridan kelib chiqib, eng samarali chiziqli bog‘lanishni tanlashdan iborat. Tanlangan approksimatsiya tenglamalarida tenglikning chap tomonining qiymati 0 yoki 1 ga teng ekanligini aniqlash uchun yetarlicha ko‘p miqdordagi ochiq matn va shifr matn juftliklari ustida statistik tahlil olib borish kerak bo‘ladi. Natijada, faqat kalit bitlari ishtirok etgan tenglamalar sistemasiga ega bo‘linadi. Ushbu tenglamalar sistemasini yechish orqali kalit bitlarini aniqlash mumkin bo‘ladi[1, 4-7b].

Muhokama

Simmetrik blokli shifrlash algoritmlarida chiziqsiz akslantirishlar S-bloklar bo‘lib hisoblanadi. Demak S-bloklarini kriptoanaliz qilish asosida algoritmning kriptobardoshliligi xususida xulosa bildirish mumkin. S–bloklarni chiziqli kriptoanaliz qilish uchun chiziqli approksimatsiya tenglamalarini tuzish kerek. Bunda “korrelyatsion matritsa” jadvalidan foydalanish samarali usul hisoblanib, aynan ushbu jadval chiziqli kriptoanalizning asosiy xarakteristikasi hisoblanadi.

Korrelyatsion matritsani tuzish quyidagicha amalga oshiriladi. Masalan, shifrlash algoritmida $Y = \varphi(X): GF(2^n) \to GF(2^m)$ chiziqsiz akslantirish bajarilgan bo‘lsin. Ya’ni, $X[x_1, x_2, \dots . x_n)$ – akslantirishga kiruvchi bitlarni, $Y[y_1, y_2, \dots . y_n)$–akslantirishdan chiquvchi bitlarni ifodalaydi.

Ta’rif. $Y = \varphi(X)$ - akslantirishga nisbatan korrelyatsion matritsa deb, har bir (i,j) - elementi quyidagi tenglik bilan aniqlanuvchi C – jadvalga aytiladi:

$C(\mathrm{i}, \mathrm{j}) = \#\{X < X, i >= Y < Y, j >\}$ bu yerda

$$i \in 2^n, j \in 2^m,$$

$< X, i > [x_1 i_1 \oplus x_2 i_2 \oplus, \dots . x_n i_n),$

$$< Y, i > [y_1 i_1 \oplus y_2 i_2 \oplus, \dots . y_n i_n)$$

Ta’rifdan korrelyatsion matritsa akslantirishga kiruvchi va chiquvchi bitlar turli xil pozitsiyalarining o‘zaro bog‘lanishlarini, ya’ni kiruvchi i–bitlarni XOR amali yordamida yig‘indisining chiquvchi j–bitlarni XOR amali yordamida yig‘indisiga necha marta teng bo‘lishini ifodalaydi.

Chiziqli tahlilning maqsadi nochiziqli qismlarni chiziqli tenglamalar bilan taxminiy ifodalashga qaratiladi. Matematiklar uchun chiziqli tenglamalarni yechish oson, agar shunday ehtimolliklar topilsa, bu hujumni shifrmatnga qaratish mumkin. DES algoritmining nochiziqli qismi bu S-bloklardir, shuning uchun chiziqli kriptoanaliz S-bloklar ustida amalga oshiriladi.

Ya’ni, 4.1-jadvaldagi S-blokni ko‘rib chiqilsa, uchta kirish bitlarini x_0, x_1, x_2 va ikkita chiqish bitlarini y_0, y_1 kabi belgilab olinadi. Jadvalning satri x_0 qiymatni, ustuni x_1, x_2 qiymatlarini belgilaydi. Ajratilmagan satrdagi belgilar y_0, y_1 chiqish qiymatlarini ifodalaydi. Masalan S-blokga $x_0 x_1 x_2 = 000$ qiymati kiritilganda undan $y_0 y_1 = 10$ ga teng qiymat chiqadi va hakozo.

1-jadval.

3 bit kirish qiymatini 2 bit chiqishga akslantiruvchi S blok

Satr	Ustun			
	00	01	10	11

0	10	01	11	00
1	00	10	01	11

Chiziqli kriptoanalizning asosiy g‘oyasi nochiziqli S-bloklardan chiqish qiymatilarining kirish qiymatlariga bo‘g‘liqligidan kalit qiymatini aniqlash hisoblanadi. Shundan kelib chiqib ushbu kriptoanaliz usulida kirish bitlarining chiqish bitlarini bilan bo‘g‘liqligini ifodalovchi 1.5-jadvaldagi kabi korrelyatsion matrisa tuziladi. Korelyatsion matrisa jadvalini tuzish quyidagicha amalga oshiriladi. Kirish va chiqish bitlarining bog‘liqligi jadvali tuzib olinadi:

Kirish bitlaring barcha kirish qiymatlari $000_2=0_{10}$ dan $111_2=8_{10}$ ga 1-jadvaldagi chiqish qiymatlari mosligini quyidagi 2-jadvaldagi kabi yozib olinadi.

2-jadval.

1-jadvaldagi chiqish qiymatlari mosligi

x0	x1	x2	y0	y1
0	0	0	1	0
0	0	1	0	1
0	1	0	1	1
0	1	1	0	0
1	0	0	0	0
1	0	1	1	0
1	1	0	0	1
1	1	1	1	1

Kriptoanalizda 0 ga teng kirish va 0 ga teng chiqish qiymatlari kalit bitlarini aniqlashda yordam bermaganligi sababli ularning qiymati olib tashlanadi va quyidagi 3-jadvaldagi kabi 7x3 o‘lchamdagi korelatsion matrisa tuziladi. Korelatsion matrisaning jadvali quyidagicha to‘ldiriladi. Masalan jadvalning 2 satr va 2 ustuni kesishmasida joylashgan 6 ga teng qiymat quyidagicha hisoblangan:

$2_{10}=01_2=0*x_0⊕1*x_1=x_1$ qiymatning $2_{10}=01_2=0*y_0⊕1*y_1=y_1$ qiymatga 4.2-jadval asosida 6 marta tengligini ko‘rsatadi;

$7_{10}=111_2=1*x_0⊕1*x_1⊕1*x_2=x_0⊕x_1⊕x_2$ qiymatning $7_{10}=111_2=1*y_0⊕1*y_1⊕1*y_2=y_0⊕y_1⊕y_2$ qiymatga 1.4-jadval asosida 2 marta tengligini ko‘rsatadi va hakozo.

3-jadval.

1-jadvaldagi S-blokning korrelatsion matritsa jadvali

Kirish bitlari	***Chiqish bitlari***		
	y_0	***y_1***	***$y_0⊕y_1$***
x_0	4	4	4
x_1	4	6	2
x_2	4	4	4
$x_0⊕x_1$	4	2	2
$x_0⊕x_2$	4	4	4
$x_1⊕x_2$	4	6	6
$x_0⊕x_1⊕x_2$	4	6	2

Yuqoridagi 1.5-jadval natijalari shuni ko‘rsatadiki, masalan, $y_1=x_1$, ya’ni y_1 ning x_1 ga teng bo‘lish imkoniyati 8 ta dan 6 ta holatda bajarilgan. Bu tenglamaning ¾ ehtimollik bilan bajarilishini bildiradi. $x_0 \oplus x_1 \oplus x_2 = y_0 \oplus y_1$ tenglik 1.5-jadvalga asosan 8 ta holatdan 2 ta holatda qanoatlangan. Bu tengliknini bajarilish ehtimolligi ¾ ga teng. Demak bu tenglikning teskarisi bajarilishi ehtimolligi katta. Unga 1 ni XOR amali bilan qo‘shib bemalol 1 qiymatga amashtirish mumkin. 4.3-jadvalda kirish va chiqish bitlarining teng bo‘lish ehtimolligi ko‘rib chiqilgan. Jadvalda “4” ga teng bo‘lmagan qiymatlar tasodifiy bo‘lmagan, ya’ni chiqish bitining tasodifiy almashmaganini bildiradi.

Ushbu ma’lumotlardan foydalanib, S-bloklarni chiziqli funksiyalar bilan almashtirib tahlil qilish mumkin. Natijada nochiziqli S-bloklardan chiziqli tenglamalarni hosil qilib olish, bu yerda chiziqli tenglamalar aniqlilikka asoslangan bo‘lishi shart emas, lekin bu tenglamalarni muhim bo‘lmagan ehtimolliklar bilan bajarish imkoniyati mavjud.

Bu chiziqli ehtimollik tenglamalaridan DES shifrlash bloklariga hujum foydaliroq bo‘lishi uchun bu yodashuvni kengaytirishga harakat qilish kerak. Natijada kalitni topishga qaratilgan chiziqli tenglamalarni yechish imkoniyatiga ega bo‘linadi. Xuddi differensial tahlilda bo‘lgani kabi barcha raundlar uchun “ketma-ketlik zanjiri” kabi bog‘langan tenglamalar sistemasini hosil qilish mumkin.

Chiziqli funksiyalar bilan DES algoritmi S-bloklarining qanchalik yaqin ehtimollik bilan ifodalash mumkin. DES algoritmining har bir S-bloki nochiziqli kombinatsiyalar asosida loyihalashtirilgani uchun kirish bitlari chiqish bitiga yaxshi ehtimollik bilan almashadi. Biroq, kirish bitlarining chiziqli kombinatsiyasi orqali taxmin qilingan chiqish bitlarining chiziqli kombinatsiyasini aniqlash mumkin. Natijada DES algoritmini muaffaqiyatli chiziqli kriptoanaliz qilish mumkin.

Chiziqli kriptoanalizni ko‘rsatish uchun, DES algoritmiga o‘xshash Tiny(sodda) DES algoritmi va AES shifrlash algoritmlari uchun chiziqli kriptotahlil usulini o‘tkazish jarayoni 2-bobda ma’lumot beriladi[2, 3-7b].

Tiny DES yoki TDES algoritmi, bu DES algoritmiga nisbatan oson va oddiy kriptoanaliz qilinadigan sodda shifrlash algoritmi. TDES algoritmi chiziqli va differensial kriptoanalizni amalga oshirish uchun yaratilgan sodda shirflash algoritmi. Shunga qaramay bu tahlillarni amalga oshirish uchun DES algoritmiga o‘xshashdir. TDES quyidagilardan tarkib topgan DES algoritmining soddalashtirilgan variantidir:

- blok uzunlidigi 16-bit;
- kalit uzunligi 16-bit;
- to‘rtta raund;
- ikkita S-blok, xar biri 6 bit kirish 4 bit chiqish;
- har bir round uchun 12-bitli qism kalit.

TDES algoritmida boshlangich va oxirgi o‘rniga qo‘shish amalini bajaruvchi P-blok yo‘q. Asosan, bunda DES algoritmiga tegishli barcha xavfsizlik xususiyatlariga katta ta’sir qilmagan holda, blok va kalit uzunliklari kamaytirilgan.

Kalit va blok uzunligining kichikligi TDES algoritmining xavfsizlikni ta’minlay olmasligini bildiradi va tahlil natijasi qanday bo‘lishidan qat’iy nazar kerakli algoritm bo‘lolmasligini bildiradi. Shunga qaramay, TDES algoritmini chiziqli va differensial tahlilda hamda simmetrik

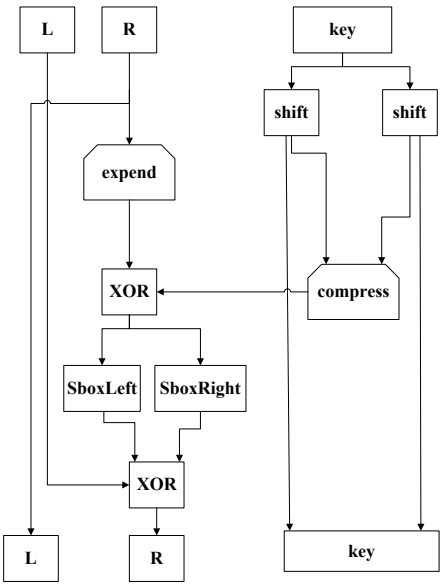
blokli shifrlarning boshqa muammolarini yechishda sodda algoritm sifatida foydalanish mumkin.

TDES algoritmida Feystel tarmog‘iga asosan ochiq matn (L_0, R_0) qismlarga ajratiladi. Keyin to‘rtta $(for\ i = 1,2,3,4)$ raundlar uchun quyidagi almashtirish bajariladi:

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$

oxirida shifrlangan matn (L_4, R_4) ga teng bo‘linadi. TDES algoritmining bir raundi quyida 1-rasmda tasvirlangan. Bu yerda har bir satrda bitlar nomerlarda ko‘rsatilgan.



1-rasm. Tiny DES algoritminining bir raundi

TDES algoritmida ikkita S-blok, $SboxLeft(X)$ va $SboxRight(X)$ bor. Har ikkisi ham DES algoritmidagidek 6 bit kirish 4 bit chiqishga ega. TDES algoritmida kriptoanaliz uchun muhim jihat S-bloklar va ularga kirish qiymatlari hisoblanadi. Tizimni soddalashtirish uchun F funksiya aniqlanadi

$$F(R, K) = Sboxes(expand(R) \oplus K) \quad (4)$$

Bu yerda

$$Sboxes(x_0x_1x_2..x_{11}) = (SboxLeft(x_0x_1..x_5), SboxRight(x_6x_1x_7..x_{11})).$$

Bunda kengaytirish o‘rniga qo‘yish quyidagicha amalga oshiriladi

$$expand(R) = expand(r_0r_1..r_7) = (r_7r_7r_2r_1r_5r_7r_0r_2r_6r_5r_0r_3).$$

Quyida TDES algoritmining chap $SboxLeft(X)$ S-blokini keltirilgan. S-blokning 16 lik sanoq sistemasida ifodalanganishi 4-jadvalda keltirilgan.

4-jadval.

S-blokning 16 lik sanoq sistemasida ifodalanishi

	X1X2X3X4															
0X5																

Bu yerda o‘ng $SboxRight$ (X), S-bloki quyidagicha:

	$x_1x_2x_3x_4$															
$0x_5$																

DES algoritmida bo‘lgani kabi, TDES algoritmida ham S-bloklar almashtirishlari 16 lik sanoq sistemasida ifodalangan, ya’ni *0,1,2,...,E,F.* TDES algoritminig kalit hosil qilish jarayoni juda oddiy. 16 bitli dastlabki kalit olinadi:

$$K = k_0k_1k_2k_3k_4k_5k_6k_7k_8k_9k_{10}k_{11}k_{12}k_{13}k_{14}k_{15}$$

va yordamchi kalitni quyidagicha hosil qilinadi:

1. Dastlabki kalit o‘rtasidan teng ikkiga LK chap va RK o‘ng qism kalitga ajratiladi

$$LK = k_0k_1k_2k_3k_4k_5k_6k_7$$
$$RK = k_8k_9k_{10}k_{11}k_{12}k_{13}k_{14}k_{15}$$

2. Har bir raund $(i = 1,2,3,4)$ uchun qism kalitlar chap tomonga quyidagicha siklik suriladi

$$LK = rotate\ LK\ (2\ birlik\ chapga\ surish)$$
$$RK = rotate\ RK\ (1\ birlik\ chapga\ surish)$$

3. Hosil bo‘lganlardan (LK, RK) tartibida 16-bitli kalit yasaladi. Yasalgan kalitni 12 bitga siqish uchun uning *0,2,3,4,5, 7,9,10,11,13,14 va 15* tartibidagi bitlaridan yangi qism kalit hosil qilinadi.

K_i raund kalitlari quyidagicha ifodalanishi mumkin:

$$K_1 = k_2k_4k_5k_6k_7k_1k_{10}k_{11}k_{12}k_{14}k_{15}k_8$$
$$K_2 = k_4k_6k_7k_{10}k_1k_3k_{11}k_{12}k_{13}k_{15}k_8k_9$$
$$K_3 = k_6k_0k_1k_2k_3k_5k_{12}k_{13}k_{14}k_8k_9k_{10}$$
$$K_4 = k_0k_2k_3k_4k_5k_7k_{13}k_{14}k_{15}k_9k_{10}k_{11}$$

Keyingi bo‘limda TDES algoritmi chiziqli kriptoanaliz qilinadi. Undan keyin TDES algoritmiga qaratilgan differensial kriptoanaliz ko‘rib chiqiladi. Ushbu ma’lumotlar DES va boshqa blokli shifrlash algoritmlari uchun differensial va chiziqli kriptoanalizni amalga oshirishga taalluqli muhim prinsiplarni aks ettiradi.

TDES algoritmining chiziqli kriptoanalizi

TDES algoritmini chiziqli kriptoanalizi differensial kriptoanaliziga nisbatan soddaroq hisoblanadi. Quyida TDESning algoritmining chiziqli kriptoanalizi chap S-blokiga qaratilgan.

Quyidagi belgilar bilan berilgan:

$y_0y_1y_2y_3$=Sboxleft(x_0 $x_1x_2x_3x_4x_5$).

TDES algoritmining chap S-blokini chiziqli approksiomatiya tenglamalari

$y_1 = x_2$ va $y_2 = x_3$ (2.1)

¾ ehtimollik bilan bajariladi. Bunga o‘xshash approsiya tenglamalariga asoslangan chiziqli tahlilni rivojlantirish uchun ushbu usulni barcha roundlarga ketma-ket qo‘llash shart.

5-jadval.

S-blokning 16 lik sanoq sistemasida ifodalanishi

	$x_1x_2x_3x_4$															
$0x_5$																

Ochiq matn $P=(L_0,R_0)$dan $R_0=r_0r_1r_2r_3r_4r_5r_6\ r_7$ o‘ng qismi tanlab olinadi. Keyin kengaytirish funksiyasidan quyidagiga ega bo‘linadi:

$expend(R_0)= expend\ (r_0r_1r_2r_3r_4r_5r_6\ r_7)= r_4r_7r_2r_1r_5r_7r_0\ r_2\ r_6r_5r_0\ r_3.$ (2.2)

2.2-tenglamadagi F funksiyaning ta’rifidan, S-blokga birinchi raunddagi kirish qiymatini $expand(R_0) \oplus K_1$ tenglikdan olish mumkin. Keyin, 2.2-tenglama va K_1 round kaliti ta’rifidan, chap S-blokga birinchi raundda kirish qiymatini quyidagiga tengligini ko‘rish mumkin:

$r_4r_7r_2r_1r_4r_5\ r_7 \oplus k_2k_4k_5k_6k_7k_1.$

Demak $y_0y_1y_2y_3$ chap S-blokdan birinchi raundda chiqish qiymatlari deb qaraladi. Keyin yuqoridagi 4.1-tenglama quyidagini nazarda tutadi:

$y_1= r_2 \oplus k_5\ va\ y_2= r_1 \oplus k_6,$ (2.3)

bu yerdagi har bir tenglikning bajarilish ehtimolligi ¾ ga teng. Boshqa so‘z bilan aytganda, chap S-blok uchun, chiqishdagi 1-indeksdagi bit kirishdagi 2-indeksdagi bit hisoblanadi. XOR amali bilan hisoblanganda, chiqish bitining 2-raqami kirish bitining 1-raqamiga teng bo‘lishi ¾ ehtimollik bilan hisoblanadi (5-jadval).

TDES algoritmida (DES algoritmida bo‘lgani kabi) S-blokdan chiqish qiymatlari oldingi qadamdagi chap yarim bloki bilan XOR amali bilan qo‘shiladi. Demak $L_0=l_0l_1l_2l_3l_4l_5l_6l_7$ va $R_1=r'_0r'_1r'_2r'_3r'_4r'_5r'_6r'_7$ bo‘lsin, keyin bu S-blokdan birinchi roundda chiqish qiymatlari $r'_0r'_1r'_2r'_3$ ni chap blok $l_0l_1l_2l_3$ bilan XOR amali orqali qo‘shiladi. Ushbu belgilarni 2.3-tenglama orqali birlashtirib, quyidagiga ega bo‘linadi:

$r'_1=r_2 \oplus k_5 \oplus l_1\ va\ r'_2=r_1 \oplus k_6 \oplus l_2,$ (2.4)

bu tenglamalarning har biri ¾ ehtimollik bilan bajariladi. Xuddi shunga o‘xshash natijalar keyingi raundlarda takrorlanadi, bu yerda maxsus kalit bitlari qism kalit K_i ga bog‘liq.

2.4-tenglama natijasida, barcha raundlar uchun 2.3-tenglamadagidek chiziqli approksiya tenglamalarini tuzish mumkin. Ular quyida 5-jadvalda tasvirlangan. Chiziqli kiriptotahlil bu ochiq matnni bilish hujumi (known plaintext attack) bo‘lgani uchun, bunda hujumchi ochiq matnni $P = p_0p_1..p_{15}$ va shunga mos shifrmatnni $C=c_0c_1c_2..c_{15}$ biladi. 2.3-jadvalning oxirgi satrida $L_4=c_0c_1c_2c_4c_5c_6c_7$ ekanligi keltirilgan.

Ushbu tenglamalarni quyidagicha qayta yozish mumkin:

$k_0 \oplus k_1=c_1 \oplus p_{10}$ (2.5)

va

$k_7 \oplus k_2=c_2 \oplus p_9.$ (2.6)

Natijalar

Yuqoridagi tenglamalarning har ikkalasi ham (¾)^3 ehtimollik bilan bajariladi. c_1, c_2, p_9 va p_{10} ma’lumligidan, k_0, k_1, k_2 va k_7 kalit bitlari haqida ba’zi ma’lumotlarga ega bo‘linadi.

6-jadval.

TDES algoritmining chiziqli tahlili

$(L_0,R_0)=(p_0...p_7,p_8...p_{15})$	1 va 2 bitlar (raqamlar 0 dan boshlangan)	Bajarilish ehtimolligi
$L_1=R_0$	p_9,p_{10}	1
$R_1=L_0⊕F(R_0,K_1)$	$p_9⊕p_{10}⊕k_5$, $p_2⊕p_9⊕k_6$	¾
$L_2=R_1$	$p_1⊕p_{10}⊕k_5$, $p_2⊕p_9⊕k_6$	¾
$R_2=L_1⊕F(R_1,K_2)$	$p_9⊕k_6⊕k_7$, $p_1⊕k_5⊕k_0$	(¾)^2
$L_3=R_2$	$p_2⊕k_6⊕k_5$, $p_1⊕k_5⊕k_0$	(¾)^2
$R_3=L_2⊕F(R_2,K_3)$	$p_{10}⊕k_0⊕k_1$, $p_9⊕k_7⊕k_2$	(¾)^3
$L_4=R_3$	$p_{10}⊕k_0⊕k_1$, $p_9⊕k_7⊕k_2$	(¾)^3
$R_4=L_3⊕F(R_3,K_4)$		
$C=(L_4,R_4)$	$c_1=p_{10}⊕k_0⊕k_1$, $c_2=p_9⊕k_7⊕k_2$	(¾)^3

6-jadval natijalariga asoslangan holda chiziqli hujumni amalga oshirish sodda hisoblanadi. Ma’lum ochiq matn $P=p_0p_1p_2..p_{15}$ va unga mos shifrmat $C=c_0c_1c_2..c_{15}$ berilgan bo‘lsin, har bir juftlik uchun inkrement qiymatini quyidagilarga qarab mos ravishda amalga oshirib, ushbu

$c_1⊕p_{10}=0$ *yoki* $c_1⊕p_{10}=1$

tenglik yoki quyidagi tenglama bajariladi:

$c_2⊕p_9=0$ *yoki* $c_2⊕p_9=1$.

Quyida 100 ta tanlab olingan ochiq matnlardan foydalanilganda quyidagi natijalar olingan:

$c_1⊕p_{10}=0$ *– 38* marta bajarildi

$c_1⊕p_{10}=1$ *– 62* marta bajarildi

$c_2⊕p_9=0$ *– 62* marta bajarildi

$c_2⊕p_9=1$ *– 38* marta bajarildi.

Ushbu holatdan, quyidagi xulosaga kelish mumkin. 2.5-tenglamadan kelib chiqib katta 62% li ehtimollikni inobatga olib

$k_0⊕k_1=1$

va 2.6-tenglama katta 62% li ehtimollik bilan quyidagiga teng:

$k_7⊕k_2=0$.

Ushbu misolda haqiqiy kalit

$K = 1010\ 0011\ 0101\ 0110$,

va bundan $k_0⊕k_1=1$ yoki $k_0⊕k_1=0$ osonlik bilan aniqlanadi.

Xuloasa

Yuqoridagi chiziqli kriptoanalizda kalit ma’lumotining ikki bitini tiklash keltirilgan. Butun K kalitni qayta tiklash uchun qolgan noma’lum bitlarni ham to‘liq aniqlash kerak. Bu taxminan 2^{13} ta shifrlashni bajarish va chiziqli kriptoanalizni amalga oshirishni talab qiladi. Bu hujum juda

muhim ahamiyatga ega bo‘lmasa ham samarali hujum hisoblanadi. Shuning uchun qilingan tahlil TDES algoritmining xavfsiz algoritm emasligini ko‘rsatadi.

Adabiyotlar/Литература/References:

1. Aliqulov B. M. «Korrelyatsion matritsalar va ularning simmetrik shifrlash algoritmlari kriptobardoshligini baholashdagi qo‘llanilishi»: Axborot xavfsizligi yo‘nalishi bo‘yicha magistr darajasidagi dissertatsiya ishi. Toshkent, 2010. 116 b.
2. Бабенко Л.К. и др.Современные алгоритмы блочного шифрования и методы анализа.-М., “Гелиос АРВ”, 2006.-376с.
3. Дарахвелидзе П.Г., Марков Е.П. Delphi – среда визуального программирования: СПб.: BHV – Санкт-Петербург, 1996. 352 с.
4. Жуков А.Е. Нелинейность булевых функций: Курс лекций. – М., МГТУ, 2006 г.
5. Зензин О.С., Иванов М. А. «Стандарт криптографической защиты – AES». "КУДИЦ-ОБРАЗ", Москва – 2002г.
6. Imomov E. M. «Simmetrik blokli shifrlash algoritmlari kriptografik akslantirishlarning matematik xossalari tahlili»: Axborot xavfsizligi yo‘nalishi bo‘yicha magistr darajasidagi dissertatsiya ishi. Toshkent, 2008. 103 b.

O‘ZBEKISTON — 2030: INNOVATSIYA, FAN VA TA’LIM ISTIQBOLLARI

I RESPUBLIKA ILMIY-AMALIY KONFERENSIYASI MATERIALLARI

2025-yil, 23-iyun

Mas’ul muharrir: *F.T.Isanova*
Texnik muharrir: *N.Bahodirova*
Diszayner: *I.Abdihakimov*

O‘ZBEKISTON — 2030: INNOVATSIYA, FAN VA TA’LIM ISTIQBOLLARI. *II Respublika ilmiy-amaliy konferensiyasi materiallari.* – Toshkent: Scienceproblems team, 2025. – 138 bet.

Elektron nashr: https://konferensiyalar.uz/uzbekistan-2030

Konferensiya tashkilotchisi: Scienceproblems Team

Konferensiya o‘tkazilgan sana: 2025-yil, 23-iyun

ISBN 978-9910-09-204-6