XAOTIK AKSLANTIRISHLARGA ASOSLANGAN S JADVALLARNI HOSIL QILISH ALGORITMI

Xudoykulov Zarifjon Turakulovich

TATU, “Kriptologiya” kafedrasi dotsenti, E-mail: zarif.khudoykulov@tuit.uz

K E Y W O R D S

xaotik akslantirish, S jadval, umumiy kriptografik talablar, bifrukatsiya diagrammasi, Lyapunov ko‘rsatkichi (LE), hisoblash imkoniyati cheklangan blokli shifrlash algoritmlari (Lightweight block ciphers).

A B S T R A C T

Mazkur maqolada sinus va tent xaotik akslantirishlaridan birgalikda foydalanish orqali hosil qilingan akslantirish yordamida S jadvallarni hosil qilish algoritmi taklif etilgan. Hosil qilingan xaotik akslantirishning bifrukatsiya diagrammasi va LE ko‘rsatkichi bo‘yicha tahlil natijasi uni kriptografik akslantirishlarni hosil qilishda yetarligini ko‘rsatdi. Taklif etilgan algoritm asosida 4, 5 va 8 bitli S jadvallar hosil qilinib, umumiy kriptografik talablarga baholandi. Baholash natijalari hosil qilingan S jadvallarni amaldagi mavjudlaridan qolishmasligini va ulardan amaldagi kriptografik shifrlash algoritmlarida foydalanish mumkinligini ko‘rsatdi.

1. Kirish

O‘rniga qo‘yish jadvallari (Substitution boxes, S-boxs) simmetrik blokli shifrlardagi yagona chiziqsiz akslantirish bo‘lib, Klod Shennon tomonidan taklif etilgan akslantirishlarni qurishning ikki tamoilidan bir bo‘lgan tarqalishni (confusion) ta’minlaydi [1]. S jadvallarni hosil qilishnining ko‘plab usullari mavjud. Amalda algebraik konstruksiyaga [11] asoslangan S jadvallardan keng foydalanilsada [10], u algebraik kriptotahlilga nisbatan zaiflikka ega [12, 13]. Kriptografik bardoshli S jadvallarni hosil qilish juda katta hisoblash murakkabligini keltirib chiqaradi. Masalan, 8 bitli kirish va chiqish qiymatli S jadvalning barcha mumkin bo‘lgan variantlari soni 256! ga teng. Bu esa to‘liq tanlash usulini qo‘llashni amalda mumkin emasligini ko‘rsatadi. Shu sababli amalda S jadvallarni qurishning yevristik yondoshuvidan foydalanishni taqqazo etadi. Xususan, imitatsiyani yumshatish (simulated annealing) yondashuviga [14, 15], genetik algoritmlarga [16, 17, 18, 19], xaotik akslantirishga (chaotic map) [7, 8, 20] asoslangan S jadvalni hosil qilish usullari amalda keng qo‘llanilib kelinmoqda.

Ushbu maqolada hisoblash imkoniyati cheklangan blokli shifrlash algoritmlari (Lightweight block ciphers) uchun xaotik akslantirishga asoslangan S jadvallarni qurish usuli bilan yaqindan tanishib chiqiladi.

2. Mavjud ishlar tahlili

2.1. Xaotik akslantirish

Xaotik tizim fizika fani sohasiga ko‘ra boshlang‘ich sharoitlarga juda sezgir bo‘lgan fizik tizimlarga nisbatan ishlatilib, aslida esa xaotiklik tushunchasi mutloq tartibsizlikni anglatadi [21]. Xaotik tizimlar kirish qiymati va chiqish o‘rtasida bevosita aloqadorlik bo‘lmagani bois chiziqsiz dinamik tizimlar deb ham ataladi [22]. Xaotik akslantirishlardan nafaqat fizika, matematika sohasida, balki, kriptografiya sohasida keng qo‘llaniladi. Xususan, psevdotasodifiy, tasodifiy sonlar generatorini, rasm va ovozni shifrlashda va simmetrik blokli shifrlar uchun S chiziqsiz akslantirishini qurishda keng ishlatiladi [23].

Umumiy holda xaotik jarayonlar diskret xaotik akslantirish (discrete chaotic map) va uzluksiz tizimlarga (continuous system) ajratiladi. Takrorlanuvchi formulalar yordamida hosil qilingan tizimlar diskret vaqtli tizimlarga tegishli bo‘lib, ular xaotik akslantirishlar sifatida belgilanadi. Ushbu akslantirishlar bir o‘lchamli va ko‘p o‘lchamli sinflarga ajratiladi. Ikkinchi tur, ya’ni, differensial tenglamalar bilan boshqariladigan tizimlar uzluksiz vaqtli dinamik tizim deb ataladi va ular uch va undan yuqori o‘lchamlarga xos bo‘lgan xaotik tizim deb

©Xudoykulov Zarifjon Turakulovich

ataladi [21]. [21] manbada xaotik akslantirish va tizimlar haqida to‘liq ma’lumotlar aks ettirilgan.

Amalda akslantirish va tizimlarni xaotiklik darajasini aniqlash uchun qator usullardan foydalanib, ular orasida bifurkatsiya diagramma (Bifurcation Diagram) va Lyapunov ko‘rsatkichidan (Lyapunov Exponent, LE) keng qo‘llaniladi [21].

Bifurkatsiya diagrammasi – parametr o‘zgarishi bilan dinamik tizimning sifat harakati qanday o‘zgarishini ko‘rsatadigan vizual tasvirdir. Bu chiziqsiz dinamikani va xaos nazariyasini o‘rganishda muhim vosita hisoblanib, u tizimning bir turdagi holatidan ikkichisiga o‘tish nuqtalarini ko‘rsatadi va u tizimning barqarorligi va mumkin bo‘lgan xaotik tabiati haqida tushuncha beradi.

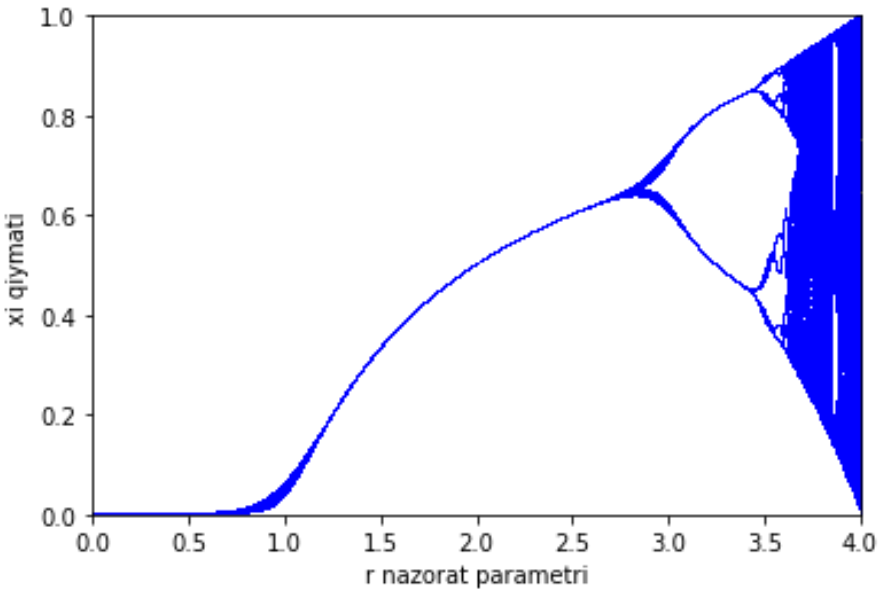
Bifurkatsiya diagrammasi parametr qiymatlarini tizimning mumkin bo‘lgan barqaror holatlariga nisbatan ifodalab, parametr o‘zgarishi bilan tizimning holati o‘zgarishini ko‘rsatuvchi bifurkatsiyalar (bo‘linishlar) qayerda sodir bo‘lishini ko‘rsatadi. Ushbu o‘zgarishlar barqaror fiksirlangan nuqtalardan davriy sikllarga, kvazdavrli sikllarga yoki haotik xatta harakatlarga o‘tishini o‘z ichiga olishi mumkin.

Masalan, logistik akslantirish (Logistic map) deb ataluvchi xaotik akslantirish quyidagicha ifodalanadi:

$$x_{n+1} = r x_n (1 - x_n)$$

bu yerda, r – nazorat parametri, x_n – esa n-marta hosil qilingan qiymat.

Logistik akslantirish uchun bifurksiya diagrammasi 1-rasmda keltirilgan. Tasvirdan ko‘ringani kabi taxminan nazorat qiymatining 3.57 dan keyingi qiymatlari uchun tizim xaotiklik xususiyatiga ega bo‘ladi.



1-rasm. Logistik akslantirish uchun bifurksiya diagrammasi

Lyapunov ko‘rsatkichi dinamik tizimda cheksiz yaqin trayektoriyalarning ajralish tezligini tavsiflovchi kattalik bo‘lib, u xaos nazariyasini o‘rganishda asosiy tushunchalardan biri hisoblanadi. LE tizimdagi xaosning mavjudligini va darajasini aniqlash uchun ishlatilib, boshlang‘ich sharoitdagi kichik farqlar vaqt o‘tishi bilan eksponent ravishda ajralib chiqadigan trayektoriyalarga olib kelishini anglatgan holda ijobiy LE ko‘rsatkichi odatda xaotik xatti harakatni ko‘rsatadi.

LE ko‘rsatkichi dinamik tizimning boshlang‘ich shartlardagi o‘zgarishlarga sezgirligi va oldindan bashorat qilinishini o‘lchovi sifatida ishlatiladi. U $\Delta R_0 = \|X_0 - Y_0\|_2$ boshlang‘ich masofa bilan ajratilgan ikkita X_t va Y_t vaqt ketma-ketligining yaqin nuqtasini ajratish yoki yaqinlashishning o‘rtacha logarifmik tezligi sifatida sonli hisoblanadi. LE

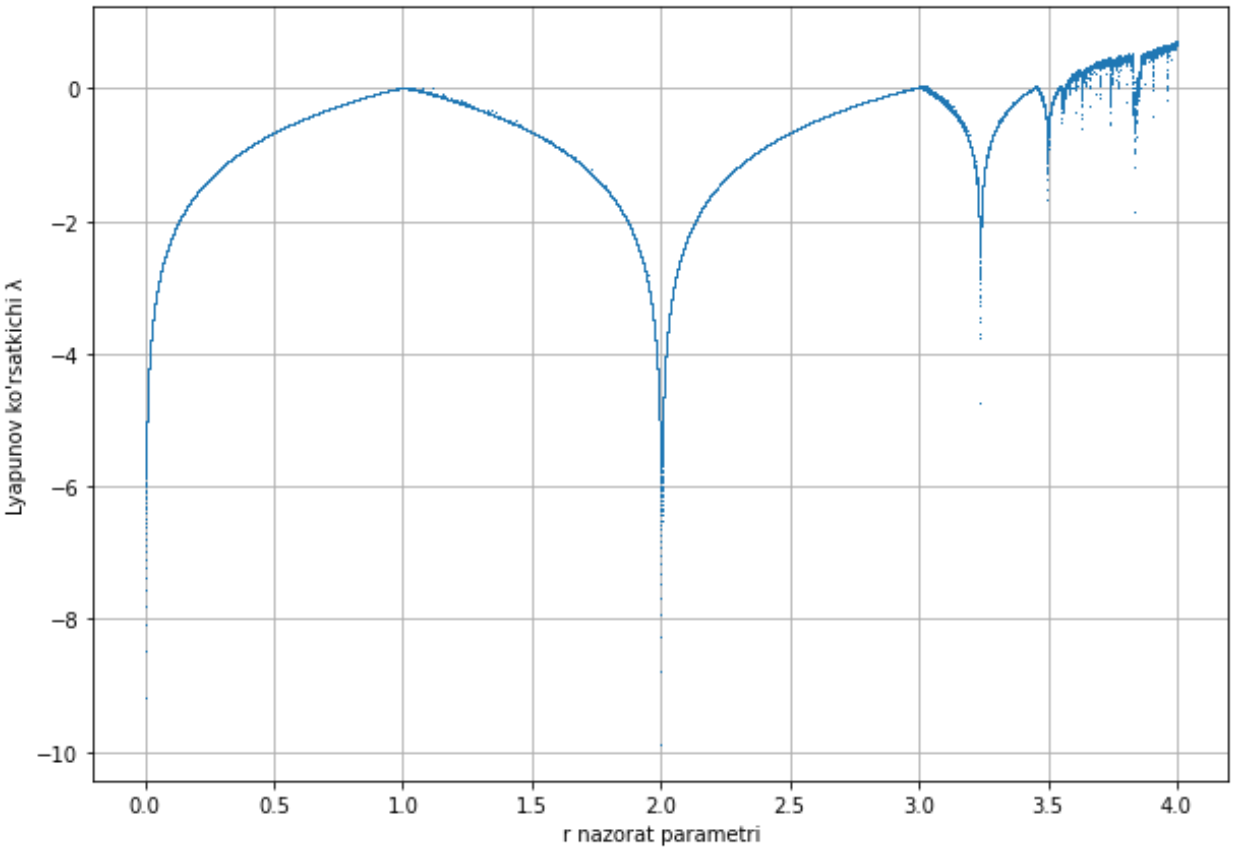
©Xudoykulov Zarifjon Turakulovich

ko‘rsatkichi quyidagi tenglik yordamida ifodalanadi:

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \ln \left| \frac{\Delta R_i}{\Delta R_0} \right|$$

bu yerda, λ – LE ko‘rsatkichi. n o‘lchamli dinamik tizim n ta LE ko‘rsatkichiga ega.

Logistik akslantirish uchun LE ning ko‘rinishi 2-rasmda keltirilgan. Ushbu tasvirdan ham 1-rasmda keltirilgani kabi nazorat parametrining 3.57 dan katta qiymatlari uchun LE ni 0 dan kattaligini ko‘rish mumkin.



2-rasm. Logistik akslantirish uchun LE qiymatlari

2.2. Xaotik akslantirishga asoslangan S jadvallarni qurish usullari

Xaotik akslantirishlardan yuqorida aytib o‘tilganidek, tasodifiy/ psevdotasodifiy sonlar generatorlarini, chiziqsiz S akslantirishlarini hosil qilishda keng qo‘llaniladi. Ushbu bo‘limda aynan chiziqli S akslantirishlarni hosil qilishda xaotik akslantirishlardan foydalanishga oid amalga oshirilgan ishlar bilan tanishib chiqiladi. Xaotik akslantirishga asoslangan ko‘plab S jadvallarni hosil qilish usullari mavjud bo‘lib, ular haqidagi umumiy ma’lumotlar 1-jadvalda keltiriladi.

1-jadval

Xaotik akslantirishlar asosida hosil qilingan S jadvallar tahlili

№	Manba	Xaotik akslantirish usuli	O‘lchami	Asosiy omillar					DPA hujumiga qarshi omillar			Qo‘shimcha		
				NL	DP	LP	SAC	BIC-SAC	TO	CCV	SNR	FP	OFP	AI
1.	Duong [7]		4x4	4	0.25	0.25	0.500	0.500	**3.400**	1.352	1.612	0	0	2, 21

©Xudoykulov Zarifjon Turakulovich

2.	Duong [7]	Kengaytirilgan logistik va sin akslantirsh	5x5	10	0.187	0.25	0.500	0.500	4.580	1.275	2.085	0	0	2, 24
3.	Thakor [24]	Kengaytirilgan logistik akslantirish	5x5	8.4	0.25	0.25	0.540	0.507	4.596	0.347	3.408	0	1	2, 24
4.	Irfan [25]	Logistik akslantirish	5x5	8.8	0.25	0.25	0.540	0.525	4.532	0.259	3.713	0	0	2, 24
5.	Manzoor [26]	MAZa	8x8	107	0.039	0.125	0.495	0.504	7.825	0.130	9.113	2	1	3, 441
6.	Manzoor [26]	MAZa	8x8	110	0.039	0.132	0.503	0.504	7.818	0.098	9.976	2	1	3, 441
7.	Alqahtani [27]	Giperxaotik	8x8	102.5	0.039	0.132	0.505	0.502	7.807	0.124	9.306	1	2	3, 441

Bundan tashqari, amalda keng qo‘llanilayotgan turli o‘lchamli S jadvallar va ularning umumiy kriptografik talablarga nisbatan baholash natijalari 2-jadvalda keltirilgan.

2-jadval

Amalda keng qo‘llaniladigan S jadvallar tahlili

№	**Manba**	**O‘lchami**	**Asosiy omillar**					**DPA hujumiga qarshi omillar**			**Qo‘shimcha**		
			NL	DP	LP	SAC	BIC-SAC	TO	CCV	SNR	FP	OFP	AI
1.	PRESENT	4x4	4	0.25	0.25	0.625	0.562	3.600	0.657	2.128	0	1	2, 21
2.	FEATHER	4x4	4	0.375	0.25	0.562	0.531	3.533	0.457	2.398	1	0	2, 21
3.	ARSHAD (8)	4x4	4	0.375	0.25	0.5	0.520	3.666	0.382	2.529	0	4	2, 21
4.	IVLBC	4x4	4	0.25	0.25	0.546	0.531	3.666	0.257	2.806	4	0	2, 21
5.	DBST (1)	4x4	4	0.25	0.25	0.640	0.468	3.600	0.307	2.685	1	0	2, 21
6.	ELEPHANT	4x4	4	0.25	0.25	0.656	0.520	3.266	0.457	2.398	0	1	2, 21
7.	GIFT	4x4	4	0.375	0.25	0.625	0.541	3.600	0.457	2.398	0	1	2, 21
8.	KNOT	4x4	4	0.25	0.25	0.671	0.479	3.333	0.607	2.187	0	2	2, 21
9.	PYJAMASK	4x4	4	0.25	0.25	0.593	0.520	3.466	0.607	2.187	0	2	2, 21
10.	SATURNIN	4x4	4	0.25	0.25	0.531	0.500	3.533	0.357	2.578	1	0	2, 21
11.	SPOOK	4x4	4	0.25	0.25	0.515	0.562	3.666	0.307	2.685	1	2	2, 21
12.	KLEIN	4x4	4	0.25	0.25	0.593	0.500	3.466	1.207	1.691	0	0	2, 21
13.	RECTANGLE	4x4	4	0.25	0.25	0.671	0.479	3.400	0.607	2.187	0	0	2, 21
14.	PRIDE	4x4	4	0.25	0.25	0.500	0.541	3.533	0.307	2.685	4	0	2, 21
15.	CRAFT	4x4	4	0.25	0.25	0.406	0.562	3.466	1.257	1.663	4	2	2, 21
16.	ASCON	5x5	8	0.25	0.25	0.619	0.520	4.322	0.501	3.015	0	0	2, 25
17.	PRIMATE	5x5	12	0.062	0.125	0.540	0.510	4.838	0.308	3.535	0	2	2, 25
18.	ICEPOLE	5x5	8	0.25	0.25	0.425	0.550	4.516	0.190	4.025	0	2	2, 24
19.	SYCON	5x5	8	0.25	0.25	0.620	0.520	**4.258**	0.501	3.015	0	0	2, 25
20.	ABDURAZZOKOV [19]	8x8	105	0.039	0.132	0.494	0.497	7.801	0.118	9.408	0	1	3, 441
21.	AES	8x8	112	0.015	0.062	0.504	0.504	7.860	0.111	9.599	0	0	2, 39
22.	KUZNECHIK	8x8	106.5	0.031	0.109	0.512	0.494	7.835	0.112	9.570	0	0	3, 441

©Xudoykulov Zarifjon Turakulovich

3. Kriptografik bardoshli S jadvallarning xususiyatlari

3.1. Balanslashganlik va regulyarlik xossalari

Ta'rif. Agar $f(x),\ x \in GF(2^n)$ – bul funksiyaning chinlik jadvalida 0 va 1 lar soni teng bo'lsa, u holda $f(x)$ funksiya *balanslashgan* deyiladi, ya'ni, $\#\{x|f(x)=0\} = \#\{x|f(x)=1\} = 2^{n-1}$ [2].

Balanslashganlik qiymati **Ha** yoki Yo'q qiymatga ega.

Ta'rif. Agar $Y = \varphi(X): GF(2^n) \to GF(2^m)$ akslantirish chiqishida uning barcha (2^m ta) chiquvchi qiymatlari 2^{n-m} tadan takrorlansa, u holda Y akslantirish *regulyar* deyiladi [2].

Regulyarlik qiymati **Ha** yoki Yo'q qiymatga ega bo'lib, blokli shifrlarni differensial kriptotahlil usuliga, oqimli shifrlarni statistik kriptotahlil usullariga bardoshligini ta'minlashdagi muhim omil hisoblanadi.

3.2. Chiziqsizlik

Ta'rif. $f(x), x \in GF(2^n)$ – funksiyaning chiziqsizligi deb quyidagi tenglik bilan aniqlanuvchi qiymatga aytiladi [2]:

$$N(f) = 2^{n-1} - \frac{1}{2} \cdot \max_{\forall \alpha \in GF(2^n)} \left|\widehat{U}_\alpha(f)\right|$$

Bu yerda, $\widehat{U}_\alpha(f)$ - Uolsh-Adamar almashtirishi deb ataladi.

Ta'rif. $f(x), x \in GF(2^n)$ – funksiyaning chiziqliligi deb quyidagi tenglik bilan aniqlanuvchi qiymatga aytiladi:

$$L(f) = 1 - \frac{1}{2^{n-1}} N(f)$$

Ta'rif. $Y = \varphi(X): GF(2^n) \to GF(2^m)$ akslantirishning chiziqsizligi deb quyidagi tenglik bilan aniqlanuvchi qiymatga aytiladi:

$$N\big(\varphi(X)\big) = \min_{c \in GF(2^m), c \neq 0} N < c, \varphi >$$

Bu yerda, $\varphi = \{f_1, f_2, \cdots, f_m\}$, $c = \{c_1, c_2, \cdots, c_m\}$, $< c, \varphi >= c_1 f_1(x) + c_2 f_3(x) + \cdots + c_m f_m(x)$ – skalyar ko'paytma natijasidagi bul funksiya.

$N(f)$ va $N\big(\varphi(X)\big)$ kattaliklar uchun qiymatning **kattasi** yaxshi bo'lib, ushbu xususiyat akslantirishning blokli shifrlarni chiziqli kriptotahlil usuliga, oqimli shifrlarni korrelyatsion hujumga bardoshligini ta'minlovchi muhim omil hisoblanadi.

3.3. Qat'iy lavin samaradorlik va tarqalish mezoni

Aytaylik, $\Delta f(x, \beta) = f(x) \oplus f(x \oplus \beta)$, $x, \beta \in GF(2^n)$, $f(x) \in GF(2)$ o'rinli bo'lsin.

Ta'rif. Agar Xemming og'irligi $1 \leq Wt(\beta) \leq e$ oraliqda bo'lgan barcha $\beta \in GF(2^n)$ vektorlar uchun $\Delta f(x, \beta)$ funksiya balanslashgan bo'lsa, $f(x), x \in GF(2^n)$ – bul funksiya e darajali *tarqalish mezoniga (Propagation Criteria, PC)* ega deyiladi [2].

Kattalikning **yuqori** qiymati yaxshi hisoblanadi.

Ta'rif. Agar $Wt(\beta) = 1$ bo'lgan barcha β vektorlar uchun $\Delta f(x, \beta)$ balanslashgan bul funksiya bo'lsa (ya'ni, $PC(1)$), u holda $f(x), x \in GF(2^n)$ – bul funksiya *qat'iy lavin samaradorlik darajasiga (Strict Avalanche Criterion, SAC)* ega deyiladi.

Ta'rif. Agar $f(x)$ bul funksiyaning ixtiyoriy k ta $x_1, x_2, \cdots, x_k$ argumentlarini fiksirlashdan (0 yoki 1 qiymat bilan almashtirishdan) hosil bo'lgan $f(x)$ funksiya qat'iy lavin samaradorlik darajasiga ega bo'lsa, $f(x), x \in GF(2^n)$ – bul funksiya k tartibli qat'iy lavin samaradorlikka ega deyiladi ($SAC(k)$ kabi belgilanadi, $0 \leq k \leq n-2$ o'rinli).

Ushbu kattalikning ham yuqori qiymati yaxshi hisoblanib, algoritmni chiziqli kriptotahlil usuliga bardoshligini ta'minlashdagi muhim omil hisoblanadi.

©Xudoykulov Zarifjon Turakulovich

3.4. Chiquvchi bitlar bog'liqsizligi mezoni

Ta'rif. Agar ixtiyoriy $i, j, k \in \{1,2,3,\cdots,n\}$, $j \neq k$ qiymatlar uchun $Y = \varphi(x): GF(2^n) \to GF(2^n)$ akslantirishga kiruvchi i-bitni inversiyalash (teskarilash) akslantirishidan chiquvchi j- va k-bitlarning o'zaro bog'liqsiz tarzda o'zgarishini taqazo etsa, $Y = \varphi(x)$ akslantirish *bitlar bog'liqsizligi mezonini* qanoatlantiradi deyiladi [2].

Akslantirishdan chiquvchi ikkita bit bog'liqsizligini aniqlash uchun chiquvchi vektorning $j-$ va $k-$ komponentlari o'rtasidagi korrelyatsiya koeffitsiyenti $BIC(a_j, a_k)$ dan foydalaniladi:

$$BIC(a_j, a_k) = \max_{1 \le i \le n} \left| corr(a_j^{ei}, a_k^{ei}) \right|.$$

Bu yerda, $A^{ei} = \varphi(x) \oplus \varphi(x \oplus ei) = [a_1^{ei}, a_2^{ei}, a_3^{ei}, \cdots, a_n^{ei}]$, $corr(x,y) = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i-\bar{x})^2}\sqrt{\sum_{i=1}^{n}(y_i-\bar{y})^2}}$, $x,\ y,\ ei \in GF(2^n)$, ei – kattalik i – biti 1 ga teng qolgan barcha bitlari 0 ga teng bo'lgan vektor.

Umumiy holda, $Y = \varphi(x)$ – funksiya uchun BIC parametr qiymati quyidagicha aniqlanadi [2]:

$$BIC = \max_{1 \le j,k \le n, j \neq k} BIC(a_j, a_k).$$

Ushbu parametr uchun $0 \le BIC \le 1$ – o'rinli bo'lib, aynan ushbu qiymat $Y = \varphi(x)$ – funksiyani bitlar bog'liqsizligi mezonini qanchalik qanoatlantirishini ko'rsatadi. Ya'ni, agar $BIC = 0$ bo'lsa, chiquvchi bitlar maksimal bog'liqsizlikka ega va aksincha agar $BIC = 1$ bo'lsa, minimal bog'liqlikka ega deyish mumkin.

Ushbu parametrning kichik qiymati yaxshi bo'lib, ushbu kattalik shifrlash algoritmini statistik kriptotahlil usullariga bardoshligini ta'minlashda muhim ahamiyat kasb yetadi.

$Y = \varphi(x)$ akslantirish *bitlar bog'liqsizligi mezonini* qanoatlantirishi uchun yuqori chiziqsizlik darajasi va SAC talabini qanoatlantirishi kerak. Demak, BIC me'zonini baholash chiqish funksiyalarida XOR amali orqali hosil qilingan funksiyalarning chiziqli emasligini (BIC-NL) va SAC (BIC-SAC) ni qanoatlantirishini hisobga olgan holda amalga oshirilishi kerak. Boshqacha aytganda, BIC qiymatini hisoblash chiziqsizlik va SAC me'zonlarini birlashtiradi [7, 8].

3.5. Korrelyatsion immunitetlik darajasi

Ta'rif. Agar $1 \le Wt(\alpha) \le k$ $(1 \le k \le n)$ shartni qanoatlantiruvchi barcha $\alpha \in GF(2^n)$ vektorlar uchun $\widehat{U}_\alpha(f) = 0$ tenglik o'rinli bo'lsa, $f(x), x \in GF(2^n)$ – bul funksiya k darajali korrelyatsion immunitetga ega deyiladi va $CI(k)$ kabi belgilanadi.

Demak, berilgan $f(x)$ – bul funksiyaning korrelyatsion immunitetlik darajasi k ga teng bo'lsa, u holda $Y = f(x)$ funksiya qiymati ixtiyoriy $x \in GF(2^n)$ argumentning k ta komponentida statistik bog'liqsiz hisoblanadi.

k darajaning qiymati qanchalik **katta** bo'lsa, algoritm korrelyatsion hujumlarga shuncha yuqori bardoshli bo'ladi.

3.6. Algebraik immunitet

Ta'rif. $f(x), x \in GF(2^n)$ – bul funksiyaning algebraik chiziqsizlik darajasi (deg (f)) deb uning ANF tarkibidagi birhadning eng yuqori darajasiga aytiladi.

Kattalikning **yuqori** qiymati talab etiladi.

Ta'rif. Aytaylik, biror $Y = \varphi(x): GF(2^n) \to GF(2^m)$ akslantirishni qanoatlantiruvchi bul tenglamalar sistemasi quyidagicha bo'lsin:

$$G = \begin{cases} g_1(x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_m) = 0; \\ g_2(x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_m) = 0; \\ g_3(x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_m) = 0; \\ \cdots \\ g_r(x_1, x_2, \cdots, x_n, y_1, y_2, \cdots, y_m) = 0. \end{cases}$$

$Y = \varphi(x)$ – funksiyaning *Algebraik immuniteti (AI(Y))* deb, yuqoridagi tenglamalar sistemasidagi minimal chiziqsizlik darajasiga aytiladi.

Kattalikning **yuqori** qiymati talab etilib, algoritmlarning algebraik kriptotahlil usuliga

(cc) BY ©Xudoykulov Zarifjon Turakulovich

bardoshligini ta'minlashdagi muhim omil hisoblanadi. Bundan tashqari, tenglamalar soni r ni ham yuqori qiymati yaxshi hisoblanadi.

3.7. Differensial quvvat tahlili (Differential power analysis, DPA) hujumiga qarshi turish qobiliyatini ko'rsatuvchi omillar

Ta'rif. Berilgan $F: GF(2^n) \to GF(2^m)$ akslantirish $TO(F)$ *shaffoflik chegarasi* (Transparency order, TO) deb quyidagi tenglik bilan ifodalanuvchi kattalikka aytiladi:

$$TO(F) = \max_{\beta \in F_2^m} \left(|m - 2H(\beta)| - \frac{1}{2^{2n} - 2^n} \sum_{a \in F_2^{n*}} \left| \sum_{\substack{v \in F_2^m \\ H(v)=1}} (-1)^{v \cdot \beta} W_{D_a F}(0, v) \right| \right)$$

Berilgan $\varphi(x): GF(2^n) \to GF(2^m)$ akslantirish $TO(\varphi(x))$ chegara qiymati uchun $0 \le TO \le m$ o'rinli. Ushbu qiymatning kichigi yaxshi.

TO kattaligi Prouff tomonidan [3] taklif etilgan bo'lib, keyinchalik Li va boshqalar tomonidan [4] ushbu tenglikdagi kamchiliklar aniqlangan. Aniqlangan kamchiliklarni o'zida tuzatilgan RTO (Revisited TO) ko'rinishi taklif etilgan bo'lib, uning ko'rinishin quyidagicha:

$$RTO(F) = \max_{\beta \in F_2^m} \left(m - \frac{1}{2^{2n} - 2^n} \sum_{a \in F_2^{n*}} \left| \sum_{j=1}^{m} \sum_{i=1}^{m} (-1)^{\beta_i \oplus \beta_j} \mathcal{C}_{F_i, F_j}(a) \right| \right)$$

Bu yerda, $\mathcal{C}_{F_i,F_j}$ – ikkita bul funksiyasi o'rtasidagi *o'zaro bog'liqlik spektri (cross-correlation spectrum)* bo'lib, har bir $u \in F_2^n$ uchun $\mathcal{C}_{f_1,f_2}(u) = \sum_{x \in F_2^n} (-1)^{f_1(x) \oplus f_2(x \oplus u)}$ tenglik bilan ifodalanadi.

Ta'rif. $F: GF(2^n) \to GF(2^m)$ akslantirishning DPA signal shovqin nisbati (Signal-to-Noise Ratio, SNR) deb $SNR(DPA)(F)$ kabi belgilanuvchi quyidagi tenglikka aytiladi [5]:

$$SNR(DPA)(F) = n * 2^{2n} \left(\sum_{a \in F_2^n} \left(\sum_{i=0}^{n} \widehat{U}_a(f_i) \right)^4 \right)^{-\frac{1}{2}}.$$

Ushbu kattalikning kichik qiymati yaxshi bo'lib, umumiy holda balanslashgan akslantirish uchun $1 \le SNR(DPA)(F) \le 2^{n/2}$ tengsizlik o'rinli.

Ta'rif. $k_i,\ k_j \in F_2^n$ kalitlar berilgan bo'lsin. (k_i, k_j) uchun chalkashish koeffitsiyenti (Confusion coefficient, SS) κ deb quyidagi tenglik bilan ifodalanuvchi kattalikka aytiladi [6]:

$$\kappa = \kappa(k_i, k_j) = \Pr\left[(\psi|k_i) \neq \left(\psi\middle|k_j\right)\right] = \frac{N_{(\psi|k_i) \neq (\psi|k_j)}}{N_t}.$$

Bu yerda, N_t – tegishli shifmatr bitlari uchun umumiy qiymatlar soni, $N_{(\psi|k_i) \neq \left(\psi\middle|k_j\right)}$ – esa ψ qiymatlarida turli faraz qilingan k_i va k_j natijalarining paydo bo'lish sonini ko'rsatadi.

CC qiymati uchun $0 \le \kappa < 1$ tenglik o'rinli bo'lib, kichik qiymat akslantirishni DPA hujumiga bardoshli qiladi.

Ta'rif. $F: GF(2^n) \to GF(2^m)$ akslantirishning chalkashish koeffitsiyenti dispersiyasi (Confusion coefficient variance, CCV) deb $k_i,\ k_j,\ k_i \neq k_j$ juftliklar uchun quyidagi tenglik bilan hisoblanuvchi kattalikka aytiladi:

$$\mathrm{CCV}(F) = Var(\mathrm{E}[(H\left(F(k_i \oplus p)\right) - H(F(k_j \oplus p)))^2]).$$

Bu yerda, E – o'rtacha qiymatni hisoblash funksiyasi, Var – dispersiyani hisoblash funksiyasi va p – ochiq matn, H – Xemming og'irligi.

Ushbu qiymatning kattasi yaxshi bo'lib, akslantirishni DPA hujumiga bardoshli qiladi.

3.8. DP (Differential Approximation Probability, differensial yaqinlashish ehtimoli) va LP (Linear Approximation Probability, chiziqli yaqinlashish ehtimoli)

(cc) BY ©Xudoykulov Zarifjon Turakulovich

Ta'rif. Berilgan $S: GF(2^n) \to GF(2^m)$ akslantirishning differensial yaqinlashish ehtimoli deb differensial tenglik (Differential Uniformity) uchun o'lchov bo'lgan quyidagi ifodaga aytiladi:

$$DP(\Delta x \to \Delta y) = \frac{\#\{x \in X | S(x) \oplus S(x \oplus \Delta x) = \Delta y\}}{2^n}$$

bu yerda, n – kiruvchi bit uzunligini, X – kiruvchi qiymatni va # - elementlar sonini ifodalaydi.

Ta'rif. Chiziqli yaqinlashish ehtimoli $S: GF(2^n) \to GF(2^m)$ akslantirishning ma'lum bir bitlar ketma-ketligiga nisbatan kirish va chiqishlari o'rtasidagi chiziqli bog'lanish ehtimolini o'lchaydi hamda quyidagi tenglik bilan ifodalanadi:

$$LP = \max_{\Delta x, \Delta y \neq 0} \{\frac{\#\{x \in X | x \cdot \Delta x = S(x) \cdot \Delta y\}}{2^n} - \frac{1}{2}\}$$

DP va LP qiymatlarning kichik qiymatlari yaxshi bo'lib, mos holda differensial va chiziqli kriptotahlil usullariga bardoshlik darajasini ko'rsatadi.

4. Xaotik akslantirishga asoslangan S jadvallarni qurish usuli

4.1. Taklif etilgan xaotik akslantirish

Ushbu bo'limda xaotik akslantirishlar orqali S jadvalni hosil qilish usuli bilan tanishib chiqiladi. Taklif etilayotgan xaotik akslantirish takomillashtirilgan sinus (Enhanced Sine map) va tent (Enhanced Tent map) akslantirishidan tashkil topgan. Ushbu akslantirishlarning alohida ifodalanishlari quyida keltirilgan.

Takomillashtirilgan sinus akslantirish quyidagicha ifodalanadi:

$$x_{i+1} = \sin(a\pi \sin(\pi x_i))$$

bu yerda, a nazorat parametri va $a \in (0, +\infty)$ o'rinli.

Tent akslantirish quyidagicha ifodalanadi:

$$x_{i+1} = \begin{cases} \sin(\pi a x_i) & x_i < 0.5 \\ \sin(\pi a(1 - x_i)) & x_i \geq 0.5 \end{cases}$$

bu yerda, a nazorat parametri va $a \in (0, +\infty)$ o'rinli.

Yuqoridagi ikki akslantirishni mujassamlashtirish orqali quyidagi xaotik akslantirishni olish mumkin. Ushbu tenglikda x_i kattaligi qiymatlari $[-2, 2]$ oraliqda yotadi.

$$x_{i+1} = f(x_i, a) = \begin{cases} \sin(a\pi \sin(\pi x_i)) + \sin(\pi a x_i) & x_i < 0.5 \\ \sin(a\pi \sin(\pi x_i)) + \sin(\pi a(1 - x_i)) & x_i \geq 0.5 \end{cases}$$

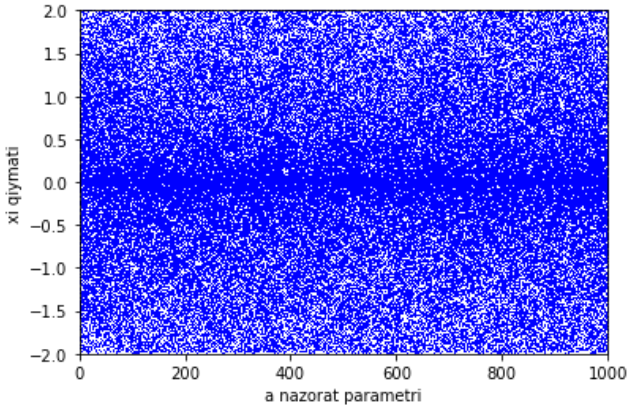
bu yerda, a nazorat parametri va $a \in (0, +\infty)$ o'rinli.

Taklif etilgan xaotik akslantirish uchun LE quyidagi tenglik orqali hisoblanadi:

$$\lambda = \begin{cases} \lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} \ln\left|f_1'(x_i)\right| & x_i < 0.5 \\ \lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} \ln\left|f_2'(x_i)\right| & x_i \geq 0.5 \end{cases}$$

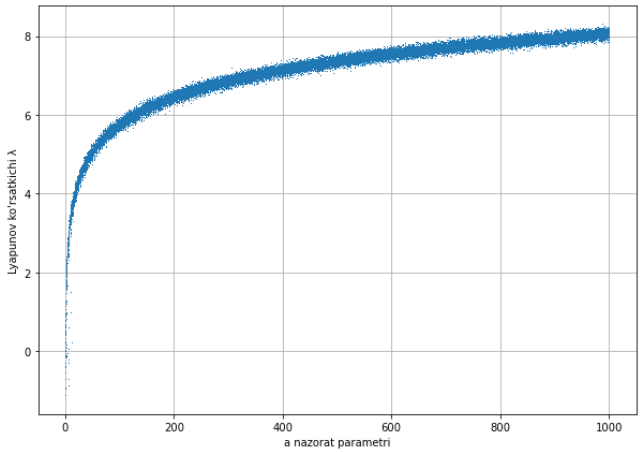
bu yerda, $f_1'(x_i) = a\pi(\pi \cos(\pi x) \cos(\pi \sin(\pi x)) + \cos(\pi a x))$ va $f_2'(x_i) = \pi a(\pi \cos(\pi x) \cos(\pi \sin(\pi x)) - \cos(\pi a(1 - x)))$.

Taklif etilgan xaotik akslantirish uchun bifrukatsiya diagrammasi va LE akslantirishi mos holda 3 va 4 rasmlarda berilgan.



3-rasm. Taklif etilgan xaotik akslantirishning bifrukatsiya diagrammasi

©Xudoykulov Zarifjon Turakulovich



4-rasm. Taklif etilgan xaotik akslantirishning LE ko‘rsatkichi

4.2. Taklif etilgan S jadvalni hosil qilish algoritmi

Taklif etilgan xaotik akslantirishga asosan S jadvalni qurish algoritmi 5-rasmda keltirilgan. Ushbu algoritm xaotik akslantirishdan hosil bo‘lgan qiymatlardan S jadvalni qurishda oldindan belgilangan talablarga nisbatan tekshirishga asoslanadi. Mazkur holatda oldingan tanlab olingan talablar 3-jadvalda keltirilgan.

3-jadval

Algoritm uchun tanlab olingan talablar

O‘lchami	**Asosiy omillar**					**DPA hujumiga qarshi omillar**			**Qo‘shimcha**		
	NL≥	DP≤	LP≤	SAC=	BIC-SAC=	TO≤	CCV≥	SNR≤	FP=	OFP=	AI≥
4x4	4	0.25	0.25	0.500	0.500	3.8	1.0	1.8	0	0	2, 21
5x5	10	0.25	0.25	0.500	0.500	4.7	1.0	3.0	0	0	2, 24
8x8	105	0.04	0.14	≈0.500	≈0.500	7.9	0.1	9.9	0	0	3, 441

3-jadvaldagi talablar 1 va 2 jadvallardagi natijalar asosida shakllantirildi. Hisoblash davomida $\Delta x = 0.0001$ qiymat belgilandi.

Taklif etilgan algoritm asosida Sagemath amaliy dasturlar paketidan foydalanib, dasturiy vosita ishlab chiqildi. Ishlab chiqilgan dasturiy vosita yordamida hosil qilingan S jadvallar quyida keltirilgan.

4 bitli S jadvallar quyida keltirilgan:

S_Box1 = (11, 5, 6, 4, 8, 12, 7, 13, 14, 10, 2, 3, 0, 1, 15, 9);

S_Box2 = (1, 0, 9, 2, 10, 14, 13, 15, 4, 12, 8, 3, 5, 7, 6, 11);

S_Box3 = (11, 6, 15, 14, 8, 1, 12, 3, 0, 4, 2, 5, 10, 9, 13, 7);

S_Box4 = (2, 4, 10, 6, 15, 11, 14, 9, 5, 0, 1, 8, 13, 12, 7, 3);

5 bitli S jadvallar quyida keltirilgan:

S_Box5 = (18, 8, 19, 4, 14, 23, 3, 6, 12, 0, 30, 5, 11, 27, 2, 10, 7, 26, 17, 28, 21, 20, 15, 29, 25, 31, 1, 9, 22, 16, 13, 24);

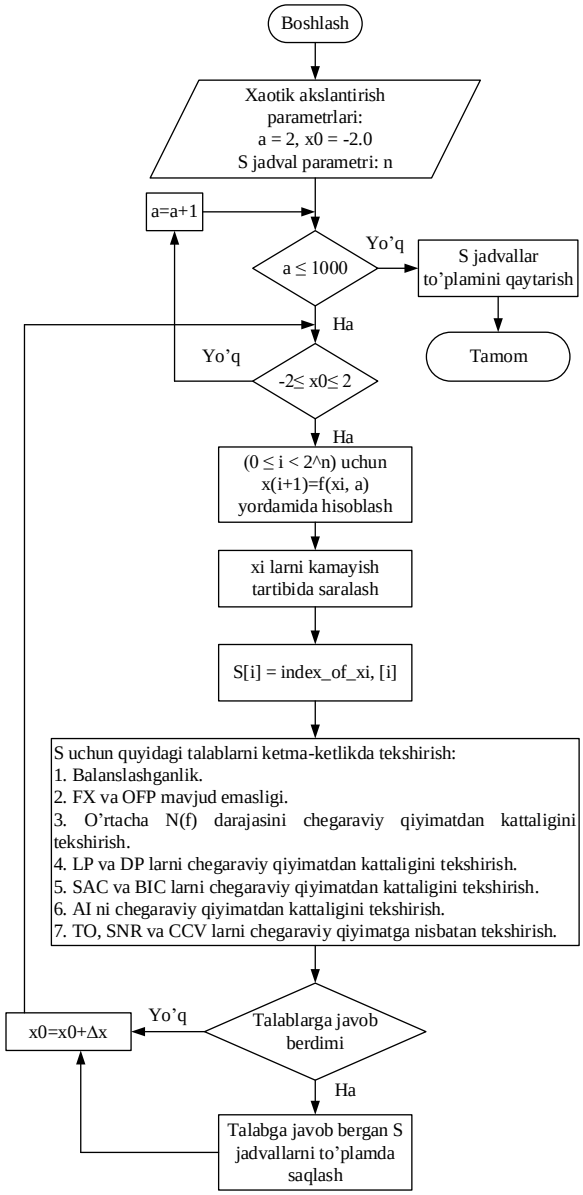
S_Box6 = (6, 4, 24, 9, 16, 30, 26, 28, 11, 27, 18, 3, 7, 22, 10, 20, 14, 15, 8, 21, 25, 31, 5, 17, 1, 2, 13, 29, 0, 12, 19, 23);

4-jadvaldagi 8 bitli 7 tartibli S jadval quyida keltirilgan:

S_Box7 = (63, 74, 152, 13, 174, 137, 211, 20, 113, 72, 40, 216, 249, 79, 97, 10, 104, 170, 200, 187, 139, 222, 60, 128, 120, 99, 192, 181, 122, 48, 252, 88, 90, 25, 168, 59, 121, 77, 125, 15, 167, 0, 21, 85, 254, 11, 126, 6, 209, 247, 49, 235, 204, 159, 169, 65, 143, 245, 33, 54, 45, 108, 232, 22, 202, 46, 116, 7, 212, 37, 184, 194, 155, 177, 179, 146, 61, 84, 55, 70, 30, 123, 42, 138, 220, 98, 44, 17, 196, 133, 234, 253, 127, 23, 189, 107, 215, 214, 51, 64, 119, 67, 71, 38, 188, 111, 240, 151, 14, 182, 142, 251, 76, 145, 164, 228, 52, 56, 81, 110, 241, 153, 8, 217, 244, 31, 100, 242, 96, 5, 183, 158, 134, 243, 39, 231, 29, 246, 43, 26, 229, 103, 141, 236, 62, 80, 87, 225, 224,

(cc) BY ©Xudoykulov Zarifjon Turakulovich

203, 69, 32, 68, 35, 16, 195, 132, 226, 208, 136, 210, 92, 95, 18, 144, 239, 149, 89, 27, 58, 83, 75, 150, 34, 53, 50, 86, 255, 47, 28, 118, 12, 156, 248, 91, 57, 82, 129, 131, 221, 9, 115, 19, 114, 41, 162, 219, 109, 238, 73, 140, 223, 166, 2, 171, 201, 1, 157, 180, 106, 199, 206, 186, 218, 207, 130, 191, 172, 197, 163, 227, 250, 78, 117, 3, 176, 173, 161, 213, 66, 94, 105, 190, 148, 102, 135, 237, 124, 24, 147, 112, 93, 101, 193, 178, 154, 4, 175, 165, 233, 160, 185, 198, 205, 230, 36).



5-rasm. S jadvalni qurish algoritmi

5. S jadvallarning xavfsizlik tahlili

Generatsiyalangan S jadvallarni 3 bo‘limda keltirilgan xavfsizlik talablari bo‘yicha natijalar 4-jadvalda keltirilgan. 4x4 o‘lchamli jadvallar tahlili taklif etilgan barcha S jadvallarning NL, DP, LP, SAC, BIC-SAC, FP, OFP va AI bo‘yicha olingan natijalari Duong [7] va boshqalar tomonidan olingan natijalar bilan bir xil bo‘lgan bo‘lsa, TO tahlili bo‘yicha eng yaxshi natija Duong [7] va boshqalar tomonidan taklif etilgan S jadvalga tegishli bo‘lgan (1-jadvalga qarang). CCV va SNR bo‘yicha olingan natijalar esa 4-jadvalning 3-tartibidagi S jadvalga tegishli bo‘lgan.

4-jadval

Taklif etilgan algoritm yordamida hosil qilingan S jadvallarning tahlil natijalari

№	Parametrlar (a, x_0)	O‘lchami	Asosiy omillar					DPA hujumiga qarshi omillar			Qo‘shimcha		
			NL	DP	LP	SAC	BIC-SAC	TO	CCV	SNR	FP	OFP	AI
1.	$a = 16$	4x4	4	0.25	0.25	0.500	0.500	3.733	1.207	1.691	0	0	2, 21

(cc) BY ©Xudoykulov Zarifjon Turakulovich

	$x_0 = -0.9886$												
2.	$a = 107$ $x_0 = 1.2567$	4x4	4	0.25	0.25	0.500	0.500	3.533	1.182	1.705	0	0	2, 21
3.	$a = 164$ $x_0 = 0.6630$	4x4	4	0.25	0.25	0.500	0.500	3.533	**1.382**	**1.600**	0	0	2, 21
4.	$a = 213$ $x_0 = 1.2706$	4x4	4	0.25	0.25	0.500	0.500	3.666	1.207	1.691	0	0	2, 21
5.	$a = 94$ $x_0 = 1.8526$	5x5	10	0.187	0.25	0.500	0.500	4.645	1.194	2.144	0	0	2, 24
6.	$a = 114$ $x_0 = -1.8890$	5x5	10	0.187	0.25	0.500	0.500	4.661	**1.293**	**2.072**	0	0	2, 24
7.	$a = 13$ $x_0 = 1.2822$	8x8	106.5	0.039	0.125	0.494	0.507	7.799	0.126	9.208	0	0	3, 441
8.	$a = 10$ x_0 =-0.91980	8x8	106.25	0.039	0.132	0.499	0.495	7.814	0.133	9.045	0	0	3, 441
9.	$a = 11$ $x_0 = 1.13139$	8x8	106	0.039	0.132	0.501	0.504	7.809	0.139	8.908	0	0	3, 441
10	$a = 11$ $x_0 = 1.47839$	8x8	105.5	0.039	0.125	0.489	0.504	7.809	0.122	9.300	0	0	3, 441
11	$a = 11$ $x_0 = 1.50509$	8x8	105.25	0.039	0.132	0.499	0.496	7.804	0.180	8.124	0	0	3, 441
12	$a = 11$ x_0 =1.52219	8x8	105.0	0.039	0.125	0.502	0.499	7.811	0.101	9.866	0	0	3, 441

5 bitli S jadval uchun amalga oshirilgan tahlil natijalari hosil qilingan har ikkala jadvalning NL, DP, LP, SAC, BIC-SAC, FP, OFP va AI bo'yicha olingan natijalari Duong [7] va boshqalar tomonidan olingan natijalar bilan bir xil bo'lgan bo'lsa, TO tahlili bo'yicha eng yaxshi natija SYCON va boshqalar tomonidan taklif etilgan S jadvalga tegishli bo'lgan (2-jadvalga qarang). CCV va SNR bo'yicha olingan natijalar esa 4-jadvalning 6-tartibidagi S jadvalga tegishli bo'lgan.

8 bitli S jadvallar tahlili esa taklif etilgan algoritm asosida generatsiyalangan S jadvallarning barchasi kamida 105 chiziqsizlik darajasini qayd etib, qolgan ko'rsatkichlar bo'yicha mavjud S jadvallardagi kabi natijalarni qayd etgan. Bundan tashqari, ushbu S jadvallarning barchasi yuqori algebraik immunitetlik darajasini qayd etgan, bu esa ularni algebraik kriptotahlil usuliga bardoshligini ko'rsatadi.

6. Xulosa

Ushbu maqolada sinus va tent xaotik akslantirishlarini birgalikda foydalanish orqali S jadvallarni hosil qilish algoritmi taklif etildi. Mazkur akslantirishning xaotik ekanligi bifrukatsiya diagrammasi va LE ko'rsatkichlari bilan tekshirildi. Taklif etilgan algoritm yordamida bir nechta sondagi 4, 5 va 8 bitli S jadvallar generatsiya qilindi va umumiy kriptografik talablarga nisbatan tekshirildi. Tahlil natijalari hosil bo'lgan S jadvallarni yuqori bardoshlikka egaligini va ulardan amalda foydalanish mumkinligini ko'rsatdi.

Keyingi ilmiy ishlarda ushbu S jadvallarni apparat va dasturiy tomonidan amalga oshirish masalasi ko'rib o'tiladi.

7. Foydalanilgan adabiyotlar ro'yxati

1. Claude E. Shannon, "A Mathematical Theory of Cryptography", Bell System Technical Memo MM 45-110-02, September 1, 1945.
2. Kuryazov D.M., Sattarov A.B., Axmedov B.B. Blokli simmetrik shifrlash

(cc) BY ©Xudoykulov Zarifjon Turakulovich

algoritmlari bardoshliligini zamonaviy kriptotahlil usullari bilan baholash. O'quv qo'llanma. Toshkent. 2017, 224 bet.
3. Prouff, E.: DPA attacks and S-Boxes. In: International Workshop on Fast Software Encryption. pp. 424–441. Springer (2005).
4. Li H, Zhou Y, Ming J, Yang G, Jin C (2020) The notion of transparency order, revisited. Comput J 63(12):1915–1938. https://doi.org/10.1093/comjnl/bxaa069
5. de la Cruz Jiménez R. A. On some methods for constructing almost optimal s-boxes and their resilience against side-channel attacks //Cryptology ePrint Archive. – 2018.
6. Fei Y., Luo Q., Ding A. A. A statistical model for DPA with novel algorithmic confusion analysis //Cryptographic Hardware and Embedded Systems–CHES 2012: 14th International Workshop, Leuven, Belgium, September 9-12, 2012. Proceedings 14. – Springer Berlin Heidelberg, 2012. – S. 233-250.
7. P. -P. Duong et al., "Construction of Robust Lightweight S-Boxes Using Enhanced Logistic and Enhanced Sine Maps," in IEEE Access, vol. 12, pp. 63976-63994, 2024, doi: 10.1109/ACCESS.2024.3396452.
8. H. Kim et al., "A New Method for Designing Lightweight S-Boxes With High Differential and Linear Branch Numbers, and its Application," in IEEE Access, vol. 9, pp. 150592-150607, 2021, doi: 10.1109/ACCESS.2021.3126008.
9. http://www.ciphersbyritter.com/RES/SBOXDESN.HTM
10. J. Daemen, V. Rijmen, Specification of Rijndael, in: J. Daemen, V. Rijmen (Eds.), The Design of Rijndael: The Advanced Encryption Standard (AES), Springer, Berlin, Heidelberg, 2020: pp. 31–51. https://doi.org/10.1007/978-3-662-60769-5_3.
11. Nyberg, K. 1991. Perfect nonlinear S-boxes. Advances in Cryptology -- EUROCRYPT '91. 378-386.
12. G.V. Bard, Algebraic Cryptanalysis, Springer US, Boston, MA, 2009. https://doi.org/10.1007/978-0-387-88757-9.
13. N.T. Courtois, G.V. Bard, Algebraic Cryptanalysis of the Data Encryption Standard, in: S.D. Galbraith (Ed.), Cryptography and Coding, Springer, Berlin, Heidelberg, 2007: pp. 152–169. https://doi.org/10.1007/978-3-540-77272-9_10.
14. J.A. Clark, J.L. Jacob, S. Stepney, The design of S-boxes by simulated annealing, New Gener Comput 23 (2005) 219–231. https://doi.org/10.1007/BF03037656.
15. D. Souravlias, K.E. Parsopoulos, G.C. Meletiou, Designing bijective S-boxes using Algorithm Portfolios with limited time budgets, Applied Soft Computing 59 (2017) 475–486. https://doi.org/10.1016/j.asoc.2017.05.052 .
16. L.D. Burnett, Heuristic Optimization of Boolean Functions and Substitution Boxes for Cryptography, phd, Queensland University of Technology, 2005. https://eprints.qut.edu.au/16023/ (accessed May 19, 2021).
17. W. Millan, L. Burnett, G. Carter, A. Clark, E. Dawson, Evolutionary Heuristics for Finding Cryptographically Strong S-Boxes, in: V. Varadharajan, Y. Mu (Eds.), Information and Communication Security, Springer, Berlin, Heidelberg, 1999: pp. 263–274. https://doi.org/10.1007/978-3-540-47942-0_22.
18. P. Tesar, A New Method for Generating High Non-Linearity S-Boxes, (2010). http://dspace.lib.vutbr.cz/xmlui/handle/11012/56957 (accessed August 16, 2020).
19. J.R. Abdurazzokov, Algorithm for generation of s-box using trigonometric transformation in genetic algorithm parameters, Shemical technology. Control and management 2023, №3 (111) pp.69-75
20. Hua Z. et al. Design and application of an S-box using complete Latin square //Nonlinear Dynamics. – 2021. – T. 104. – №. 1. – S. 807-825.
21. Muthu J. S., Murali P. Review of chaos detection techniques performed on chaotic maps and systems in image encryption //SN Computer Science. – 2021. – T. 2. – S. 1-24.
22. Szemplinska-Stupnicka W. Chaos, bifurcations and fractals around us. World

(cc) BY ©Xudoykulov Zarifjon Turakulovich

Sci Ser Nonlinear Sci; 2003. https:// doi. org/ 10.1142/ 5419.
23. Naik R. B., Singh U. A review on applications of chaotic maps in pseudo-random number generators and encryption //Annals of Data Science. – 2024. – T. 11. – №. 1. – S. 25-50.
24. V. A. Thakor, M. A. Razzaque, A. D. Darji, and A. R. Patel, ''A Novel 5-bit S-box Design for Lightweight Cryptography Algorithms,'' Journal of Info. Secu. and Appl., vol. 73, p. 103444, Mar. 2023.
25. M. Irfan, M. A. Khan, and G. Oligeri, ''Design of key-dependent s-box using chaotic logistic map for iot-enabled smart grid devices,'' in 2024 4th International Conference on Smart Grid and Renewable Energy (SGRE), 2024, pp. 1–6.
26. A. Manzoor, A. H. Zahid and M. T. Hassan, "A New Dynamic Substitution Box for Data Security Using an Innovative Chaotic Map," in IEEE Access, vol. 10, pp. 74164-74174, 2022, doi: 10.1109/ACCESS.2022.3184012.
27. J. Alqahtani, M. Akram, G. A. Ali, N. Iqbal, A. Alqahtani and R. Alroobaea, "Elevating Network Security: A Novel S-Box Algorithm for Robust Data Encryption," in IEEE Access, vol. 12, pp. 2123-2134, 2024, doi: 10.1109/ACCESS.2023.3348144

©Xudoykulov Zarifjon Turakulovich