RAQAMLI TEXNOLOGIYALARNING NAZARIY VA AMALIY MASALALARI XALQARO JURNALI

P-ISSN: 2181-3086 E-ISSN: 2181-3094

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Samarqand filiali

Web: https://ijdt.uz/index.php/ijdt

YENGIL VAZNLI KRIPTOGRAFIK ALGORITMLARDA FOYDALANILGAN CHIZIQSIZ AKSLANTIRISHLASH TAHLILI

Zarif Xudoykulov[1], Ilhom Rahmatullayev[2]

[1] Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, Toshkent, O‘zbekiston
[2] Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Samarqand filiali, Samarqand, O‘zbekiston
zarif.khudoykulov@tuit.uz, ilhom9001@gmail.com

Citation: *Xudoykulov, Z., & Rahmatullayev, I. (2024). Yengil vaznli kriptografik algoritmlarda foydalanilgan chiziqsiz akslantirishlash tahlili. Международный Журнал Теоретических и Прикладных Вопросов Цифровых Технологий, 7(2), 51–58. извлечено от https://ijdt.uz/index.php/ijdt/article/view/181*

Kelib tushdi: 5-aprel 2024-yil
Qabul qilindi: 25-aprel 2024-yil
Chop etildi: 30-iyun 2024-yil

DOI: https://ijdt.uz/index.php/ijdt/article/view/181

UDK 004.056.55

YENGIL VAZNLI KRIPTOGRAFIK ALGORITMLARDA FOYDALANILGAN CHIZIQSIZ AKSLANTIRISHLASH TAHLILI

Xudoykulov Z.T.[1], *Rahmatullayev I.R.*[2]
[1] Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, Toshkent, O‘zbekiston
[1] Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Samarqand filiali, Samarqand, O‘zbekiston
zarif.khudoykulov@tuit.uz, ilhom9001@gmail.com

Annotatsiya. *Ushbu maqolada NIST LWC tanlovining final bosqichida ishtirok etgan 10 ta algoritmlarda foydalanilgan chiziqsiz akslantirishlar orasidan S jadval shaklida ifodalanganlarini umumiy kriptografik talablarga javob berishi tahlil qilingan. Tahlil natijalari yengil vaznli kriptografik algoritmlarda foydalanilgan S jadvallar umumiy kriptografik talablarga to‘liq javob bera olmasligini ko‘rsatdi. Bu holat akslantirishlarni kod uzunligini kamaytirish, apparat amalga oshirilishida kamsonli mantiqiy elementlarni talab etishi bilan asoslanadi. Bundan tashqari, chiziqsiz akslantirishning NFSR, Keccak va ARX ko‘rinishlaridan ham foydalanilgan bo‘lib, ular S jadvallar kabi yuqori chiziqsizlikni ta’minlay olmasada, amalga oshirishga qulay hisoblanadi.*

Kalit so‘zlar: *NIST LWC, yengil vaznli kriptografiya, chiziqsiz akslantirish, umumiy kriptografik talablar, S jadval, Keccak, NFSR.*

I. KIRISH

Hozirda ananaviy hisoblash muhitida axborotni himoyalashning asosiy mexanizmlaridan biri bo‘lgan kriptografik algoritmlardan amalda keng qo‘llanilmoqda. Shuning bilan birga foydalanilayotgan kriptografik algoritmlarning bardoshliligini baholash masalasi ham yetarlicha amalga oshirilgan va yana davom etmoqda. Xususan, simmetrik blokli va oqimli shifrlash algoritmlari guruhiga kiruvchi qator xalqaro va davlat standartlari kriptotahlili usullariga va samaradorlikka nisbatan baholangan. Jumladan, mazkur algoritmlar uchun chiziqsiz akslantirishlar muhim ahamiyat kasb etib, kriptotahlilda odatda ushbu funksiyalarni baholashga katta e’tibor beriladi [1-4]. Shu sababli, qator ishlarda: AES, DES, keng tarqalgan 4x4 o‘lchamli S jadvallar [1-3], Camellia, UzDSt 1105:2009, GOST P 34.12-2015 [4], mashhur kriptografik algoritmlardagi chiziqsiz akslantirishlar tahlil qilingan.

Shu bilan birga, Buyumlar Interneti (Internet of Things, IoT) texnologiyalarining keng tarqalishi va turli muhitlarda foydalanish holatlari ortmoqda. Ushbu texnologiyalarda foydalanilgan qurilmalar cheklangan quvvat, hisoblash va tarmoq imkoniyatlariga egaligi sababli, mavjud an’anaviy kriptografik algoritmlar ushbu muhit uchun mos emas. Bu esa IoT muhiti uchun yengil vaznli kriptografiya (Lightweight cryptography, LWC) deb nomlanuvchi kriptografik algoritmlarning yangi turini keng tarqalishiga sababchi bo‘lmoqda. Mazkur sohada ko‘plab tanlovlar (NIST LWC, CAESAR, eSTREAM) o‘tkazilgan hamda qator xalqaro (ISO/IEC 29192) va davlat standartlari qabul qilingan [5]. Biroq, mazkur soha va ishlab chiqilgan algoritmlar nisbatan yangi bo‘lgani bois, ularni kriptografik va samaradorlik nuqtai nazaridan baholash yetarli darajada amalga oshirilmagan, ayniqsa ularda foydalanilgan chiziqsiz akslantirishlarni. Shu sababli, ushbu maqolada keng tarqalgan LWC algoritmlarida foydalanilgan chiziqsiz akslantirishlarni baholash masalasi ko‘rib o‘tiladi.

LWC sohasida amalga oshirilgan katta tanlovlardan biri NIST tomonidan o‘tkazilgan bo‘lib, unda ASCON algoritmi oilasi tanlab olingan. Ushbu oilada AEAD (Authenticated Encryption with Associated Data) turidagi shifrlash va xeshlash algoritmi mavjud. Bundan tashqari, ushbu tanlovning so‘ngi bosqichida 10 ta algoritm ishtirok etgan bo‘lib, ular ham xavfsizlik ham samaradorlik bo‘yicha yaxshi baholashga ega bo‘lgan. Ushbu algoritmlarning tahliliga oid qator ilmiy ishlar amalga oshirilgan. Xususan, [6] manbada algoritmlar tasodifiyligi testlar to‘plami yordamida baholangan bo‘lsa, [7] da algoritmlarning apparatda amalga oshirilish darajasi sinovdan o‘tkazilgan. Mualliflar [8] ishda NIST final bosqichida ishtirok etgan algoritmlar energiya samaradorligi, shifrlash va xeshlash vaqtlari bo‘yicha qiyosiy tahlil qilishgan. [9] maqolada NIST final bosqichi algoritmlarini turli

buzilish hujumlariga (Fault attacks) baholash amalga oshirilgan. [10] ish AEAD turidagi CAESAR va NIST LWC tanlovida qatnashgan algoritmlar loyihalash asosi, xavfsizlik xususiyatlari bo‘yicha tahlillangan. Bundan tashqari, [11,12] larda eSTREAM loyihasi algoritmlarining apparat amalga oshirish va kriptotahlil usullariga baholash masalasi ko‘rib o‘tilgan.

II. ASOSIY QISM

ASCON algoritmlar oilasi Ascon-128, Ascon-128a, Ascon-80pq (kvantga asoslangan kalitlarni qidirishga qarshi) autentifikatsiyalashli shifrlash algoritmlari, Ascon-Hash va Ascon-Xof xeshlash algoritmlaridan iborat [13]. ASCON 320 bitli almashtirish ichki holatiga ega bo‘lib, ham apparat ham dasturiy ko‘rinishda amalga oshirishga qulay. Ushbu algoritm oilasi haqida ma’lumotlar 1-jadvalda keltirilgan. ASCON oilasida foydalanilgan p almashtirish akslantirishidagi yagona chiziqsiz funksiya p_S bo‘lib, u 5x5 o‘lchamga ega. S jadvalning ko‘rinishi (Look-Up Table, LUT) 2-jadvalda keltirilgan.

1-jadval. NIST LWC final bosqichi algoritmlarining xususiyatlari

Nomi	Turi	Variantlari	Asos sxema	Holat (bit)	Kalit (bit)	Rejim	Blok uzunligi, rate (bit)	Teg (bit)	Xavfsizligi (bit)
Ascon	Sponge	Ascon-128	Ascon-p	320	128	Duplex	64	128	128
		Ascon-128a	Ascon-p	320	128	Duplex	128	128	128
Elephant	Sponge	Jumbo	Spongent	176	128	Elephant	176	64	127
		Dumbo	Spongent	160	128	Elephant	160	64	112
		Delirium	Keccak	200	128	Elephant	176	128	127
GIST-COFB	Block	GIST-COFB	GIFT-128	192	128	COFB	128	128	128
Grain-128AEAD	Oqimli	Grain-128AEAD	N/A	256	128	N/A	1	64	128
ISAP	Sponge	ISAP-A-128	Ascon-p	320	128	ISAP	64	128	128
		ISAP-K-128	Keccak	400	128	ISAP	144	128	128
		ISAP-K-128A	Keccak	400	128	ISAP	144	128	128
		ISAP-A-128A	Ascon-p	320	128	ISAP	64	128	128
PHOTON-Beetle	Sponge	PHOTON-Beetle-AEAD [128]	PHOTON256	256	128	Beetle	128	256	121
		PHOTON-Beetle-AEAD	PHOTON256	256	128	Beetle	32	256	128
Romulus	Block	Romulus-M	Skinny-128/384	384	128	COFB	128	128	128
		Romulus-N	Skinny-128/384	384	128	COFB	128	128	128
		Romulus-T	Skinny-128/384	384	128	COFB	128	128	128
SPARKLE	Sponge	SCHWAEMM256-128	SPARKLE	384	128	SPARKLE	256	128	120
		SCHWAEMM128-128	SPARKLE	256	128	SPARKLE	128	128	120
		SCHWAEMM192-192	SPARKLE	384	192	SPARKLE	192	192	184
		SCHWAEMM256-256	SPARKLE	512	256	SPARKLE	256	256	248
TinyJambu	Sponge	TinyJambu	TinyJambu	128	128	TinyJambu	32	64	120
Xoodyak	Sponge	Xoodyak	Xoodoo	384	128	Cyclist	352	128	128

Elephant. Ushbu simmetrik blokli shifrlash algoritmi almashtirish akslantirishiga asoslangan bo‘lib, xabar autentifikatsiyasi uchun shifrlashdan keyin MAC (Message Authentication Code) sxemasidan foydalanilgan. Ushbu algoritmda foydalanilgan loyihalash sxemasi algoritmni ham apparat ham dasturiy ko‘rinishda parallel hisoblash imkoniyatini beradi. Ushbu algoritm haqidagi asosiy ma’lumotlar 1-jadvalda keltirilgan [14].

2-jadval. ASCON S jadvalining LUT ko‘rinishi

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	10	11	12	13	14	15	16	17	18	19	1a	1b	1c	1d	1e	1f
S(x)	4	b	1f	14	1a	15	9	2	1b	5	8	12	1d	3	6	1c	1e	13	7	e	0	d	11	18	10	c	1	19	16	a	f	17

Elephant oilasining Jumbo va Dumbo versiyalari mos holda Spongent-π va Spongent-π almashtirishiga asoslangan va ularda 3-jadval keltirilgan 4x4 jadvaldan foydalanilgan. Delirium versiyasida esa Keccak almashtirishidan foydalanilgan.

3-jadval. Elephant oilasining dastlabki ikki algoritmida foydalanilgan S jadvalning LUT ko‘rinishi

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(x)	E	D	B	0	2	1	4	F	7	A	8	5	9	C	3	6

NIST LWC tanlovida ishtirok etgan 3 algoritm GIFT-COFB bo‘lib, u GIFT blokli shifriga asoslangan va Combined FeedBack (COFB) rejimida autentifikatsiyalashli shifrlashni qo‘llab-quvvatlaydi. Ushbu algoritm 40 raund davomida 4 ta fazadan (initsializatsiya, uyani o‘rniga qo‘yish, bit o‘rnini almashtirib va 128 bitli raund kalitini qo‘shish) iborat SPN (Substitution-permutation network, SPN) iborat shifrlashni amalga oshiradi. Ushbu algoritmning asosi hisoblangan GIFT-128

algoritmi 3 ta fazadan iborat: SubCells, PermBits, va AddRoundKey [15]. Mazkur algoritmda ham 4x4 o‘lchamli S jadvaldan foydalanilgan bo‘lib, uning LUT ko‘rinishi 4-jadvalda keltirilgan.

4-jadval. GIFT-128 algoritmi *S* jadvali

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(x)	1	A	4	C	6	F	3	9	2	D	B	7	5	0	8	E

Grain-128AEAD algoritmi NIST LWC tanlovida ishtirok etgan kam sonli oqimli shifrlardan biri bo‘lib, u Grain shifriga asoslangan. Ushbu algoritm ikki quruvchi blokdan iborat: (1) chiziqli va chiziqsiz teskari aloqali siljitish registrlaridan (Linear Feedback Shift Register, LFSR, Non-linear Feedback Shift Register, NFSR) tashkil topgan chiqishdan oldingi generator va chiqishdan oldingi funksiya, (2) siljitish registori va akkumulyatordan iborat autentifikatsiya generatori. Ushbu algoritm tuzilishi haqiqiy Grain-128a algoritmiga juda o‘xshash bo‘lsada, AEADni qo‘llab quvvatlashi va kattaroq autentifikatorga mo‘ljallangani bilan farqlanadi. Ushbu algoritmning umumiy xususiyatlari 1-jadvalda keltirilgan. Ushbu algoritmda chiziqsiz akslantirish sifatida *S* jadvaldan foydalanilmagan [17].

ISAP algoritmi Christoph Dobraunig, Maria Eichlseder, Stefan Mangard, Florian Mendel, Bart Mennink, Robert Primas va Thomas Unterluggauerlar tomonidan yozilgan yengil blokli shifrlash algoritmi bo‘lib, kichik kod o‘lchamli, quvvat tahlili va buzulish hujumlariga bardoshli qilib loyihalashtirilgan [8, 18]. Ushbu algoritmlar oilasi 4 ta variantdan iborat: Isap-K-128a, Isap-A-128a, Isap-K-128, va Isap-A-128, bo‘lib, ularning barchasi kriptografik hujumlarga nisbatan 128 bit xavfsizlik darajasiga ega sifatida loyihalashtirilgan. Ularning 1 va 3-variantlari Keccak-p almashtirishiga asoslangan bo‘lsa, qolganlari 320-bitli Ascon-p almashtirishidan foydalanadi (Ascon-p almashtirishida foydalanilgan *S* jadval 2-jadvaldagi kabi bir xil).

Photon-Beetle algoritmlar oilasi ham Sponge konstruksiyasiga asoslangan bo‘lib, Zhenzhen Bao, Avik Chakraborti, Nilanjan Datta, Jian Guo, Mridul Nandi, Thomas Peyrin, va Kan Yasudalar tomonidan taqdim etilgan. Ushbu algoritm amalga oshirishdagi kichik resurs talab qilgani bilan alohida ajralib turadi [19]. Ushbu algoritm oilasining asosini P256 almashtirishi (PHOTON256) tashkil qilib, ushbu almashtirish AddConstant, SubCells, ShiftRows, va MixColumnSerial bosqichlaridan iborat. Ulardan SubCells bosqichi chiziqsiz akslantirishni amalga oshirib, unda foydalanilgan 4 bitli *S* jadval 5-jadvalda keltirilgan.

5-jadval. P256 algoritmi *S* jadvali

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(x)	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

Romulus yuqoridagi tanlovning ushbu ishtirokchisi aytib o‘tilgan algoritmlar kabi, Sponge konstruksiyasiga emas balki, an’anaviy simmetrik blokli shifrlarni qurish usuli sozlanuvchan blokli shifr (Tweakable block cipher, TBC) deb nomlanuvchi yondashuvdan foydalangan bo‘lib, buning uchun SKINNY algoritmidan foydalangan [8]. Ushbu algoritm 64 va 128-bitli blok uzunligini, 128 va 256-bitli kalit uzunligini qo‘llab-quvvatlaydi. Ushbu algoritm oilasi haqidagi batafsil ma’lumotlar 1-jadvalda keltirilgan. Ikki turdagi blok uzunligi uchun mos holda 4 bitli va 8 bitli *S* jadvallardan foydalangan [20]. Ushbu algoritm oilasining faqat 128 bitli blok uzunligi NIST LWC tanlovida taqdim etilgani bois, 8 bitli *S* jadvalning 16 sanoq tizimidagi ifodasi 6-jadvalda keltirilgan.

Sparkle algoritmi oilasi almashtirishga asoslangan bo‘lib, Schwaemm algoritmi konfidensiyallik, yaxlitlik va autentifikatsiyani amalga oshirsa, Esch xeshlash algoritmi esa kolliziyaga bardoshli xesh funksiya hisoblanadi [8]. Har ikkala algoritm ham Sponge konstruksiyasiga asoslangan bo‘lib, ushbu algoritmning NIST LWC tanlovida taqdim etilgan varianlari haqida 1-jadvalda ma’lumotlar keltirilgan. Ushbu algoritm oilasi Sparkle almashtirishiga asoslangan bo‘lib, ushbu akslantirish o‘z navbatida ARX simmetrik blokli shifrlarni qurish usuliga asoslangan Sparx shifrlash algoritmidan foydalanadi [21]. Boshqacha aytganda, Sparkle oilasi algoritmlarida chiziqsiz akslantirish sifatida *S* jadvallar o‘rniga ARX almashtirishdan foydalanilgan.

TinyJambu algoritmi JAMBU algoritmining ixchamlashtirilgan ko‘rinishi bo‘lib, JAMBU o‘z navbatida CAESAR tanlovining 3-bosqich ishtirokchisi hisoblanadi. TinyJAMBU algoritmi

kalitli almashtirishga asoslangan bo‘lib, ushbu algoritmning NIST LWC tanlovida taqdim etilgan varianti haqidagi umumiy ma’lumotlar 1-jadvalda keltirilgan [8]. Ushbu algoritm 128-bit kalitli almashtirishga asoslangan bo‘lib, bunda kalitlarni kengaytirish talab etilmaydi. Ushbu almashtirishning asosini 128-bitli chiziqsiz teskari aloqali siljitish registori tashkil etadi[22].

6-jadval. Skinny algoritmi S jadvali

x\y	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	65	4c	6a	42	4b	63	43	6b	55	75	5a	7a	53	73	5b	7b
01	35	8c	3a	81	89	33	80	3b	95	25	98	2a	90	23	99	2b
02	e5	cc	e8	c1	c9	e0	c0	e9	d5	f5	d8	f8	d0	f0	d9	f9
03	a5	1c	a8	12	1b	a0	13	a9	05	b5	0a	b8	03	b0	0b	b9
04	32	88	3c	85	8d	34	84	3d	91	22	9c	2c	94	24	9d	2d
05	62	4a	6c	45	4d	64	44	6d	52	72	5c	7c	54	74	5d	7d
06	a1	1a	ac	15	1d	a4	14	ad	02	b1	0c	bc	04	b4	0d	bd
07	e1	c8	ec	c5	cd	e4	c4	ed	d1	f1	dc	fc	d4	f4	dd	fd
08	36	8e	38	82	8b	30	83	39	96	26	9a	28	93	20	9b	29
09	66	4e	68	41	49	60	40	69	56	76	58	78	50	70	59	79
0a	a6	1e	aa	11	19	a3	10	ab	06	b6	08	ba	00	b3	09	bb
0b	e6	ce	ea	c2	cb	e3	c3	eb	d6	f6	da	fa	d3	f3	db	fb
0c	31	8a	3e	86	8f	37	87	3f	92	21	9e	2e	97	27	9f	2f
0d	61	48	6e	46	4f	67	47	6f	51	71	5e	7e	57	77	5f	7f
0e	a2	18	ae	16	1f	a7	17	af	01	b2	0e	be	07	b7	0f	bf
0f	e2	ca	ee	c6	cf	e7	c7	ef	d2	f2	de	fe	d7	f7	df	ff

Xoodyak algoritmi Keccak algoritmini yaratgan olimlar jamoasi tomonidan taqdim etilgan bo‘lib, algoritm asosini Xoodoo almashtirish tashkil etadi. Ushbu almashtirish 5 ta bosqichdan iborat [23], aralashtirish bosqichi (mixing layer) θ, fazoda siljitish bosqichi (plane shifting) $\rho west$, raund konstantasini qo‘shish bosqichi (addition of round constants) ι, chiziqsiz akslantirish bosqichi (non-linear layer) χ va yana bir fazoda siljitish bosqichi $\rho east$. χ akslantirish 3 o‘lchamli holat massivining y tekisligi (8x3) ustida amalga ishiriladigan quyidagi ifodadan iborat: $A_0 \leftarrow A_0 + \overline{A_1} \cdot A_2$, $A_1 \leftarrow A_1 + \overline{A_2} \cdot A_0$, $A_2 \leftarrow A_2 + \overline{A_0} \cdot A_1$.

NIST LWC tanlovi 3-bosqich ishtirokchisi bo‘lgan algoritmlarda foydalanilgan chiziqsiz akslantirishlar haqidagi umumiy ma’lumot quyida keltirilgan (7-jadval).

7-jadval. NIST LWC tanlovining 3-raund ishtirokchisi bo‘lgan algoritmlarda foydalanilgan chiziqsiz akslantirishlar

№	Algoritm nomi	Chiziqsiz akslantirish turi	Akslantirish o‘lchami
1.	ASCON	S jadval	5→5 (bit)
2.	Elephant	S jadval, Keccak [200] χ akslantirishi	4→4 (bit), 5x5xw→5x5xw (bit)
3.	GIFT-COFB	S jadval	4→4 (bit)
4.	Grain-128AEAD	NFSR	128 bit
5.	ISAP	S jadval, Keccak [400] χ akslantirishi	5→5 (bit), 5x5xw→5x5xw (bit)
6.	Photon-Beetle	S jadval	4→4 (bit)
7.	Romulus	S jadval	8→8 (bit)
8.	Sparkle	ARX almashtirish	-
9.	TinyJambu	NFSR	128 bit
10.	Xoodyak	Xoodoo χ akslantirishi	8x4→8x4 (bit)

Yuqoridagi tahlil natijalari taqdim etilgan algoritmlarning aksariyati S jadvaldan chiziqsiz akslantirish sifatida foydalanganidan dalolat berib, xususan, LWC uchun mos algoritmlarda 4x4 o‘lchamli S jadvallarni eng mosligini ko‘rish mumkin.

III. S JADVALLAR TAHLILI

Yuqorida keltirilgan algoritmlarda foydalanilgan S jadvallar ko‘rinishidagi chiziqsiz akslantirishlar algoritm bardoshligini ta’minlashning asosiy omili bo‘lgani bois, ularni umumiy kriptografik talablarga baholash zarur hisoblanadi [24] hamda mualliflar tomonidan chiziqsiz akslantirish S uchun umumiy kriptografik talablar sifatida quyidagilar muhimligi belgilangan:

1. Akslantirishning bul funksiya komponentalari uchun arifmetik normal funksiyalami qurish va ularning deg (f_i) qiymatini hisoblash.

2. Akslantirishlar (bul komponentalar) uchun reguliyarlik (balanslashganlik) xossasini tekshirish.

3. Akslantirishlar bul komponentalari uchun korrelyatsion immunitetlik darajasini $(CI(f_i))$ hisoblash.

4. Akslantirish (bul funksiya komponentalar) uchun $(N(f_i), N(\varphi(X)))$ chiziqsizlikni hisoblash.

5. Akslantirishlar bul komponentalari uchun qatiy lavin samaradorligi va tarqalish mezoni darajasini $(SAC(k), PC(e))$ hisoblash.

6. Akslantirish uchun chiquvchi bitlar bog‘liqsizligi mezonini (BIC) hisoblash.

7. Akslantirish uchun algebraik immunitetni hisoblash $(AI(\varphi(X)))$.

Ushbu kattalikni tanlab olingan S jadvallar uchun hisoblashda SageMath vositasidan foydalanib dasturiy vosita yaratildi. Ushbu yaratilgan dasturiy vosita yordamida 7-jadvalda keltirilgan S jadvallar uchun olingan natijalar 8, 9 va 10-jadvallarda keltirilgan.

8-jadval. Romulus algoritmida foydalanilgan S jadvalning umumiy kriptografik talablarga baholash natijalari

Kriptografik talablar	**Max**	**S jadval**							
		f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
Balanslashgan (f) +	+	+	+	+	+	+	+	+	+
Regulyar (S) +	+	+							
Fiksirlangan nuqtalar ↓	**0**	1 (255)							
Teskari fiksirlangan nuqtalar ↓	**0**	0							
deg (f) ↑	**7**	4	2	2	4	2	2	5	6
$N(f)$ ↑	**112**	64	64	64	64	64	64	64	64
$N(S)$ ↑	**112**	64							
$CI(f)$ ↑	**7**	0	0	0	0	0	0	0	0
$CAI(f)$ ↑	**7**	3	2	2	2	2	2	3	3
$AI(S)$ ↑, r ↑	**3**	2, 34							
$PC(f)$ ↑	**8**	0	0	0	0	0	0	0	0
$SAC(f)$ ↑	+	-	-	-	-	-	-	-	-
$SAC\_DIFF\_128(f)$ **0**	**0**	32	64	64	32	48	64	32	40
$SAC(k)$ ↑	**6**	0	0	0	0	0	0	0	0
$BIC(S)$ ↓	**0**	0.287550							

9-jadval. Elephant, GIFT-COFB va Photon-Beetle algoritmlarida foydalanilgan 4x4 S jadvallarning umumiy kriptografik talablarga baholash natijalari

Kriptografik talablar	**Max**	**Elephant**				**GIFT-COFB**				**Photon-Beetle**			
		f_1	f_2	f_3	f_4	f_1	f_2	f_3	f_4	f_1	f_2	f_3	f_4
Balanslashgan (f) +	+	+	+	+	+	+	+	+	+	+	+	+	+
Regulyar (S) +	+	+				+				+			
Fiksirlangan nuqtalar ↓	**0**	0				0				0			
Teskari fiksirlangan nuqtalar ↓	**0**	0				0				0			
deg (f) ↑	**3**	3	3	3	2	3	3	2	2	3	3	3	2
$N(f)$ ↑	**4**	4	4	4	4	4	4	4	4	4	4	4	4
$N(S)$ ↑	**4**	4				4				4			
$CI(f)$ ↑	**3**	0	0	0	1	0	0	1	1	0	0	0	1
$CAI(f)$ ↑	**3**	2	2	2	2	2	2	2	2	2	2	2	2
$AI(S)$ ↑, r ↑	**2**	2, 21				2, 21				2, 21			
$PC(f)$ ↑	**4**	0	0	0	0	0	0	0	0	0	0	0	0
$SAC(f)$ ↑	+	-	-	-	-	-	-	-	-	-	-	-	-
$SAC\_DIFF\_8(f)$ **0**	**0**	-2	-2	-2	-4	0	-2	-2	-4	-1	-2	-1	-4
$SAC(k)$ ↑	**2**	0	0	0	0	0	0	0	0	0	0	0	0
$BIC(S)$ ↓	**0**	1.0				1.0				1.0			

NIST LWC tanlovining final bosqishi ishtirokchilari bo‘lgan algoritmlarda foydalanilgan S jadvallarning umumiy kriptografik talablarga javob berish darajasidan olingan natijalarga asoslangan holda quyidagi xulosalarni olish mumkin:

1. Tanlov ishtirokchisi bo‘lgan Romulus algoritmida foydalanilgan chiziqsiz akslantirish-

ning umumiy kriptografik talabalarga javob berish natijasi mazkur o‘lchamdagi maksimal qiymatlardan ancha pastligi, akslantirishni LUT shaklidan ko‘ra ancha samarali va kam xotira talab qiluvchi bit darajasidagi amallar (bitsliced form) bilan ifodalanganligi bilan ifodalanadi. Ma’lumki, akslantirishdagi chiziqsizlik darajasi ortishi bilan uni bit darajasidagi amallar bilan ifodalash murakkablashadi va bu o‘z navbatida kodni saqlash uchun yuqori xotira, apparat amalga oshirish uchun ko‘p sonli mantiqiy elementlarni talab etadi.

2. Tanlovning aksariyat ishtirokchi algoritmlarida kichik o‘lchamli 4x4 chiziqsiz akslantirishlardan foydalanilgan va ular ham bit darajasidagi amallar orqali ifodalangan. Algoritmlarning chiziqsizligi va algebraik immuniteti kabi ko‘rsatkichlari yuqori bo‘lsada, SAC, BIC kabi ko‘rsatkichlarni talab darajasida emasligini ko‘rish mumkin.

3. ASCON-p almashtirishi tanlovda ishtirok etgan ikkita algoritmlarda foydalanilgan bo‘lib, unda chiziqsiz akslantirish sifatida 5x5 o‘lchamli S jadvaldan foydalanilgan. Ushbu akslantirish ham bit darajasidagi amallar orqali ifodalangan.

10-jadval. ASCON-p almashtirishida foydalanilgan 5x5 o‘lchamli S jadvalning umumiy kriptografik talablarga baholash natijalari

Kriptografik talablar	**Max**	**ASCON-p**				
		f_1	f_2	f_3	f_4	f_5
Balanslashgan (f) +	**+**	+	+	+	+	+
Regulyar (S) +	**+**	+				
Fiksirlangan nuqtalar ↓	**0**	0				
Teskari fiksirlangan nuqtalar ↓	**0**	0				
deg (f) ↑	**4**	2	2	2	2	2
$N(f)$ ↑	**12**	8	8	8	8	8
$N(S)$ ↑	**12**	8				
$CI(f)$ ↑	**4**	1	1	1	1	1
$CAI(f)$ ↑	**2**	2	2	2	2	2
$AI(S)$ ↑, r ↑	**2**	2, 24				
$PC(f)$ ↑	**5**	0	0	0	0	0
$SAC(f)$ ↑	**+**	-	-	-	-	-
$SAC\_DIFF\_16(f)$ **0**	**0**	-3	-6	-3	-6	0
$SAC(k)$ ↑	**3**	0	0	0	0	0
$BIC(S)$ ↓	**0**	1.0				

IV. XULOSA

Ushbu maqolada NIST LWC tanlovining final bosqichida ishtirok etgan yengil vaznli kriptografik algoritmlarda foydalanilgan chiziqsiz akslantirishlarning umumiy kriptografik talablarga javob berishi tahlil qilindi. Tahlil natijalari algoritmlarda asosan kichik o‘lchamli S jadval ko‘rinishidagi chiziqsiz akslantirishlardan, NFSR registorlaridan va Keccak almashtirishida foydalanilgan bir tomonlama chiziqsiz akslantirishlardan foydalanilganligini ko‘rsatdi. S jadval ko‘rinishida foydalanilgan chiziqsiz akslantirishlar umumiy kriptografik talablarga ananaviy algoritmlar kabi javob bera olmagan. Buning sababi esa algoritmlarni loyihalashda kichik kod o‘lchamiga ega bo‘lishi va ularni bit darajasidagi amallar orqali oson ifodalash mumkinligiga e’tibor berilganligi bilan asoslanadi. Biroq, bit darajasidagi amallar bilan ifodalanishi mumkin va yuqori chiziqsizlik, algebraik immunitet darajasiga, SAC va BIC xususiyatlariga ega bo‘lgan chiziqsiz akslantirishlardan foydalanish algoritmning kriptobardoshligiga katta ijobiy ta’sir ko‘rsatadi. Shu sababli, keyingi ishlar ushbu muammoning yechimiga bag‘ishlanadi.

ADABIYOTLAR

[1] *Abderrahmane Nitaj, Willy Susilo, Joseph Tonien*. A New Improved AES S-box With Enhanced Properties. 25th Australasian Conference on Information Security and Privacy (ACISP 2020), Nov 2020, Perth, France. ffhal-03437913f.

[2] *Picek, S., Batina, L., Jakobović, D., Ege, B., Golub, M.* (2014). S-box, SET, Match: A Toolbox for S-box Analysis. In: Naccache, D., Sauveron, D. (eds) Information Security Theory and Practice. Securing the Internet of Things. WISTP 2014. Lecture Notes in Computer Science, vol 8501. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-43826-8_10

[3] *Saarinen M. J. O.* Cryptographic analysis of all 4× 4-bit S-boxes //Selected Areas in

Cryptography: 18th International Workshop, SAC 2011, Toronto, ON, Canada, August 11-12, 2011, Revised Selected Papers 18. – Springer Berlin Heidelberg, 2012. – S. 118-133.

[4] *Sattarov A. B., Abdurahimov B. F.* An algorithm for constructing S-boxes for block symmetric encryption //Universal Journal of Mathematics and Applications. – 2018. – T. 1. – №. 1. – S. 29-32.

[5] *Thakor V. A., Razzaque M. A., Khandaker M. R. A.* Lightweight cryptography for IoT: A state-of-the-art //arXiv preprint arXiv:2006.13813. – 2020.

[6] *E. Bellini and Y. J. Huang*, "Randomness testing of the nist light weight cipher finalist candidates," in NIST Lightweight Cryptography Workshop, May, 2022.

[7] *I. Elsadek, S. Aftabjahani, D. Gardner, E. MacLean, J. R.* Wallrabenstein, and E. Y. Tawfik, "Hardware and energy efficiency evaluation of nist lightweight cryptography standardization finalists," in 2022 IEEE International Symposium on Circuits and Systems (ISCAS). IEEE, 2022, pp. 133–137.

[8] *Buchanan W. J., Maglaras L.* Review of the NIST Light-weight Cryptography Finalists //2023 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT). – IEEE, 2023. – S. 469-474.

[9] *Madushan H., Salam I., Alawatugoda J.* A review of the NIST lightweight cryptography finalists and their fault analyses //Electronics. – 2022. – T. 11. – №. 24. – S. 4199.

[10] *Jimale, M.A.; Z'aba, M.R.; Kiah, M.L.M.; Idris, M.Y.I.; Jamil, N.; Mohamad, M.S.; Rohmad, M.S.* Authenticated encryption schemes: A systematic review. IEEE Access 2022, 10, 14739–14766.

[11] *Alharbi, F.; Hameed, M.K.; Chowdhury, A.; Khalid, A.; Chattopadhyay, A.; Javed, I.T.* Analysis of Area-Efficiency vs. Unrolling for eSTREAM Hardware Portfolio Stream Ciphers. Electronics 2020, 9, 1935. https://doi.org/10.3390/electronics9111935

[12] *Stefan D.* Analysis and implementation of eSTREAM and SHA-3 cryptographic algorithms: dis. – Cooper Union for the Advancement of Science and Art, Albert Nerken School of Engineering, Graduate Division, 2011.

[13] *Dobraunig, C.; Eichlseder, M.; Mendel, F.; Schläffer, M.* Ascon v1.2. Submission to NIST LWC Project. 2021. Available online: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/ascon-spec-round2.pdf (accessed on 01 May 2024).

[14] *Dobraunig C., Mennink B.* Elephant v1 //Submission to NIST lightweight cryptography project. – 2019.

[15] GIFT-COFB v1.0 [sayt]: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/GIFT-COFB-spec.pdf

[16] *Banik S. et al.* GIFT: A small present: Towards reaching the limit of lightweight encryption //Cryptographic Hardware and Embedded Systems–CHES 2017: 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings. – Springer International Publishing, 2017. – S. 321-345.

[17] *Hell M. et al.* Grain-128AEAD-A lightweight AEAD stream cipher cover sheet corresponding submitter: Backup point of contact. – 2019.

[18] *Dobraunig C. et al.* NIST Update: ISAP v2. 0. – 2022.

[19] *Bao Z. et al.* PHOTON-Beetle Authenticated Encryption and Hash Family, Submission to the NIST Lightweight Cryptography Standardization Process. – 2019.

[20] Lightweight Cryptography [sayt]: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/Romulus-spec.pdf, murojaat vaqti: 06.05.2024 y.

[21] *Beierle C. et al.* Schwaemm and esch: lightweight authenticated encryption and hashing using the sparkle permutation family //NIST round. – 2019. – T. 2.

[22] *Wu H., Huang T.* TinyJAMBU: A family of lightweight authenticated encryption algorithms //Submission to the NIST Lightweight Cryptography Standardization Process. – 2019.

[23] *Daemen J. et al.* Xoodyak, a lightweight cryptographic scheme. – 2020.

[24] *Kuryazov D.M., Sattarov A.B., Axmedov B.B.* Blokli simmetrik shifrlash algoritmlari bardoshliligini zamonaviy kriptotahlil usullari bilan baholash. O'quv qo'llanma. Toshkent. 2017, 224 bet.

Поступила в редакцию 05.04.2024

Citation: *Xudoykulov Z.T., Rahmatullayev I.R.* (2024). Yengil vaznli kriptografik algoritmlarda foydalanilgan chiziqsiz akslantirishlash tahlili. Raqamli texnologiyalarning nazariy va amaliy masalalari xalqaro jurnali. 7(2). – B. 51-58. https://doi.org/10.62132/ijdt.v7i2.181

ANALYSIS OF NONLINEAR TRANSFORMATION USED IN LIGHTWEIGHT CRYPTOGRAPHIC ALGORITHMS

Khudoykulov Z.T.[1], *Rakhmatullayev I.R.*[2]

[1] Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan

[2] Samarkand branch of Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Samarkand, Uzbekistan

zarif.khudoykulov@tuit.uz, ilhom9001@gmail.com

Abstract. *In this paper, among the 10 nonlinear representations used in the final stage of the NIST LWC competition, those presented in the form of S boxes are analyzed to meet the general cryptographic requirements. The results of the analysis showed that the S boxes used in lightweight cryptographic algorithms cannot fully meet the general cryptographic requirements. This situation is justified by the fact that transformations reduce the length of the code, require fewer logical elements in the hardware implementation. In addition, NFSR, Keccak, and ARX representations of nonlinear transformation are used, which are convenient to implement, although they do not provide as high nonlinearity as S boxes.*

Keywords: *NIST LWC, lightweight cryptography, nonlinear transformation, general cryptographic requirements, S box, Keccak, NFSR.*

АНАЛИЗ НЕЛИНЕЙНЫХ ПРЕОБРАЗОВАНИЙ, ИСПОЛЬЗУЕМЫХ В ЛЕГКОВЕСНЫХ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМАХ

Худойкулов З.Т.[1], *Рахматуллаев И.Р.*[2]

[1] Ташкентский университет информационных технологий имени Мухаммада ал-Хорезми, Ташкент, Узбекистан

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

zarif.khudoykulov@tuit.uz, ilhom9001@gmail.com

Аннотация. *В данной статье было проанализировано выраженный в виде S-таблиц, на соответствие общим криптографическим требованиям, среди нелинейных отображений использованных в 10 алгоритмах, представленных в финальном этапе конкурса NIST LWC. Результаты анализа показали, что S-таблицы, используемые в облегченных криптографических алгоритмах, не могут в полной мере отвечать общим криптографическим требованиям. Данная ситуация обосновывается тем, что отображения сокращают длину кода, требуют меньше логических элементов в аппаратной реализации. Кроме того, используются виды нелинейного отображения NFSR, Keccak и ARX, которые удобны в реализации, хотя они и не обеспечивают столь высокую нелинейность, как S-таблицы*

Ключевые слова: *NIST LWC, облегченная криптография, нелинейное отображение, общие криптографические требования, S-таблица, Keccak, NFSR, ARX.*