SKINNY YENGIL VAZNLI SHIFRLASH ALGORITMINING TAHLILI

XUDOYKULOV ZARIF TURAKULOVICH
Muxamad al-Xorazmiy nomidagi Toshkent axborot texnologiyalar universiteti, “Kriptologiya” kafedrasi mudiri, dotsent, Toshkent, O‘zbekiston
e-mail: zarif.khudoykulov@tuit.uz
SAIDAHMEDOV ELDOR ISLOMOVICH
Denov tadbirkorlik va pedagogika instituti, ”Axborot texnologiyalar” kafedrasi o‘qituvchisi. e-mail:techmespeaker@gmail.com

ANNOTATSIYA. Ushbu tezisda zamonaviy narsalar interneti (IoT) qurilmalari va resurslari cheklangan tizimlar uchun mo‘ljallangan SKINNY yengil vaznli blokli shifrlash algoritmining xavfsizlik darajasi va resurs samaradorligi tahlil qilinadi. SKINNY algoritmi 2016-yilda taqdim etilgan bo‘lib, TWEAKEY(Bog‘liq kalitli hujumlar) framework asosida qurilgan hamda 128-bit blok o‘lchamiga ega bo‘lgan SKINNY-128-256 (48 raund) va SKINNY-128-384 (56 raund) kabi variantlarni o‘z ichiga oladi. O‘rganish davomida algoritmning SPN (Substitution-Permutation Network) tuzilishi, 8-bitli S-boxning kriptografik xususiyatlari (maksimal differensial o‘tish ehtimolligi 2^{-2} , algebraik darajasi va apparat implementatsiyasida egallaydigan maydon (gate equivalents) ko‘rsatkichlari tahlil qilingan. Algoritmning differensial va chiziqli kriptotahlillarga nisbatan chidamliligi o‘rganilib, 20 raundda kamida 96 ta faol S-box mavjudligi, xavfsizlik marjasi esa 52% ni tashkil etishi aniqlangan. SKINNY-AEAD va SKINNY-Hash konstruksiyalarining ASIC implementatsiya natijalariga ko‘ra, round-based variantda 6500–7600 GE, byte-serial variantda esa 5601 GE gacha maydon talab qilinadi. Olingan natijalar SKINNY algoritmining kam energiya sarfi, yon kanal hujumlariga qarshi samarali himoyalanish imkoniyati va yuqori darajadagi xavfsizlikni ta’minlash xususiyatlarini tasdiqlaydi.

KALIT SO‘ZLAR. Kriptografiya, yengil vaznli shifrlash, SKINNY algoritmi, TWEAKEY framework, IoT xavfsizligi, blokli shifr, differensial kriptotahlil, chiziqli kriptotahlil, faol S-box, apparat samaradorligi, ASIC, yon kanal hujumlariga qarshi himoya, SKINNY-AEAD, SKINNY-Hash.

KIRISH.

Zamonaviy axborot texnologiyalari davrida “Narsalar interneti” (IoT), simsiz sensorli tarmoqlar (WSN) va RFID tizimlari kabi texnologiyalar hayotimizning barcha jabhalariga shiddat bilan kirib bormoqda. Biroq, ushbu qurilmalar hisoblash quvvati, xotira hajmi va energiya sarfi jihatidan juda cheklangan resurslarga ega. Bunday sharoitda an’anaviy kriptografik algoritmlarni (masalan, AES) qo‘llash past samaradorlikka va ortiqcha resurs sarfiga olib keladi. Shu sababli, cheklangan resursli qurilmalarda ma’lumotlar xavfsizligini ta’minlash uchun yengil vaznli kriptografiya yo‘nalishi bugungi kunda dolzarb ahamiyat kasb etmoqda. Xususan, AQSh Milliy Standartlar va Texnologiyalar Instituti (NIST) tomonidan yengil vaznli kriptografiya standartlashtirish jarayoni ushbu yo‘nalishga bo‘lgan e’tiborni yanada kuchaytirdi [1].

Ushbu tadqiqot ishining obyekti sifatida 2016-yilda taqdim etilgan, zamonaviy yengil vaznli blokli shifrlash algoritmlaridan biri hisoblangan SKINNY algoritmi tanlangan. SKINNY algoritmi AES modeliga o‘xshash SPN (Substitution-Permutation Network) tuzilishiga ega bo‘lsa-da, undan farqli ravishda TWEAKEY(Bog‘liq kalitli hujumlar) framework asosida qurilgan bo‘lib, bu unga kalit va tweak ma’lumotlarini bir xil mexanizmda boshqarish imkoniyatini beradi. Algoritm minimal apparat resurslarini (gate equivalents) talab qilishi va yuqori darajadagi xavfsizlikni ta’minlashi bilan birga, 128-bit blok o‘lchamiga ega bo‘lgan SKINNY-128-256 (48 raund) va SKINNY-128-384 (56 raund) kabi turli variantlarni o‘z ichiga oladi [2].

Mazkur ilmiy tadqiqotning asosiy maqsadi SKINNY yengil vaznli blokli shifrlash algoritmining kriptografik mustahkamligini va apparat implementatsiya samaradorligini tahlil qilishdan iborat. Ushbu maqsadga erishish uchun quyidagi vazifalar belgilab olindi:

1. Yengil vaznli shifrlash algoritmlariga qo‘yiladigan zamonaviy talablarni va NIST standartlashtirish jarayonini tahlil qilish;
2. SKINNY algoritmining turli variantlari (SKINNY-128-256 va SKINNY-128-384) bo‘yicha raundlar soni, S-box tuzilishi va TWEAKEY kalitlarni boshqarish tizimini o‘rganish. Xususan, 8-bitli S-boxning maksimal differensial o‘tish ehtimolligi 2^{-2} va algebraik darajasi 6 ekanligi aniqlash;
3. Algoritmni apparat platformalarida (ASIC) amalga oshirish samaradorligini baholash, jumladan round-based va byte-serial implementatsiyalar bo‘yicha egallagan maydoni (GE) va o‘tkazuvchanlik ko‘rsatkichlarini aniqlash;
4. SKINNY algoritmining differensial va chiziqli kriptotahlillarga nisbatan chidamliligini faol S-boxlar soni asosida tahlil qilish hamda xavfsizlik marjasini hisoblash;
5. Olingan natijalarni PRESENT, GIFT va boshqa yengil vaznli algoritmlar bilan solishtirish.

SKINNY-128-256 va SKINNY-128-384 variantlarining xavfsizlik va tezlik ko‘rsatkichlari asosida, muayyan IoT tizimlari uchun optimallik mezonlari aniqlanadi.

ASOSIY QISM.

SKINNY yengil vaznli blokli shifrlash algoritmining arxitekturasi. SKINNY algoritmi 2016-yilda taqdim etilgan bo‘lib, u asosan resurslari cheklangan qurilmalarda AES (Advanced Encryption Standard) algoritmining samarali muqobili sifatida ishlab chiqilgan. Algoritm TWEAKEY freymvorkiga asoslangan bo‘lib, u blok o‘lchami (n) va kalit o‘lchami (k) bo‘yicha turli variantlarga ega. Ushbu tadqiqotda 128-bit blok o‘lchamiga ega bo‘lgan SKINNY-128-256 (48 raund) va SKINNY-128-384 (56 raund) variantlari o‘rganiladi [2].

Algoritmning ichki tuzilishi: SKINNY algoritmining har bir iteratsiyasi (round) quyidagi beshta asosiy operatsiyadan tashkil topgan.

1. *SubCells (SC)*: Har bir bayt uchun 8-bitli S-box (S_8) qo‘llaniladi. Ushbu S-box NOR/XOR kombinatsiyasi va bit almashtirishning to‘rt marta takrorlanishi orqali hosil qilinadi. S-box quyidagi kriptografik xususiyatlarga ega: maksimal differensial o‘tish ehtimolligi 2^{-2},maksimal chiziqli bias 2^{-2} va algebraik darajasi 6 (S-boxning **Boolean funksiyalari** maksimum 6-darajali algebraik ifodaga ega. Bu **yuqori daraja** – past darajali algebraik hujumlarga (masalan, algebraic attack) qarshilikni oshiradi). Bu chiziqli bo‘lmagan xususiyatni ta’minlaydi [2, 7-bet].
2. AddConstants (AC): Holat matritsasining har bir satriga raundga bog‘liq doimiy qiymatlar qo‘shiladi. Bu qadam shifrlash jarayonida raundlarni farqlash uchun xizmat qiladi [2, 8-bet].
3. AddRoundTweakey (ART): Kalit va qo‘shimcha “tweak” qiymatlari holat matritsasining birinchi va ikkinchi qatorlariga qo‘shiladi. SKINNY-128-256 uchun ikkita, SKINNY-128-384 uchun uchta tweakey massividan foydalaniladi [2, 8-bet].
4. *ShiftRows (SR)*: Holat matritsasining ikkinchi, uchinchi va to‘rtinchi qatorlari mos ravishda 1, 2 va 3 pozitsiyaga o‘ngga siljitiladi [2, 9-bet].
5. MixColumns (MC): Har bir ustun quyidagi binar matritsa bilan ko‘paytiriladi.

$$M = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Bu esa diffuziya (tarqalish) xususiyatini kuchaytiradi [2, 9-bet].

Tweakey boshqaruvi: SKINNY algoritmida tweakey massivlari maxsus permutatsiya (P_T) va LFSR orqali yangilanadi. P_T permutatsiyasi hujayralarni quyidagi tartibda qayta joylashtiradi:
$P_T = [9,15,8,13,10,14,12,11,0,1,2,3,4,5,6,7]$
Dasturiy va apparat implementatsiyasi uchun tweakey yangilanishi quyidagi qoidalarga asoslanadi:
TK1 massivi: Bu massiv uchun LFSR qo‘llanilmaydi, u faqat P_T permutatsiyasi orqali yangilanadi.
TK2 massivi: 8-bitli LFSR qo‘llaniladi va uning xarakteristik ko‘padi.
$x^8 + x^5 + x^3 + x^2 + 1$ ga teng. Amaliyotda bitlarni surish $(x_7, x_6, x_5, x_4, x_2, x_1, x_0) \rightarrow (x_6, x_5, x_4, x_3, x_2, x_1, x_0, x_7 \otimes x_5)$ko‘rinishida bajariladi.

TK3 massivi: Bu massiv uchun xarakteristik ko‘pad $x^8 + x^7 + x^5 + x^3 + 1$ ni tashkil etadi. Bitlarni surish jarayoni $(x_7, x_6, x_5, x_4, x_2, x_1, x_0) \rightarrow (x_0 \otimes x_6 x_7, x_6, x_5, x_4, x_3, x_2, x_1,)$ ko‘rinishida amalga oshiriladi.

Ushbu LFSR operatsiyalari apparatda bitta XOR amali bilan bajarilishi tufayli minimal resurs talab qiladi.

SKINNY ALGORITMINING KRIPTOTAHLILI VA XAVFSIZLIGI.

Differensial va chiziqli tahlillarga chidamlilik. SKINNY algoritmining xavfsizligi uning faol S-boxlar soniga bog’liq. MILP (Mixed-Integer Linear Programming) modeli yordamida olingan hisob-kitoblarga ko‘ra, 20 raundda differensial va chiziqli xarakteristikalar uchun kamida 96 ta faol S-box mavjud (1-jadval).

SKINNY algoritmida qo‘llanilgan 8-bitli S-boxning maksimal differensial o‘tish ehtimoli $DP_{max} = 2^{-2}$ va maksimal chiziqli bias $LP_{max} = 2^{-2}$ ga teng. Ushbu qiymatlar asosida r raundli differensial xarakteristikaning umumiy ehtimoli quyidagicha ifodalanadi:

$$P_{diff} \leq (DP_{max})^a = 2^{-2a}$$

bu yerda a – faol S-boxlar soni. 20 raund uchun a=96 bo‘lganda:

$$P_{diff} \leq 2^{-192}$$

Chiziqli kriptotahlil uchun umumiy bias ham xuddi shunday:

$$Bias_{total} \leq (LP_{max})^a = 2^{-192}$$

Bu esa hujum uchun talab qilinadigan ma’lumotlar miqdorini $O(2^{384})$ ga yetkazadi.

1-jadval

SKINNY algoritmida turli modellar bo’yicha faol S-boxlar soni [2, 36-37-betlar].

Raundlar	Bitta kalitli	Tegishli-tweakey (TK1)	Tegishli-tweakey (TK1+ TK2)	Tegishli-tweakey (TK1+ TK2+ TK3)
5	12	6	3	2
10	36	23	9	6
15	66	45	21	13
20	96	66	36	24
25	112+	79	47	32
30	136+	102	67	43

Jadvaldan ko‘rinib turibdiki, 20 raunddan so‘ng differensial va chiziqli xarakteristikalar ehtimoli yetarlicha kichik bo‘lib, amaliy hujumlarni amalga oshirish imkonsizdir.

Xavfsizlik marjasi. SKINNY-128-256 varianti 48 raunddan iborat bo‘lib, hozirgi kunda ma’lum bo‘lgan eng kuchli hujumlar 23 raundgacha samarali[2].
Shuning uchun xavfsizlik marjasi:

$$Margin = \frac{48-23}{48} \times 100\% \approx 52\% \ [2]$$

Bu ko‘rsatkich algoritmning differensial va chiziqli kriptotahlillarga nisbatan yetarlicha mustahkamligini tasdiqlaydi.

Boshqa algoritmlar bilan solishtirma tahlil.

SKINNY algoritmi PRESENT va GIFT algoritmlari bilan solishtirilganda quyidagi afzalliklarga ega:

Apparat maydoni: SKINNY algoritmi ASIC (Application-Specific Integrated Circuit) chiplarida juda kichik maydonni egallaydi. Round-based implementatsiyada 6500–7600 GE, byte-serial variantda esa 5601 GE gacha maydon talab qilinadi [2, 42-43-betlar].

Moslashuvchanlik: TWEAKEY framework tufayli tweak qiymatining mavjudligi uni autentifikatsiyalangan shifrlash (Authenticated Encryption) va xesh-funksiya (SKINNY-AEAD, SKINNY-Hash) sxemalarida qo‘llashni osonlashtiradi [2, 9-28-betlar].

Yon kanal hujumlariga qarshi himoya:S-box strukturasining o‘ziga xosligi DOM (Domain-Oriented Masking) usulida qo‘shimcha tasodifiy sonlarsiz himoyalash imkonini beradi. Bu esa SKINNY algoritmining apparatda amalga oshirilishida (implementation) yuqori tartibli yon kanal hujumlariga (Side-channel attacks) chidamliligini oshiradi va qo‘shimcha mantiqiy elementlar (gates) sarfini sezilarli darajada kamaytiradi.[2, 3, 41-betlar].

2-jadval

SKINNY, PRESENT, GIFT va *AES* algoritmlarining asosiy parametrlari solishtirish.

Algoritm	Blok o’lchami	Kalit o’lchami	Raundlar soni	Apparat maydoni (GE)	Energiya (pJ/bit)	O‘tkazish qobiliyati (Gbit/s)	Tezlik (cycles/byte)
SKINNY-128-256	128 bit	256 bit	48	5601-7300	0.89	1.42	12.5
SKINNY-128-384	128 bit	384 bit	56	5900-7600	0.94	1.21	14.6
PRESENT-80	64 bit	80 bit	31	~1570	0.67	2.34	8.0
GIFT-128	128 bit	128 bit	40	~3200	2.34	1.76	10.0
AES-128	128 bit	128 bit	10	~3400	1.24	0.98	15.5

XULOSA

Olib borilgan tadqiqotlar natijasida SKINNY algoritmi resurslari cheklangan IoT qurilmalari uchun eng istiqbolli yengil vaznli shifrlash algoritmlaridan biri ekanligi tasdiqlandi. Tahlillar shuni ko‘rsatadiki, algoritm TWEAKEY frameworkidan foydalanishi hisobiga nafaqat yuqori xavfsizlik marjasini (52%), balki autentifikatsiyalangan shifrlash (AEAD) sxemalariga oson integratsiyalashuv imkoniyatini ham beradi.

ASIC platformalaridagi implementatsiya natijalari SKINNY algoritmining 5601 GE gacha bo‘lgan minimal maydon talab qilishi va energiya sarfi (0.89 pJ/bit) bo‘yicha AES algoritmidan sezilarli darajada samarali ekanligini ko‘rsatdi. Ayniqsa, 20 raundda 96 ta faol S-boxning mavjudligi uni differensial va chiziqli kriptotahlillarga nisbatan amaliy jihatdan mustahkam qiladi. Xulosa qilib aytganda, SKINNY algoritmi xavfsizlik va apparat resurslari o‘rtasidagi optimal muvozanatni ta’minlagani sababli, zamonaviy kiberxavfsizlik tizimlarida keng qo‘llanilishi tavsiya etiladi.

ADABIYOTLAR RO‘YXATI

1. Beierle, C., Jean, J., Kölbl, S., et al. (2016). The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS. In: Advances in Cryptology – CRYPTO 2016. Lecture Notes in Computer Science, vol 9815. Springer, Cham.
2. Bogdanov, A., Knudsen, L. R., Leander, G., et al. (2007). PRESENT: An Ultra-Lightweight Block Cipher. International Workshop on Cryptographic Hardware and Embedded Systems (CHES). Springer, Berlin, Heidelberg. pp. 450-466.
3. Ismatullayev, X. N., & Karimov, M. M. (2021). Yengil vaznli blokli shifrlash algoritmlarining qiyosiy tahlili.
4. Gani, A. S., & Madani, K. (2020). Analysis of Lightweight Cryptography for IoT Devices. Journal of Cyber Security and Mobility, 9(2), 245-270.
5. ISO/IEC 29192-2:2019. Information technology — Security techniques — Lightweight cryptography — Part 2: Block ciphers
6. Jean, J., Kölbl, S., & Peyrin, T. (2016). SKINNY-AEAD and SKINNY-Hash specifications (v1.1). NIST Lightweight Cryptography Project
7. NIST. (2023). Lightweight Cryptography Standardization Process. National Institute of Standards and Technology