ISSN: 3030-3346

TAMGA-F[1600] KRIPTOGRAFIK AKSLANTIRISHI: TUZILISHI, AMALGA OSHIRISH VA DASTLABKI KRIPTOTAHLILI

Xudoykulov Zarifjon Turakulovich

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
"Kriptologiya" kafedrasi mudiri, DSc,
E-mail: zarif.khudoykulov@tuit.uz

K E Y W O R D S

TAMGA-f, kriptografik akslantirish, gubka konstruksiyasi, Keccak-f, differensial kriptotahlil, chiziqli kriptotahlil, aktiv S-jadval, iz og'irligi

A B S T R A C T

Maqolada 1600 bitli TAMGA-f kriptografik akslantirishining (permutation) tuzilishi, raund qatlamlari, diffuziya xususiyatlari va apparat/dasturiy amalga oshirish (hardware/software implementation) jihatlari bayon etiladi. Akslantirish 24 raundli CA→IL→Θ→P→S tuzilmasiga ega. Bir aktiv S-jadval modelida 2 raund uchun 26/31 aktiv S-jadval hamda 73/64 iz og'irligi (trail weight) olindi. Natijalar Keccak-f[1600] bilan qiyoslandi

1. Kirish

Kriptografik xesh-funksiyalar, kengaytiriladigan chiqishli funksiyalar (extendable-output function, XOF), kalitli xesh va autentifikatsiyalangan shifrlash konstruksiyalarida akslantirishga asoslangan yondashuvning muhim afzalligi — bitta puxta loyihalangan ichki akslantirishdan turli domen ajratish qoidalari hamda gubka (sponge) yoki dupleks rejimlarida foydalanish imkoniyatidir. Keccak-f[1600] ushbu yondashuvning amaliy jihatdan sinovdan o'tgan namunasi bo'lib, SHA-3 va SHAKE standartlarining ichki akslantirishi sifatida qo'llanadi [1, 2]. TAMGA loyihasida mazkur tamoyil saqlanadi, biroq Keccakdagi θ–ρ–π ketma-ketligidan farqli ravishda 64 bitli so'z (lane) ichidagi qo'shimcha IL diffuziya qatlami, ustun nazorat qiymati (parity) asosidagi Θ qatlami va maxsus P koordinata almashtirishi qo'llanadi.

TAMGA-f[1600] ni loyihalashda ikki talab muvozanatlashtirildi. Birinchisi, bitta yoki bir nechta aktiv 5 bitli guruh (bundle) ta'sirini qisqa raundlar ichida ko'p sonli S-jadvallarga tarqatish; ikkinchisi esa raund amallarini XOR, AND, OR, NOT va doimiy siklik siljitish (rotation) kabi sodda amallar bilan ifodalashdir. Bunday tuzilma 64 bitli protsessorlarda tabiiy amalga oshiriladi, 32, 16 va 8 bitli mikrokontrollerlarda esa so'z segmentatsiyasi qo'llanadi. Apparat narxi (cost) faqat mantiqiy amallar soni bilan emas, balki bog'lash (wiring), kritik yo'l, vaqtinchalik registrlar va himoyalangan amalga oshirish xarajatlari bilan birgalikda baholanishi lozim.

Mazkur maqolada TAMGA-f[1600] akslantirishining matematik tavsifi, diffuziya xususiyatlari, dastlabki kriptotahlil va amalga oshirish ko'rsatkichlari tizimlashtirildi. Hisoblash natijalari maqomiga ko'ra aniq (exact), cheklangan aniq (constrained exact) va evristik nomzod (heuristic candidate) sifatida ajratildi. Xususan, differensial/chiziqli tarmoqlanish soni (differential/linear branch number), aktiv S-jadvallar va iz og'irliklari bo'yicha olingan natijalarning qaysi qismi to'liq hisoblash (exhaustive enumeration) bilan tasdiqlangani alohida ko'rsatildi. Keccak-f[1600] bilan qiyoslash [1–6] manbalardagi natijalarga tayangan holda amalga oshirildi.

2. TAMGA-f[1600] holati va umumiy raund tuzilishi

TAMGA-f akslantirishining holati A = (A[y][x]) ko'rinishidagi 5×5 massiv sifatida ifodalanadi. Har bir element 64 bitli so'z bo'lib, y satr indeksini, x esa ustun indeksini bildiradi. Bit pozitsiyasi $z \in \{0, \dots, 63\}$ bilan belgilanadi. Shunday qilib, umumiy holat uzunligi $5 \cdot 5 \cdot 64 = 1600$ bit yoki 200 baytga teng (1-jadval).

$$A = (A[y][x]),\ 0 \le y, x < 5,\ A[y][x] \in GF(2)^{64},\ b = 1600.$$

Dasturiy amalga oshirilishda so'zlar satrlar bo'yicha ketma-ket (row-major) A[0][0], A[0][1],

(cc) BY dtai.uz

…, A[4][4] tartibida joylashtiriladi va har bir 64 bitli so‘z kichik razryadli bayt avval (little-endian) tamoyiliga muvofiq tashqi bayt oqimiga o‘tkaziladi. Ushbu tartib Python, C tilidagi etalon (Reference C) va 8/16/32 bitli mikrokontroller realizatsiyalarida bitma-bit moslikni ta’minlaydigan spetsifikatsiya talabidir.

Bitta raund besh qatlamdan tashkil topadi: raund o‘zgarmasini qo‘shish (CA), so‘z ichidagi chiziqli aralashtirish (IL), ustun nazorat qiymatlarini aralashtirish (Θ), so‘z koordinatalarini almashtirish (P) va 5 bitli chiziqsiz qatlam (S). Funksional kompozitsiya o‘ngdan chapga qarab o‘qilganda, raund quyidagi ifoda bilan aniqlanadi:

$$\mathcal{R}_i = S \circ \mathcal{P} \circ \Theta \circ \Lambda \circ \iota_i.$$

TAMGA-f[1600] akslantirishi 24 raunddan iborat:

$$TAMGA\text{-}f[1600] = \mathcal{R}_{23} \circ \mathcal{R}_{22} \circ \ldots \circ \mathcal{R}_1 \circ \mathcal{R}_0.$$

1-jadval.

TAMGA-f[1600] akslantirishining asosiy parametrlari

Xususiyat	**TAMGA-f[1600] qiymati**
Holat kengligi	1600 bit = 25 × 64 bit
Holat shakli	5 satr × 5 ustun
Raundlar soni	24
Raund tartibi	CA → IL → Θ → P → S
Chiziqsiz qatlam	5 bitli bijektiv, bitlarga ajratilgan (bitslice) S-jadval
Parallel S-jadvallar / raund	5 × 64 = 320
Asosiy amallar	XOR, AND, OR, NOT, ROTR64, bog‘lash

3. TAMGA-f akslantirishi raund qatlamlarining matematik tavsifi

3.1. CA - raund konstantasini qo‘shish, ι

Raundlar orasidagi simmetriya va takroriy strukturalarni buzish uchun 64 bitli RC_i konstanta faqat A[0][0] so‘ziga XOR amalida qo‘shiladi. Boshqa so‘zlar o‘zgarmaydi:

$$B[0][0] = A[0][0] \oplus RC_i, \quad B[y][x] = A[y][x] \ agar \ (y,x) \neq (0,0).$$

Raund o‘zgarmasini qo‘shish farq va chiziqli maskaning tarqalish vazniga bevosita ta’sir qilmaydi, chunki u xabar yoki kalitga bog‘liq bo‘lmagan affin almashtirishdir. Shu sababli qisqartirilgan raundli (reduced-round) iz qidiruvlarida CA odatda aktivlik hisobiga kiritilmaydi. Biroq, u raundlararo simmetriyalarni, invariant strukturalarni va siljishga asoslangan takroriyliklarni buzishda muhim rol o‘ynaydi. Joriy 24 raund o‘zgarmasi o‘zaro farqli bo‘lib, ularning Xemming og‘irligi 2–6 oralig‘ida. 1, 2, 4, 8, 16 va 32 bitli oddiy siklik siljitishlar bo‘yicha o‘tkazilgan tekshiruvlarda o‘zgarmaslar uchun trivial invariantlik kuzatilmadi (2-jadval).

2-jadval.

Raund o‘zgarmaslari

Raund	**Raund o‘zgarmasi**	**Og‘irlik, bit**	**Raund**	**Raund o‘zgarmasi**	**Og‘irlik, bit**
0	0x0000000000000083	3	12	0x0000000080008083	5
1	0x800000008000808A	6	13	0x0000000080000082	3
2	0x0000000000008003	3	14	0x0000000000000082	2
3	0x0000000000008008	2	15	0x8000000080000081	4
4	0x800000000000808B	6	16	0x8000000080000002	3
5	0x8000000080000082	4	17	0x0000000000008088	3
6	0x8000000000000001	2	18	0x000000000000008B	4
7	0x8000000000008001	3	19	0x0000000000008083	4
8	0x800000008000000A	4	20	0x8000000000000008	2
9	0x8000000080008008	4	21	0x000000008000008A	4
10	0x800000008000800B	6	22	0x800000008000008B	6
11	0x8000000000008081	4	23	0x000000008000808A	5

(cc) BY dtai.uz

3.2. IL - so‘z ichidagi chiziqli aralashtirish, Λ

IL qatlamining vazifasi har bir 64 bitli so‘z ichida bit pozitsiyalarini tarqatishdir. Har bir (y, x) so‘z uchun alohida $(a[y][x], b[y][x])$ siklik siljitish jufti beriladi va quyidagi chiziqli funksiya qo‘llaniladi (3-jadval):

$$\Lambda(A)[y][x] = A[y][x] \oplus ROTR64(A[y][x], a[y][x]) \oplus ROTR64(A[y][x], b[y][x]).$$

IL chiziqli qatlam bo‘lib, har bir so‘z uchun ikki xil doimiy siklik siljitilgan nusxa asl qiymat bilan XOR qilinadi. To‘liq parallel ASIC yoki FPGA arxitekturasida doimiy siljitishlar, odatda, alohida mantiqiy element talab qilmaydigan bog‘lash orqali amalga oshiriladi; asosiy mantiqiy xarajat XOR tarmog‘iga to‘g‘ri keladi. Dasturiy muhitda esa maxsus siklik siljitish ko‘rsatmasi mavjud bo‘lmasa, amal bir necha siljitish va OR ko‘rsatmalariga ajraladi. Shu sababli IL qatlami ayniqsa 8 va 16 bitli mikrokontrollerlarda bajarilish vaqtiga sezilarli ta’sir ko‘rsatadi.

3-jadval.

IL qatlami uchun siklik siljitish qiymatlari

y\ x	0	1	2	3	4
0	(3,13)	(7,21)	(9,47)	(37,59)	(19,17)
1	(23,37)	(59,25)	(27,5)	(41,11)	(11,45)
2	(25,63)	(31,57)	(21,57)	(57,27)	(49,51)
3	(29,19)	(13,31)	(61,15)	(17,23)	(51,61)
4	(43,9)	(55,49)	(5,55)	(15,41)	(47,29)

Har bir 64×64 lokal IL akslantirishining GF(2) ustidagi rangi 64 ga tengligi tekshirildi. Demak, har bir lokal akslantirish bijektiv, 25 ta lokal akslantirishning to‘g‘ri ko‘paytmasi sifatida IL ham 1600 bitli bijektiv chiziqli akslantirishdir. So‘zlar bo‘yicha turli siljitish juftlaridan foydalanish bir xil bit strukturalarining barcha so‘zlarda sinxron saqlanishini qiyinlashtiradi; shunga qaramay, ko‘p raundli siklik va invariant strukturalar alohida tahlilni talab qiladi.

3.3. Θ - ustun nazorat qiymatini aralashtirish

IL chiqishidan keyin Keccak θ funksiyasiga strukturaviy jihatdan yaqin ustun nazorat qiymatini aralashtirish qatlami qo‘llanadi. Avval har bir x ustun uchun besh so‘z XOR amalida qo‘shilib, C[x] hosil qilinadi:

$$C[x] = A[0][x] \oplus A[1][x] \oplus A[2][x] \oplus A[3][x] \oplus A[4][x].$$

So‘ng chap va o‘ng qo‘shni ustun nazorat qiymatlaridan D[x] hosil qilinadi:

$$D[x] = C[(x-1) \bmod 5] \oplus ROTR64(C[(x+1) \bmod 5], 1).$$

Natijada shu D[x] ustundagi barcha so‘zlarga qo‘shiladi:

$$\Theta(A)[y][x] = A[y][x] \oplus D[x].$$

Θ ning vazifasi bir so‘z yoki bir ustundagi farqni qo‘shni ustunlar orqali boshqa satrlarga ham yoyishdir. IL bit pozitsiyalarini so‘z ichida tarqatsa, Θ so‘zlararo tarqalishini hosil qiladi. Shu ikki qatlam ketma-ketligi TAMGA diffuziyasining asosiy manbai hisoblanadi. Apparat nuqtai nazaridan C[x] ni hisoblash uchun 5 kirishli nazorat qiymati daraxti, D[x] uchun bitta XOR va bitta 1-bit siklik siljitish, so‘ng 25 so‘zga D[x] ni qo‘shish talab qilinadi. Keccakdagi θ bilan asosiy farq, TAMGA akslantirishida θ dan oldin qo‘shimcha IL qatlamning mavjudligi hisoblanadi.

3.4. P - so‘z koordinatalarini almashtirish

P qatlami so‘z qiymatining ichki bitlarini o‘zgartirmaydi; faqat 5×5 koordinatalarni GF(5) ustidagi chiziqli akslantirish orqali almashtiradi. Manba koordinata (x, y) uchun:

$$x' = (x + 2y) \bmod 5,\ y' = (3x + 3y) \bmod 5.$$

Bu akslantirish $M = [[1,2],[3,3]]$ matritsaga mos keladi. $\det(M) = 1 \cdot 3 - 2 \cdot 3 = -3 \equiv 2 \pmod 5$ bo‘lib, nol emas; demak P bijektiv. M matritsaning GF(5) dagi teskari matritsasi $[[4,4],[1,3]]$ ga teng. To‘liq parallel apparatda P mantiqiy element talab qilmaydigan bog‘lash/o‘rin almashtirish qatlami sifatida

(cc) BY

amalga oshirilishi mumkin. Dasturiy realizatsiyada esa massiv indekslari yoki so‘zlarni tartiblash orqali yashiriladi. P ning muhim roli Θ orqali hosil qilingan ustun strukturasini keyingi raundda boshqa satr va ustunlarga ko‘chirishdan iborat.

3.5. S - 5 bitli chiziqsiz qatlam

Har bir y satr va har bir z bit pozitsiyasi uchun besh so‘zlarning z-bitlari bitta 5 bitli S jadval kirishini hosil qiladi. Shu sababli bitta raundda 5·64=320 ta S jadval parallel bajariladi. Agar $x_i = A[y][i]_Z$ deb belgilansa, Bul tarmoq quyidagi yordamchi o‘zgaruvchilar orqali ifodalanadi:

$$v5 = \neg x0;\ v6 = v5 \vee x1;\ v7 = x3 \oplus v6;\ s1 = v7 \oplus x2;$$

$$v9 = x3 \wedge x4;\ v10 = v9 \oplus x1;\ v11 = x3 \vee x0;\ s3 = v10 \oplus v11;$$

$$v13 = x3 \vee x2;\ v14 = v13 \oplus x0;\ v15 = v14 \oplus x4;\ v16 = s1 \wedge x1;\ s0 = v15 \oplus v16;$$

$$v18 = x3 \oplus s3;\ s4 = v18 \oplus v15;$$
$$v20 = v18 \wedge x0;\ v21 = v20 \oplus s1;$$

$$v22 = v18 \vee x4;\ s2 = v21 \oplus v22;$$

$$(y_0, y_1, y_2, y_3, y_4) = (\neg s3, \neg s4, s0, s1, s2).$$

Mazkur S-jadvalning 5 bitli qidiruv jadvali (lookup table, LUT) quyidagicha:

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

S jadval barcha 32 qiymatni bir martadan qabul qiluvchi bijektiv funksiya hisoblanadi. DDT va LAT asosida maksimal DDT elementi 8, maksimal |LAT| 16, chiziqsizlik 8, algebraik daraja 2, differensial tarmoqlanish soni 3 va chiziqli tarmoqlanish soni 3 ga tengligi aniqlangan. Maksimal differensial ehtimollik $8/32 = 2^{-2}$; maksimal korrelyatsiya moduli $16/32 = 1/2$ bo‘lib, kvadratik korrelyatsiya $1/4 = 2^{-2}$ ga teng. Shu ma’noda bitta S jadval uchun minimal lokal differensial va chiziqli kvadratik korrelyatsiya og‘irligi 2 bitga teng. Shuningdek, o‘zgarmas va teskari o‘zgarmas nuqtalarga ega emas. Bundan tashqari, S-jadvalning sikl uzunligi {15, 17} ga teng va 5 ga teng minimal invariantlik darajasiga ega.

Joriy S jadval Ascon S jadvalining affin-ekvivalent oilasidan olingan: $S_{TAMGA}(x) = A[=1] \cdot S_{Ascon}(x) \oplus 4$, bunda A - 5×5 almashtirish matritsasi. Shuning uchun A=1 apparatda qo‘shimcha XOR amalisiz bitlar o‘rnini almashtirish sifatida bajarilishi mumkin va differensial xususiyati, chiziqlilik, chiziqsizlik hamda algebraik daraja kabi asosiy affin-invariant xususiyatlar saqlanadi. Biroq, yuqorida keltirilgan Bul tarmoqning o‘zi avtomatik ravishda minimal mantiqiy element tarmoq degani ma’noni anglatmaydi; ASIC/FPGA uchun alohida optimallashtirish talab qilinadi.

4. Bijektivlik, diffuziya va strukturaviy xususiyatlar

4.1. Raund funksiyasining bijektivligi

TAMGA-f ning har bir raundi bijektiv qatlamlar kompozitsiyasidan tashkil topadi. CA affin translatsiya sifatida teskari akslantirishga ega; IL ning 25 ta lokal 64×64 akslantirishi to‘liq rangli; Θ joriy parametrlar uchun bijektiv chiziqli akslantirish sifatida tekshirilgan; P ning GF(5) dagi koordinata matritsasi teskari matritsaga ega; S-jadval esa 32 ta kirish qiymatini o‘zaro bir qiymatli almashtiradi. Shu sababli bitta raund ham, 24 raundli kompozitsiya ham bijektivdir.

4.2. IL+Θ qatlamlari uchun diffuziya ko‘rsatkichlari

Kriptotahlilda aktivlik 5 bitli S-jadval kirishlariga mos guruhlar bo‘yicha hisoblanadi: fiksirlangan (y,z) koordinatada besh bitdan kamida bittasi 1 bo‘lsa, ushbu guruh aktiv hisoblanadi. IL+Θ chiziqli qatlami uchun bitta aktiv 5 bitli guruhdan boshlangan to‘liq hisoblashda differensial yo‘nalishda minimal chiqish aktivligi 25, chiziqli transpanirlangan yo‘nalishda esa 30 ga teng bo‘ldi. Shunday qilib, bitta aktiv kirish sharti ostidagi ikki qatlamli diffuziya ko‘rsatkichlari mos ravishda 26 va 31 ni tashkil etadi.

26 va 31 qiymatlari global tarmoqlanish sonlari emas, balki bitta aktiv kirish guruhi sharti ostidagi aniq diffuziya ko‘rsatkichlaridir. Ko‘p

(cc) BY

aktiv guruhlar chiqishda XOR orqali o‘zaro kompensatsiyalanishi mumkin. Ko‘p guruhli qidiruvda global chiziqli tarmoqlanish soni B_L=8 ekanligi aniqlandi (2 aktiv kirish → 6 aktiv chiqish). Differensial yo‘nalishda 3 aktiv kirish → 16 aktiv chiqish beruvchi B_D≤19 nomzod topildi; 4 va undan ortiq aktiv guruhlar uchun global minimum hali formal ravishda isbotlanmagan.

4.3. P qatlamining diffuziyadagi roli

P qatlam S jadvalga kiruvchi 5 bitli guruhning o‘zini aralashtirmaydi, biroq so‘zlarni boshqa (y, x) koordinatalarga yuborib, bir raundda Θ hosil qilgan ustun korrelyatsiyalarini keyingi raundda boshqa satr/ustun topologiyasiga ko‘chiradi. Shu sababli samarali chiziqli qatlam sifatida aktiv S jadval qidiruvlarida $P \circ \Theta \circ IL$ ko‘rinishida olinadi. P qatlam bog‘lash sifatida arzon bo‘lsada, uning koordinata sikllari ko‘p raundli diffuziya uchun muhim loyihalash parametridir.

5. Dastlabki kriptotahlil natijalari

5.1. Aktiv S-jadvallar tahlili

Differensial va chiziqli iz xavfsizligini tez baholash usullaridan biri ketma-ket raundlardagi aktiv S-jadvallar sonini minimallashtirishdir. Ikki raund uchun bitta aktiv boshlang‘ich S-jadval, barcha 31 ta nol bo‘lmagan 5 bitli farq yoki maska hamda barcha bit pozitsiyalari bo‘yicha hisoblandi. Differensial yo‘nalishda minimal profil 1+25=26, chiziqli yo‘nalishda esa 1+30=31 bo‘ldi. Ushbu natijalar faqat bitta aktiv boshlang‘ich S-jadval modeli doirasida aniq bo‘lib, ixtiyoriy ko‘p aktivli kirish uchun global minimum sifatida talqin qilinmaydi.

Uch raundli lokal qidiruvda differensial yo‘nalish uchun 1+25+238=264, chiziqli yo‘nalish uchun esa 1+30+274=305 aktiv S-jadvalga ega nomzodlar topildi. Ushbu qiymatlar lokal/evristik qidiruv natijalari bo‘lib, global minimum sifatida talqin qilinmaydi. Shuning uchun 264 va 305 qiymatlari hozirgi bosqichda mos ravishda differensial va chiziqli minimumlar uchun topilgan yuqori chegaralar sifatida qaraladi.

5.2. Differensial va chiziqli iz og‘irligi

S jadvalning DDT va LAT qiymatlari aktiv S jadval soniga qaraganda aniqroq xavfsizlik bahosini beradi. Differensial o‘tish uchun $w_D(\Delta x \to \Delta y) = -\log2(\mathrm{DDT}[\Delta x][\Delta y]/32)$ aniqlanadi. Chiziqli maska o‘tishida esa absolut korrelyatsiya og‘irligi $w_L, \mathrm{abs}(\alpha \to \beta) = -\log2(|\mathrm{LAT}[\alpha][\beta]|/32$, standart kvadratik korrelyatsiya og‘irligi esa $w_L, \mathrm{sq} = 2 \cdot w_L, \mathrm{abs}$ ko‘rinishida olinadi. Bir iz og‘irligi raundlar bo‘yicha lokal S jadval vaznlarining yig‘indisidir.

$$w_D = -log2(DDT/32),\ w_L, sq = -log2((|LAT|/32)\text{^}2).$$

Bitta aktiv boshlang‘ich S-jadval modeli doirasida ikki raund uchun o‘tkazilgan aniq qidiruv differensial iz og‘irligini 73, chiziqli izning mutlaq korrelyatsiya og‘irligini 32 va kvadratik korrelyatsiya og‘irligini 64 sifatida aniqladi. Ushbu hisoblash faol S-jadvallar sonigagina emas, balki DDT va LAT dagi konkret o‘tishlarga hamda chiziqli qatlam orqali tarqaladigan farq va maska qiymatlariga tayanganligi sababli oddiy aktivlik bahosiga nisbatan aniqroqdir.

Uch raund uchun uzoq davom etuvchi lokal qidiruvlarda differensial iz og‘irligi 804 va chiziqli kvadratik korrelyatsiya og‘irligi 922 bo‘lgan nomzodlar topildi. Bu qiymatlar formal quyi chegara emas; ular topilgan eng yaxshi izlar orqali minimum uchun yuqori chegarani beradi. Natijalar kuchli diffuziya mavjudligini ko‘rsatsada, xavfsizlik chegarasi sifatida qo‘llashdan oldin qidiruv fazosini aniq usullar bilan yopish zarur.

5.3. Natijalarni talqin qilishdagi cheklovlar

Aktiv S-jadvallar va iz og‘irliklari bo‘yicha natijalarni ularning qidiruv modeli bilan birga talqin qilish lozim. 26/31 qiymatlari bitta aktiv boshlang‘ich S-jadval shartiga tegishli va ixtiyoriy ko‘p aktivli kirish uchun global minimumni anglatmaydi. Uch raundli 264/305 va 804/922 qiymatlari evristik nomzodlardir. Bundan tashqari, bitta iz og‘irligi butun differensial yoki chiziqli hull ehtimolini to‘liq ifodalamaydi. Shu sababli keyingi bosqichda global chegaralar va ko‘p izli ta’sirlarni baholash talab etiladi [7].

6. Dasturiy va apparat amalga oshirish xususiyatlari

6.1. 64 bitli muhitlarda amalga oshirish

(cc) BY

TAMGA holatining 25 ta 64 bitli so‘zdan tashkil topishi x86-64 va ARMv8 kabi arxitekturalarda tabiiy amalga oshirish imkonini beradi. C tilidagi etalon variantida so‘zlar 64 bitli butun sonlar bilan ifodalanadi, XOR va mantiqiy amallar to‘g‘ridan-to‘g‘ri bajariladi, doimiy siljitishlar esa kompilyator tomonidan mos mashina ko‘rsatmalariga o‘giriladi. Platformalararo bir xil natijani ta’minlash uchun tashqi bayt oqimi kichik razryadli bayt avval tartibida aniq yuklash va saqlash amallari bilan qayta ishlanadi.

6.2. 8, 16 va 32 bitli mikrokontrollerlarda amalga oshirish

8 bitli platformada bitta 64 bitli so‘z sakkizta uint8_t, 16 bitli platformada to‘rtta uint16_t, 32 bitli platformada esa ikkita uint32_t bo‘lak orqali ifodalanadi. Holat hajmi barcha variantlarda 200 baytligicha qoladi; farq 64 bitli XOR va siklik siljitishning nechta kichik amallarga ajralishida namoyon bo‘ladi. 8 bitli mikrokontrollerda r-bitli siklik siljitish bayt bo‘yicha aylantirish va bayt ichidagi siljitishga ajratiladi. Bu yondashuv kompilyatorning yashirin yordamchi funksiyalariga bog‘liqlikni kamaytiradi, biroq IL va Θ qatlamlaridagi siljitishlar sabab ko‘p yuklash (load), siljitish (shift) va OR amallarini talab qiladi.

32 bitli mikrokontrollerda bitta 64 bitli so‘z ikki 32 bitli qismga ajratilgani sababli XOR va siklik siljitish narxi 8 yoki 16 bitli platformalarga qaraganda kamayadi. Biroq, real unumdorlik ko‘p razryadli siljitgich (barrel shifter), maxsus siklik siljitish ko‘rsatmalari, konveyerli bajarish (pipeline), Flash kutish taktlar soni va kompilyator optimallashtirishiga bog‘liq. Shuning uchun platformalar o‘rtasidagi ustunlik amaliy o‘lchovlar bilan tasdiqlanishi kerak.

6.3. Apparat amalga oshirish narxi

To‘liq parallel bir raundli apparatda doimiy siklik siljitishlar mantiqiy element (gate) talab qilmaydigan sim bog‘lanishlari sifatida amalga oshirilishi mumkin, biroq yo‘naltirish (routing) va chiqish yuklamasi (fan-out) xarajatlari saqlanib qoladi. Joriy Bul tarmog‘i bo‘yicha TAMGA raundida CA uchun 1 XOR; IL uchun 50 XOR va 50 doimiy siklik siljitish; Θ uchun 50 XOR va 5 ta bir bitli siklik siljitish; P uchun faqat bog‘lash; S qatlami uchun 55 XOR, 15 AND, 20 OR va 15 NOT talab etiladi. Jami 156 XOR, 15 AND, 20 OR, 15 NOT va 55 doimiy siklik siljitish hosil bo‘ladi. Bu sintezdan oldingi funksional baho bo‘lib, real LUT yoki standart elementlar soniga bevosita tenglashtirilmaydi.

6.4. FPGA prototipi va uning talqini

TAMGA-f uchun ishlab chiqilgan Verilog prototipida chiziqli qism (CA+IL+Θ+P) bir taktli ma’lumotlar yo‘li (datapath), S qatlami esa besh satr bo‘yicha ketma-ket ishlovchi besh taktli qism sifatida tashkil etilgan. Mazkur boshqaruv sxemasida 24 raundli akslantirish holatni yuklash bilan birga 145 takt talab qiladi. 50 MHz sinov chastotasida bu 2,9 mks ga teng. Mazkur qiymat faqat TAMGA-f[1600] akslantirish yadrosining kechikishi (latency) bo‘lib, gubka konstruksiyasidagi to‘ldirish (padding), domen ajratish, ko‘p blokli boshqaruv va xesh natijasini chiqarish xarajatlarini o‘z ichiga olmaydi.

7. Keccak-f[1600] akslantirishi bilan qiyosiy tahlil

7.1. Tuzilmaviy taqqoslash

Keccak-f[1600] ham 25 ta 64 bitli so‘zdan iborat 1600 bitli holat va 24 raunddan foydalanadi. Uning raundi $\theta \rightarrow \rho \rightarrow \pi \rightarrow \chi \rightarrow \iota$ ketma-ketligidan tashkil topadi [1, 2]: θ ustun nazorat qiymatlarini aralashtiradi, ρ har bir so‘zga doimiy siklik siljitish qo‘llaydi, π so‘z koordinatalarini almashtiradi, χ 5 bitli qatorlarda kvadratik chiziqsizlik hosil qiladi, ι esa A[0][0] ga raund o‘zgarmasini qo‘shadi. TAMGA-f bilan umumiyliklar holat geometriyasi, nazorat qiymati asosidagi diffuziya, so‘zlarni qayta joylashtirish va 5 bitli parallel chiziqsizlikdan iborat. Asosiy farq TAMGA-f da Θ dan oldin har bir so‘z uchun ikki siklik siljitishli IL qatlamining mavjudligidir (4-jadval).

Keccak χ uchun har chiqish biti $x_i \oplus ((\neg x_{i+1}) \wedge x_{i+2})$ shaklida bo‘lib, to‘g‘ridan-to‘g‘ri apparat yo‘li NOT→AND→XOR tarzida juda qisqa. TAMGA joriy S jadvali ham algebraik daraja 2 va DDT/LAT maksimumlari bo‘yicha shu lokal xavfsizlik sinfiga yaqin, ammo Bul tarmoq ko‘proq XOR/OR va chuqurroq bog‘liqlik zanjiriga ega. TAMGA S jadvalining affin-ekvivalent kelib chiqishi sabab kelgusida minimal mantiqiy elementlar tarmog‘ini qayta sintez qilish orqali bu farqni kamaytirish imkoniyati mavjud.

(cc) BY

4-jadval.

Keccak-f[1600] va TAMGA-f[1600] akslantirishlarining qiyosiy tavsifi

Mezon	**TAMGA-f[1600]**	**Keccak-f[1600]**	**Izoh**
Holat	5×5×64 = 1600 bit	5×5×64 = 1600 bit	Bir xil geometriya
Raundlar	24	24	Bir xil
Raund tartibi	CA→IL→Θ→P→S	θ→ρ→π→χ→ι	TAMGA-f qo‘shimcha IL qatlamidan foydalanadi
So‘z ichidagi siklik siljitish	IL: har bir so‘z uchun 2 ta	ρ: har bir so‘z uchun 1 ta	TAMGA-f da siljitishlar soni ko‘proq
Nazorat qiymatlarini aralashtirish	Θ	θ	Strukturaviy jihatdan o‘xshash
So‘zlarni almashtirish	P, GF(5) matritsa	π	Ikkalasi ham bijektiv koordinata almashtirish
Chiziqsizlik	5 bitli bijektiv S-jadval	5 bitli χ	Har raundda 320 ta parallel 5 bitli funksiya
Raund o‘zgarmasining joylashuvi	A[0][0], raund boshida	A[0][0], raund oxirida	Affin qatlam
S-jadvalning algebraik darajasi	2	2	Teng
Maksimal DDT / maksimal |LAT|	8 / 16	8 / 16	Mahalliy o‘tish ko‘rsatkichlari teng
S-jadval sikl tuzilishi	{15, 17}	12 ta sikl	Tuzilmalar turlicha
S-jadvalning minimal invariantlik darajasi	5	—	TAMGA-f uchun hisoblangan
S-jadval ANF monomlari	35	15	TAMGA-f Bul tarmog‘i murakkabroq
S-jadvalning apparat narxi, amallar soni	20	15	χ soddaroq

7.2. Apparat narxi va kritik yo‘l

Keccak raundining soddalashtirilgan vektor amallari hisobida θ uchun 50 XOR va 5 siklik siljitish, ρ uchun 25 siklik siljitish, π uchun bog‘lash, χ uchun 25 XOR+25 AND+25 NOT, ι uchun esa 1 XOR talab etiladi; jami taxminan 76 XOR, 25 AND, 25 NOT va 30 doimiy siklik siljitish hosil bo‘ladi. TAMGA raundida XOR va siklik siljitishlar soni ko‘proq. Shu sababli, doimiy siljitishlar apparatda bog‘lash sifatida bajarilgan taqdirda ham, TAMGA-f ning XOR tarmog‘i Keccak-f ga nisbatan kattaroq bo‘lishi kutiladi. 8/16/32 bitli mikrokontrollerlarda esa siljitishlar real ko‘rsatmalar bilan bajarilgani sababli ushbu farq yanada sezilarli bo‘lishi mumkin [3].

7.3. Qisqa raundli kriptotahlil natijalarini taqqoslash

Keccak uchun qisqa raundli differensial izlar nazariyasi batafsil o‘rganilgan. Adabiyotlarda ikki raundli minimal differensial va chiziqli iz og‘irligi 8 sifatida keltiriladi [2], uch raundli Keccak-f[1600] uchun esa differensial iz og‘irligi 32 bo‘lgan izlar va ularga mos chegaralar o‘rganilgan [4–6]. TAMGA-f uchun ikki raundli 73 va 64 qiymatlari faqat bitta aktiv boshlang‘ich S-jadval modeli doirasida aniq olingan; uch raundli 804/922 qiymatlari esa evristik nomzodlardir. Shu sababli TAMGA va Keccak sonlarini to‘g‘ridan-to‘g‘ri nisbatlab xavfsizlik ustunligi haqida xulosa chiqarish metodologik jihatdan asosli emas.

Shunga qaramay, mahalliy diffuziya natijalari TAMGA-f dagi IL qatlamining loyihaviy vazifasini ko‘rsatadi: bitta aktiv S-jadvaldan keyingi chiziqli qatlam differensial yo‘nalishda

(cc) BY

kamida 25, chiziqli yo‘nalishda esa 30 aktiv S-jadval hosil qiladi. Bu ko‘rsatkich qisqa raundlarda aktivlikni tez oshirishga qaratilgan konstruktiv yechimning samaradorligini ko‘rsatadi, biroq global xavfsizlik chegaralarini almashtirmaydi.

8. Muhokama: xavfsizlik va amalga oshirish samaradorligi

TAMGA-f ni loyihalashdagi asosiy yondashuv Keccakga nisbatan so‘z ichidagi diffuziyani kuchaytirib, bir aktiv chiziqsizlik ta’sirini keyingi raundlarda ko‘proq S-jadvallarga tarqatishdan iborat. Bitta aktiv boshlang‘ich S-jadval uchun 26/31 ko‘rsatkichlari mazkur maqsadga erishilganini ko‘rsatadi. Buning evaziga har raundda qo‘shimcha 50 ta 64 bitli siklik siljitish va 50 XOR bajariladi. Demak, TAMGA-f da xavfsizlik signali bilan apparat/dasturiy narx o‘rtasida aniq muvozanat mavjud va yakuniy parametrlar aynan shu ikki mezon asosida baholanishi kerak.

Keyingi tadqiqotlarda biz, avvalo, differensial tarmoqlanish sonining global minimumini va uch-to‘rt raundli aktiv S-jadvallar hamda iz og‘irliklari uchun aniq chegaralarni SAT, MILP va O‘rtada uchrashish (meet-in-the-middle) usullari bilan tekshirishni rejalashtiramiz. Shundan so‘ng algebraik, integral, invariant, siklik va ko‘p izli tahlillar bajarilib, olingan natijalarga ko‘ra raundlar soni, IL siljitishlar to‘plami hamda Θ/P topologiyasini qayta optimallashtirish zarurati baholanadi. Parallel ravishda FPGA/ASIC sintezi va turli razryadli mikrokontrollerlardagi bir xil sharoitdagi qiyosiy sinovlar amalga oshiriladi.

9. Xulosa

TAMGA-f[1600] uchun 5×5×64 bitli holat geometriyasi va 24 raundli CA→IL→Θ→P→S tuzilma shakllantirildi. Keccakga o‘xshash holat geometriyasi saqlangan holda, har bir 64 bitli so‘zga ikki siklik siljitishli IL qatlami kiritilib, qisqa raundlarda diffuziyani kuchaytirish maqsad qilingan. Chiziqsiz qatlam har raundda 320 ta parallel 5 bitli bijektiv S-jadvaldan iborat. S-jadval uchun maksimal DDT qiymati 8, maksimal |LAT| 16, chiziqsizlik 8 va algebraik daraja 2 ekanligi aniqlandi.

Bitta aktiv boshlang‘ich S-jadval modelida ikki raund uchun differensial va chiziqli aktiv S-jadvallar soni mos ravishda 26 va 31, differensial iz og‘irligi 73 hamda chiziqli kvadratik korrelyatsiya og‘irligi 64 bo‘ldi. Uch raund uchun 264/305 aktiv S-jadval va 804/922 iz og‘irligiga ega evristik nomzodlar topildi. Global chiziqli tarmoqlanish soni 8 ekanligi aniqlandi; global differensial tarmoqlanish soni uchun esa hozircha 19 qiymatli nomzod mavjud. Ushbu natijalar TAMGA-f ning kuchli mahalliy diffuziya xususiyatini ko‘rsatsa-da, Keccakdagi kabi global ko‘p raundli aniq chegaralar hali olinmagan.

Keyingi bosqichda biz global differensial chegarani formal tasdiqlash, uch va to‘rt raund uchun aniq aktivlik hamda iz og‘irligi chegaralarini olish, algebraik/integral va invariant tahlillarni kengaytirish, shuningdek FPGA/ASIC va 8/16/32/64 bitli platformalarda bir xil metodika asosida samaradorlikni baholashni rejalashtiramiz. Mazkur ishlar TAMGA-f parametrlarini yakuniy tanlash va uning amaliy qo‘llanish sohasini asoslash uchun zarur.

Foydalanilgan adabiyotlar

1. National Institute of Standards and Technology. FIPS PUB 202: SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. 2015.
2. G. Bertoni, J. Daemen, M. Peeters, G. Van Assche. The Keccak Reference. Version 3.0, January 2011.
3. G. Bertoni, J. Daemen, M. Peeters, G. Van Assche, R. Van Keer. Keccak Implementation Overview. 2012.
4. J. Daemen, G. Van Assche. Differential Propagation Analysis of Keccak. Fast Software Encryption / IACR ePrint 2012/163, 2012.
5. A. Duc, J. Guo, T. Peyrin, L. Wei. Unaligned Rebound Attack: Application to Keccak. Fast Software Encryption, 2012.
6. S. Mella, J. Daemen, G. Van Assche. New Techniques for Trail Bounds and Application to Differential Trails in Keccak. IACR Transactions on Symmetric Cryptology, 2017.
7. G. Bertoni, J. Daemen, M. Peeters, G. Van Assche. Cryptographic Sponge Functions. 2011.

(cc) BY