ISSN: 3030-3346

MAC ALGORITMLARI TAHLILI

Allanov Orif Menglimuratovich

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
E-mail: orif_allanov@mail.ru

K E Y W O R D S

Xabarlarni autentifikatsiyalash, MAC, HMAC, OMAC, CCM, GCM, PMAC, Poly1305, SipHash, LightMAC, Tsudik keymode, Chaskey-12

A B S T R A C T

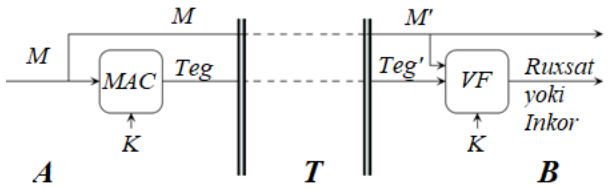
Ushbu maqolada MAC(Message authentification code – xabarlarni autentifikatsiyalash kodi) algoritmlari, ularning turlari, vazifalar va axborot xavfsizligini ta’minlashdagi o‘rni haqida ma’lumotlar berilgan. Shuningdek MAC algoritmlarining ishlash prinsipi, kriptografik asosi, afzalliklari va kamchiliklari hamda qo‘llanilish sohasi bo‘yicha tahlil amalga oshirilib foydalanish uchun zarur tizimni tanlash bo‘yicha xulosalar berilgan.

I. Kirish

MAC algortimlari kriptografiyada xabarning butunligini va haqiqiyligini ta’minlash uchun ishlatiladigan muhim mexanizm hisoblanadi. Bunda xabarga simmetrik kriptotizim yordamida yaratilgan qisqa kod *(teg)* qo‘shiladi, bu kod orqali xabar o‘zgartirilganligi yoki o‘zgartirilmaganligi, hamda haqiqiy yuboruvchidan kelganligi tekshiriladi.

Xabarni autentifikatsiya qilish kodi buzg‘unchining o‘zboshimchalik bilan, tanlangan yoki barcha xabarlar uchun, shu jumladan ma’lum yoki tanlangan xabar shartlari ostida teglarni soxtalashtirishga urinishlariga qarshi turishi kerak. Berilgan xabarning haqiqiy tegini kalitni bilmasdan hisoblash imkonsiz bo‘lishi kerak, hatto buzg‘unchi har qanday xabarning tegini biladi deb taxmin qilinganda ham.

Ko‘p hollarda autentifikatsiyalangan xabar M′, asl xabar M va belgilangan uzunlikdagi tegdan iborat bo‘ladi. Ushbu teg xabar M ning asl ekanligini tasdiqlash uchun ishlatiladi.



1-rasm. Xabar autentifikatsiyasi kodi (MAC)

MAC - bu xabar autentifikatsiyasi sxemasining maxsus holati bo‘lib, bunda autentifikatsiyalangan xabar asl xabar M va Teg dan iborat bo‘ladi (1-rasm). Buzg‘unchi kanalni nazorat qiladi, shuning uchun M va Teg maqsad qilingan manzilga yetib borishi kafolatlanmagan. Buning o‘rniga, qabul qiluvchi B, M va Teg ni oladi. Qabul qiluvchi tasdiqlash funksiyasini K, M va Teg ga qo‘llab, M ni haqiqiy yuborilgan xabar deb hisoblash yoki buzg‘unchi T tomonidan yaratilgan xabar sifatida rad etish qarorini qabul qiladi [1].

II. Asosiy tushunchalar

MAC tizimi quyidagi uch xil (*G*, *S*, *V*) algoritmlardan tuziladi [2]:

- G (kalit generatori) 1^n kirishdan k kalitni generatsiyalash, bu yerda n xavfsizlik parametri hisoblanadi;
- S (imzo) k kalitdan foydalanib va x kirish satridan hosil qilingan t tegni imzolash;
- V (tekshiruvchi): Kirishda rad etilgan yoki chiqishda qabul qilingan k kalit, x satr va t tegni tekshirish.

S va *V* quyidagilarni qanoatlantirishi kerak:

$$Pr_{k \leftarrow G\,(1^n)}[V(k, x, S\,(k, x)) = 1] = 1$$

bu yerda G (1^n) - kalit generatsiya qilish algoritmi, k – maxfiy kalit, S(k,x) – xabar x uchun MAC (teg) yaratish algoritmi, V(k,x,t) – tekshirish algoritmi, t=$S(k,x)$ – yaratilgan MAC qiymati, 1 yoki accept(qabul) – tekshirish muvaffaqiyatli o‘tganligini bildiradi.

MAC algoritmlari boshqa kriptografik primitivlardan, masalan, kriptografik xesh

(cc) BY

funksiyalaridan (HMAC kabi) yoki blokli shifrlash algoritmlaridan (OMAC, CCM, GCM va PMAC) tuzilishi mumkin. Biroq, UMAC - VMAC va Poly1305-AES kabi eng tezkor MAC algoritmlarining aksariyati universal xeshlash asosida qurilgan.

SipHash kabi ichki kalitli xesh algoritmlari ham ta'rifi bo'yicha MAC algortimlaridir. Ular hatto universal xeshga asoslangan MAC algoritmlaridan ham tezroq bo'lishi mumkin [3].

Bundan tashqari, MAC algoritmi ikki yoki undan ortiq kriptografik primitivlarni birlashtirishi mumkin, shunda ulardan birida zaiflik topilsa ham, himoya saqlanib qoladi. Masalan, Transport Layer Security (TLS) protokoli versiyalarida kirish ma'lumotlari ikkiga bo'linadi, ularning har biri turli xil xesh algoritmlari (SHA-1 va SHA-2) bilan qayta ishlanadi va keyin MAC qiymatini chiqarish uchun birgalikda XOR amali bilan qo'shiladi.

III. MAC algoritmlari tahlili

MAC algoritmlarining xesh funksiyalarga asoslangan turi HMAC(keyed-hash message authentication code) tizimlari hisoblanadi**.** HMAC tizimlari o'zining ichki(inner) va tashqi (outer) qismlarida siqish funksiyasi h asosida qurilgan H xesh funksiyasining iterativ MD (Merkle–Damgard) konstruksiyasiga asoslanadi [4].

Ushbu konstruksiya quyidagicha aniqlanadi:

$$H(IV, M) = h\,(\ldots\ h\,(h\,(IV, M_1), M_2)\ \ldots, M_{\mathrm{n}})$$

bu yerda IV — l bitli o'zgarmas boshlang'ich qiymat, M esa ixtiyoriy uzunlikdagi xabar bo'lib, u b bitga karrali bo'lishi uchun to'ldiriladi (padding qilinadi) va b bitli bloklarga ajratiladi:

$$M_1 \,||\, M_2 \,||\, \cdots \,||\, M_{\mathrm{n}}.$$

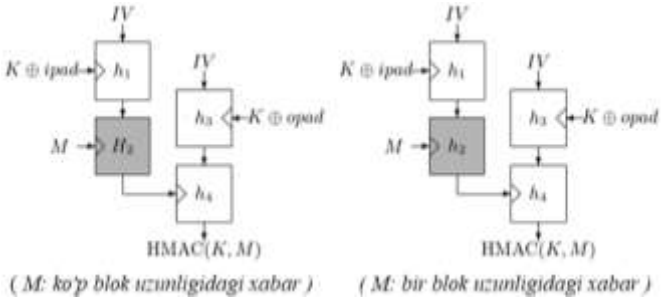
Shuni ta'kidlash joizki, h va H funksiyalarining chiqishlari l bitli satrlardan iborat bo'ladi.

$$HMAC\ (K, M) = H\ (IV, (K \oplus opad) || H\ (IV, (K \oplus ipad)\ ||\ M)) = h\ (h\ (IV, (K \oplus opad)), H\ (h\ (IV, (K \oplus ipad)), M))\quad (1)$$

bu yerda K — maxfiy kalit, opad va ipad — doimiy o'zgarmaslar bo'lib, $|K \oplus \mathrm{opad}| = |K \oplus \mathrm{ipad}| = b$ shartni qanoatlantiradi. Agar HMAC bir blokli M xabarni qabul qilsa, uni quyidagicha ifodalanishi mumkin:

$$HMAC\ (K, M) = h\ (h\ (IV, (K \oplus opad)), h\ (h\ (IV, (K \oplus ipad)), M))(2)$$

HMAC tavsifini yengillashtirish maqsadida, (2) formuladagi to'rtta siqish funksiyasi h ni h_1, h_2, h_3 va h_4 deb belgilanadi, (1) formuladagi to'rtta funksiya esa h_1, H_2, h_3 va h_4 deb belgilanadi. Ushbu belgilash asosidagi HMAC ning sxematik tavsifi 2-rasmda keltirilgan. Shuni ta'kidlash joizki, H_2 va h_2 funksiyalarining chiqishlari h_4 ga kiritilishidan oldin b-bitli satrga to'ldiriladi (padding qilinadi).



2-rasm. HMAC ning sxematik tavsifi

Amaliyotda h funksiyasi HAVAL, MD4, MD5, SHA-0, SHA-1 va shunga o'xshash kriptografik xesh funksiyalarining siqish funksiyasi bilan almashtirilishi mumkin. Ushbu kriptografik xesh funksiyalarining har bir siqish funksiyasi quyidagi ko'rinishga ega:

$$H\ (I, M) = E\ (I, M) + I$$

bu yerda I — l-bitli boshlang'ich qiymat, M — b-bitli xabar bloki, E esa iterativ qadam funksiyasidir. E funksiyasi odatda 3, 4 yoki 5 ta passdan iborat bo'lib, har bir pass 16, 20 yoki 32 ta raundni o'z ichiga oladi.

Poly1305-AES. Poly1305 algoritmi universal xesh oilasiga mansub bo'lib, 2002-yilda Daniel J. Bernstein tomonidan ishlab chiqilgan. Universal xesh oilasidagi boshqa algoritmlar singari, Poly1305 bir martalik xabar autentifikatsiya kodi (MAC) sifatida ishlatiladi. Bunda yuboruvchi va qabul qiluvchi oldindan almashgan maxfiy kalit yordamida bitta xabarni autentifikatsiya qiladi. Bu bir martalik *pad*

(cc) BY

yordamida bitta xabar mazmunini yashirishga o‘xshaydi [5].

Aslida Poly1305 dastlab Poly1305-AES tarkibida taklif qilingan bo‘lib, bu Carter–Wegman autentifikatori hisoblanadi. Poly1305 xesh va AES-128 algoritmini birlashtirib, bitta qisqa kalit va har bir xabar uchun turli xabar raqamlari yordamida ko‘p xabarlarni autentifikatsiyalash imkoniyati yaratilgan. Keyinchalik Poly1305 NaCl (Networking and Cryptography Library**)** dagi crypto_secretbox_xsalsa20poly1305 shifrlash sxemasida har bir xabar uchun bir martalik kalit hosil qilishda, shuningdek, TLS internet protokolida ishlatiladigan ChaCha20-Poly1305 autentifikatsiyalangan shifrlashda qo‘llanilgan.

Poly1305 16 baytli maxfiy kalit r va L baytli xabar m ni oladi va 16 baytli hash $\mathrm{Poly1305_r(m)}$ hosil qiladi. Buning uchun Poly1305 quyidagilarni bajaradi:

1. r ni little-endian 16 baytli butun son sifatida qabul qiladi;
2. Xabar $\mathrm{m} = (\mathrm{m}[0], \mathrm{m}[1], \dots, \mathrm{m}[\mathrm{L}-1])$ ni ketma-ket 16 baytli bo‘laklarga ajratadi;
3. Har bir 16 baytli bo‘lakni 17 baytli little-endian son sifatida qabul qiladi, 1 bayt qo‘shiladi va polinom koeffitsiyentlar sifatida ishlatiladi;
4. Polinom r nuqtasida $2^{130}-5$ ga modul qilib baholanadi;
5. Natija 2^{128} ga modul bo‘yicha qo‘shilib, little-endian formatida 16 baytli hash hosil qilinadi.

Polinomning koeffitsiyentlari □□ quyidagicha aniqlanadi:

$$c_i = m[16i-16] + 2^8 m[16i-15] + 2^{16} m[16i-14] + \cdots + 2^{120} m[16i-1] + 2^{128}$$

Agar $L \not\equiv 0 (mod 16)$ *bo‘lsa, so‘nggi bo‘lak shunday aniqlanadi:*

$$c_q = m[16q-16] + 2^8 m[16q-15] + \cdots + 2^{8(L mod 16)-8} m[L-1] + 2^{8(L mod 16)}$$

Maxfiy kalit $\mathrm{r} = (\mathrm{r}[0], \mathrm{r}[1], \dots, \mathrm{r}[15])$ quyidagi cheklovlarga ega:

- $r[3], r[7], r[11], r[15] \in \{0,1,\dots,15\}$ *(yuqori 4 bit tozalangan);*
- $r[4], r[8], r[12] \in \{0,4,8,\dots,252\}$ *(pastki 2 bit tozalangan).*

Shu bilan r ning 2^{106} turli qiymati mavjud, bir martalik autentifikator sifatida ishlatiladi.

Agar s 16 baytli maxfiy satr bo‘lsa:

$$a := (Poly1305_r(m) + s) mod\ 2^{128}$$

degan qiymat xabar m uchun autentifikator deb ataladi. Agar yuboruvchi va qabul qiluvchi oldindan tasodifiy tanlangan 32 baytli kalit (r, s) ni baham ko‘rsa, yuboruvchi autentifikatsiyalangan xabar (a, m) ni yuborishi mumkin. Qabul qiluvchi tomon da’vo qilingan autentifikatsiyalangan xabarni $(\mathrm{a}', \mathrm{m}')$ (u uzatish jarayonida hujumchi tomonidan o‘zgartirilgan bo‘lishi mumkin) qabul qilganda, u xabarning haqiqiyligini quyidagi shartni tekshirish orqali tasdiqlaydi:

$$a' = (Poly1305_r(m') + s) mod\ 2^{128}$$

agar qiymatlar teng bo‘lsa, xabar haqiqiy hisoblanadi. Kalitni ikki marta ishlatish mumkin emas, aks holda hujumchi maxfiy kalitni topib, xabarni soxtalashtirishi mumkin.

LightMAC. Buyumlar Interneti (IoT) rivojlanishi bilan bog‘langan qurilmalar kommunikatsiya uchun samaradorlik, barqarorlik va funksionallik bo‘yicha turli talablarni yuzaga keltirmoqda. Kommunikatsiyani himoyalash muhim bo‘lib, ko‘plab blokli shifrlash algoritmlari cheklangan resurslarga ega muhitlarda samarali ishlashi uchun yaratilgan. Ushbu blokli shifrlash algoritmlari 128 dan 32 bitgacha bo‘lgan turli blok va kalit o‘lchamlarini taklif qiladi. Kalit o‘lchami ko‘pincha yetarlicha yuqori xavfsizlik darajasini ta’minlash uchun ehtiyotkorlik bilan tanlanadi, natijada xavfsizlikni belgilashda blok o‘lchami asosiy omilga aylanadi. Ma’lumki, blok o‘lchamini kamaytirish blokli shifrlash algoritmlari “ishlash rejimlarida” ishlatilganda ichki holat kolliziyasi ehtimolini oshiradi. Bu rejimlar blokli shifrlash funksiyasini takroriy qo‘llash orqali oddiy blok shifrdan tashqari funksionallikni ta’minlaydigan konstruksiyalardir.

LightMAC uchun xavfsizlikning yuqori chegarasi quyidagicha ifodalanadi:

(cc) BY

$$(1+\varepsilon)\cdot\frac{q^2}{2^n}, \text{ bu yerda } \varepsilon \in O\left(\frac{1}{2^{\frac{n}{2}}-1}\right),$$

LightMAC uchun xavfsizlikning yuqori chegarasi xabar uzunligiga bog‘liq emas. Boshqacha aytganda, 32-bitli blok o‘lchami va xabar uzunligi parametri s ni 16 ga o‘rnatganda, taxminan 64 ta xabar teglanishi mumkin, ularning uzunligi 2^{15} blokgacha bo‘ladi. Kalitlar eng samarali tarzda xabarlar iloji boricha uzun bo‘lganda ishlatiladi: bitta kalit uchun $64 \cdot 2^{15} \cdot 32 = 2^{26}$ bit, yoki 8 Mb ma’lumot teglanishi mumkin.

LightMAC ikkita mustaqil kalitdan foydalanadi, ammo kalitlar soniga nisbatan normallashtirilganda ham bitta kalit uchun qayta ishlangan ma’lumot miqdori 4 Mb bo‘lib, bu 1 Kb bilan solishtirganda sezilarli darajada yaxshilanish hisoblanadi.

$\{0,1\}^n$ to‘plami uzunligi (n) bo‘lgan barcha bit-qatlamlarni ifodalaydi; $\{0,1\} \le n$ to‘plami uzunligi (n) yoki undan kam bo‘lgan barcha bit-qatlamlarni o‘z ichiga oladi. Ikki bit-qatlam (A) va (B) uchun (A || B) va (AB) yozuvlari bir-birining o‘rnida ishlatiladi va ular (A) va (B) ni birlashtirishni bildiradi.

Ayni paytda (r) butun son bo‘lsin, unda M [1]M [2] ... M [l] $\xleftarrow{r}$ M M ni (r) −bitli bloklarga bo‘lishni bildiradi, bunda oxirgi blok (M[l]) uzunligi 0 dan $(r-1)$ bitgacha bo‘lishi mumkin.

Blokli shifr quyidagi funksiya bo‘lsin: $E:\{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ ya’ni, bu yerda E(K) barcha $K \in \{0,1\}^k$ uchun permutatsiyani belgilaydi. Butun son (n), (E) blok uzunligi bo‘lib, EK(X) yozuvi E(K, X) ni bildiradi. Berilgan blok uzunligi (n) bo‘lsa, satrga 10^* qo‘shish satr oxiriga bitta 1 va keyin minimal miqdordagi 0 larni qo‘shish orqali umumiy uzunlikni n bitga ko‘paytiladi. 0^n belgisi faqat nol bitlardan tashkil topgan n-bitli satrni bildiradi.

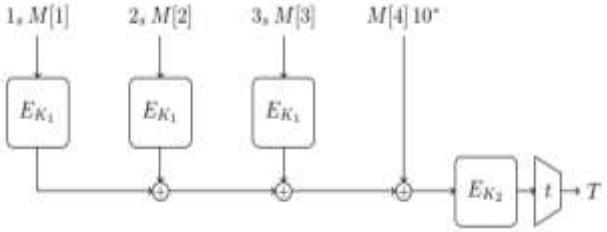
Uzunligi n bo‘lgan A satri va t≤n butun son berilgan bo‘lsa, $|A|_t$ ifoda A ning eng kam ahamiyatga ega t bitlarini bildiradi.

$1 \le i \le 2^s$ bo‘lgan butun son uchun (i_s) ba’zi s-bitli konstantani bildiradi, shunda agar $1 \le i < j \le 2^s$ bo‘lsa, ($i_s \neq j_s$). Masalan, i_s butun son i ning s -bitli ifodasi yoki i −chi s −bitli Gray kodi bo‘lishi mumkin.

$E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ blok shifri bo‘lsin. s va t butun sonlar bo‘lib, mos ravishda n/2 va n dan oshmasligi kerak. LightMAC $\{0,1\}^k$ dan mustaqil va bir xil taqsimlangan ikkita kalit K_1 va K_2 hamda uzunligi $2^s(n-s)$ bitdan oshmaydigan M xabarni qabul qiladi. LightMAC t bit uzunlikdagi natija chiqaradi. Natijaning qanday hosil qilinishi 3-rasm va 1-algoritmda ko‘rsatilgan.

LightMAC pseudotasodifiy funksiyasi (PRF) yoki MAC sifatida ishlatilishi mumkin. PRF sifatida ishlatilganda, LightMAC to‘liq 1-algoritm orqali tavsiflanadi. MAC sifatida ishlatilganda, teglari 1-algoritm yordamida hosil qilinadi va xabar-teg jufti (M, T) tekshiruvi LightMAC(M) bilan T ni solishtirish orqali amalga oshiriladi: agar ular teng bo‘lsa, tekshirish muvaffaqiyatli, aks holda muvaffaqiyatsiz bo‘ladi.

LightMAC parametrlariga s va t butun sonlari, i_s ifodasi va blok shifri E kiradi, bu esa k va n ni bilvosita belgilaydi. Parametrlar sessiya boshlanishidan oldin kelishib olinishi kerak va sessiya davomida doimiy bo‘lib qoladi [6].



3-rasm. LightMAC algoritmining tuzilishi

To‘rtburchaklar blok shifrlash chaqiruvlarini, trapetsiya esa t bitgacha qisqartirishni ifodalaydi.

1. 1-algoritm: LightMAC K1, K2(M)
2. Kirish: $K_1, K_2 \in \{0,1\}^k, M \in \{0,1\} \le 2s(n-s)$
3. Chiqish: $T \in \{0,1\}^t$
4. $V \leftarrow 0n \in \{0,1\}n$
5. M [1] M [2] · · · M[ℓ] ←n−s M
6. i = 1 to ℓ − 1 do
7. $V \leftarrow V \oplus EK1(is \| M[i])$
8. end
9. $V \leftarrow V \oplus (M[\ell]\ 10^*)$

(cc) BY

10. T ← ⌊ EK2(V)⌋ t (natijani t bitgacha qisqartirish)
11. return T

Tsudik keymode. Tsudik keymode — bu xesh-funksiyaga asoslangan MAC algoritmi hisoblanadi. Tsudik keymodedan foydalanish uchun yengil (lightweight) xesh-funksiya *h* tanlanishi va tomonlar o‘rtasida kelishib olinishi lozim. Xesh-funksiya ISO/IEC 29192-5:2016 standartida ko‘rsatilgan yengil vaznli xesh-funksiyalar orasidan tanlanishi kerak. MAC hosil qiluvchi subyekt maxfiy K kalit bilan ta’minlangan bo‘lishi lozim va ushbu kalit MAC ni tekshirishi zarur bo‘lgan barcha tomonlarda ham mavjud bo‘lishi kerak.

Tezkor bir tomonlama xesh funksiyalar asosan xabar ma’lumotlarining yaxlitligini (integrity) ta’minlash uchun qo‘llaniladi. Xavfsiz aloqa sohasida esa faqat xabar yaxlitligi ayrim hujumlardan yetarli darajada himoya qila olmaydi. Xesh funksiya ma’lumotni o‘zgartirishdan himoya qilsada, xabarni almashtirish (message substitution) hujumlaridan himoyalanish uchun xabar yaxlitligi qiymati faqat xabar jo‘natuvchisi tomonidan hosil qilinishi, ya’ni boshqalar tomonidan o‘zgartirib bo‘lmasligi talab etiladi. Shifrlashga asoslangan yaxlitlikni ta’minlash usullari bunday talabni bajara oladi, chunki yaxlitlik funksiyasining kirish qiymatlaridan biri maxfiy kalit hisoblanadi. MD4 yoki boshqa shunga o‘xshash xesh funksiyalarda bunday holat mavjud emas. MD4 keng tarqalganligi sababli, istalgan kishi ixtiyoriy soxta xabar uchun MD4 qiymatini hisoblab, oqimga $[\text{msg}, \text{MD4}(\text{msg})]$ juftligini qo‘shib yuborishi mumkin. Bu muammoning oddiy yechimlardan biri xabar dayjestining shifrlanishi (imzolashi)dir. Ochiq kalitli kriptotizimda bu jo‘natuvchining shaxsiy(private) kaliti yordamida amalga oshiriladi. An’anaviy (simmetrik) kriptotizimda tomonlar o‘rtasida bo‘lishilgan maxfiy kalitdan foydalanilishi mumkin. Xabarni almashtirish (message substitution) va o‘zgartirish (message modification) hujumlariga qarshi ideal holat quyidagilarni o‘z ichiga oladi:

1. Shifrlashdan butunlay qochish;

2. Takror yaratilishi mumkin bo‘lmagan (unforgeable) yaxlitlik qiymatlarini hosil qilish.

Bu ikki xususiyat qarama-qarshi ko‘rinadi, ammo tezkor bir tomonlama xesh funksiyalarni innovatsion tarzda qo‘llash ularni birlashtirish imkonini beradi. Quyida MD4 algoritmining asosiy xususiyatlariga qisqacha to‘xtalib o‘tiladi.

Ikki subyekt, A va B, noaniq (insecure) kanal orqali muloqot qilmoqchi. Bundan tashqari, subyektlarni autentifikatsiya qilishning xavfsiz usullari mavjud. Sessiya boshlanishi paytida, o‘zaro autentifikatsiya amalga oshirilgandan so‘ng, bir subyekt, masalan A, tasodifiy 512-bitli S_{AB} qiymat yaratadi: So‘ngra A, S_{AB} ni B ga maxfiy ravishda yuboradi (zarurat bo‘lsa, shifrlash orqali).

A tomon B ga xabar M xabarni yuborishi kerak bo‘lganda, u quyidagini hisoblaydi: $\text{MD}_\text{M} = \text{MD4}(\text{M} \parallel S_{AB})$. Shundan so‘ng A tomon $[\text{M}, \text{MD}_\text{M}]$ juftligini B ga yuboradi. B, S_{AB} qiymatiga ega bo‘lgani uchun, u $\text{MD4}(\text{M} \,||\, S_{AB})$ ni qayta hisoblab, MD_M ni tekshirishi mumkin. Bu “secret suffix” (maxfiy qo‘shimcha) usuli sifatida tanilgan.

Boshqa tomondan, A va B, MD_M ni $\text{MD}_\text{M} = \text{MD4}(S_{AB} \parallel \text{M})$ kabi hisoblashga kelishishlari mumkin va S_{AB} ni maxfiy prefiks (secret prefix) sifatida ishlatadi. Secret prefix usuli mustaqil ravishda Internet Security and Privacy Working Group (SPWG) tomonidan ishlab chiqilgan va Simple Network Management Protocol (SNMP) da qo‘llanishiga mo‘ljallangan.

Quyidagilar MD4 algoritmining ikkinchi xossasiga asoslanadi:

1. Agar xabar xeshi MD va xabar M_1 berilgan bo‘lsa, quyidagini hisoblashning qiyinligi: xabar M_2 ni topish $\text{MD4}(M_2 \parallel M_1) =$ MD taxminan 2^{128} operatsiyalarni talab qiladi.

2. Agar xabar xeshi MD va xabar M_2 berilgan bo‘lsa, quyidagini hisoblashning qiyinligi: xabar M_1 ni topish $\text{MD4}(M_1 \parallel M_2) =$ MD taxminan 2^{128}operatsiyalarni talab qiladi.

Agar ushbu ikki da’vo (ikki xususiyat) to‘g‘ri bo‘lsa, hujumchi uchun qoladigan yagona imkoniyat bu brute-force(to‘liq tanlash) hujumi hisoblanadi. Ko‘pgina holatlarda, 2^{128} operatsiya talab qiladigan hujumlar imkonsiz deb

(cc) BY

hisoblanadi, ya’ni hujum qilinayotgan tizim xavfsiz hisoblanadi.

Shunga qaramay, mumkin bo‘lgan hujumlarning tahlilini tushunish kerak bo‘ladi. Quyida ta’riflangan ikki ko‘rinishi bir-biriga o‘xshash bo‘lishiga qaramay, ular brute-force hujumlariga chidamlilik darajasi bo‘yicha farq qiladi.

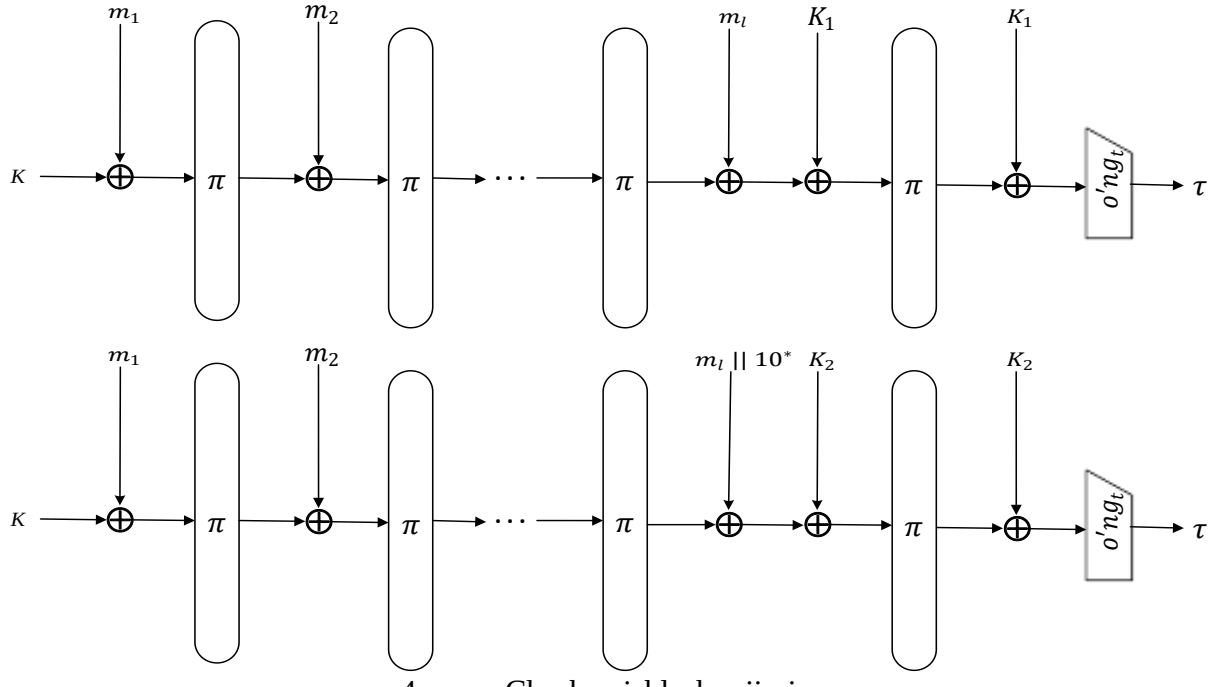
Ikki 512-bitli blok M_1 va M_2 berilgan bo‘lsin. Agar $MD4(M_1) = MD4(M_2)$ bo‘lsa, $M_1 \equiv M_2$ bo‘ladi. “≡” belgisi M_1 va M_2 prefiks-ekvivalent ekanini bildiradi. Berilgan 512-bitli blok M uchun, PEC_M, M ning prefiks-ekvivalentlik sinfini bildiradi.

Ikki 512-bitli blok $M_1 \approx M_2$, agar har qanday M blok uchun $MD4(M \parallel M_1) = MD4(M \parallel M_2)$ tenglik bajarilsa. “ ≈ ” belgisi M_1 va M_2 suffiks-ekvivalent ekanini anglatadi. Berilgan 512-bitli blok M uchun, SEC_M M ning suffiks-ekvivalentlik sinfini bildiradi [7].

Chaskey-12. Quyida permutatsiyaga asoslangan MAC algoritmi — Chaskey haqida ma’lumot taqdim etiladi. Chaskey 128-bitli K kalitni qabul qiladi va m xabarni 128-bitli bloklarda 128-bitli π permutatsiya yordamida qayta ishlaydi. Ushbu permutatsiya Addition-Rotation-XOR (ARX) metodologiyasiga asoslangan. Uning dizayni SipHash permutatsiyasidan olingan bo‘lib, farqi shundaki, u 64-bitli emas, balki 32-bitli so‘zlardan foydalanadi.

Chaskey algoritmi m xabarini qabul qiladi va uni har biri n bitdan iborat bo‘lgan ℓ ta blokga - $m_1, m_2, \ldots, m_l$ ajratadi. Faqat oxirgi blok m_l to‘liq bo‘lmasligi mumkin, hatto $|m| = 0$ bo‘lgan holatda u butunlay bo‘sh ham bo‘lishi mumkin. Shuningdek, Chaskey 128 bitli K kalitni qabul qiladi; bu kalit butun kalit maydonidan mustaqil va teng taqsimot bo‘yicha tanlanishi kerak. K kalitidan ikkita 128 bitli qism kalitlar - K_1 va K_2 , hosil qilinadi; ularning har biri 128 bitli siljitish (shift) va 128 bitli shartli XOR yordamida olinadi. Qism kalitlarni generatsiyalash quyida keltirilgan algoritmlar yordamida amalga oshiriladi:

Chaskey n-bitli K kalitdan foydalanib, ixtiyoriy uzunlikdagi m xabarni $t \leq n$ bitli τ tegga aylantiradi. Har bir K kalit uchun K_1 va K_2 nomli ikkita subkalit 2-algoritmda ko‘rsatilganidek hosil qilinadi. m xabar ℓ ta blokka — $m_1, m_2, \ldots, m_l$ ajratiladi, har bir blok n bitdan iborat bo‘ladi, faqat oxirgi m_l blok to‘liq bo‘lmasligi mumkin. Bo‘sh xabar $m = \emptyset$ bitta bo‘sh blokdan iborat: $|m_1| = 0$. n bitli π permutatsiya xabar bo‘ylab iteratsiya qilinadi. Bu jarayon quyidagi 4-rasmda tasvirlangan.



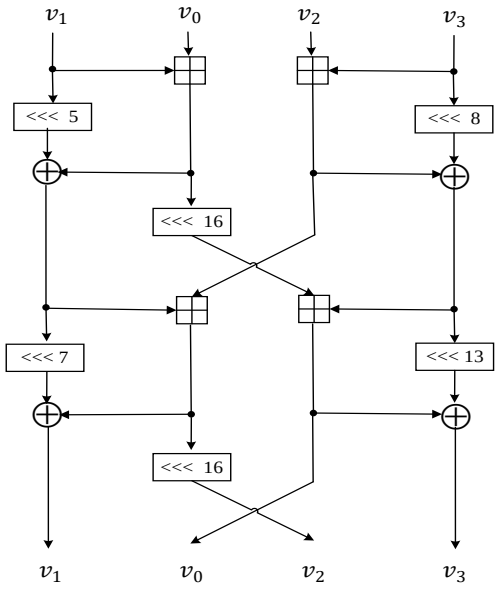
4-rasm. Chaskey ishlash rejimi

(cc) BY

ISSN: 3030-3346

Chaskeyda π permutatsiyasi raund funksiyasining sakkiz marta qo‘llanishidan iborat. Ushbu raund funksiyasi 5-rasmda ko‘rsatilgan.Sakkiz raund xavfsiz konstruktsiya uchun yetarli ekanligiga ishonch komil bo‘lsada, kriptotahlilda kutilmagan muvofaqiyatli vaziyatlar yuzaga kelishi ehtimolini hisobga olib, amalga oshiruvchilarga 16 raundli Chaskey-LTS (long term security) variantini zaxira (fallback) sifatida qo‘shish tavsiya etiladi. Chaskey-LTS Chaskey ga nisbatan taxminan ikki baravar ko‘p tsikl va shunga mos ravishda ikki baravar ko‘p energiya sarflaydi, biroq u baribir AES-CMAC dan ancha tez ishlaydi. Raundlar sonidan boshqa farq bo‘lmagani sababli, Chaskey va Chaskey-LTS ni kod hajmida deyarli hech qanday ortiqcha yuklamasiz birgalikda amalga oshirish mumkin.

Chaskey permutatsiyasi π ning bitta raundi quyidagicha aniqlanadi: $v_0 \,||\, v_1 \,||\, v_2 \,||\, v_3 \leftarrow \pi\,(v_0 \,||\, v_1 \,||\, v_2 \,||v_3)$. Rasmda chiziqlarning kesishish sonini kamaytirish maqsadida v_0 va v_1 lar o‘rni almashtirilgan [8].



5-rasm. Chaskeyda π permutatsiyasi raund funksiyasi

Yuqoridagi ma’lumotlar asosida MAC algoritmlarining afzalliklari va kamchiliklarini tahlil qilish ulardan maqbulini tanlash va foydalanishga yordam beradi.

1-jadval.

MAC algoritmlarining tahliliy jadvali

№	1	2	3	4	5	6
Algoritm	**MAC (Message Authentication Code)**	**HMAC**	**Poly1305-AES**	**LightMAC**	**Tsudik keymode**	**Chaskey-12**
Algoritm turi	Simmetrik autentifikatsiya mexanizmi	Xesh-funksiyaga asoslangan MAC	Polinom asosidagi MAC	Blok shifr asosidagi MAC	Xesh asosidagi MAC	Permutatsiya asosidagi MAC
Kriptografik asos	Blok shifr yoki xesh funksiyaga asoslanishi mumkin	SHA-256, SHA-1 va boshqa xesh funksiyalar	Mod (2^{130}-5) polinom hisoblash	Blok shifr (AES va boshqalar)	Bir tomonlama xesh funksiya	ARX (Addition-Rotation-XOR) operatsiyalari
Kalit uzunligi	Algoritmga bog‘liq	Odatda 128–256 bit	256 bit (r va s)	k bit	Maxfiy kalit K	128 bit
Teg (MAC) uzunligi	O‘zgaruvchan	Xesh natijasiga teng	128 bit	t bit	Xesh natijasiga bog‘liq	128 bit

(cc) BY *dtai.uz*

№	1	2	3	4	5	6
Algoritm	**MAC (Message Authentication Code)**	**HMAC**	**Poly1305-AES**	**LightMAC**	**Tsudik keymode**	**Chaskey-12**
Asosiy ishlash prinsipi	Xabar va maxfiy kalit asosida autentifikatsiya tegi hosil qiladi	Ichki va tashqi kalitli xesh hisoblash orqali MAC hosil qiladi	Xabar bloklari polinom ko‘rinishida hisoblanadi va kalit bilan modulyar arifmetika ishlatiladi	Blok shifrni iterativ qo‘llash orqali MAC hosil qiladi	Xabar va maxfiy kalitni birlashtirib xesh qiymati hisoblanadi	Xabar bloklari ARX permutatsiyasi yordamida qayta ishlanadi
Afzalliklari	Xabar yaxlitligi va autentifikatsiyani ta’minlaydi	Juda keng qo‘llaniladi va kriptotahlilga chidamli	Juda tez va yuqori xavfsizlik	Kichik blok shifrlarda ham xavfsizlik darajasi yuqori	Implementatsiyasi sodda	Mikrocontrollerlarda juda tez ishlaydi
Kamchiliklari	Turli konstruksiyalarda xavfsizlik darajasi farq qiladi	Xesh hisoblash sababli tezligi ba’zi MAClardan past	Har bir xabar uchun noyob nonce talab qilishi mumkin	Ikki mustaqil kalit talab qiladi	Ba’zi xesh konstruksiyalarda hujumlar mumkin	Raundlar soni oshsa energiya sarfi ortadi
Qo‘llanilish sohasi	Kriptografik protokollar, tarmoq xavfsizligi	TLS, IPsec, API autentifikatsiyasi	TLS, ChaCha20-Poly1305	IoT va lightweight kriptografiya	Tarmoq autentifikatsiyasi	IoT, embedded tizimlar

IV. Xulosa

Xulosa qilib aytganda MAC algoritmlari axborot xavfsizligini ta’minlashda muhim rol o‘ynaydi, ular uzatilayotgan xabarlarning yaxlitligini va autentifikatsiyasini kafolatlaydi. Tahlil qilingan MAC, HMAC, Poly1305-AES, LightMAC, Tsudik keymode hamda Chaskey-12 algoritmlari turli kriptografik yondashuvlarga asoslangan bo‘lib, ularning har biri ma’lum qo‘llanish muhitlari uchun mo‘ljallangan. Umumiy MAC konstruksiyasi xabar va maxfiy kalit asosida autentifikatsiya tegi hosil qilish orqali ma’lumotlarning o‘zgarmaganligini tekshirish imkonini beradi. HMAC algoritmi xesh-funksiyaga asoslangan bo‘lib, ikki bosqichli xeshlash mexanizmi orqali yuqori darajadagi kriptografik barqarorlikni ta’minlaydi va hozirgi kunda ko‘plab tarmoq protokollarida keng qo‘llaniladi. Poly1305-AES algoritmi polinom arifmetikasiga asoslangan bo‘lib, yuqori tezlik va kuchli xavfsizlik xususiyatlariga ega hamda

(cc) BY

zamonaviy kriptografik protokollarda samarali ishlatiladi.

Shuningdek, resurslari cheklangan qurilmalar uchun ishlab chiqilgan LightMAC va Chaskey-12 algoritmlari IoT va embedded tizimlarda samarali ishlash imkoniyatini beradi. LightMAC blokli shifrlarga asoslangan konstruksiya bo‘lib, kichik blok o‘lchamli shifrlardan foydalanishda ham yetarli xavfsizlik darajasini ta’minlaydi. Chaskey-12 esa ARX (Addition–Rotation–XOR) operatsiyalariga asoslangan bo‘lib, mikrocontroller arxitekturalarida yuqori samaradorlikka ega. Tsudik keymode xesh-funksiyalarga asoslangan sodda MAC konstruksiyasi bo‘lib, xabar va maxfiy kalitni birlashtirish orqali autentifikatsiya tegi hosil qiladi.

Umuman olganda, tahlil natijalari shuni ko‘rsatadiki, zamonaviy kriptografik tizimlarda MAC algoritmlarini tanlashda qurilmaning hisoblash resurslari, xavfsizlik talablari va qo‘llanish muhiti muhim omil hisoblanadi.

V. Adabiyotlar

1. NIST Computer Security Resource Center (CSRC). *Message Authentication Codes (MAC) Project.*
2. Knospe H. A course in cryptography. – American Mathematical Soc., 2019. – T. 40
3. Aumasson J. P., Bernstein D. J. SipHash: a fast short-input PRF //International Conference on Cryptology in India. – Berlin, Heidelberg : Springer Berlin Heidelberg, 2012. – C. 489-508
4. Kim J. et al. On the security of HMAC and NMAC based on HAVAL, MD4, MD5, SHA-0 and SHA-1 //International Conference on Security and Cryptography for Networks. – Berlin, Heidelberg : Springer Berlin Heidelberg, 2006. – C. 242-256
5. Bernstein D. J. The Poly1305-AES message-authentication code //International workshop on fast software encryption. – Berlin, Heidelberg : Springer Berlin Heidelberg, 2005. – C. 32-49.
6. Luykx A. et al. A MAC mode for lightweight block ciphers //International Conference on Fast Software Encryption. – Berlin, Heidelberg : Springer Berlin Heidelberg, 2016. – C. 43-59.
7. Tsudik G. Message authentication with one-way hash functions //ACM SIGCOMM Computer Communication Review. – 1992. – T. 22. – №. 5. – C. 29-38.
8. Mouha N. et al. Chaskey: an efficient MAC algorithm for 32-bit microcontrollers //International conference on selected areas in cryptography. – Cham : Springer International Publishing, 2014. – C. 306-323.

(cc) BY