BULUTLI MA’LUMOTLAR OMBORINING HIMOYALANISH DARAJASINI OSHIRISH UCHUN AUTENTIFIKATSIYALANGAN SHIFRLASH USULIDAN FOYDALANISH

O‘rinov Nodirbek Toxirjonovich[1], Akbarova Madina Shavkatbek qizi[1]

[1]Zahiriddin Muhammad Bobur nomidagi Andijon davlat universiteti, Dasturiy injiniringi kafedrasi
Email: nodirbekurinov1@gmail.com

KEYWORDS

shifrlash, himoyalanish, bulutli saqlash, autentifikatsiyalangan shifrlash

ABSTRACT

Autentifikatsiyalangan shifrlash (ya’ni shifrlash va o‘zaro bog‘liq funksiyalarni bir vaqtda bajarish jarayoni) ma’lumotlarning maxfiyligini, yaxlitligi ustidan nazoratni va ularning haqiqiyligini ta’minlash uchun mo‘ljallangan. Umumiy kalitlarga ega bo‘lgan tomonlar nafaqat shifrlangan xabarlar almashinuvini tashkil etishlari, balki xabarga imzoga o‘xshash maxsus qo‘shimchalar (imitovstavkalar) kiritish orqali yaxlitlikni nazorat qilish imkoniyatiga ham ega bo‘ladilar. Bu esa qabul qilingan xabarning haqiqiyligiga ishonch hosil qilish imkonini beradi. Autentifikatsiyalangan shifrlash ma’lum bir funksional moslashuvchanlikni ta’minlaydi: kalitlar ma’lumotlarni qayta ishlash jarayonida yangilanib turishi mumkin; xabarning faqat ayrim qismlarini shifrlash yoki shifrlangan hamda ochiq qismlarni navbatma-navbat yuborish imkoniyati mavjud; imitovstavkalar (nazorat qo‘shimchalari) ba’zan umuman bo‘lmasligi yoki aksincha, bir necha marta qo‘llanilishi mumkin. Asosan autentifikatsiyalangan shifrlash algoritmlari blokli kriptotizimlar asosida quriladi. Ularning ayrimlari klassik yondashuvni taqlid qilib, ikki kalitdan foydalanishni istisno etadi, boshqalari esa butunlay yangi, original konstruktsiyalardir.

KIRISH

Axborot texnologiyalarining jadal rivojlanishi natijasida bulutli ma’lumotlar omborlari zamonaviy axborot infratuzilmasining ajralmas qismiga aylandi. Bulutli muhitda foydalanuvchilar o‘z ma’lumotlarini masofadan turib saqlash, qayta ishlash va ulardan turli qurilmalar orqali foydalanish imkoniga ega bo‘ladilar. Biroq bu qulayliklar bilan birga, axborot xavfsizligi masalalari — xususan, ma’lumotlarning maxfiyligi, yaxlitligi va autentifikatsiyasini ta’minlash zarurati yanada keskinlashmoqda.

An’anaviy shifrlash usullari odatda faqat maxfiylikni ta’minlashga yo‘naltirilgan bo‘lib, ma’lumot yaxlitligi yoki haqiqiyligini tasdiqlash funksiyalarini qamrab olmaydi. Shu sababli, so‘nggi yillarda autentifikatsiyalangan shifrlash (Authenticated Encryption – AE) texnologiyasi alohida e’tiborga tushdi. Ushbu yondashuvda shifrlash va yaxlitlikni nazorat qilish birgalikda amalga oshirilib, ma’lumotlarning uzatilish jarayonida buzilish, o‘zgartirish yoki qalbakilashtirish holatlariga qarshi ishonchli himoya yaratiladi.

Autentifikatsiyalangan shifrlashning amaliy modellaridan biri Galois/Counter Mode (GCM) bo‘lib, u AES algoritmi asosida ishlab chiqilgan va yuqori tezlik hamda apparat darajasidagi moslashuvchanligi bilan ajralib turadi. Biroq GCM va unga o‘xshash klassik AE rejimlarining asosiy cheklovi — ularning murakkab tuzilmasi va ko‘p bosqichli hisoblash talabidir. Shu sababli, sponge tipidagi konstruksiyalar asosida qurilgan shifrlash tizimlari yangi avlod autentifikatsiyalangan shifrlash usuli sifatida qaralmoqda.

© N.T. O‘rinov, M.Sh. Akbarova

Sponge-funksiyalar LRX (Logical, Rotation, XOR) sinfiga mansub bo‘lib, ular dasturlashtiriladigan mantiqiy integral sxemalarda (PLIS/FPGA) yuqori samaradorlik bilan amalga oshiriladi. Bash-f sponge-funksiyasi ana shunday ilg‘or konstruktsiyalardan biri bo‘lib, u ma’lumotlarni qayta ishlashda ichki holatning dinamik o‘zgaruvchanligini ta’minlaydi va autentifikatsiyalangan shifrlashni soddalashtirilgan, lekin xavfsiz shaklda amalga oshirish imkonini beradi.

Hozirgi kunga qadar Bash-f asosidagi autentifikatsiyalangan shifrlash algoritmlarining standart va tradeoff hujumlarga (BG, BS, HBG, DK) nisbatan barqarorligi yetarli darajada o‘rganilmagan. Shuningdek, bazaviy hujumlar (path finding, cycle finding, state recovery, internal collision) bo‘yicha ham to‘liq tahliliy natijalar mavjud emas. Shu sababli, ushbu tadqiqot Bash-f sponge-funksiyasi asosida autentifikatsiyalangan shifrlash algoritmining barqarorligini baholashga qaratilgan bo‘lib, algoritmning kalitni tiklash, imitovstavka soxtalashtirish va ochiq matnni aniqlash hujumlariga nisbatan chidamliligini aniqlashni maqsad qiladi.

Ushbu tadqiqot natijalari bulutli ma’lumotlar omborlarida saqlanayotgan axborot xavfsizligini oshirish, ma’lumot almashinuvi jarayonida yaxlitlik va autentifikatsiyani ta’minlash hamda real vaqt rejimida ishlovchi kriptotizimlar uchun samarali yechimlarni ishlab chiqishga xizmat qiladi.

ADABIYOTLAR SHARHI

O‘z tadqiqotlarida Guido Bertoni, Joan Daemen, Michaël Peeters va Gilles Van Assche [1] sponge-funksiyalar asosida autentifikatsiyalangan shifrlash algoritmlarini yaratish g‘oyasini taklif etganlar. Ular “Cryptographic Sponge Functions” ishida *absorb–squeeze* modeli, ichki holat (state) strukturasini va xavfsizlikni ifodalovchi parametrlar (r va c) o‘rtasidagi muvozanatni matematik asoslab berganlar. Ushbu konsepsiya keyinchalik Keccak va SHA-3 algoritmlarining nazariy poydevorini yaratgan. Tadqiqotlarda sponge-funksiyalar LRX sinfiga mansubligi, ularni PLIS (FPGA) muhitida yuqori tezlikda amalga oshirish mumkinligi isbotlangan.

David A. McGrew va John Viega [2] o‘z ishlarida *Galois/Counter Mode (GCM)* rejimini ishlab chiqib, autentifikatsiyalangan shifrlashning amaliy modelini yaratganlar. Ularning yondashuvi yordamida AES asosidagi simmetrik shifrlashda bir vaqtning o‘zida maxfiylik va yaxlitlikni ta’minlash mexanizmi joriy etilgan. Ushbu ishlanmalar autentifikatsiyalangan shifrlashni amaliy axborot tizimlarida keng qo‘llashga asos bo‘lgan.

Mihir Bellare, Phillip Rogaway va David Wagner [3] tomonidan ishlab chiqilgan *EAX rejimi* autentifikatsiyalangan shifrlashning nazariy va amaliy jihatlarini yanada mustahkamladi. Ularning tadqiqotlari AEAD (Authenticated Encryption with Associated Data) xavfsizlik modelini matematik asoslab, AE algoritmlarining ishonchliligini isbotlashga qaratilgan.

Alex Biryukov va Adi Shamir [4] tomonidan olib borilgan tadqiqotlarda tradeoff-hujumlar (Time-Memory-Data Tradeoff) oqimli shifrlash algoritmlarining turg‘unligini baholash vositasi sifatida ishlab chiqilgan. Ular ichki holatni tiklash, kalitlarni aniqlash va prefikslar asosida hujum muvaffaqiyat ehtimolini hisoblash bo‘yicha nazariy modellarga asos solganlar. Bu ishlar keyinchalik DK-, BG-, BS- va HBG-hujumlar uchun asos bo‘lgan.

Martin E. Hellman [5] esa klassik Time-Memory Tradeoff (TMTO) modelini kiritgan. U kriptotizimlarda hisoblash murakkabligi va xotira hajmi o‘rtasidagi bog‘liqlikni birinchi bo‘lib matematik tarzda ifodalab bergan. Hellman modeli keyinchalik zamonaviy TMTO va “rainbow table” kabi yondashuvlarning asosi bo‘lgan.

Philippe Oechslin [6] o‘z tadqiqotida TMTO g‘oyasini amaliy jihatdan takomillashtirib, rainbow tables orqali hujumlarning samaradorligini oshirgan. U kalitlarni tiklash jarayonida hisoblash va xotira xarajatlarini sezilarli kamaytiruvchi yondashuvni taklif etgan.

Elaine Barker va Morris Dworkin [7] tomonidan ishlab chiqilgan NIST standarti – *SHA-3 (FIPS 202)* – sponge-funksiyalarga asoslangan kriptografik standart sifatida qabul qilingan bo‘lib, ularning ishlari autentifikatsiyalangan shifrlash algoritmlarining xavfsizlik talablarini rasmiylashtirishga xizmat qilgan.

© N.T. O‘rinov, M.Sh. Akbarova

Bash-f sponge-funksiyasi bo‘yicha olib borilgan tadqiqotlar [8] yangi iteratsion konstruktsiyalarni sinovdan o‘tkazish, tradeoff va bazaviy hujumlarga nisbatan turg‘unlikni matematik baholashga qaratilgan. Bash-f konstruktsiyasi Keccak oilasining optimallashtirilgan varianti sifatida ko‘riladi. Ushbu yondashuv hozirda autentifikatsiyalangan shifrlash tizimlarida, xususan, bulutli ma'lumotlar omborlari xavfsizligini oshirish uchun istiqbolli yo‘nalishlardan biri hisoblanadi.

Autentifikatsiyalangan shifrlash algoritmlarini yaratishning muqobil yondashuvi "*sponge*" turidagi konstruksiyalardan foydalanishdir [11–12]. *Sponge* konstruksiyalari nisbatan yangi kriptografik usullar bo‘lib, ular turli xil kriptografik algoritmlarni yaratishda qo‘llanilishi mumkin.

Sponge-funksiyalar *LRX* sinfiga mansub kriptografik o‘zgartirishlarga kiradi va ularni dasturlashtiriladigan mantiqiy integral sxemalarda (PLIS) samarali va yuqori tezlikda amalga oshirish mumkin. Buning sababi — ushbu funksiyalarda faqat mantiqiy amallar (L), tsiklik siljitishlar (R) va XOR (X) amallari qo‘llaniladi, bu esa zamonaviy telekommunikatsiya tezliklari sharoitida juda muhim hisoblanadi [13–14].

Ishda [15] *Bash-f* deb nomlangan qiziqarli *sponge*-funksiyasi taklif etilgan. Kriptografiya sohasida yangi yechimlarni, xususan *sponge*-funksiyalar asosidagi autentifikatsiyalangan shifrlash algoritmlarini o‘rganish va baholash doimo dolzarbdir, chunki ularni zamonaviy kiberxavfsizlik vazifalarida qo‘llash imkoniyati mavjud.

Axborotni kriptografik himoya qilish usullari va vositalari kiberxavfsizlikni ta'minlash tizimida muhim o‘rin tutadi. Zamonaviy kriptohimoya vositalariga bir qator talablar qo‘yiladi, avvalo — asoslangan barqarorlik va tezkorlik, ya'ni bugungi texnologik talablar darajasiga mos ishlash. Kriptografiya sohasida amaliy qo‘llash uchun taklif etilayotgan barcha yangi yechimlar mos tadqiqotlardan o‘tishi lozim.

Hozirgi kunga qadar mahalliy va xorijiy olimlarning ishlarida *Bash-f sponge*-funksiyasi asosida qurilgan autentifikatsiyalangan shifrlash algoritmining standart hujumlarga nisbatan barqarorligi masalalari yetarli darajada o‘rganilmagan.

Shu sababli ushbu maqolaning maqsadi — *Bash-f sponge*-funksiyasidan foydalangan holda autentifikatsiyalangan shifrlash algoritmining barqarorligini tadqiq etish, xususan, shifrlangan matnni deshifrlash (kalitni tiklash) hujumlariga hamda yaxlitlikni buzish (qalbaki imitatsiya qo‘shimchalari) hujumlariga nisbatan kriptotizimning bardoshliligini baholashdan iboratdir.

Sponge tipidagi iteratsion konstruksiyalardan foydalanish autentifikatsiyalangan shifrlash algoritmlarini yaratishda alternativ yondashuv hisoblanadi. Ushbu yondashuvning asosi sponge-funksiyasiga tayanadi, u esa ichki holat $S \in \{0,1\}^b$ ustida murakkab ikki faol o‘zgarishni amalga oshiradi. Holat S ikki qismga bo‘linadi: $S_r \in \{0,1\}^r$ va $S_c \in \{0,1\}^c$, bunda $b = r + c$ va $S = S_r || S_c$ Bu yerda S_r konstruktsiyaning ochiq qismi, S_c esa yashirin (maxfiy) qismi sifatida qaraladi. Parametrlar $_r$ va $_c$ qiymatlarining turlicha tanlanishi ma'lumotlarni qayta ishlash tezligi va tizimning barqarorligi o‘rtasida muvozanatni belgilaydi: $_r$ qiymatini oshirish va $_c$ ni kamaytirish tezlikni oshiradi, biroq turg‘unlikni pasaytiradi.

USUL

Manba [13] da sponge-algoritmlar uchun kalit K maxfiy saqlanadi va ehtimoliy to‘plam $\{0,1\}^{|K|}$ dan tasodifiy tanlanadi deb faraz qilinadi. Quyidagi xavfsizlik talablari keltirilgan (bu yerda A – ochiq ma'lumotlar yoki sarlavha, C – shifrlangan matn, M – ochiq matn, T – imzovchi kod yoki imitovstavka):

Kalitni tiklab bo‘lmasligi

Hujumchi tomonidan kalitni topish ehtimoli, u n ta kalitni tekshirishi mumkin bo‘lgan holatda, $n * 2^{|K|}$ dan oshmasligi kerak.

Imitatsiya qo‘shimchasini qalbakilashtirishning iloji yo‘qligi

Agar kalitni tiklashning imkoni bo‘lmasa, unda hujumchining har qanday (A, M) juftligi uchun to‘g‘ri imitovstavkani aniqlash ehtimoli $2^{-|T|}$ ga teng bo‘ladi — hatto hujumchiga (A, M)

(cc) BY © N.T. O‘rinov, M.Sh. Akbarova

ga mos keluvchi shifrlangan matn C ma'lum bo'lsa ham. Bundan tashqari, u o'zi tanlagan kirish qiymatlarining (C_i, T_i) juftliklariga mos chiqish qiymatlari (A_i, M_i) ni bilsa ham, bunda $(A_i, M_i) \neq (A, M)$.

Ochiq matnni tiklab bo'lmasligi

Hujumchi uchun M haqidagi (uzunligi haqidagi ma'lumotdan tashqari) har qanday ma'lumotni olishning eng samarali usuli — bu chiqish qiymatlari (C, T) ga mos keluvchi kirish qiymatlari (A, M) ni aniqlashdir. Bunda A hujumchi tomonidan tanlanadi, M esa noma'lum o'zgaruvchi bo'lib, u kalitni tiklash jarayonini ifodalaydi. Hatto hujumchiga mos keluvchi chiqish qiymatlari (C_i, T_i) va ularga mos kirish qiymatlari (A_i, M_i) ma'lum bo'lsa ham, agar $A_i \neq A$ bo'lsa, u holda kalitni tiklash imkoni mavjud emas.

E'tibor bering, ochiq matnni tiklab bo'lmaslik talabi shundan kelib chiqadiki, bitta kalit uchun ikkita turli kirish juftligi $(\mathrm{A}', \mathrm{M}')$ va (A, M) bo'lmasligi kerak, ya'ni $\mathrm{A}' = \mathrm{A}''$ bo'lsa ham, $\mathrm{M}' \neq \mathrm{M}''$holati yuz bermasligi zarur. Shu sababli, bir xil kalit uchun ochiq ma'lumotlarning unikal bo'lishi kriptografik turg'unlik nuqtai nazaridan muhim ahamiyatga ega.

Barqarorlik bahosi shunday taxminga asoslanadiki, *Bash-f sponge*-funksiyasining asosiy o'zgarish funksiyasi F tasodifiy funksiya bilan farq qilmaydi.

Shifrlash algoritmini baholashning asosiy parametrlari odatda uning shifrlangan matnni deshifrlashga (ya'ni shifrlash kalitini tiklashga) qaratilgan hujumlarga nisbatan barqarorligi hamda shifrlash jarayonining tezkorligidir. Natijada, autentifikatsiyalangan shifrlash algoritmida yaxlitlikni buzishga (ya'ni imzo yoki imitovstavkani soxtalashtirishga) qaratilgan hujumlarga nisbatan barqarorlikni baholash mezoni ham qo'shiladi.

Asosan, algoritmning barqarorligi umumiy maqsadli ma'lum hujum turlariga (masalan, kalitlar fazosini to'liq tanlab chiqish yoki tradeoff-turdagi hujumlar [6–8]) hamda aynan shu algoritm uchun maxsus ishlab chiqilgan asosiy hujumlarga nisbatan baholanadi.

Deshifrlashga (shifrlash kalitini tiklashga) qaratilgan hujum shartlari shundan iboratki: hujumchi tasodifiy kirish ketma-ketligini sirli kalit bilan shifrlangan matndan ajratib bera olishi kerak; bunda hujumchi deshifrlash generatoriga murojaat qilishi mumkin (generatorga ajratilishi kerak bo'lgan kirish ketma-ketligini kiritish taqiqlangan) va shuningdek sponge-funktsiyasiga murojaat qilish huquqiga ega bo'ladi.

Yaxlitlikni buzishga (Imitatsiya qo'shimchasini qalbakilashtirishning iloji yo'qligi) qaratilgan hujum shartlari esa shundan iboratki: hujumchi berilgan kirish xabariga mos imitatsiya qo'shimchasi soxtalashi kerak; buning uchun u imitatsiya qo'shimchasi hosil qiluvchi generatorga (kirishga asl xabarni kiritish zarur) yoki sponge-funktsiyasiga murojaat qilishi mumkin.

Autentifikatsiyalangan shifrlashning barqarorligini baholash uchun, hujumchi ma'lum bir turdagi hujumni amalga oshirish sharoitida sezilarli ustunlikka ega emasligini isbotlash kerak.

Agar autentifikatsiyalangan shifrlash ma'lum ochiq matnni shifrlash uchun qo'llanilsa, u holda bu jarayon bloklar bo'yicha gamma hosil qiluvchi joriy algoritm sifatida qaralishi mumkin.

Tradeoff-hujumi oqimli shifrlash algoritmlariga qarshi samarali universal hujumlardan biridir [19]. Ushbu hujum bir tomonlama funksiyani teskari yo'nalishda ishlatish — ya'ni ma'lum tasvir (image) bo'yicha noma'lum preobrazni (preimage) aniqlash uchun qo'llaniladi. Bunday bir tomonlama funksiyalar ichki holatni yoki kalit va algoritmning sinxronizasiyasini chiqish ketma-ketligiga (prefiks deb ataladi) aks ettiradi [16]. Kerakli prefiks uzunligi hujum sinfiga bog'liq. Agar hujum ichki holatni tiklashga qaratilgan bo'lsa, prefiks uzunligi kalit va sinxronizatsiya uzunliklari yig'indisiga teng bo'lishi lozim. Hujumda ishlatiladigan prefikslar bir xil kalitga yoki turli kalitlarga mos bo'lishi mumkin.

Hujum ikki bosqichdan iborat [17]:

– oldindan hisoblash bosqichi, bunda hujumchi algoritmni o'rganib, unga muvofiq ma'lum jadval(lar)ni hosil qiladi;

(cc) BY © N.T. O'rinov, M.Sh. Akbarova

- real vaqt bosqichi (qidiruv bosqichi), bunda chiqish prefikslari kuzatilib, birinchi bosqichda yaratilgan jadvallar yordamida ichki holat yoki kalit tiklanadi.

Tradeoff-hujumini quyidagi parametrlar bilan tavsiflashadi [18]:

N – ichki holatlar va kalitlarning kuchi (qidiruv maydoni hajmi);

P – oldin hisoblash bosqichi uchun vaqt;

M – oldin hisoblangan jadvallarni saqlash uchun kerakli xotira hajmi (hujumchining mavjud xotirasi);

T – real vaqt bosqichi uchun vaqt;

D – hujumni amalga oshirish uchun zarur prefikslar soni;

ψ – hujum muvaffaqiyati ehtimoli.

Hujum muvaffaqiyatli bo'lishi uchun parametrlar ma'lum kompromiss tenglamasiga javob berishi kerak, bu tenglama hujum sinfigiga bog'liq. Odatda hujum muvaffaqiyati ehtimoli $\psi = 0.63$ uchun yechimlar ko'rib chiqiladi.

MUHOKAMA VA TAHLIL

Autentifikatsiyalangan shifrlash algoritmining eng samarali tradeoff-hujumlarga nisbatan barqarorligini tahlil qilamiz.

Hujum maqsadi — sirli kalit $K \in \{0,1\}^l$ ni aniqlash, bu yerda $l \in \{128,256\}$ — xavfsizlik darajasi. Faraz qilaylik, hujum ochiq matn ma'lum bo'lgan holatda (ya'ni gamma ma'lum) amalga oshirilmoqda. Bu holda hujumchiga qidiruv maydonining faqat bir qismi noma'lum bo'ladi: $S(1571 - 2l \ldots) \in \{0,1\}^{2l-8}$— ya'ni$S \in \{0,1\}^{1563}$. Agar qidiruv maydoni S ning qiymatini ba'zi bir vaqtda t da muvaffaqiyatli tiklash mumkin bo'lsa, kalitni ham osonlik bilan aniqlash mumkin.

Manba [19] da BG-hujumi (Brute-Force yoki "zo'ravon kuch" usuli) ko'rib chiqiladi — u barcha mumkin bo'lgan parol variantlarini tekshirishga asoslangan va boshlang'ich holatni tiklashga qaratilgan. BG-hujumining kompromiss tenglamasi:
$TM = N$ bu yerda $M = D,; P = M = N/D$ Ushbu tenglamaning mumkin bo'lgan yechimlaridan biri:

$$T = M = D = P = N^{1/2}$$

Manba [20] da klassik tradeoff-hujumining modifikatsiyasi (uni BS-hujumi deb belgilaymiz) taklif qilingan. Ushbu hujum dastlabki holatni tiklashga qaratilgan. BS-hujumining tenglamasi:

$$T * M^2 * D^2 = N^2$$

bu yerda $P = N/D,\ 1 \le D^2 \le T,\ N$ — kalitlar to'plamining hajmi. Ushbu tenglama uchun mumkin bo'lgan yechimlardan biri:

BG va *BS* hujumlari ichki holatni tiklashga qaratilgan. Agar kalit va sinxronizatsiya uzunliklarining yig'indisi ichki holat o'lchamidan kichik bo'lsa, bunday hujumlarning yanada samarali modifikatsiyalari ishlatiladi. Masalan, manba [6] da *BG* va *BS* hujumlarining kalitni bir kalit ostida, ammo turli sinxronizatsiyalarda olingan prefikslar orqali tiklashga yo'naltirilgan modifikatsiyalari (mos ravishda *HBG* va *HBS* deb ataymiz) keltirilgan. Kalit uzunligi k, sinxronizatsiya uzunligi ν va kalitlar to'plami kuchi N bo'lganda, ushbu modifikatsiyalar uchun yechimlar:

$$(P, D, M, T) = (N^{1/2}, N^{1/2}, N^{1/2}, N^{1/2}), \quad (1)$$

bu yerda $P = 2^{(k+\nu)/2} < 2^k$ agar $k > \nu$;

$$(P, D, M, T) = (N^{2/3}, N^{1/3}, N^{1/3}, N^{2/3}), \quad (2)$$

bu yerda $P = 2^{(k+\nu)/3} < 2^k$ *agar* $k > 2\nu$;

$$(P, D, M, T) = (N^{3/4}, N^{1/4}, N^{1/2}, N^{1/2}), \quad (3)$$

bu yerda $P = 2^{(k+\nu)/4} < 2^k$ agar $k > 3\nu$.

Formulalar (1) va (2) *HBG*-hujumlariga, (3) esa *BS*-hujumiga mos keladi.

Manba [7] da *BS*-hujumining yana bir modifikatsiyasi (uni *DK*-hujum deb ataymiz) tasvirlangan — u turli kalitlarda, lekin bir xil sinxronizatsiyada olingan prefikslar orqali kalitni tiklashga qaratilgan. Bunday hujum uchun kompromiss tenglamasi:

$$T * M^2 * D^2 = N^2$$

bu yerda $1 \le D^2 \le T, P = N/D, N$ — kalitlar to'plami kuchi. Ushbu tenglama uchun mumkin bo'lgan yechimlardan biri:

$$(P, D, M, T) = (N^{2/3}, N^{1/3}, N^{1/3}, N^{2/3});$$

© N.T. O'rinov, M.Sh. Akbarova

$(P, D, M, T) = (N^{3/4}, N^{1/4}, N^{1/2}, N^{1/2})$.

Jadval 1 va 2 da tadqiq etilayotgan algoritmga nisbatan ayrim tradeoff-hujumlarning xususiyatlari keltirilgan, u yerda mustahkamlik darajasi $l = 128$ va $l = 256$ uchun *HBG*-hujumida sinxronizatsiya uzunligi $\nu = 1/2$ deb olingan.

1-jadval.

$l = 128$ qarshilik darajasi uchun murosaga kelish hujumlarining xususiyatlari

Hujum	***N***	***T***	***M***	***D***	***P***
BG	2248	2124	2124	2124	2124
BS	2248	2124	2124	262	2186
HBG	2192	296	296	296	296
DK	2128	285.3	242.7	242.7	285.3

2-jadval.

$l = 256$ qarshilik darajasi uchun murosaga kelish hujumlarining xususiyatlari

Hujum	*N*	*T*	*M*	*D*	*P*
BG	2504	2252	2252	2252	2252
BS	2504	2252	2252	2126	2378
HBG	2384	2192	2192	2192	2192
DK	2256	2170.7	285.3	285.3	2170.7

Quyidagi ma'lumotlardan ko'rinib turibdiki, eng yaxshi xususiyatlarga *DK*-hujum ega. *DK*-hujumining hisoblash murakkabligi "zo'ravon kuch" (brute-force) hujumidan kichik bo'lsa-da, muvaffaqiyatli hujum uchun talab qilinadigan xotira hajmi va prefikslar soni ancha katta. Shuning uchun uning amaliy qo'llanilishi kam ehtimoliy hisoblanadi.

Endi algoritmning bazaviy hujumlarga (basic attacks) nisbatan mustahkamligini ko'rib chiqamiz.

Manba [13] da *sponge*-funktsiyalar bazaviy hujumlarga nisbatan mustahkamligi o'rganilgan — bu yerda F funksiyasiga nisbatan oldindan hech qanday taxmin yo'q. Tadqiqotda hujumchi F ga (agar F funksiya bo'lsa, shu jumladan F^{-1}ga) β dan ortiq bo'lmagan chaqiruvlar (queries) amalga oshirishi mumkin deb faraz qilingan. Algoritm mustahkamligi quyidagi bazaviy hujumlar nuqtai nazaridan ko'rib chiqilgan:

- Yo'llarni qidirish (path finding). Algoritmdan "so'rilish" (absorb) bosqichi o'tgach, berilgan ichki holatga olib keluvchi qatorni topish kerak. Agar F — bijektsiya bo'lsa, hujum muvaffaqiyati ehtimoli $\beta^2/2^{c+2}$ ga teng.
- Sikllarni topish (cycle finding). To'g'ri kirishlar ostida chiqish ketma-ketliklarida sikllarni izlash amalga oshiriladi. Agar F — bijektsiya bo'lmasa, hujum muvaffaqiyati ehtimoli $\beta^2/2^{c+r+1}$ ga teng.
- Holatni tiklash (state recovery). Berilgan qator Z uchun unga mos keluvchi holat S tiklanadi. Hujum muvaffaqiyati ehtimoli$\beta/2^c$.
- Chiqishni bog'lash (output linking). Berilgan Z uchun mos chiqishni beruvchi holat S qidiriladi; bunday holat mavjudligi kafolatlanmaydi. Hujum muvaffaqiyati ehtimoli $\beta/2^{|Z|-r}$.
- Ichki kolliziya (internal collision). "So'rilish" bosqichi natijasida ichki holatlari bir xil bo'ladigan ikki qatorni topish uchun qidiruv o'tkaziladi (tashqi holatlar farq qilishi mumkin). Hujum muvaffaqiyati ehtimoli $\beta^2/2^{c+1}$.

Sponge-funktsiyaning bunday hujumlarga nisbatan zaifligi uning holati cheklangan bo'lgani bilan izohlanadi — shu bois hujumlar tashqi o'zgarishlarga chidamli emas. Bazaviy hujumlar uchun muvaffaqiyat ehtimolliklari sponge-funktsiyaning mustahkamligi bo'yicha yuqori cheklovlarni beradi. Bir muvaffaqiyatli hujum uchun kerakli minimal chaqiruvlar soni β — $O(2^{c+2})$.

Kalitga bog'liq rejimlar uchun quyidagi hujumlar ko'rib chiqiladi.

- Gamma (keystream) ni prognoz qilish. Agar joriy holatni qayta tiklash bo'yicha hujum muvaffaqiyatli amalga oshirilgan bo'lsa va ochiq gamma qismining ma'lum qismi mavjud bo'lsa, gamma-ning boshqa qismi prognoz qilinadi. Kutilayotgan F chaqiruvlar soni $2^{c/2}$ ga teng; agar $l \leq c$ bo'lsa, bu hujum umuman xavf tug'dirmaydi.
- Soxta imitatsiya qo'shimchasi. Joriy holatni tiklash hujumiga muvaffaqiyatli ega bo'lingach, «xabar+imitovstavka» —

(cc) BY © N.T. O'rinov, M.Sh. Akbarova

«imitovstavka» juftliklarini kuzatish orqali yangi xabarga imitovstavka (imzo)ni soxtalashtirish mumkin. F funksiyasiga murojaatlarining kutilgan soni $2^{r+c-n}/(m+1)$ ga teng, bunda m — kuzatilgan xabarlar soni, n — imitovstavka uzunligi. Agar $l \leq c - \log_2(m)$ bo'lsa, hujum xavf tug'dirmaydi. Agar $m = 2^{c/2}$ deb olinsa, unda baho $c \geq 2l$. Imitovstavkani soxtalashtirishning yana bir usuli — kalitli *sponge*-funktsiyaning ichki kolliziyasini qidirishdir. Bunda kuzatiladigan bloklar sonining kutilgan qiymati $2^{c/2}$ ga teng. Ichki kolliziya aniqlangandan so'ng imitovstavkalar osonlik bilan hisoblanishi mumkin.

Olingan natijalar tadqiq etilayotgan autentifikatsiyalangan shifrlash algoritmi mustahkam ekanligini ko'rsatadi. Oldinroq ushbu algoritmning ijrosi bo'yicha olingan tezlik baholarini hisobga olsak [10], sponge-funktsiyasiga asoslangan ushbu sinf algoritmlari kiberxavfsiz muhit yaratishda istiqbolli bo'lishi mumkin, deb aytish mumkin.

XULOSA

Tadqiqot natijalari shuni ko'rsatdiki, bulutli ma'lumotlar omborlarida axborot xavfsizligini ta'minlashda an'anaviy shifrlash algoritmlari yetarli darajada samarali emas, chunki ular faqat maxfiylikni kafolatlaydi, ammo yaxlitlik va autentifikatsiya masalalarini to'liq qamrab olmaydi. Shu sababli, autentifikatsiyalangan shifrlash (AE) texnologiyasi bulutli infratuzilmalarda ma'lumotlarni kompleks himoya qilishning muhim yo'nalishlaridan biri sifatida e'tirof etiladi.

Tadqiqot davomida Bash-f sponge-funksiyasi asosida autentifikatsiyalangan shifrlash algoritmining barqarorligi tahlil qilindi. Ushbu yondashuvning asosiy ustunligi — ma'lumotlarni qayta ishlash tezligi bilan xavfsizlik darajasi o'rtasida optimal muvozanatni ta'minlashidadir. Tahlil jarayonida kalitni tiklash, imitovstavka (imzo)ni soxtalashtirish va ochiq matnni qayta tiklash kabi hujum turlariga nisbatan algoritmning bardoshliligi baholandi.

Natijalar shuni ko'rsatdiki, Bash-f sponge-funksiyasi asosidagi autentifikatsiyalangan shifrlash algoritmi tradeoff-hujumlar (BG, BS, HBG, DK) va bazaviy hujumlar (path finding, cycle finding, state recovery, internal collision) ga nisbatan yuqori darajada mustahkamlik namoyish etdi. Ayniqsa, DK-hujum bilan solishtirganda, Bash-f asosidagi konstruksiya hisoblash murakkabligini sezilarli darajada oshiradi va amaliy sharoitda bunday hujumlarni amalga oshirishni deyarli imkonsiz qiladi.

Shuningdek, tadqiqot davomida shifrlash tizimining ichki holat o'lchamlari va kalit uzunligining o'zaro bog'liqligi tahlil qilinib, 2^{-128} va 2^{-256} xavfsizlik darajalari uchun optimal parametrlar to'plami aniqlangan. Bu natijalar Bash-f asosidagi autentifikatsiyalangan shifrlashni real vaqt rejimida ishlaydigan bulutli tizimlar, axborot omborlari, hamda Internet orqali ma'lumot almashish platformalarida qo'llash imkonini beradi.

Umuman olganda, tadqiqot sponge-funksiyalar asosidagi autentifikatsiyalangan shifrlash algoritmlarining amaliy ahamiyatini asoslab berdi va ularning kiberxavfsizlikni ta'minlashdagi istiqbolliligini ko'rsatdi. Kelgusida ushbu yondashuvni boshqa kriptografik modellar — masalan, hashlash, raqamli imzo yoki post-kvant kriptotizimlari bilan integratsiyalash orqali yanada mukammallashtirish imkoniyati mavjud.

ADABIYOTLAR

1. Bertoni, G., Daemen, J., Peeters, M., & Van Assche, G. (2011). The Keccak reference. Submission to NIST (Round 3).
2. McGrew, D. A., & Viega, J. (2004). The Galois/Counter Mode of operation (GCM). Submission to NIST. https://csrc.nist.gov
3. Whiting, D., Housley, R., & Ferguson, N. (2003). Counter with CBC-MAC (CCM). NIST Submission. https://csrc.nist.gov
4. Bellare, M., Rogaway, P., & Wagner, D. (2003). EAX: A conventional authenticated-encryption mode. In FSE 2003 (pp. 389–407). Springer.
5. Bertoni, G., Daemen, J., Peeters, M., & Van Assche, G. (2011). Cryptographic sponge functions. https://keccak.team
6. Author(s) unknown. (n.d.). Bash-f: A sponge-based cryptographic function (technical report/preprint). [Update with correct authorship & venue].

(cc) BY © N.T. O'rinov, M.Sh. Akbarova

7. Hellman, M. E. (1980). A cryptanalytic time-memory trade-off. IEEE Transactions on Information Theory, 26(4), 401–406.
8. Biryukov, A., & Shamir, A. (2000). Cryptanalytic time/memory/data tradeoffs for stream ciphers. In ASIACRYPT 2000 (pp. 1–13). Springer.
9. Oechslin, P. (2003). Making a faster cryptanalytic time-memory trade-off. In CRYPTO 2003 (pp. 617–630). Springer.
10. Dworkin, M. (2015). SHA-3 Standard: Permutation-based hash and extendable-output functions (FIPS 202). NIST.
11. Митяков А.В. Разработка методологий ориентированных на архитектуру облачных хранилищ данных / А.В. Митяков, Ю.С. Татаринов // Информационные технологии моделирования и управления. 2011. № 2. С. 221-227.
12. Земцов И.А. Использование семантической сети для выбора знаний с целью обеспечения информационной безопасности интеллектуальных систем / И.А. Земцов, О.Г. Иванова, Ю.В.Минин, С.В. Данилкин // Информация и безопасность. 2020. Т. 23. Вып. 2. С. 261–268.
13. Гомаш М. Генерация Пуасонновского ключа с помощью криптосистемы для безопасности облачного хранилища данных / М. Гомаш, С. Прасанна // Журнал перспективных исследований в области динамических систем и систем управления. 2018. №10. С. 804–817.
14. Громов Ю.Ю. Размещение узлов сетевой информационной системы с комбинаторной топологией с целью повышения эффективности защиты информации в условиях неопределенности / Ю.Ю. Громов, Ю.В. Минин, С.А. Копылов // Информация и безопасность. 2019. Т. 22. Вып. 2. С. 272–279.
15. Максимовский А.Ю. О выборе параметров автоматных моделей мониторинга информационной безопасности сетевых объектов (часть 2) / А.Ю. Максимовский // Информация и безопасность. 2020. Т. 23. №. 3. С.327-336.
16. Хан К. Смена обмена данными по безопасности и эффективности для облачного хранилища / К. Хан, К. Ли, З. Дэн // Хаос. 2016. № 86. С. 107–116.
17. Арки О. Многоагентная среда безопасности для облачного хранилища данных / О. Арки, А. Зитуни //Мультиагентные и сетевые системы. 2017. №14 (4). С. 357–382.
18. Громов Ю.Ю. Построение непрерывных законов распределения для оценки рисков в информационных системах / Ю.Ю. Громов, Ю.В. Минин, В.Е. Дидрих, Н.Г. Шахов, С.А, Копылов // Информация и безопасность. 2019. Т. 22. Вып. 1. С. 86–91.
19. Громов Ю.Ю. Формализованное представление и классификация конфликтов тренажной подготовки операторов эрготехнических радиоэлектронных средств / Ю.Ю. Громов, И.Н. Ишук, А.Н. Потапов // Приборы и системы. Управление, контроль, диагностика. 2019. Вып. 2. С. 44–50.
20. Симановский Е.А. Метод повышения безопасности передачи данных в сети интернет/Е.А.Симановский, М.А.Макаров // Информатизация образования и науки. 2021. № 2. С. 22–36.

© N.T. O'rinov, M.Sh. Akbarova