SIMMETRIK BLOKLI SHIFRLASH ALGORITMLARIGA BARDOSHLI S-BLOKLARNI GENERATSIYA QILISH MUAMMOLARI

Abdurazzoqov Javohir Rustamovich
Raqamli texnologiyalar va sun’iy intellektni rivojlantirish ilmiy-tadqiqot instituti,
https://doi.org/10.5281/zenodo.7857170

Abstract. *The use of the S-box is an important component of many symmetric block cipher algorithms used in modern cryptography. However, creating durable S-blocks that can resist various cryptanalysis methods is a complex problem. In this paper, we describe the challenges of achieving randomness and nonlinearity in the design of S-blocks, and the challenges of generating large numbers of these blocks to ensure security. By analyzing these issues, we discussed the challenges of creating robust S-blocks in symmetric block cipher algorithms and the importance of careful design and testing in achieving strong security.*

Keywords: *Symmetric encryption algorithms, block encryption, S-block, P-block, cryptography, generation, nonlinearity.*

Kirish

Zamonaviy kriptografiyada blokli shifrlash axborot xavfsizligini ta’minlovchi algoritmlarning muhim tarkibiy qismidir, chunki u maxfiy kalit bilan shifrlash orqali ma'lumotlarning maxfiyligi va yaxlitligini ta'minlaydi.

Simmetrik blokli shifrlash - ma'lumotlarning ma’lum bir bitli uzunlikdagi bloklarida ishlaydigan shifrlash algoritmining turidir. Ochiq matn belgilangan o'lchamdagi bloklarga bo'linadi va shifrlash algoritmi maxfiy kalit yordamida har bir bloklarda shifrlanadi. Shifrlash algoritm orqali chiquvchi natija berilgan ochiq matn bilan bir xil uzunlikka ega bo'lgan shifrmatndir.

Blok shifrlash shifrlari yuqori darajadagi xavfsizlikni ta'minlaydi va xavfsiz aloqa, elektron bank va raqamli imzolar kabi ko'plab kriptografik ilovalarda qo'llaniladi. Eng keng tarqalgan blokli shifrlash shifrlaridan ba'zilari AES (Advanced Encryption Standard), DES (Data Encryption Standard), and 3DES (Triple Data Encryption Standard).

AES shifrlash simmetrik kalitli shifrlash algoritmi bo'lib, u 128 bit blok o'lchamidan foydalanadi va 128, 192 yoki 256 bit uzunlikdagi kalitlarni qo'llab-quvvatlaydi. U simsiz xavfsizlik, elektron to'lov tizimlari va VPN kabi ko'plab ilovalarda keng qo'llaniladi.

DES shifrlash simmetrik kalitli shifrlashning yana bir algoritmi bo'lib, blok o'lchami 64 bit va kalit o'lchami 56 bitdan iborat. U ko'p yillar davomida keng qo'llanilgan, ammo hozirda kalit uzunligi qisqa bo'lgani uchun xavfli hisoblanadi.

3DES shifrlash DESga nisbatan takomillashtirildi va algoritm xavfsizligini oshirish uchun shifrlashning uch bosqichidan foydalanadi. U 64 bitli blok o'lchamidan va 168 bitli kalit hajmidan foydalanadi, bu DESga qaraganda yuqori darajadagi xavfsizlikni ta'minlaydi.

Blok shifrlash shifrlari ma'lumotlarning maxfiyligi, yaxlitligi va haqiqiyligini ta'minlash uchun mo'ljallangan. Ular bunga almashtirish, almashtirish va diffuziya kabi turli usullardan foydalanish orqali erishadilar. O'zgartirish - almashtirish jadvali yordamida ochiq matnni shifrlangan matn bilan almashtirishni o'z ichiga oladi, almashtirish esa ochiq matnning bitlarini qayta tartibga solishni o'z ichiga oladi. Diffuziya ochiq matnning bir bitining ta'sirini shifrlangan matnning ko'p bitlariga tarqatishni o'z ichiga oladi.

Kriptobardoshli shifrlash algoritmlarni ishlab chiqishda uning asosiy qismlaridan biri chiziqsiz akslantirishdan iborat S-blok muhim hisoblanadi. S-blok Feystel yoki SP tarmoqqa asoslangan simmetrik shifrlash algoritmlar standartlarida keng qo‘llaniladi [1,2]. Bardoshli kriptografik algoritmlarni loyihalashda kuchli S-blok ochiq matnning shifrmatn bo‘ylab yaxshi diffuziyasini ta’minlaydi, bu ochiq matn va shifrlangan matn o‘rtasidagi munosabatni aniqlashni qiyinlashtiradi. Shifrlash algoritmlarini ishlab chiqishda statik va dinamik S-bloklardan foydalaniladi.

Blokli shifrlashning asosiy operatsiyasi nochiziq akslantirish qiymatlari (S-blok) va chiziqli akslantirish qiymatlari (P-blok) dan iborat bo'lgan almashtirish-o'zgartirish tarmog'i (SP tarmoq) yoki Feystel tarmog’iga asoslangan shifrlash algoritmlarda ishlatiladi. S-blok har bir kirish bitlari qiymatini mos keladigan chiqish qiymatga chiziqsiz almashtiradi, P-blok esa S-blokldan chiquvchi qiymatlarini chiziqli akslantirish orqali aralashtirib yuboradi. Mazkur jarayonlarning kombinatsiyasi kiruvchi ochiqmatn va kalit bitlarini shifrmatn bo’ylab chalkashishini va tarqalishni ta'minlaydi. Bu esa tajovuzkorlarga shifrlangan matnni tahlil qilishni va ochiq matnni tiklashni qiyinlashtiradi.

Bardoshli S-bloklarni loyihalash muammolari.

Blokli shifrlash standartlari uchun bardoshli S-blok loyihalash ilmiy tomonlama qiyin vazifalardan biri hisoblanadi. Zaif S-bloklar shifrlash algoritmlari uchun xavfsizlik muammolarini keltirib chiqarishi mumkin. Agar S-blok turli mezonlarga asoslangan holda ishlab chiqilmagan bo'lsa, u differentsial kriptoanaliz, chiziqli kriptotahlil va algebraik kriptotahlil kabi turli xil hujumlarga bardosh bera olmasligi mumkin. Shuning uchun, hujumlar va tahlillarga bardoshli S-bloklarni loyihalash blokli shifrlash algoritmlarining xavfsizligi uchun juda muhimdir. Bardoshli S-bloklarni ishlab chiqarishda yuzaga keladigan ba'zi muammolar:

Xavfsizlik: S-bloklarni loyihalashda asosiy masala ularning hujumlarga qarshi xavfsizligini ta'minlashdir. S-bloklarning differentsial kriptotahlil, chiziqli kriptoanaliz va qo'pol kuch hujumlari kabi turli xil hujumlarga chidamliligini ta'minlash muhimdir.

Statistik xususiyatlar: S-bloklar chiqishda noaniqliklarga yo'l qo'ymaslik uchun yaxshi statistik xususiyatlarga ega bo'lishi kerak. S-bloklar chiqish qiymatlarining bir xil taqsimlanishiga ega bo'lishi kerak va ularning chiqishi kirishdan mustaqil bo'lishi kerak. Agar chiqish kirishdan mustaqil bo'lmasa, tajovuzkor kalit yoki ochiq matn haqida ma'lumot olish uchun undan foydalanishi mumkin.

Tezlik: S-bloklar tez va samarali bo'lishi uchun mo'ljallangan bo'lishi kerak. Sekin S-bloklar butun shifrlash tizimining ishlashiga ta'sir qilishi mumkin.

Chidamlilik: S-bloklar bardoshli bo'lishi va uzoq vaqt davomida hujumlarga qarshi turishi uchun mo'ljallangan bo'lishi kerak. Agar S-bloklar bardoshli bo'lmasa, tajovuzkor shifrlash tizimini buzish uchun S-bloklardagi zaif tomonlardan foydalanishi mumkin.

Kriptografik kalitlarni boshqarish: S-bloklar odatda kriptografik kalitlarni boshqarish usullari yordamida yaratiladi. Shuning uchun S-bloklarining xavfsizligi kalitlarni boshqarish tizimining xavfsizligiga bog'liq. Kalitlarni boshqarish tizimidagi har qanday zaifliklar S-bloklari va butun shifrlash tizimining xavfsizligini buzishi mumkin.

S-bloklar kirish(bit)ini chiqish(bit)iga nochiziqli bo’lishini ta’minlash uchun mo'ljallangan, ya'ni S-blokining chiqish(bit)i kirish(bit)ning chiziqli funktsiyasi sifatida ifodalanishi mumkin emas. Agar S-blok chiziqli bo'lsa, u butun shifrlash algoritmining

xavfsizligini buzishi mumkin bo'lgan chiziqli kriptoanaliz yordamida osongina hujum qilinishi mumkin.

Differentsial kriptotahlil - bu ochiq matn juftlari va ularga mos keladigan shifrlangan matnlar orasidagi farqni solishtirish orqali blokli shifrlarning xavfsizligini tahlil qilish usuli. Yetarli nochiziqlikka ega bo'lmagan S-bloklari differensial kriptoanalizga nisbatan zaif bo'lishi mumkin [3].

Ushbu muammolarni yetarlicha bartaraf etish uchun S-bloklarni sinchkovlik bilan loyihalash va bardoshliligini tekshirish kerak. Ularning yetarli darajada chiziqsizligini ta’minlash va turli mezonlarga testlash mavjud hujumlarga chidamliligini ta'minlaydi.

S-bloklarni loyihalash usul(algoritm)lari.

Kriptografik algoritmlarda foydalanish uchun S-bloklarini yaratish uchun turli xil algoritmlar qo'llaniladi. Ko'p ishlatiladigan algoritmlardan ba'zilarini keltiramiz:

Tasodifiy tanlash: Ushbu usul kirish va chiqish qiymatlarini tasodifiy almashtirish orqali S-blok hosil qiladi. Ushbu yondashuv oddiy usul hisoblanadi va turli xil hujumlarga qarshi himoyasiz bo'lgan S-bloklarni keltirib chiqarishi mumkin [4].

Mantiqiy funktsiyalar: Bu algoritm S-blokni yaratish uchun mantiqiy funktsiyalardan foydalanadi. Mantiqiy funktsiyalar ma'lum kriptografik xususiyatlar asosida tanlanadi, masalan, yuqori nochiziqlik hamda chiziqli va differentsial kriptoanalizga tekshirish orqali generatsiya qilinadi.

Evolyutsion (Genetik) algoritmlar: Bu algoritm muayyan xavfsizlik talablariga javob beradigan S-blokni qidirish uchun genetik algoritmdan foydalanadi. Algoritm S-bloklarining populyatsiyasini hosil qiladi va fitnes funksiyasi asosida ularning yaroqliligini baholaydi. Agar natija qanoatlantirsa generatsiya qilingan S-blok natija sifatida chiqariladi va algoritm generatsiya qilishdan to‘xtaydi. Aks holsa yangi avlod nomzodlarini yaratish uchun eng mos S-bloklar tanlanadi. Generatsiya qilish davom etadi.

Algebraik hisoblashlar orqali yaratiluvchi konstruktsiyalar: Bu algoritmlar S-blokni yaratish uchun chekli maydonlar va Galua maydoni kabi algebraik tenglamalar va funksiyalardan foydalaniladi. Ushbu konstruktsiyalar yuqori nochiziqlik hamda chiziqli va differentsial kriptoanalizga qarshilik kabi ma'lum kriptografik xususiyatlar asosida tanlanadi. 2018 yilda B. F. Abduraximov va A. B. Sattarovlar tomonidan “S-blokni ifodalovchi algebraik tenglamalar sistemasini qurish algoritmi nomli maqolasida” blokli simmetrik shifrlash algoritmlarida foydalaniluvchi o‘rniga qo‘yish (S-blok) jadvalini ifodalovchi ikkinchi darajali chiziqsiz tenglamalar sistemasini qurish usuli taklif etilgan [5].

Sun’iy neyron tarmoqlar orqali generatsiya qilish: Bu algoritm S-blokni yaratish uchun sun’iy neyron tarmoqdan foydalanadi. Neyron tarmoq almashtirish operatsiyasini o'rganish uchun ochiq matn-shifr matn juftlarining katta ma'lumotlar to'plamida o'qitiladi. Ushbu yondashuv yuqori samarali S-bloklarni yaratishga olib kelishi mumkin bo'lsa-da, ularning xavfsizligini tahlil qilish va tekshirish qiyin. Hisoblashlar uchun katta ma’lumot bazalari va o‘qitish uchun kuchli hisoblash qurilmalaridan foydalanish kerak [6].

Xulosa:

S-box-ni ishlab chiqish usulini tanlash kriptografik algoritmning o'ziga xos talablariga va zarur bo'lgan xavfsizlik darajasiga bog'liq. Har bir yondashuvning o'ziga xos afzalliklari va kamchilliklari mavjud bo’lib eng yaxshi yondashuv usullarda amalga oshiriladigan

kombinatsiyalardan kelib chiqqan holda tanlash mumkin. Umuman olganda, yuqori darajadagi xavfsizlikni ta'minlaydigan usullar hisoblash quvvatlari qimmat va keng masshtabdagi hisoblashni talab qilgani uchun ancha qiyindir, amalga oshirish osonroq bo'lgan algoritmlarning esa xavfsizlik darajasi pastroq bo'lishidir. Shu sababli, umumiy kriptografik tizimning samaradorligini ta'minlash uchun hosil bo'lgan S-bloklarning xavfsizligini sinchkovlik bilan baholash va tahlil qilish juda muhimdir.

REFERENCES

1. H. Feistel, W. A. Notz and J. L. Smith, "Some cryptographic techniques for machine-to-machine data communications," in Proceedings of the IEEE, vol. 63, no. 11, pp. 1545-1554, Nov. 1975, doi: 10.1109/PROC.1975.10005
2. Biryukov, A. (2005). Substitution–Permutation (SP) Network. In: van Tilborg, H.C.A. (eds) Encyclopedia of Cryptography and Security. Springer, Boston, MA . https://doi.org/10.1007/0-387-23483-7_420
3. Kim, Jongsung & Hong, Seokhie & Sung, Jaechul & Lee, Sangjin & Lim, Jongin & Sung, Soohak. (2003). Impossible Differential Cryptanalysis for Block Cipher Structures. 2904. 105-132. 10.1007/978-3-540-24582-7_6.
4. Zivkovic, Miodrag & Lambic, Dragan. (2013). Comparison of random S-Box generation methods. Publications de l'Institut Mathematique. 93. 109-115. 10.2298/PIM1307109L.
5. Abduraximov, B. F. S-blokni ifodalovchi algebraik tenglamalar sistemasini qurish algoritmi / B. F. Abduraximov, A. B. Sattarov // Проблемы вычислительной и прикладной математики. – 2018. – No 2(14). – P. 132-145. – EDN KYSDAD.
6. M. N. A. Noughabi and B. Sadeghiyan, "Design of S-boxes based on neural networks*," 2010 International Conference on Electronics and Information Engineering, Kyoto, Japan, 2010, pp. V2-172-V2-178, doi: 10.1109/ICEIE.2010.5559741.