SM4 shhifrlash algoritmidagi S-blokning tuzilishi va matematik tahlili

Kalbayev Davran Niyetbayevich

Mirzo Ulug‘bek nomidagi O‘zbekiston milliy universiteti

Amaliy matematika (sohalar boyicha) fakultetining

2-kurs magistratura talabasi:

Tel: (93) 365-08-06

Mail address: davranqalbaev@gmail.com

Anotatsiya: Bu tezisda AES vaSM4 shifrlash algoritmning asosiy qismi bolgan S-blokning tuzilishi va matematik modellashtirish ko‘rib chiqildi.

Kalit soz: SM4, affin transformatsiya, Galois moydani, GF (2^8)

Kirish

SM4 – Xitoy tomonidan ishlab chiqilgan 128-bitli blokli shifrlash algoritmi bo‘lib, Xitoyning raqamli xavfsizlik standartlari uchun ishlatiladi. Algoritmning muhim komponentlaridan biri – **S-blok** (Substitution-box) bo‘lib, u chiziqli bo‘lmagan almashtirishlarni amalga oshiradi va shifrlash jarayonida xavfsizlikni oshirishga yordam beradi. Ushbu maqolada SM4 shifrlash algoritmidagi S-blok tuzilishi, uning matematik asosi, chiziqli va chiziqli bo‘lmagan transformatsiyalari tahlil qilinadi.

S-boxning umumiy tuzilishi

S-box kiruvchi baytni boshqa baytga o‘zgartirish orqali amalga oshiriladigan chiziqli bo‘lmagan transformatsiya funktsiyasi sifatida ishlaydi. S-boxning ishlash jarayoni ikki asosiy qismdan iborat:

1.1 Galois maydonida teskari element olish **(GF(2^8))**

1.2 Affine transformatsiya**.**

1.1 Galois maydonida teskari element olish

SM4 S-boxi baytlarni Galois maydonida (GF(2^8))teskari elementga o‘zgartiradi. Har bir baytni Galois maydoni sifatida ifodalash mumkin va bu operatsiya quyidagicha amalga oshiriladi:

$$x^{-1} \mod p(x)$$

Bu yerda $p(x) = x^8 + x^4 + x^3 + x + 1$ – **irreducible polinom** bo‘lib, u AES va SM4 algoritmlarida ishlatiladi.

Galois maydonida har bir bayt:

$$x = a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x^1 + a_0x^0$$

bu yerda a_i koeffitsyentlar har bir bitni ifodalaydi va ular 0 yoki 1 qiymatga ega boladi.

Misol sifatda, bayt 63_{16} ni olamiz:

$$63_{16} = 01100011_2$$

bu baytni GF(2^8) maydonida teskari qiymatga o‘zgartirish natijasida boshqa baytga o‘zgartiriladi.

1.2 Affine transformatsiya

Affine transformatsiya – Galois maydonidagi teskari elementga chiziqli kombinatsiya qo‘llanadigan operatsiyadir. Bu transformatsiya S-boxda chiziqli bo‘lmagan almashtirishni kuchaytiradi va shifrlash jarayonidagi xavfsizlikni oshiradi.

Affine transformatsiya matematik ko‘rinishda quyidagicha ifodalanadi:

$$y = M \bullet x + b$$

bu yerda:

- M – oldindan aniqlangan 8x8 o‘lchamdagi matritsa;
- x – teskari element (8-bitli vector ko‘rinishida)
- b – doimiy vektor (constant)

Affine transformatsiya uchun matritsa**:**

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

Affine transformatsiya uchun konstantalar (vektor b):

$$b = (1,1,0,0,0,1,0,1)$$

Affine transformatsiyada har bir bit uchun operatsiya quyidagicha amalga oshiriladi:

$$y_i = \bigoplus_{j=0}^{7} M_{i,j} \bullet x_j \oplus b_i \qquad (i = 0,1,2,3, \dots 7)$$

Bu yerda har bir kiruvchi bayt x, 8 bitli vektor sifatida ifodalanadi va matritsa bilan ko‘paytiriladi, so‘ngra konstant bilan qo‘shiladi.

S-box algoritmi quyidagi qadamlar asosida ishlaydi:

1. Kiruvchi baytni teskari elementga o‘zgartirish: Har bir kiruvchi bayt x, Galois maydonida x^{-1} ga o‘zgaradi. Agar bayt 0 bo‘lsa, teskari element o‘zini saqlab qoladi.

2. Affine transformatsiya: Teskari element olingandan so‘ng, u yuqoridagi M matritsa va b konstant vektori orqali affine transformatsiyadan o‘tadi.

3. Chiqish baytini olish: Har bir kiruvchi bayt S-box orqali o‘tib, chiqish baytiga aylanadi.

Jadval va formulalar bilan chiziqli o‘zgarishlar

S-box transformatsiyasi har bir kiruvchi baytni o‘zgartiradi. Quyida S-box o‘zgarish jadvalining bir qismi keltirilgan:

Kirish (16 lik)	Chiqish(16 lik)
00	63
01	7c
02	77
03	7b
…	…
ff	16

Jadvalda har bir kiruvchi bayt (hexadecimal ko‘rinishda) o‘ziga mos chiqish baytiga almashtiriladi.

Chiziqli o‘zgarish

SM4 algoritmi doirasida chiziqli o‘zgarishlar quyidagi formulalar orqali amalga oshiriladi:

$$L(B) = B \oplus (B \ll 2) \oplus (B \ll 10) \oplus (B \ll 18) \oplus (B \ll 24)$$

bu yerda << - chapka tsikllik surish operatori.

Xulosa

SM4 shifrlash algoritmining S-box qismi Galois maydonida teskari element olish va affine transformatsiya orqali chiziqli bo‘lmagan almashtirishni amalga oshiradi. S-box, blokli shifrlashning xavfsizligini oshiruvchi muhim komponent hisoblanadi. Chiziqli bo‘lmagan transformatsiyalar va chiziqli o‘zgarishlar bilan kombinatsiyalangan S-box algoritmi SM4’ning murakkabligini oshiradi va unga qarshi xurujlarga barqaror bo‘ladi.

Foydalanilgan adabiyotlar:

1. **James, G., Witten, D., Hastie, T., & Tibshirani, R.** (2013). An Introduction to Statistical Learning with Applications in R. Springer.
2. **Goodfellow, I., Bengio, Y., & Courville, A.** (2016). Deep Learning. MIT Press.
3. **Chollet, F.** (2018). Deep Learning with Python. Manning Publications.
4. **Bishop, C. M.** (2006). Pattern Recognition and Machine Learning. Springer.
5. **Hyndman, R. J., & Athanasopoulos, G.** (2021). Forecasting: Principles and Practice. OTexts.
6. **Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., ... & Duchesnay, E.** (2011). Scikit-learn: Machine Learning in Python. Journal of Machine Learning Research, 12, 2825–2830.
7. **Zheng, A., & Casari, A.** (2018). Feature Engineering for Machine Learning: Principles and Techniques for Data Scientists. O’Reilly Media.
8. **Chen, T., & Guestrin, C.** (2016). XGBoost: A Scalable Tree Boosting System. In Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (pp. 785–794).