УДК 004.056.55:519.7

SIMMETRIK KALITLI ShIFRLASh ALGORITMLARI UChUN XOSMAS MATRITSANI TANLASh ASOSIDA S-BLOKLARNI GENERATSIYA QILISh

Abdurazzoqov Javohir Rustamovich – *texnika fanlari bo'yicha falsafa doktori, dotsent*
javohirjon.1992@gmail.com
Toshkent xalqaro universiteti

ГЕНЕРАЦИЯ S-БЛОКОВ ДЛЯ АЛГОРИТМОВ СИММЕТРИЧНОГО ШИФРОВАНИЯ НА ОСНОВЕ ВЫБОРА НЕВЫРОЖДЕННОЙ МАТРИЦЫ

Абдураззоков Жавохир Рустамович – *доктор философии по техническим наукам, доцент*
Ташкентский международный университет

SYMMETRIC ENCRYPTION ALGORITHMS S-BOX GENERATION BASED ON NONSINGULAR MATRIX SELECTION

Abdurazzolov Javolhir Rustamovich – *PhD in Technical Sciences, Associate Professor*
Tashkent International University

Tayanch so'zlar: S-blok, xosmas matritsa, affin almashtirish, nochiziqlilik, qat'iy lavin samaradorligi.

Rezyume. Mazkur ishda simmetrik kalitli shifrlash algoritmlari uchun S-bloklarni generatsiya qilish yondashuvi taklif etildi. Taklif etilgan yondashuv xosmas matritsani tanlashga asoslanadi. S-blok Rijndael algoritmidagi hisoblash yordamida hosil qilindi. Hisoblash jarayoni chekli maydon arifmetikasiga asoslandi. Affin almashtirishda xosmas binar matritsadan foydalanildi. Hosil qilingan S-blokning kriptografik xossalari tahlil qilindi. Nochiziqlilik ko'rsatkichlari yuqori natijalarni namoyish etdi. SAC qiymatlari kuchli diffuziya xususiyatini ko'rsatdi. Olingan natijalar differensial va chiziqli kriptotahlilga bardoshlilikni tasdiqladi. Taklif etilgan yondashuv yuqori kriptografik samaradorlikka ega ekanligi bilan tavsiflandi.

Ключевые слова: S-блок, невырожденная матрица, аффинное преобразование, нелинейность, строгий лавинный критерий.

Резюме. В данной работе предложен подход к генерации S-блоков для алгоритмов симметричного шифрования. Предложенный подход основан на выборе невырожденной матрицы. S-блок формировался с использованием вычислительного механизма алгоритма Rijndael. Процесс вычисления основан на арифметике конечных полей. При аффинном преобразовании использовалась невырожденная бинарная матрица. Были исследованы криптографические свойства полученного S-блока. Показатели нелинейности продемонстрировали высокие результаты. Значения SAC подтвердили наличие сильного диффузионного свойства. Полученные результаты подтвердили устойчивость к дифференциальному и линейному криптоанализу. Предложенный подход характеризуется высокой криптографической эффективностью.

Key words: S-box, nonsingular matrix, affine transformation, nonlinearity, strict avalanche criterion.

Summary. This paper proposes an approach for generating S-boxes for symmetric encryption algorithms. The proposed approach is based on selecting a nonsingular matrix. The S-box was generated using the computational mechanism of the Rijndael algorithm. The computation process was based on finite field arithmetic. A nonsingular binary matrix was used in the affine transformation stage. The cryptographic properties of the generated S-box were analyzed. The nonlinearity results demonstrated high performance. The SAC values indicated strong diffusion characteristics. The obtained results confirmed resistance against differential and linear cryptanalysis. The proposed approach is characterized by high cryptographic efficiency.

Kirish. Axborot-kommunikatsiya texnologiyalarining rivojlanishi ma'lumotlarni ishonchli himoyalash zaruratini oshirmoqda. Kriptografik usullar ma'lumotlarning maxfiyligi va yaxlitligini ta'minlashda muhim ahamiyatga ega. Simmetrik kalitli shifrlash algoritmlari yuqori tezkorligi sababli keng qo'llaniladi. Ushbu algoritmlarning asosiy tarkibiy qismlaridan biri S-bloklar hisoblanadi. S-bloklar algoritmning nochiziqliligini ta'minlab, differensial va chiziqli kriptotahlilga bardoshliligini oshiradi. AES, Kuznyechik va SM4 kabi zamonaviy standartlarda S-bloklardan samarali foydalaniladi. Shu sababli yuqori kriptografik xossalarga ega S-bloklarni yaratish dolzarb ilmiy masalalardan biri hisoblanadi.

O'rganilgan adabiyotlar tahlili. Raqamli texnologiyalar jadal rivojlanayotgan hozirgi davrda ma'lumotlarni uzatish, saqlash va himoyalash jarayonlari keng ko'lamda qo'llanilmoqda. Shu sababli, ishonchli axborot xavfsizligi tizimlarini yaratish muhim ahamiyat kasb etadi. Kriptografiya tamoyillariga asoslangan shifrlash usullari ma'lumotlarni uzatish va saqlash xavfsizligini ta'minlashning asosiy vositalaridan biri hisoblanadi [1, 2].

S-bloklar kriptografik arxitekturaning turli komponent-larida yuqori darajadagi shifrlash samaradorligini ta'minlovchi muhim elementlardan biridir. Ular, ayniqsa, Substitution-Permutation (SP) tarmoqlari hamda Feistel tarmog'iga asoslangan simmetrik shifrlash algoritmlari standartlarida keng qo'llaniladi [2]. Simmetrik kalitli kriptografiyada blokli shifrlar va oqimli shifrlar shifrlash-ning asosiy shakllari hisoblanadi. Sun'iy intellekt texnologiyalarining kriptotahlil bilan integratsiyalashuvi kriptografiya sohasining rivojlanishiga sezilarli ta'sir ko'rsatib, axborot xavfsizligi va maxfiylikni ta'minlash masalalarini yanada dolzarb holga keltirdi [3]. Ushbu muvozanatni ta'minlash matematik usullar, kriptografik tizimlarning statistik tahlili hamda turli hisoblash strategiyalarini chuqur o'rganishni talab etadi. Umuman olganda, S-bloklar Bul funksiyalarining xossalaridan foydalanishga asoslangan turli hisoblash usullari yordamida

quriladi [4]. Chiziqli, integral, differensial hamda algebraik kriptotahlil kabi usullarning rivojlanishi yanada bardoshli almashtirish bloklarini yaratishga bo‘lgan ehtiyojni oshirmoqda [5, 6]. So‘nggi tadqiqotlar chiziqlilik va differensial bir jinslilik ko‘rsatkichlarining muhimligini ko‘rsatdi. Ushbu xususiyatlar S-bloklarning differensial va chiziqli kriptotahlilga bardoshliligini baholashda asosiy mezonlardan hisoblanadi [7, 8].

Yuqorida o‘rganilgan S-blok qiymatlarini hisoblash algoritmlari mavjud bo‘lsa-da, turli kriptotahlil usullariga bardosh bera oladigan S-bloklarni shakllantirish masalasi hanuzgacha dolzarb yo‘nalishlaridan biri bo‘lib qolmoqda.

Taklif etilayotgan S-blokni hisoblash usuli. Taklif etilayotgan S-blokni hisoblash uchun Rijndael algoritmida qo‘llaniladigan affin almashtirish usulidan foydalanildi. Buning uchun $m(x)=x^8+x^7+x^6+x^5+x^4+x^2+x+1$ keltirilmaydigan ko‘phad, $b=(1,0,1,0,1,0,1,1)$ vektor va A – xosmas matritsa tanlab olindi.

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

Taklif etilayotgan S-blokni hisoblash jarayoni $GF(2^8)$ chekli maydonida bajariladi. Har bir kiruvchi bayt x, 8 bitli vektor yoki darajasi 7 dan katta bo‘lmagan ko‘phad ko‘rinishida ifodalanadi. Dastlab x – elementining $m(x)$ – ko‘phad modulidagi multiplikativ teskari elementi x^{-1} aniqlanadi. Agar $x=0$ bo‘lsa, odatdagidek uning teskari elementi 0 deb olinadi. Shundan so‘ng hosil qilingan x^{-1} – qiymatiga xosmas A matritsa yordamida affin almashtirish qo‘llaniladi. Bunda S-blok qiymati quyidagi ko‘rinishda hisoblanadi:

$$S(x)=A\cdot x^{-1}\oplus b$$

Bu yerda A – 8×8 o‘lchamli xosmas binar matritsa, b – 8 bitli siljitish vektori, $\oplus$ esa $GF(2)$ maydonidagi qo‘shish, ya’ni XOR amalini bildiradi. A matritsaning xosmas bo‘lishi affin almashtirishning teskari mavjudligini ta’minlaydi va natijada hosil qilinadigan S-blokning biyektivligini saqlashga xizmat qiladi.

Ushbu jarayon barcha $x\in\{0,1,\ldots,255\}$ qiymatlar uchun ketma-ket bajariladi. Har bir kirish qiymatiga mos bitta chiqish qiymati hosil qilinadi va natijada 256 ta elementdan iborat 8×8 S-blok shakllantiriladi. Hisoblash jarayonida qo‘llanilgan xosmas matritsa S-blokning chiziqli va differensial xossalariga bevosita ta’sir ko‘rsatadi. Shu sababli A – matritsani to‘g‘ri tanlash yuqori nochiziqlilik, past differensial ehtimollik hamda qat’iy ko‘chki mezoniga yaqin qiymatlarni ta’minlashda muhim omil hisoblanadi. Taklif etilayotgan yondashuvda S-blokni qurishning asosiy bosqichlari quyidagilardan iborat: avvalo $GF(2^8)$ maydoni tanlangan keltirilmaydigan ko‘phad yordamida aniqlanadi; keyin har bir kirish elementi uchun multiplikativ teskari qiymat hisoblanadi; so‘ngra tanlangan xosmas matritsa va siljitish vektori asosida affin almashtirish bajariladi. Natijada quyidagi *S=[171, 12, 118, 237, 158, 88, 48, 103, 207, 102, 195, 70, 5, 238, 49, 190, 101, 245, 252, 206, 109, 130, 229, 174, 97, 55, 177, 89, 200, 169, 214, 40, 125, 21, 136, 38, 159, 226, 168, 98, 167, 15, 165, 61, 234, 129, 180, 188, 175, 146, 86, 142, 95, 94, 14, 187, 54, 156, 231, 184, 16, 31, 189, 219, 197, 0, 3, 10, 51, 9, 249, 114, 2, 216, 185, 204, 42, 52, 46, 37, 163, 78, 247, 178, 239, 108, 192, 92, 99, 194, 36, 134, 64, 183, 154, 127, 121, 223, 199, 4, 135, 107, 173, 18, 144, 81, 93, 26, 58, 24, 201, 25, 155, 60, 131, 79, 166, 143, 72, 45, 28, 111, 149, 27, 87, 75, 213, 248, 243, 6, 126, 91, 255, 65, 232, 33, 132, 100, 105, 217, 128, 122, 76, 254, 50, 19, 84, 116, 133, 41, 228, 240, 241, 34, 215, 141, 35, 225, 120, 83, 113, 1, 63, 8, 196, 82, 222, 244, 124, 250, 106, 253, 236, 67, 17, 209, 227, 179, 160, 205, 181, 164, 119, 140, 123, 85, 193, 62, 29, 69, 137, 202, 23, 43, 7, 90, 191, 44, 172, 221, 186, 56, 57, 230, 53, 152, 80, 218, 139, 157, 212, 73, 220, 210, 138, 203, 147, 112, 198, 246, 251, 151, 11, 39, 208, 176, 13, 59, 104, 153, 242, 117, 110, 150, 96, 233, 161, 211, 162, 115, 20, 224, 235, 22, 148, 66, 71, 68, 74, 182, 32, 30, 145, 170, 77, 47]* hosil bo‘ldi.

Natijalarni baholash mezonlari. S-blokning kriptografik sifati faqat uning bijektivligi bilan belgilanmaydi. Kuchli S-blok chiziqli va differensial kriptotahlil usullariga nisbatan past korrelyatsiya va past differensial ehtimollik ko‘rsatishi kerak. Shu sababli baholash jarayonida bir nechta mustaqil mezonlar qo‘llanadi. Nochiziqlilik S-blokning affin yoki chiziqli funksiyalardan qanchalik uzoq ekanligini ifodalaydi. 8×8 S-blok uchun har bir koordinata Bul funksiyasi alohida baholanadi. Nochiziqlilik qiymati qancha yuqori bo‘lsa, S-blokni chiziqli ifodalar yordamida yaqinlashtirish shuncha qiyin bo‘ladi. Amaliy jihatdan 8 bitli bijektiv S-bloklar uchun 112 qiymati juda kuchli ko‘rsatkich hisoblanadi. Amalda nochiziqlik quyidagi formula asosida baholanadi.

$$N_f=2^{n-1}\left(1-2^{-n}\max_{\omega\in GF(2^n)}\left|S_{\langle f\rangle}(\omega)\right|\right)$$

Bu yerda: $S_f(\omega)=\sum_{x\in GF(2^n)}(-1)^{f(x)\oplus\omega\cdot x}$, f – Bul funksiyaning Uolsh almashtirishi, $\omega\in GF(2^n)$ – Uolsh almashtirish hisoblanadigan niqob vektori, $\omega\cdot x$ – $GF(2)$ ustidagi skalyar ko‘paytma, $\max_{\omega\in GF(2^n)}|S_f(\omega)|$ – Uolsh almashtirishi eng katta absolut qiymati.

Qat’iy ko‘chki mezoni S-blok kirishidagi bitta bit o‘zgarganda chiqish bitlarining o‘zgarish ehtimolini baholaydi. Ideal holatda har bir chiqish biti 0.5 ehtimollik bilan o‘zgarishi kerak. Agar SAC qiymatlari 0.5 ga yaqin bo‘lsa, kirishdagi kichik o‘zgarish chiqishda keng tarqaladi va diffuziya xususiyati kuchayadi.

Differensial ehtimollik berilgan kirish farqi muayyan chiqish farqiga olib kelish ehtimolini o‘lchaydi. Past differensial ehtimollik differensial kriptotahlilga qarshi muhim himoya omilidir. 8×8 S-bloklarda differensial uniformlik qiymatining 4 bo‘lishi kuchli ko‘rsatkich sifatida qaraladi.

Chiziqli yaqinlashuv ehtimoli S-blok kirish va chiqish bitlari orasidagi chiziqli bog‘lanishlar qanchalik kuchli ekanini ko‘rsatadi. LAP qiymati qanchalik kichik bo‘lsa, S-blok chiziqli kriptotahlilga shunchalik bardoshli bo‘ladi. Shu sababli xosmas matritsa tanlash jarayonida LAP ko‘rsatkichini kamaytirish ham muhim maqsadlardan biridir. Taklif etilgan S-blokning samaradorligini baholash uchun u so‘nggi yillarda taklif qilingan ayrim S-bloklar

bilan solishtirildi. Taqqoslash natijalari 1-jadvalda keltirilgan. Natijalar taklif etilgan S-blokning minimal, maksimal va o‘rtacha nochiziqlilik qiymatlari bo‘yicha yuqori statistik ko‘rsatkichlarga ega ekanligini ko‘rsatadi. S-blokdagi barcha sakkizta Bul funksiyaning yuqori nochiziqlilikka ega bo‘lishi kirish va chiqish orasidagi korrelyatsiyani kamaytiradi hamda S-blokning kriptografik bardoshliligini oshiradi.

1-jadval. Taklif etilgan hamda mavjud 8×8 S-bloklarning asosiy kriptografik xossalari bo‘yicha taqqoslama tahlili

S-blok	Nochiziqlilik			*deg(f)*	*SAC*			*LP*	*DU*
	min	max	o‘rt.		min	max	o‘rt.		
S-blok	112	112	112	7	0.4531	0.5469	0.5000	0.0276	4
AES	112	112	112	7	0.4531	0.5625	0.5048	0.0314	4
SM4	112	112	112	7	0.4375	0.5625	0.4997	0.0346	4
[3]	110	112	110	7	0.4219	0.5781	0.4953	0.0322	10
[4]	112	112	112	7	0.4375	0.5625	0.5022	0.0354	4
[5]	112	112	112	7	0.4065	0.5859	0.4980	0.0426	4
[6]	112	112	112	7	0.4375	0.5625	0.5010	0.0323	4
[7]	112	112	112	7	0.4375	0.5469	0.4978	0.0340	4
[8]	112	112	112	7	0.3906	0.5781	0.4960	0.0353	4
[9]	112	112	112	7	0.4375	0.5469	0.4980	0.0349	4

Natijalar muhokamasi. Olingan natijalar xosmas matritsani tanlash asosidagi inverse-affine konstruktsiya S-bloklarning kriptografik sifatini saqlash va ayrim ko‘rsatkichlarni yaxshilash imkonini berishini ko‘rsatadi. Xususan, hosil qilingan S-blokning barcha koordinata funksiyalari bo‘yicha nochiziqlilik qiymati 112 ga teng bo‘lib, bu 8×8 bijektiv S-bloklar uchun kuchli natija hisoblanadi.

Differensial bir xillikning darajasi 4 bo‘lishi S-blokning differensial kriptotahlilga nisbatan yetarli darajada barqaror ekanini anglatadi. Bunday natija AES va SM4 kabi mashhur standartlarda uchraydigan ko‘rsatkichlar bilan taqqoslanadigan darajadadir. Shu bilan birga, LAP qiymatining past bo‘lishi kirish va chiqish bitlari o‘rtasidagi chiziqli korrelyatsiyalar zaif ekanini bildiradi.

Taklif etilayotgan yondashuvning asosiy afzalligi uning matematik soddaligi va amaliy moslashuvchanligidadir. Xosmas matritsalar to‘plami juda katta bo‘lgani sababli, turli matritsalarni tanlash orqali bir nechta S-blok variantlarini qurish mumkin. Bu esa standart shifrlash sxemalariga mos keluvchi, lekin parametrik jihatdan farqlanuvchi nochiziqli komponentlar oilasini yaratishga imkon beradi.

Shu bilan birga, matritsa tanlash jarayoni ehtiyotkorlik bilan bajarilishi kerak. Har qanday xosmas matritsa avtomatik ravishda eng yaxshi S-blokni bermaydi. Mazkur yondashuvni amaliy blokli shifr tarkibida qo‘llashda S-blokning o‘zi bilan birga shifrning chiziqli diffuziya qatlami, kalit jadvali, raundlar soni va umumiy SPN yoki Feistel arxitekturasi ham tahlil qilinishi lozim. S-blok kuchli bo‘lishi zarur shart, ammo to‘liq shifr xavfsizligi barcha komponentlarning uyg‘un ishlashiga bog‘liq. Xosmas matritsani tanlash asosidagi S-blok generatsiyasi kelgusida dinamik S-bloklar, kalitga bog‘liq affin qatlamlar va apparat jihatdan samarali almashtirish bloklarini qurishda ham qo‘llanishi mumkin. Ayniqsa, resurslari cheklangan qurilmalar uchun qidiruv jadvali ko‘rinishida saqlanadigan, lekin kriptografik mezonlari yuqori bo‘lgan S-bloklar amaliy ahamiyatga ega.

Xulosa. Ushbu ishda simmetrik kalitli shifrlash algoritmlari uchun xosmas matritsani tanlash asosida S-bloklarni generatsiya qilish masalasi ilmiy jihatdan bayon qilindi. S-blok qurilishi $GF(2^8)$ maydonida teskari element-ni hisoblash va tanlangan xosmas binar matritsa orqali affin akslantirishni bajarish tamoyiliga asoslandi.

Tahlil shuni ko‘rsatadiki, xosmas matritsa S-blokning bijektivligini saqlash bilan birga chiqish bitlarining tarqalishiga bevosita ta’sir ko‘rsatadi. To‘g‘ri tanlangan matritsa qat’iy ko‘chki mezoni, chiziqli yaqinlashuv ehtimoli va differensial ehtimollik bo‘yicha yaxshi natijalarga erishishga yordam beradi.

Hosil qilingan S-blok uchun nochiziqlilik qiymatining 112 bo‘lishi, SAC qiymatlarining 0.4531-0.5469 oralig‘ida joylashishi va differensial ko‘rsatkichlarning kuchli darajada saqlanishi taklif etilgan yondashuvning amaliy samaradorligini tasdiqlaydi. Mazkur natijalar S-bloklarni loyihalashda affin qatlam matritsasini tanlash mustaqil va muhim tadqiqot yo‘nalishi ekanini ko‘rsatadi.

Kelgusida ushbu yondashuvni turli keltirilmaydiga ko‘phadlar, turli siljitish vektorlari, fiksirlangan nuqtalarni minimallashtirish va to‘liq blokli shifr tarkibidagi xavfsizlik tahlili bilan kengaytirish maqsadga muvofiqdir. Shuningdek, xosmas matritsalar oilasini tizimli tanlash orqali bir nechta kriptografik mezonlar bo‘yicha balanslangan S-bloklar sinfini shakllantirish mumkin.

Adabiyotlar

1. Abdurakhimov B., Boykuziyev I., Abdurazzokov J. Encryption systems and the history of their development. // InterConf, 2022.

2. Feistel H., Notz W.A., Smith J.L. Some cryptographic techniques for machine-to-machine data communications. // Proceedings of the IEEE 1975, 63: 1545–54.

3. Wang Y., Wong K.W., Li C., Li Y. A novel method to design S-box based on chaotic map and genetic algorithm. // Phys Lett *A* 2012, 376: 827–33.

4. Mahmood Malik MS, Ali MA, Khan MA, Ehatisham-Ul-Haq M, Shah SNM, Rehman M, et al. Generation of Highly Nonlinear and Dynamic AES Substitution-Boxes (S-Boxes) Using Chaos-Based Rotational Matrices. IEEE Access 2020, 8: 35682-95.

5. Nitaj A., Susilo W., Tonien J. A New Improved AES S-box with Enhanced Properties. // IACR Cryptol EPrint Arch 2020, 2020: 1597.

6. Nizam Chew LC, Ismail ES. S-box Construction Based on Linear Fractional Transformation and Permutation Function. // Symmetry (Basel) 2020, 12: 826.

7. Chen G, Chen Y, Liao X. An extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps. // Chaos Solitons Fractals 2007, 31: 571–9.

8. Daemen J. AES Proposal : Rijndael, 1998.

9. Webster A.F., Tavares S.E. On the Design of S-Boxes. Advances in Cryptology - CRYPTO ’85 Proceedings. – Berlin, Heidelberg: Springer Berlin Heidelberg; n.d. – P. 523-34.