S-BOXLARGA QO‘YILADIGAN ASOSIY KRIPTOGRAFIK TALABLAR VA ULARNI BUZISHGA QARATILGAN HUJUM TURLARI

Yuldasheva Nafisa Salimovna
Toshkent axborot texnologiyalari universiteti o‘qituvchisi, Toshkent shahri, O‘zbekiston Respublikasi
Abdusattarov Ravshanbek Rasuljon o‘g‘li
(Muhammad Al-Xorazmiy nomidagi TATU, magistrant)
abdusattorov@tuit.uz

Annotatsiya: *Ushbu tezisda S-boxlarning kriptografik tizimlardagi o‘rni, ularga qo‘yiladigan asosiy talablar hamda ularni buzishga qaratilgan asosiy hujum turlari tahlil qilingan. Tadqiqotda nochiziqlilik, differensial birxillik, biyektivlik, qat’iy qor-ko‘chki mezoni va bit mustaqilligi kabi xususiyatlarning ahamiyati yoritilgan. Shuningdek, differensial, chiziqli, algebraik, boomerang va yon-kanal hujumlariga qarshi himoya mexanizmlari hamda S-box dizaynida qo‘llaniladigan zamonaviy yondashuvlar — xaotik tizimlar, genetik algoritmlar, heuristik usullar va yengil vaznli kriptografiya misolida ko‘rib chiqilgan. Natijalar S-boxlarning kriptografik barqarorligini oshirishga qaratilgan samarali yondashuvlarni ko‘rsatadi.*

Kalit so‘zlar: *S-box, kriptografik talablar, nochiziqlilik, differensial kriptoanaliz, chiziqli kriptoanaliz, algebraik hujumlar, yengil vaznli kriptografiya, xaotik tizimlar.*

Аннотация: *В данной тезисной работе рассматриваются роль S-box’ов в криптографических системах, основные требования к ним и виды атак, направленные на их взлом. Особое внимание уделено таким свойствам, как нелинейность, дифференциальная равномерность, биективность, строгий критерий лавины и независимость битов. Также анализируются методы защиты от дифференциальных, линейных, алгебраических, бумеранг и побочных атак. Рассмотрены современные подходы к проектированию S-box’ов, включая хаотические системы, генетические алгоритмы, эвристические методы и легковесную криптографию. Результаты исследования демонстрируют эффективные подходы к повышению криптографической устойчивости S-box’ов.*

Ключевые слова: *S-box, криптографические требования, нелинейность, дифференциальный криптоанализ, линейный криптоанализ, алгебраические атаки, легковесная криптография, хаотические системы.*

Kirish

S-boxlarga qo‘yiladigan asosiy kriptografik talablar ularning nochiziqliligi (chiziqli kriptoanalizga qarshi), past differensial birxilligi (differensial kriptoanalizga qarshi), biyektivligi (qaytariluvchanlikni ta'minlash), qat'iy qor ko‘chki mezoni (SAC) va bit mustaqilligi mezoni (BIC) kabi xususiyatlarni o‘z ichiga oladi. Ushbu talablar S-boxning

shifrlash jarayoniga kiritadigan chalkashlik (confusion) va tarqalish (diffusion) xususiyatlarini maksimal darajada oshirishga qaratilgan.

S-boxlarni buzishga qaratilgan asosiy hujum turlari quyidagilardir:

1. Differensial Kriptoanaliz: S-boxning kirish va chiqish farqlari o‘rtasidagi ehtimoliy munosabatlardan foydalanadi.
2. Chiziqli Kriptoanaliz: S-boxning kirish va chiqish bitlari o‘rtasidagi chiziqli yaqinlashishlarni tahlil qiladi.
3. Algebraik Hujumlar: S-boxning ichki tuzilishini polinomial tenglamalar tizimi orqali ifodalab, kalitni topishga harakat qiladi.
4. Boomerang va Boshqa Kengaytirilgan Hujumlar: Differensial va chiziqli kriptoanalizning takomillashtirilgan turlari.
5. Yon-kanal Hujumlari: S-boxning jismoniy amalga oshirilishidan (masalan, quvvat sarfi) kelib chiqadigan ma'lumotlardan foydalanadi.

Kuchli S-boxlar yuqorida sanab o‘tilgan kriptografik talablarni yuqori darajada qondirish orqali ushbu hujum turlariga qarshi mustahkam himoyani ta'minlaydi.

S-boxlar: Kriptografik talablar, hujum turlari va yondashuvlar hisoboti

S-boxlar (Substitution Boxes) zamonaviy blokli shifrlash algoritmlari va xesh funksiyalarining asosiy komponenti bo‘lib, kriptografik tizimlarning xavfsizligini ta'minlashda markaziy rol o‘ynaydi. Ularning asosiy vazifasi shifrlash jarayoniga nochiziqlilik va chalkashlik (confusion) kiritishdir, bu esa ma'lumotlarni buzishni va kriptoanalitik hujumlarga qarshi turishni qiyinlashtiradi. S-boxning kriptografik sifati undan foydalaniladigan butun kriptografik algoritmlarning samaradorligini sezilarli darajada belgilaydi[1,2,3].

S-boxlarga qo‘yiladigan asosiy kriptografik talablar

S-boxning asosiy vazifasi ma'lumotlarni shifrlash jarayonida murakkab va tasodifiy o‘zgarishlarni ta'minlashdir. Shifrning xavfsizligi S-boxning kriptografik xususiyatlariga bevosita bog‘liq. Ushbu xususiyatlar quyidagilarni o‘z ichiga oladi:

1. Nochiziqlilik (Nonlinearity)

Nochiziqlilik (NL) S-boxning chiziqli kriptoanalizga qarshi mustahkamligini o‘lchovchi eng muhim xususiyatlardan biridir. Yuqori nochiziqlilik S-boxning kirish va chiqish bitlari o‘rtasida chiziqli matematik munosabatning yo‘qligini anglatadi, bu esa chiziqli kriptoanalizga qarshi mustahkam himoya ta'minlaydi. Ba'zi S-boxlar uchun nochiziqlilik qiymati 106.75, 109.75 yoki 112 ga (AES S-box) yetishi mumkin[4,5,9].

2. Differensial birxillik (Differential Uniformity)

Differensial birxillik (DU) S-boxga qarshi differensial kriptoanalizdan himoyalanishni ta'minlaydi. Past Differensial Ehtimollik (DP) qiymati har qanday kirish differensiali uchun maksimal chiqish differensialining juda past ehtimollik bilan yuz berishini anglatadi. Kuchli S-boxlar iloji boricha kichik DU qiymatiga ega bo‘lishi kerak. Agar U(S)= 〖max⁡〗 _(α≠0,β) δ_S (α,β) qiymati minimalga, ya'ni 2 ga yetsa, u Deyarli Mukammal Nochiziqli (APN) S-box deb ataladi. Yaxshi S-boxlar uchun DP qiymati odatda 0.0391 yoki undan past bo‘ladi. Eng yaxshi S-boxlar uchun DP qiymati 2^(-2) dan kam yoki teng bo‘lishi kerak[4,9,11].

3. Biyektivlik (Bijectivity)

S-boxning har bir kirish qiymati uchun noyob chiqish qiymatini berishi kerak, bu shifrlangan ma'lumotlarni teskariga aylantirish (deshifrlash) imkoniyatini ta'minlaydi. Bu birma-bir moslikni kafolatlaydi, ya'ni har qanday ikkita farqli kirish x_1 va x_2 uchun $S[x_1] \neq S[x_2]$ sharti bajarilishi kerak.[1,5]

4. Qat'iy qor-ko‘chki mezoni (Strict Avalanche Criterion - SAC)

Bu mezonga ko‘ra, agar kirish bitlaridan bittasi o‘zgartirilsa, chiqish bitlarining taxminan yarmi o‘zgarishi kerak. SAC S-boxning chalkashlik xususiyatini o‘lchaydi. Ideal qiymat 0.5 ga yaqin bo‘lishi lozim; masalan, 0.4995 yoki 0.5160 qoniqarli natijalar hisoblanadi.[6,11]

5. Bit mustaqilligi mezoni (Bit Independence Criterion - BIC)

S-box chiqish bitlari bir-biri bilan korrelyatsiyaga ega bo‘lmasligi va barcha kirish-chiqish o‘zgaruvchilari har bir qor ko‘chki vektori uchun juft-juft mustaqil bo‘lishi kerak. BIC S-boxning tarqalish xususiyatini kuchaytirishga yordam beradi.

6. Boshqa muhim talablar

Tasodifiylik (Randomness): S-boxning chiqishlari tasodifiy xususiyatlarga ega bo‘lishi kerak. Milliy Standartlar va Texnologiyalar Instituti (NIST) tomonidan belgilangan testlar (masalan, chastota, yugurishlar, avtokorrelatsiya testlari) orqali baholanadi.

Algebraik daraja (Algebraic degree): Yuqori algebraik daraja S-boxning algebraik hujumlarga qarshi chidamliligini oshiradi. LELBC kabi tizimlarda algebraik daraja 3 ga teng bo‘lishi talab etiladi.

O‘zgarmas nuqtalar (Fixed points): Ba'zi hujum turlariga qarshi xavfsizlikni oshirish uchun S-boxda o‘zgarmas nuqtalarning yo‘qligi talab qilinishi mumkin, ya'ni har qanday kirish x uchun S[x]≠x bo‘lishi kerak.

Yomon kirish va chiqish (BIBO) shakllari: BIBO shakllari yengil vaznli kriptografiyada muhim bo‘lgan bir faol S-boxga ega differensial yoki chiziqli izlarga olib kelishi mumkin. Dizaynerlar BIBO shakllarining kam sonli bo‘lishini xohlashadi.

Apparat samaradorligi: IoT (Internet of Things) qurilmalari kabi resurs cheklangan muhitlar uchun S-boxlar past energiya iste'moli, kichik maydon va past kechikish talablariga javob berishi lozim.

1-jadval: LELBC S-boxining yengil vaznli blokli shifrlash algoritmlaridagi boshqa S-boxlar bilan kriptografik xususiyatlar bo‘yicha taqqoslanishi

Algoritm	**S-box o‘lchami**	**Maydon (GE)**	**Kechikish (ps)**	**Maks. DP**	**Maks. LP**	**Algebraik daraja**
LELBC	4x4	22.33	350	2^{-2}	2^{-2}	3
CRAFT	4x4	40.0	350	2^{-2}	2^{-2}	3

Algoritm	S-box o‘lchami	Maydon (GE)	Kechikish (ps)	Maks. DP	Maks. LP	Algebraik daraja
Midori64	4x4	37.0	350	2^{-2}	2^{-2}	3
PRINCE	4x4	38.0	450	2^{-2}	2^{-2}	3
MIBS	4x4	27.2	440	2^{-2}	2^{-2}	3

Ushbu jadvalda LELBC (Low Energy Lightweight Block Cipher) S-boxining boshqa yengil vaznli shifrlarning S-boxlari bilan taqqoslanishi keltirilgan. Jadvaldan ko‘rinib turibdiki, LELBC S-boxi maydon va kechikish bo‘yicha afzalliklarga ega bo‘lib, kriptografik xususiyatlarni saqlab qoladi.

S-boxlarga qarshi hujum turlari va ulardan himoyalanish

S-boxlar simmetrik kriptografik algoritmlarning asosiy himoya mexanizmlaridan biri bo‘lganligi sababli, ularni buzishga qaratilgan bir qator kriptoanalitik hujumlar mavjud. S-boxlarning xususiyatlari bevosita ushbu hujumlarga qarshi algoritmning chidamliligini belgilaydi.

1. Differensial kriptoanaliz (Differential cryptanalysis - DC)

- Mexanizmi : bu hujum turi blokli shifrlash algoritmining kirishdagi farqlar (ochiq matn juftliklari orasidagi XOR farqi) va ularga mos keladigan chiqishdagi farqlar (shifrlangan matn juftliklari orasidagi XOR farqi) o‘rtasidagi yuqori ehtimollikdagi munosabatlardan foydalanadi. Asosiy maqsad – S-boxlarning differensial xususiyatlarini tahlil qilish orqali kalitni aniqlash.
- Himoyalanish : S-boxning past Differensial birxillik (DU) va Differensial ehtimollik (DP) qiymatlari ushbu hujumga qarshi chidamlilikni oshiradi. LELBC shifri 12 raunddan so‘ng differensial hujumlarga chidamli ekanligi ko‘rsatilgan.

2. Chiziqli kriptoanaliz (Linear cryptanalysis - LC)

- Mexanizmi : Matsui tomonidan kashf etilgan bu hujum S-box funksiyasining kirish va chiqish bitlari o‘rtasidagi chiziqli yaqinlashishlarni (ehtimollik munosabatlarini) topishga asoslangan.
- Himoyalanish : S-boxning yuqori Nochiziqlilik (NL) darajasi va past Lineer Yaqinlashish Ehtimoli (LAP) bu hujumga qarshi mustahkam himoyani ta’minlaydi. 32-bitli chiqishga ega S-boxlar uchun Lineer Approksimatsiya Jadvali (LAT) tuzish amalda imkonsiz bo‘lgani uchun ular chiziqli kriptoanalizga nisbatan kuchli hisoblanadi .

3. Algebraik kriptoanaliz (Algebraic cryptanalysis)

- Mexanizmi: Algebraik hujumlar S-boxning ichki tuzilishini polinomial tenglamalar tizimi orqali ifodalash va ushbu tenglamalar tizimini yechish orqali kalitni topishga qaratilgan.

• Himoyalanish: S-boxning Algebraik Darajasi (AD) va Algebraik Immuniteti (AI) bu turdagi hujumlarga qarshi mustahkam himoyani ta’minlaydi.

4. Boomerang hujumlari (Boomerang attacks)

• Mexanizmi: Boomerang hujumlari differensial hujumlarning kengaytmasi bo‘lib, kirish va chiqishdagi ma’lum differensial xususiyatlardan foydalanadi.

• Himoyalanish: S-boxning Feistel Boomerang Uniformity (FBU) va Feistel Boomerang Difference Uniformity (FBDU) kabi xususiyatlari Boomerang hujumlariga qarshi chidamlilikni baholashda muhim ahamiyatga ega.

5. Yon-kanal hujumlari (Side-channel attacks)

• Mexanizmi : Yon-kanal hujumlari kriptografik tizimning jismoniy amalga oshirilishidagi ma’lumotlarni (masalan, quvvat iste’moli, elektromagnit nurlanish, vaqt) tahlil qilish orqali maxfiy kalitni aniqlashga qaratilgan.

• Himoyalanish : S-boxning Chalkashlik Koeffitsienti Variansi (CCV) va DPA uchun Signal-shovqin nisbati (SNR(DPA)) DPA (Differential Power Analysis) hujumiga qarshi chidamlilikni belgilaydi.

2-jadval: LELBC shifrida raundlar soniga qarab differensial va chiziqli xususiyatlar bo‘yicha faol S-boxlar sonining o‘zgarishi

Raundlar soni	Differensial xususiyat	Chiziqli xususiyat
1	2	2
2	4	4
3	6	6
4	8	8
5	10	10
6	12	12
7	14	14
8	16	16
9	20	20
10	24	24
11	29	29
12	34	34

Ushbu jadval LELBC shifrining yagona kalit sozlamasida turli raundlar soni uchun differensial va chiziqli xususiyatlar bo‘yicha faol S-boxlarning minimal sonini ko‘rsatadi. Ko‘rinib turibdiki, raundlar soni ortishi bilan faol S-boxlar soni ham ortib boradi, bu esa differensial va chiziqli hujumlarga qarshi chidamlilikni oshiradi.

Ilmiy va praktik yondashuvlar

S-boxlarni loyihalash va baholashda ilmiy hamda amaliy yondashuvlar muhim rol o‘ynaydi. Maqsad, zamonaviy kriptoanalitik hujumlarga qarshi yuqori darajada mustahkam S-boxlarni yaratish va ularning samaradorligini ta'minlashdir.

1. S-box Dizayn Metodologiyalari

- Xaotik tizimlarga asoslangan dizaynlar: Lorenz tizimi, xaotik Boolean funksiyalar, Sine-Logistic xarita, Tent-Sine xaotik tizimi, Memristive Lu xaotik xaritasi va 3D xaotik xaritalar kabi xaotik tizimlar S-boxlarga yuqori nochiziqlilik va tasodifiylik kiritish uchun ishlatiladi.
- Genetik va evolyutsion algoritmlar: S-boxlarni optimal kriptografik xususiyatlar bilan yaratish uchun genetik algoritmlar va evolyutsion yondashuvlar keng qo‘llaniladi. Kvant krossover (quantum crossover) kabi usullar ham nochiziqlilikni oshirishga xizmat qiladi.
- Heuristik usullar: Simulated Annealing (SA) va Hill Climbing (HC) kabi heuristik qidiruv algoritmlari, ayniqsa dinamik xarajat funksiyalaridan foydalanib, yuqori nochiziqli S-boxlarni samarali yaratishda qo‘llaniladi.
- Mashinani o‘rganish (Reinforcement Learning): S-boxlarni yaratishda, xususan, yon-kanal hujumlariga qarshi samarali himoya mexanizmlari bilan S-boxlar yaratishda Reinforcement Learning usullari qo‘llanilishi mumkin 22.
- MILP (Mixed Integer Linear Programming) asosidagi yondashuvlar: MILP kriptografik jadvallardan S-boxlarni, hatto qisman jadvallardan ham, rekonstruksiya qilish uchun ishlatilishi mumkin.

2. Yengil vaznli Kriptografiya (Lightweight Cryptography - LWC)

IoT qurilmalari kabi resurs cheklangan muhitlar uchun S-boxlar nafaqat yuqori xavfsizlikni, balki past energiya iste'moli, kichik maydon va past kechikish kabi qo‘shimcha talablarni ham qondirishi lozim. LELBC uchun 4-bitli involyutsion S-boxlar genetik algoritmlar asosida ishlab chiqilgan bo‘lib, ular past maydon va kechikish xususiyatlariga ega.

Xulosa

Xulosa qilib aytganda, S-boxlar kriptografiyaning muhim elementlari bo‘lib, ularning dizaynida ham nazariy, ham amaliy talablar juda muhimdir. Kriptografik xususiyatlarni optimallashtirish va zamonaviy hujum turlarini hisobga olish orqali yanada xavfsiz va samarali kriptografik tizimlarni yaratish mumkin. Tadqiqotlar doimiy ravishda yangi dizayn metodologiyalarini va tahlil usullarini ishlab chiqishga qaratilgan bo‘lib, bu soha rivojlanishda davom etmoqda.

Foydalanilgan adabiyotlar:

1. Yilmaz Aydin, Ali Murat Garipcan, Fatih Özkaynak. A Novel Secure S-box Design Methodology Based on FPGA and SHA-256 Hash Algorithm for Block Cipher Algorithms. Arabian Journal for Science and Engineering, 2024-06-26. DOI: 10.1007/s13369-024-09251-8
2. Haitham Alsaif, Ramzi Guesmi, Anwar Kalghoum, Badr M. Alshammari, Tawfik Guesmi. A Novel Strong S-Box Design Using Quantum Crossover and Chaotic Boolean Functions for Symmetric Cryptosystems. Symmetry, 2023-03-31. DOI: 10.3390/sym15040833
3. Auday H. Saeed AL-Wattar. A Review of Block Cipher’s S-Boxes Tests Criteria. Iraqi Journal of Statistical Sciences, 2019-09-01. DOI: 10.33899/iqjoss.2019.164195
4. B. Alabduallah, Abdulbasid S. Banga, Nadeem Iqbal, Atif Ikram, Hossam Diab. Advancing Cryptographic Security with a New Delannoy-Derived Chaotic S-Box. Computer Applications and Technology, 2024-01-01. DOI: 10.0410/cata/a4bf0870f444f53b33bb733ec2230c64.
5. Farid Subkhan, M. Maarif, Nurul Taufiqu Rochman, Yudhistira Nugraha. Orchestrating Digital Economy to Foster Economic Resilience of Smart Cities: The Soft System Approach. Etikonomi: Journal of Business and Economics, 2025-03-09. DOI: 10.15408/etk.v24i1.39224
6. Asim Ali, Muhammad Asif Khan, Ramesh Kumar Ayyasamy, Muhammad Wasif. A Novel Systematic Byte Substitution Method to Design Strong Bijective Substitution Box (S-box) Using Piece-Wise Linear Chaotic Map. PeerJ Computer Science, 2022-05-12. DOI: 10.7717/peerj-cs.940
7. Jenan Namuq. S-Box Design Utilizing 3D Chaotic Maps for Cryptographic Application. Baghdad Journal of Engineering Sciences, 2024-08-18. DOI: 10.33971/bjes.24.2.9
8. Oleksandr Kuznetsov, Nikolay Poluyanenko, Emanuele Frontoni, Sergey Kandiy, Mikolaj Karpinski, Ruslan Shevchuk. Enhancing Cryptographic Primitives through Dynamic Cost Function Optimization in Heuristic Search. Electronics, 2024-05-09. DOI: 10.3390/electronics13101825
9. Omer Tariq, Muhammad Bilal Akram Dastagir, Dongsoo Han. Compact Walsh–Hadamard Transform-Driven S-Box Design for ASIC Implementations. Electronics, 2024-08-10. DOI: 10.3390/electronics13163148
10. Sinem Akyol. Hybrid Cuckoo Search–Bees Algorithm with Memristive Chaotic Initialization for Cryptographically Strong S-Box Generation. Biomimetics, 2025-09-10. DOI: 10.3390/biomimetics10090610
11. Zaid Bin Faheem, Asim Ali, Muhammad Asif Khan, Muhammad Ehatisham Ul-Haq, Waqar Ahmad. Highly Dispersive Substitution Box (S-Box) Design Using Chaos. ETRI Journal, 2020-03-04. DOI: 10.4218/etrij.2019-0138
12. Qingling Song, Lang Li, Xiantong Huang. LELBC: A Low Energy Lightweight Block Cipher for Smart Agriculture. Internet of Things, 2024-04-01. DOI: 10.1016/j.iot.2023.101022

13. Khumbelo Difference Muthavhine, Mbuyu Sumbwanyambe. Blocking Linear Cryptanalysis Attacks Found on Cryptographic Algorithms Based on Galois Field (GF(2^32)) and High Irreducible Polynomials. Applied Sciences, 2023-11-30. DOI: 10.3390/app132312834

14. Mahnoor Naseer, Sundas Tariq, Naveed Riaz, Naveed Ahmed, Mureed Hussain. S-box Security Analysis of NIST Lightweight Cryptography Candidates: A Critical Empirical Study. arXiv preprint, 2024-04-09. DOI: 10.48550/arxiv.2404.06094

15. Ardabek Khompysh, Nursulu Kapalova, Kunbolat Algazy, Dilmukhanbet Dyusenbayev, Kairat Sakan. Design of Substitution Nodes (S-Boxes) of a Block Cipher Intended for Preliminary Encryption of Confidential Information. Cogent Engineering, 2022-06-07. DOI: 10.1080/23311916.2022.2080623

16. Khumbelo Difference Muthavhine, Mbuyu Sumbwanyambe. Preventing Differential Cryptanalysis Attacks Using a KDM Function and the 32-Bit Output S-Boxes on AES Algorithm Found on IoT Devices. Cryptography, 2022-02-22. DOI: 10.3390/cryptography6010011

17. Muhammad Usama, Osama Rehman, Imran Memon, Safdar Rizvi. An Efficient Construction of Key-Dependent Substitution Box Based on Chaotic Sine Map. International Journal of Distributed Sensor Networks, 2019-12-01. DOI: 10.1177/1550147719895957

18. Oleksandr Kuznetsov, Nikolay Poluyanenko, Emanuele Frontoni, Sergey Kandiy. Enhancing Smart Communication Security: A Novel Cost Function for Efficient S-Box Generation in Symmetric Key Cryptography. Cryptography, 2024-04-25. DOI: 10.3390/cryptography8020017

19. Zhenyu Lu, Sihem Mesnager, Tingting Cui, Yanhong Fan, Meiqin Wang. An STP-Based Model Toward Designing S-boxes with Good Cryptographic Properties. Designs, Codes and Cryptography, 2022-04-02. DOI: 10.1007/s10623-022-01034-2

20. David Carcano Ventura, Lil Maria Rodriguez Henriquez, Saul E. Pomares Hernandez. Requirements for Feistel-Based Lightweight Block Cipher S-boxes to Be Resilient to Boomerang Attacks. IEEE ENC 2024 Conference, 2024-01-01. DOI: 10.1109/enc60556.2023.10508657