S-BOX BAHOLASH USULLARINING KAMCHILIKLARI VA TAKOMILLASHTIRISH ZARURIYATI

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: *Maqolada blokli shifrlarning asosiy chiziqsiz komponenti — S-boxlarni baholashning mavjud usullari tizimli tahlil qilinadi. Tadqiqotda mavjud baholash usullarining oltita asosiy kamchiligi aniqlangan: mezonlarning alohida baholanishi, og‘irlik koeffitsientlarining sub’ektivligi, kontekstga bog‘liq bo‘lmagan baholash, zamonaviy hujum turlarining hisobga olinmasligi, standartlashtirish muammolari va hisoblash murakkabligining eksponensial o‘sishi. Ko‘p mezonli qaror qabul qilish usullari (TOPSIS, VIKOR, AHP) asosida integrallashgan baholash tizimi, kvant-chidamli mezonlar va mashina o‘rganish algoritmlarini qo‘llash kabi takomillashtirish yo‘nalishlari taklif etiladi. 2024–2026 yillardagi eng so‘nggi tadqiqotlar qiyosiy tahlil qilingan.*

Kalit so‘zlar: *S-box, kriptografik baholash mezonlari, chiziqsizlik, differensial yaqinlash ehtimolligi, chiziqli yaqinlash ehtimolligi, qat’iy ko‘chki mezoni, algebraik daraja, yon kanal hujumlari, ko‘p mezonli qaror qabul qilish, kvant-chidamli kriptografiya, mashina o‘rganish, post-kvant kriptografiya, kriptotahlil.*

KIRISH

Zamonaviy axborot xavfsizligi tizimlarining asosini simmetrik kriptografiya, xususan, blokli shifrlar tashkil etadi. AES (Advanced Encryption Standard), Camellia, PRESENT, GIFT, ASCON kabi algoritmlar turli sohalarda — bank tizimlaridan tortib IoT qurilmalarigacha — keng qo‘llanilmoqda. Ushbu algoritmlarning xavfsizligi bevosita ularning tarkibiy qismlarining, birinchi navbatda S-boxlarning (almashtirish qutilarining) kriptografik mustahkamligiga bog‘liq.

S-box — blokli shifrning yagona chiziqsiz komponenti bo‘lib, u Klod Shennonning konfuziya tamoyilini amalga oshiradi [1]. S-boxning kriptografik sifati butun shifrlash algoritmining differensial kriptotahlil [2], chiziqli kriptotahlil [3], algebraik hujumlar [4] va yon kanal hujumlariga [5] qarshi chidamliligini belgilaydi. Shu sababli, S-boxlarni baholash va optimallashtirish kriptografiyaning eng muhim tadqiqot yo‘nalishlaridan biri hisoblanadi.

So‘nggi o‘n yillikda S-box baholash mezonlari va usullari sezilarli darajada rivojlandi. Chiziqsizlik (NL), differensial yaqinlash ehtimolligi (DAP), chiziqli yaqinlash ehtimolligi (LAP), qat’iy ko‘chki mezoni (SAC), bit mustaqilligi mezoni (BIC), algebraik daraja (AD) va yon kanal mezonlari (TO, CCV, SNR) kabi ko‘rsatkichlar S-boxning turli hujum turlariga qarshi chidamliligini o‘lchash uchun ishlab chiqilgan [6–10].

Biroq, mavjud baholash usullarida bir qator jiddiy kamchiliklar mavjud. Birinchidan, mezonlar alohida-alohida baholanadi va yagona integrallashgan ko‘rsatkich yo‘q. Ikkinchidan, ko‘p mezonli baholashda og‘irlik koeffitsientlari sub’ektiv tarzda belgilanadi. Uchinchidan,

baholash kontekstga — ya'ni S-box qaysi algoritmda, qanday muhitda va qanday hujum modeliga qarshi ishlatilishiga — bog'liq emas. To'rtinchidan, kvant hisoblash texnologiyalarining rivojlanishi, mashina o'rganish asosidagi yangi hujum usullarining paydo bo'lishi va IoT qurilmalarining keng tarqalishi mavjud mezonlar tizimini qayta ko'rib chiqishni talab qilmoqda.

2024–2026 yillarda bu sohada bir qator muhim tadqiqotlar amalga oshirildi. Peigen platformasi S-boxlarni baholash, amalga oshirish va generatsiya qilish uchun yagona vosita sifatida taklif etildi [11]. Springer Nature jurnalida S-box tahlili va tasvirni shifrlash metrikalari uchun integrallashgan onlayn platforma nashr etildi [12]. Nature jurnalida S-box tanlash uchun intellektual qaror qabul qilish freymvorki taklif etildi [13]. NIST yengil vaznli kriptografiya finalistlarining S-boxlari uchun miqdoriy xavfsizlik tahlili o'tkazildi [14].

Shunga qaramay, mavjud baholash usullarining kamchiliklarini tizimli ravishda tahlil qilgan va takomillashtirish yo'nalishlarini aniq belgilagan tadqiqotlar soni juda kam. Ushbu maqola aynan shu bo'shliqni to'ldirishga qaratilgan.

Mavjud usullarning tahlili va tanqidiy bahosi

Mavjud S-box baholash usullarini chuqur tahlil qilish natijasida bir qator muhim kamchiliklar aniqlandi.

1-muammo: Mezonlarning alohida-alohida baholanishi

Mavjud usullarning aksariyatida har bir kriptografik mezon alohida hisoblanadi va baholanadi. Bu yondashuv mezonlar o'rtasidagi o'zaro bog'liqlikni hisobga olmaydi.

Misol: S-box A va S-box B ni qiyoslash:

1-jadval. Ikki S-boxning mezonlar bo'yicha qiyoslanishi

Mezon	S-box A	S-box B	Qaysi yaxshi?
NL	108	104	A
DAP	0.0234	0.0156	B
LAP	0.0625	0.0781	A
SAC	0.4980	0.5010	B
BIC-NL	102	106	B
AD	7	7	Teng
TO	7.90	7.70	B

Bu holatda qaysi S-box yaxshiroq? Javob aniq emas, chunki yagona integrallashgan baholash mezoni mavjud emas.

1-rasm. Mezonlarning alohida baholanishi muammosi

2-muammo: Og‘irlik koeffitsientlarining sub’ektivligi

Ko‘p mezonli baholashda og‘irlik koeffitsientlari (w_i) odatda sub’ektiv tarzda belgilanadi. Turli tadqiqotchilar turli og‘irliklarni tanlaydi, bu esa natijalarning qayta takrorlanmasligiga olib keladi.

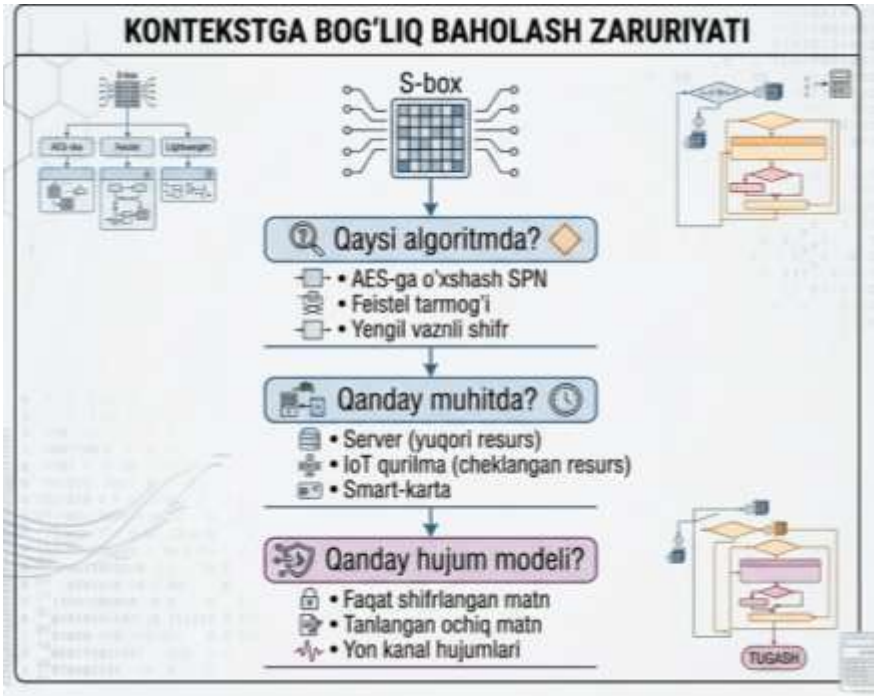
2-jadval. Turli tadqiqotlardagi og‘irlik koeffitsientlari

Tadqiqot	w(NL)	w(DAP)	w(LAP)	w(SAC)	w(BIC)	w (AD)
Tadqiqot 1	0.40	0.20	0.15	0.10	0.10	0.05
Tadqiqot 2	0.30	0.30	0.20	0.10	0.05	0.05
Tadqiqot 3	0.25	0.25	0.25	0.10	0.10	0.05
Tadqiqot 4	0.50	0.15	0.15	0.10	0.05	0.05

Bir xil S-box turli og‘irliklar bilan turlicha baholanishi mumkin.

3-muammo: Kontekstga bog‘liq bo‘lmagan baholash

Mavjud usullar S-boxni izolyatsiyada baholaydi - ya’ni u qaysi algoritmda, qanday muhitda va qanday hujum modeliga qarshi ishlatilishini hisobga olmaydi.



2-rasm. Kontekstga bog‘liq baholash zaruriyati

4-muammo: Zamonaviy hujum turlarining hisobga olinmasligi

Ko‘pgina mavjud baholash usullari faqat klassik hujumlarni (differensial va chiziqli kriptotahlil) hisobga oladi. Zamonaviy hujum turlari - algebraik hujumlar, integral hujumlar, impossible differential hujumlar, kvant hujumlari - ko‘pincha e’tibordan chetda qoladi.

3-jadval. Hujum turlari va tegishli mezonlarning qamrovi

Hujum turi	Tegishli mezon	Mavjud usullarda qamrovi	Ahamiyat darajasi
Differensial kriptotahlil	DAP	✓ To‘liq	Yuqori
Chiziqli kriptotahlil	NL, LAP	✓ To‘liq	Yuqori
Algebraik hujumlar	AD, AI	△ Qisman	Yuqori

Hujum turi	Tegishli mezon	Mavjud usullarda qamrovi	Ahamiyat darajasi
Integral hujumlar	-	X Qamrab olinmagan	O‘rtacha
Impossible differential	-	X Qamrab olinmagan	O‘rtacha
Yon kanal hujumlari	TO, CCV, SNR	△ Qisman	Yuqori
Kvant hujumlari	-	X Qamrab olinmagan	Oshib bormoqda
Mashina o‘rganish hujumlari	-	X Qamrab olinmagan	Yangi
Kub hujumlari	-	X Qamrab olinmagan	O‘rtacha

Standartlashtirish muammolari

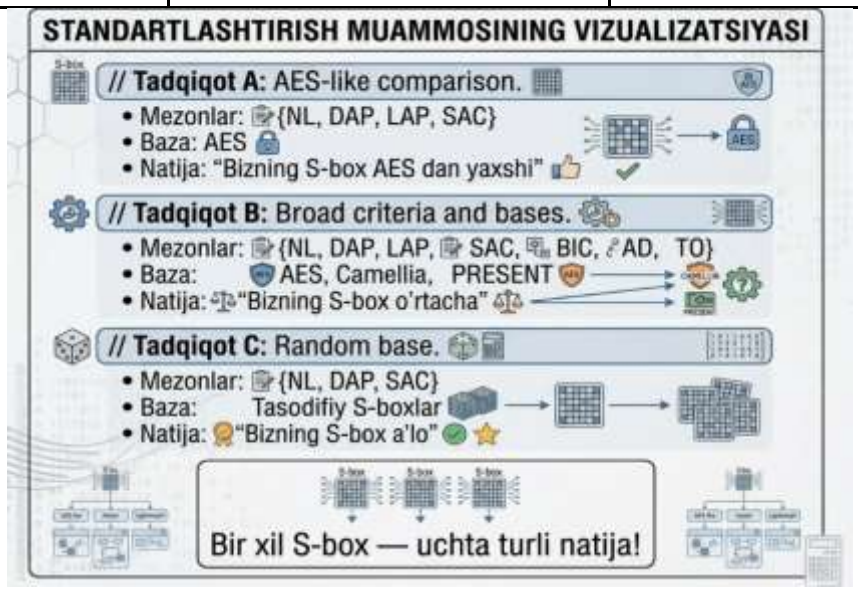
1. Yagona standart yo‘qligi:S-box baholash uchun yagona xalqaro standart mavjud emas. Turli tadqiqotchilar turli mezonlar to‘plamini, turli hisoblash usullarini va turli taqqoslash bazalarini ishlatadi.

2. Taqqoslash bazasining noaniqligi:Ko‘pgina tadqiqotlarda yangi S-box faqat AES S-boxi bilan taqqoslanadi. Boshqa mashhur S-boxlar (Camellia, PRESENT, ASCON) bilan qiyoslash kamdan-kam uchraydi.

3. Statistik ishonchlilik:Ko‘pgina tadqiqotlarda bitta S-box generatsiya qilinadi va baholanadi. Statistik ishonchlilik uchun ko‘p sonli S-boxlar generatsiya qilinishi va ularning o‘rtacha ko‘rsatkichlari tahlil qilinishi kerak.

4-jadval. Standartlashtirish muammolari va ularning oqibatlari

Muammo	Tavsif	Oqibat
Yagona standart yo‘qligi	Turli mezonlar to‘plami ishlatiladi	Natijalarni qiyoslab bo‘lmaydi
Taqqoslash bazasi	Faqat AES bilan qiyoslanadi	Noto‘liq baholash
Statistik ishonchlilik	Bitta S-box baholanadi	Natijalar ishonchsiz
Amalga oshirish farqlari	Turli dasturiy ta’minot	Natijalar farq qilishi mumkin
Hisoblash aniqligi	Suzuvchi nuqta xatoliklari	Noto‘g‘ri natijalar



3-rasm. Standartlashtirish muammosining oqibatlari

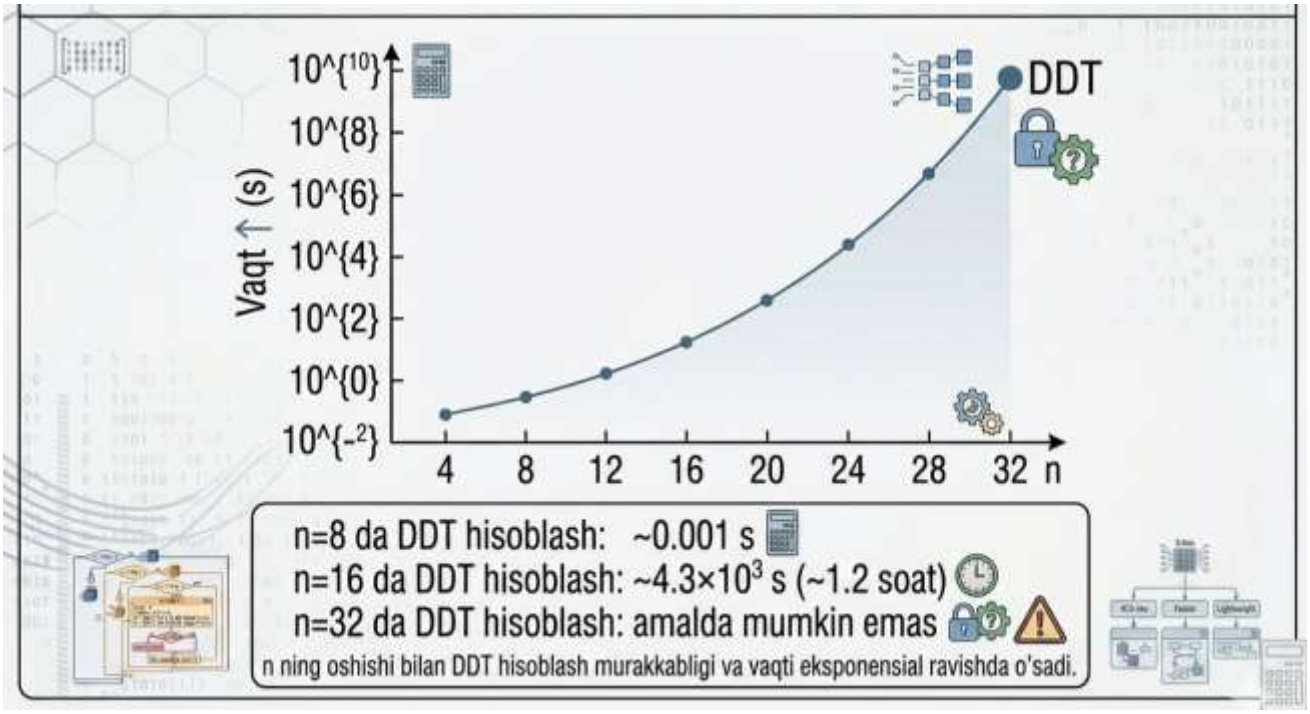
Hisoblash murakkabligi va masshtablanish

1. Katta o‘lchamli S-boxlar uchun hisoblash muammolari:n bitli S-box uchun asosiy mezonlarni hisoblash murakkabligi:

5-jadval. Mezonlarni hisoblash murakkabligi

Mezon	Vaq † murakkabligi	n = 4	n = 8	n = 16	n=32
Bijektivlik	O(2^n)	16	256	65,536	4.3 × 10^9
NL (Walsh)	O(n2^n)	64	2,048	1.05 × 10^6	1.37 × 10^11
DAP (DDT)	O(2^(2n))	256	65,536	4.3 × 10^9	1.84 × 10^19
LAP (LAT)	O(2^(2n))	256	65,536	4.3 × 10^9	1.84 × 10^19
SAC	O(n · m · 2^n n)	256	16,384	1.7 × 10^10	4.4 × 10′′21
BIC	O(nm^2 · 2^n)	1,024	131,072	2.7 × 10^11	1.4 × 10^23
AD (Möbius)	O(n · 2^n)	64	2,048	1.05 × 10^6	1.37 × 10^11

n = 8 uchun barcha mezonlarni hisoblash bir necha soniya ichida amalga oshiriladi. Lekin n = 16va undan katta qiymatlar uchun hisoblash juda qiyin bo‘ladi.



4-rasm. DDT hisoblash murakkabligining n ga bog‘liqligi

2. Peigen platformasi:

Peigen - bu S-boxlarni baholash, amalga oshirish va generatsiya qilish uchun mo‘ljallangan platforma. U quyidagi imkoniyatlarni taqdim etadi:

- Baholash: Xavfsizlik xususiyatlarini hisoblash $(3 \leq n \leq 8)$
- Amalga oshirish: BGC, GEC, MC, Depth murakkabliklarini optimallashtirish
- Generatsiya: Berilgan mezonlarga mos S-boxlarni filtrlash va generatsiya qilish
- Ekvivalentlik: Chiziqli ekvivalentlik (LE) va affin ekvivalentlik (AE) sinflari

Lekin Peigen ham $n > 8$ uchun samarali ishlamaydi.

3. Onlayn platformalar:

2026-yilda Springer Nature jurnalida nashr etilgan tadqiqotda S-box tahlili va tasvirni shifrlash metrikalari uchun integrallashgan onlayn platforma taklif etilgan. Bu platforma:

- Veb-interfeys orqali foydalanish imkonini beradi
- Bir nechta mezonlarni bir vaqtda hisoblaydi
- Natijalarni vizualizatsiya qiladi

Takomillashtirish yo‘nalishlari va istiqbollari

Mavjud kamchiliklarni bartaraf etish uchun quyidagi yo‘nalishlar taklif etiladi:

1. Integrallashgan baholash tizimi:

Barcha mezonlarni bitta yagona ko‘rsatkichga birlashtiruvchi tizim zarur. Bu tizim:

- Ob’ektiv og‘irlik koeffitsientlarini aniqlash usulini o‘z ichiga olishi kerak
- Kontekstga (algoritm, muhit, hujum modeli) moslashishi kerak
- Statistik ishonchlilikni ta’minlashi kerak

Taklif etilayotgan integrallashgan baholash formulasi:

$$Q(S) = \prod_{i=1}^{k} \left(\frac{f_i(S)}{f_i^{ideal}} \right)^{w_i}$$

bu yerda w_i – AHP (Analytic Hierarchy Process) yoki TOPSIS usuli orqali ob’ektiv tarzda aniqlanadi.

2. Kvant-chidamli mezonlar:

Kvant hisoblash texnologiyalarining rivojlanishi bilan yangi mezonlar zarur:

- Grover algoritmiga qarshi chidamlilik
- Kvant algebraik hujumlarga qarshi chidamlilik
- Post-kvant kriptografiya talablariga muvofiqlik

3. Mashina o‘rganish asosidagi baholash:

Sun’iy intellekt va mashina o‘rganish usullarini S-box baholashga qo‘llash:

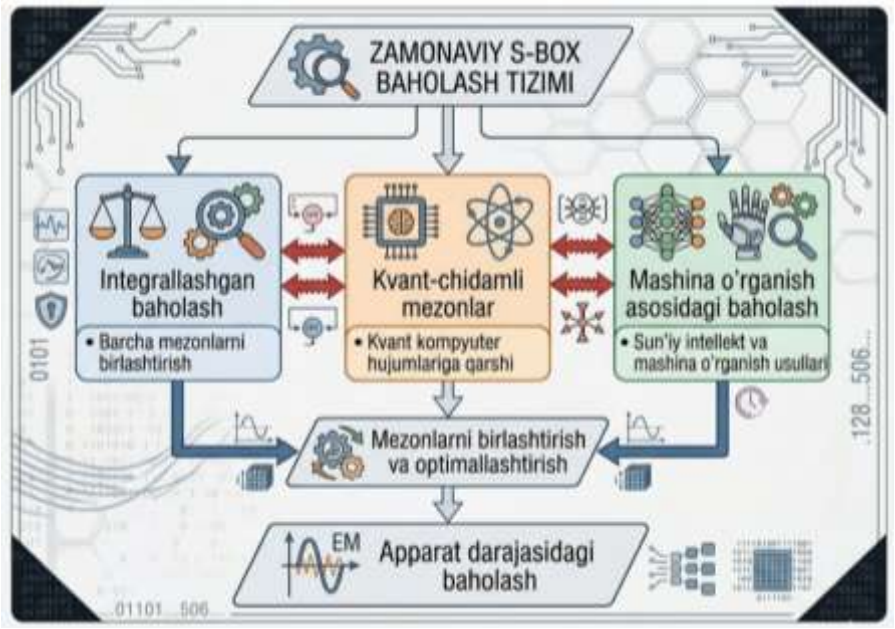
- Neyron tarmoqlar yordamida S-box sifatini bashorat qilish
- Chuqur o‘rganish yordamida yangi mezonlarni aniqlash
- Avtomatlashtirilgan S-box dizayni

4. Apparat darajasidagi baholash:

S-boxning nafaqat matematik, balki apparat darajasidagi xususiyatlarini ham baholash:

- Quvvat iste’moli
- Maydon (area) sarfi
- Kechikish (latency)

- Yon kanal oqishlarining amaliy o‘lchovi



5-rasm. Kelajakdagi takomillashtirish yo‘nalishlari

6-jadval. Takomillashtirish yo‘nalishlari va kutilayotgan natijalar

Yo‘nalish	Muammo	Taklif etilayotgan yechim	Kutilayotgan natija
Integrallashgan baholash	Mezonlarning alohida baholanishi	Ko‘p mezonli qaror qabul qilish usullari (MCDM)	Ob’ektiv va qayta takrorlanadigan baholash
Kvant-chidamlilik	Kvant hujumlarining hisobga olinmasligi	Yangi kvant-chidamli mezonlar	Post-kvant xavfsizlik
Mashina o‘rganish	Qo‘lda baholashning sekinligi	Avtomatlashtirilgan baholash va dizayn	Tezlik va aniqlikning oshishi
Apparat baholash	Faqat matematik baholash	Apparat metrikalari integratsiyasi	Amaliy qo‘llanilishning yaxshilanishi
Standartlashtirish	Yagona standart yo‘qligi	ISO/NIST standartlari taklifi	Natijalarning qiyoslanishi
Masshtablanish	Katta n uchun hisoblash qiyinligi	Parallel va taqsimlangan hisoblash	Katta S-boxlarni baholash imkoniyati

5. Intellektual qaror qabul qilish tizimlari:

2025-yilda Nature jurnalida nashr etilgan tadqiqotda S-box tanlash uchun intellektual qaror qabul qilish tizimi taklif etilgan. Bu tizim:

- TOPSIS, VIKOR, PROMETHEE kabi ko‘p mezonli qaror qabul qilish usullarini qo‘llaydi
- Turli ilovalar uchun eng mos S-boxni avtomatik tanlaydi
- Ob’ektiv og‘irlik koeffitsientlarini aniqlaydi

7-jadval. Ko‘p mezonli qaror qabul qilish usullarining qiyoslanishi

Usul	Afzalligi	Kamchiligi	S-box baholashga mosligi

Usul	Afzalligi	Kamchiligi	S-box baholashga mosligi
AHP	lerarxik tuzilma	Sub'ektiv juftlik taqqoslash	O'rtacha
TOPSIS	Ideal yechimga yaqinlik	Normallashtirishga sezgir	Yuqori
VIKOR	Kompromiss yechim	Parametrlarga sezgir	Yuqori
PROMETHEE	Ustunlik munosabatlari	Murakkab	O'rtacha
ELECTRE	Mos kelish/mos kelmaslik	Murakkab	Past
Entropiya usuli	Ob'ektiv og'irliklar	Ma'lumotga bog'liq	Yuqori

XULOSA

Ushbu maqolada kriptografik chiziqsiz akslantirishlarni (S-boxlarni) baholashning mavjud usullari va muammolari har tomonlama tahlil qilindi. Tadqiqot natijalarini quyidagicha umumlashtirish mumkin:

Asosiy xulosalar

1. S-box baholash mezonlari tizimi yetarlicha rivojlangan, lekin to'liq emas.

Bijektivlik, chiziqsizlik (NL), differensial yaqinlash ehtimolligi (DAP), chiziqli yaqinlash ehtimolligi (LAP), qat'iy ko'chki mezoni (SAC), bit mustaqilligi mezoni (BIC), algebraik daraja (AD) va yon kanal mezonlari (TO, CCV, SNR) - bular S-boxning kriptografik sifatini baholashning asosiy vositalari. Har bir mezon ma'lum bir hujum turiga qarshi chidamlilikni o'lchaydi va ularning barchasi birgalikda S-boxning umumiy xavfsizlik darajasini belgilaydi.

Biroq, zamonaviy hujum turlari - integral hujumlar, impossible differential hujumlar, kvant hujumlari va mashina o'rganish asosidagi hujumlar — uchun tegishli mezonlar hali ishlab chiqilmagan yoki yetarlicha rivojlanmagan.

2. Optimallashtirish muammosi ko'p qirrali va murakkab.

S-box optimallashtirish - bu 256 ! o'lchamli qidiruv fazosida ko'p mezonli optimallashtirish muammosi. Mavjud usullar to'rt asosiy toifaga bo'linadi:

- Algebraik konstruksiyalar - nazariy kafolatlar beradi, lekin cheklangan xilma-xillikka ega
- Xaotik xaritalar - tez va oddiy, lekin NL qiymati AES darajasiga yetmaydi
- Metaevristik algoritmlar - moslashuvchan, lekin nazariy kafolatlar yo'q
- Gibrid usullar - eng istiqbolli, lekin murakkab

2025-yilda taklif etilgan 4×4 komponentlardan 8×8 S-box qurish usuli $NL = 116$ ga erishdi - bu hozirgacha erishilgan eng yaxshi natija.

3. **Mavjud baholash usullarida jiddiy kamchiliklar mavjud.**

Asosiy kamchiliklar:

- Mezonlarning alohida-alohida baholanishi va yagona integrallashgan ko'rsatkich yo'qligi
- Og'irlik koeffitsientlarining sub'ektivligi

- Kontekstga bog‘liq bo‘lmagan baholash
- Zamonaviy hujum turlarining hisobga olinmasligi
- Standartlashtirish muammolari
- Katta o‘lchamli S-boxlar uchun hisoblash murakkabligi

FOYDALANILGAN ADABIYOTLAR:

1. Shannon, C. E. (1949). Communication theory of secrecy systems. Bell System Technical Journal, 28(4), 656-715.

2. Biham, E., & Shamir, A. (1991). Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology, 4(1), 3-72.

3. Matsui, M. (1993). Linear cryptanalysis method for DES cipher. In Advances in Cryptology — EUROCRYPT'93 (pp. 386-397). Springer.

4. Nyberg, K. (1994). Differentially uniform mappings for cryptography. In Advances in Cryptology — EUROCRYPT'93 (pp. 55-64). Springer.

5. Webster, A. F., & Tavares, S. E. (1986). On the design of S-boxes. In Advances in Cryptology — CRYPTO'85 (pp. 523-534). Springer.

6. Daemen, J., & Rijmen, V. (2002). The Design of Rijndael: AES — The Advanced Encryption Standard. Springer.

7. Prouff, E. (2005). DPA attacks and S-boxes. In Fast Software Encryption (pp. 424-441). Springer.

8. Bogdanov, A., Knudsen, L. R., Leander, G., et al. (2007). PRESENT: An ultra-lightweight block cipher. In CHES 2007 (pp. 450-466). Springer.

9. Banik, S., Pandey, S. K., Peyrin, T., et al. (2017). GIFT: A small present. In CHES 2017 (pp. 321-345). Springer.

10. Dobraunig, C., Eichlseder, M., Mendel, F., & Schläffer, M. (2019). Ascon v1.2. NIST Lightweight Cryptography Standardization Process.

11. Tang, G., Liao, X., & Chen, Y. (2005). A novel method for designing S-boxes based on chaotic maps. Chaos, Solitons & Fractals, 23(2), 413-419.

12. Belazi, A., Khan, M., Abd El-Latif, A. A., & Belghith, S. (2017). A simple yet efficient S-box method based on chaotic sine map. Optik, 130, 1438-1444.

13. Wang, Y. (2015). A novel method to design S-box based on chaotic map and genetic algorithm. Chaos, Solitons & Fractals, 80, 15-22.

14. Chen, G. (2008). A novel heuristic method for obtaining S-boxes. Chaos, Solitons & Fractals, 36(4), 1028-1036.

15. Ahmad, M., Bhatia, D., & Hassan, Y. (2015). A novel ant colony optimization based scheme for substitution box design. Procedia Computer Science, 57, 572-580.