KONFERENSIYALAR.COM
ANJUMANLAR PLATFORMASI

# O‘ZBEKISTON — 2030: INNOVATSIYA, FAN VA TA’LIM ISTIQBOLLARI

## IX RESPUBLIKA ILMIY-AMALIY KONFERENSIYA MATERIALLARI

DEKABR, 2025-YIL

O‘ZBEKISTON 2030

KONFERENSIYALAR.COM
ANJUMANLAR PLATFORMASI

# O‘ZBEKISTON — 2030: INNOVATSIYA, FAN VA TA’LIM ISTIQBOLLARI

## IX RESPUBLIKA ILMIY-AMALIY KONFERENSIYASI MATERIALLARI

2025-yil, dekabr

**TOSHKENT-2025**

**ISBN 978-9910-8337-4-8**

**O‘ZBEKISTON – 2030: INNOVATSIYA, FAN VA TA’LIM ISTIQBOLLARI.** IX Respublika ilmiy-amaliy konferensiyasi materiallari. – Toshkent: Scienceproblems team, 2025. – 69 bet.

**Elektron nashr**: https://konferensiyalar.com

**Konferensiya tashkilotchisi:** “Scienceproblems Team” MChJ

**Konferensiya o‘tkazilgan sana:** 2025-yil, 29-noyabr

**Mas’ul muharrir:**
Isanova Feruza Tulqinovna

**Annotatsiya**
Mazkur nashrda “O‘zbekiston — 2030: innovatsiya, fan va ta’lim istiqbollari” nomli IX Respublika ilmiy-amaliy konferensiyasi doirasida taqdim etilgan ilmiy maqolalar to‘plami jamlangan. Unda O‘zbekistonning turli oliy ta’lim va ilmiy-tadqiqot muassasalari, tarmoq tashkilotlari, mustaqil tadqiqotchilar tomonidan taqdim etilgan ijtimoiy-gumanitar, iqtisodiyot, huquq, biologiya, tibbiyot va boshqa sohalarga oid maqolalar kiritilgan. Maqolalarda ilm-fanning zamonaviy yo‘nalishlari, innovatsion texnologiyalar, ta’lim islohotlari hamda barqaror taraqqiyotga oid masalalar muhokama qilingan. To‘plam akademik izlanishlar, amaliy tajribalar va ilmiy xulosalarni birlashtirgan holda, fanlararo integratsiyani chuqurlashtirish va ilmiy hamkorlikni kuchaytirishga xizmat qiladi.

**Kalit so‘zlar:** ilmiy-amaliy konferensiya, innovatsiya, fan va ta’lim, O‘zbekiston 2030, barqaror rivojlanish, ilmiy izlanishlar, fanlararo integratsiya, ilmiy hamkorlik, texnologik taraqqiyot, zamonaviy ta’lim.

**ISBN 978-9910-8337-4-8**

# MUNDARIJA

# AXBOROTNI KRIPTOGRAFIK HIMOYALASHDA TASODIFIY SONLAR GENERATORLARINING AHAMIYATI VA ISTIQBOLLARI

**Safoyev Nuriddin Najmiddin o‘g‘li**
Muhammad al-Xorazmiy nomidagi TATU,
Kiberxavfsizlik va kriminalistika kafedrasi

**Annotatsiya.** Tasodifiy sonlar kriptografiya, modellashtirish va xavf tahlili kabi ko‘plab jarayonlarning ajralmas qismidir. Kompyuterlarning deterministik tabiati sababli haqiqiy tasodifiylik faqat fizik jarayonlarga asoslangan True Random Number Generator (TRNG)lar orqali hosil qilinadi. Amaliyotda keng qo‘llaniladigan Free-Running Oscillator (FRO) usuli elektron shovqindan foydalanadi, biroq uning tasodifiyligi to‘liq isbotlab berilmagan. Ushbu maqolada TRNG va FRO texnologiyalari solishtirilib, ularning ustunliklari va cheklovlari tahlil qilinadi. Shuningdek, TRNG'larning kriptografik xavfsizlikdagi o‘rni va ularning keng joriy etilishiga to‘sqinlik qilayotgan asosiy ilmiy hamda texnik muammolar muhokama qilinadi.

**Kalit so’zlar:** fizik tasodifiylik, Kriptografik xavfsizlik, Free-Running Oscillator (FRO), Deterministik va kvant tizimlari, Raqamli qurilmalar uchun RNG integratsiyasi.

# IMPORTANCE AND PROSPECTS OF RANDOM NUMBER GENERATORS IN CRYPTOGRAPHIC PROTECTION OF INFORMATION

**Safoyev Nuriddin Najmiddin oglu**
Muhammad al-Khwarizmi Tashkent State Technical University,
Department of Cybersecurity and Forensic Science

**Annotation.** Random numbers are an integral part of many processes, such as cryptography, modeling, and risk analysis. Due to the deterministic nature of computers, true randomness can only be generated by True Random Number Generators (TRNGs) based on physical processes. The Free-Running Oscillator (FRO) method, widely used in practice, uses electronic noise, but its randomness has not been fully proven. This article compares TRNG and FRO technologies, analyzes their advantages and limitations. It also discusses the role of TRNGs in cryptographic security and the main scientific and technical problems that prevent their widespread implementation.

**Keywords:** physical randomness, Cryptographic security, Free-Running Oscillator (FRO), Deterministic and quantum systems, RNG integration for digital devices.

## Kirish

Haqiqiy tasodifiy sonlar va fizik asosdagi tasodifiy son generatorlari (RNG) zamonaviy texnologiyalarda tobora o‘sib borayotgan ahamiyatga ega bo‘lmogda. Tasodifiy sonlar kriptografiya (matematik, stoxastik va kvant), Monte-Karlo usuli hisob-kitoblari, raqamli simulyatsiyalar, statistik tadqiqotlar, tasodifiylashtirilgan algoritmlar, lotereyalar va boshqa ko‘plab sohalarda muhim vazifani bajaradi.

Zamonaviy dunyoda haqiqiy tasodifiy sonlarga bo‘lgan talab, ayniqsa, kriptografiya va uning quyidagi amaliy sohalarida sezilarli darajada o‘sgan:

- Mobil aloqa tizimlari
- Elektron pochta xavfsizligi
- Onlayn va naqd pulsiz to‘lov tarmoqlari
- Bankomatlar va elektron bank xizmatlari

- Internet-savdo platformalari
- Savdo nuqtalari terminallari
- Oldindan to‘langan kartalar
- Simsiz kalitlar
- Umumiy kiberxavfsizlik yechimlari
- Taqsimlangan elektr tarmoqlari xavfsizligi (SCADA)

Kriptografiyada, ayniqsa isbotlangan xavfsizlik talab qilinadigan ilovalarda, tasodifiylik manbai yetarlicha ishonchli bo‘lmasa, butun xavfsizlik tizimi zaiflashishi mumkin. Kerxoffs printsipiga ko‘ra, kriptografik protokollarning barcha tarkibiy qismlari ommaviy bo‘lishi kerak, faqatgina maxfiy ma'lumotlar (kalit yoki boshqa muhim komponentlar) yuboruvchi va qabul qiluvchi tomonlarda saqlanadi. Agar raqib ushbu ma'lumotlarni hisoblab chiqish yoki oldindan taxmin qilish imkoniyatiga ega bo‘lsa, tizimning butun xavfsizligi yo‘qoladi. Masalan, BB84 kvant kalit almashinuv protokoli faqatgina Alyssa va Bob tomonidan yaratilgan tasodifiy sonlarni hech kim oldindan bashorat qila olmaganda xavfsiz hisoblanadi. Aks holda, protokol o‘zining barcha xavfsizlik xususiyatlarini yo‘qotadi.

Tasodifiy sonlar qimor o‘yinlari va lotereyalar sohasida ham muhim o‘rin tutadi. AQShning onlayn qimor bozori yillik hajmida taxminan 6 milliard AQSh dollariga baholanadi, shuning uchun ba'zi davlatlar RNG-larning adolatli ishlashini ta'minlash uchun qat'iy talablar joriy qilgan. Masalan, Malta Gaming Authority (MGA) tashkiloti RNG-lar uchun maxsus standartlar belgilab, ularni sertifikatlovchi organlarni tayinlagan. Qonuniy talablarga javob bermaydigan RNG-lardan qimor sanoatida foydalanish mumkin emas. Bunday qoidalar o‘yinlarning halolligini ta'minlash va firibgarlikning oldini olishga xizmat qiladi.

Tasodifiy son generatorlari ko‘p yillar davomida olimlar va ixtirochilarning diqqat markazida bo‘lib kelgan. Tasodifiy sonlarni tushunish va ularni yaratish usullarini o‘rganish uchun alohida matematik yo‘nalishlar shakllangan. Zamonaviy hisoblash texnologiyalarining dastlabki davrida, 1970-yillarda Jon fon Neyman deterministik Turing mashinalari haqiqiy tasodifiy sonlar yarata olmasligini ta'kidlagan edi.

So‘nggi o‘n yilliklarda tasodifiy son generatorlari bo‘yicha ilmiy tadqiqotlar eng dolzarb mavzulardan biriga aylangan. 1970-yildan beri 1418 dan ortiq patent ro‘yxatga olingan bo‘lsa-da, amaliyotda juda kam sonli mahsulot ishlab chiqarilgan. Ayniqsa, kvant RNG-lari bozorda kam uchraydi. Asosiy qiyinchiliklar tasodifiylikning ilmiy asosda isbotlanishi va ko‘pgina yechimlarning takror ishlab chiqarish uchun yaroqsizligidadir.

**Random Sonlar Generatorlari**

Tarixan tasodifiy sonlarni generatsiya qilishning ikki asosiy yondashuvi mavjud: algoritmik (psevdotasodifiy) generatsiya va fizik (haqiqiy, nondeterministik) generatsiya. Psevdotasodifiy sonlar generatorlari (PRNG) ilmiy adabiyotlarda juda keng o‘rganilgan, shuning uchun bu bo‘limda ular chuqur ko‘rib chiqilmaydi. Batafsil sharhlar va misollarni [1], [2] manbalardan topish mumkin.

Aslida PRNG — bu boshlang‘ich qiymat (seed) bilan to‘liq aniqlanadigan, deterministik va periodik sonlar ketma-ketligini hosil qiluvchi matematik funksiya. Ta’rifga ko‘ra, bunday generatorlar tomonidan yaratilgan ketma-ketliklarning haqiqiy tasodifiyligi matematik isbotga ega emas. Uzun muddatli balans (0 va 1 lar tengligi) odatda yaxshi bo‘lsa-da, PRNGlar ko‘pincha uzoq masofali korrelyatsiyaga ega bo‘ladi. Bu esa kriptografiyada himoyalanishning

susayishiga, Monte–Karlo modellashtirishda yoki sonli hisoblashlarda sezilmas xatoliklarga olib kelishi mumkin.

Ko‘plab zamonaviy PRNGlar statistik testlardan muvaffaqiyatli o‘tadi, ammo ayrim PRNGlarning boshqalarga nisbatan “doimiy ravishda kuchli” ekani haqidagi qarash xato. Amaliyotda har bir PRNGning ma’lum nosozliklari bor va ular faqat muayyan sharoitlarda namoyon bo‘ladi. Haqiqatan ham ayrim PRNGlar tasodifiy jarayonlarni noto‘g‘ri modellashtirishga yoki matematik hisoblashlarda jiddiy xatoliklarga sabab bo‘lgan holatlar qayd etilgan [3], [4].

PRNGlarga asoslangan barcha yirik oilalar kriptografik maqsadlar uchun turli hujumlar yordamida zaifligi isbotlangan [5], [6]. Shuning uchun yuqori darajadagi oldindan aytib bo‘lmaslik talab etiladigan kriptografik tizimlarda PRNGlardan foydalanish xavf tug‘diradi.

Ularning deterministik tabiati sabab, biror PRNG tasodifiylikning ideal ta’rifini qondira olmaydi. Agar algoritm va boshlang‘ich qiymat ma’lum bo‘lsa, ketma-ketlikni to‘liq tiklash mumkin — bu esa haqiqiy “oldindan aytib bo‘lmaslik” talab qilinadigan tizimlarda jiddiy muammo.

Shunga qaramay, PRNGlar quyidagi afzalliklarga ega:

- Arzon va qulay – integratsiya qilish oson
- Juda tez – katta hajmdagi sonlarni generatsiya qila oladi
- Protsessor tizimlari bilan to‘liq mos – shaxsiy kompyuterlar uchun ideal

Ammo iloji boricha, ayniqsa xavfsizlik kritikasida, imkon qadar fizik (haqiqiy) RNGlardan (TRNG) foydalanish tavsiya etiladi.

PRNG-lardan farqli o‘laroq, fizik RNGlar 0 va 1 ehtimolliklarining notekis taqsimlanishidan aziyat chekishi mumkin. Bunday noaniqlik bias (b) orqali aniqlanadi, u quyidagi formula orqali ifodalanadi:

$$b = \frac{p(1) - p(0)}{2} \tag{1}$$

Bundan tashqari, fizik RNGlar qisqa masofadagi bog‘liqlikka (korelyatsiyaga) ega bo‘lishi mumkin, bu esa seriyali avtokorrelyatsiya koeffitsiyenti ($a_k$) orqali baholanadi:

$$a_k = \frac{\sum_{i=1}^{N-k}(b_i - \bar{b})(b_{i+k} - \bar{b})}{\sum_{i=1}^{N-k}(b_i - \bar{b})^2} \tag{2}$$

Bu yerda $\{b_1, b_2, \dots, b_N\}$ — uzunligi **N** bo‘lgan tasodifiy bitlar ketma-ketligi, **k** esa kechikish yoki koeffitsiyentning tartib darajasi.

Har ikkisi, $b$ va $a_k$— $[-1,1]$ intervalda normallashtirilgan bo‘lib, ideal RNG $b = 0$ va $a_k = 0$ qiymatlariga ega bo‘lishi kerak. Haqiqiy RNGlar odatda bitlar orasidagi bog‘liqlikni iloji boricha kamaytirish uchun yaratiladi, chunki aynan shu tasodifiylik tushunchasining mohiyatidir. Ba’zi hollarda fizik tizim har bir bit ishlab chiqarilganidan keyin dastlabki holatiga qaytariladi, bu esa avtokorrelyatsiyani kamaytirishga yordam beradi. Natijada, aksariyat hollarda faqat eng past tartibli avtokorrelyatsiya koeffitsiyentlari ahamiyatli bo‘ladi, ideal holatda esa faqat birinchi koeffitsiyent (avtokorrelyatsiya) e’tiborga olinadi va $a$ bilan belgilanadi. TRNGlar to‘rtta asosiy toifaga bo‘linadi:

- Shovqin asosidagi RNGlar
- Erkin ishlovchi osilatorli RNGlar
- Xaos asosidagi RNGlar

• Kvant RNGlar

Taqdim etilgan ta’rif apparat darajasida ishlab chiqarilgan PRNGlar bilan adashtirilmasligi kerak — ular deterministik algoritmni temir darajasida takrorlaydi, ya’ni aslida PRNGdir.

Tasodifiylikni testlash

Biror generatorning barcha statistik testlardan o‘tishi — u haqiqiy tasodifiy ekanini isbotlamaydi. Bu faqat u testlar aniqlay oladigan xatoliklar yo‘qligini bildiradi. Ertaga yangi test ishlab chiqilishi mumkin.

Testlar bias, korrelyatsiya, blok chastotasi va boshqa xususiyatlarni tekshiradi. Mashhur to‘plamlar:

- DIEHARD — PRNGlar uchun [14]
- ENT — TRNGlar uchun [15]
- Universal Test — umumiy [16]
- NIST STS — eng keng tarqalgan [17]

Statistik testlash resurs talab qiladi. Masalan:

- $1\times10^9$ bit ma’lumotni NIST STS orqali tekshirish ≈ 6 soat
- Shu miqdordagi ma’lumotni kvant RNG generatsiya qilishi 7–250 soniya

Shuning uchun agar generatorning ma’lum xatolar turiga moyilligi oldindan ma’lum bo‘lsa, mos maxsus testlardan foydalanish yetarli.

Kvant kriptografiyada tasodifiy sonlar

Kvant kriptografiya ikki tomon (Alisa va Bob)ga ochiq kanal orqali umumiy maxfiy kalit yaratish imkonini beradi. Ular kichik boshlang‘ich kalitdan foydalanib, BB84 kabi protokollar yordamida uzun kalit yaratishi mumkin. BB84 1984-yilda taklif qilingan, 1991-yilda tajriba orqali isbotlangan [18].

BB84 protokolidagi kanallar

- Kvant kanal — optik tolada fotonlar yuboriladi
- Klassik kanal — ovozli aloqa, radio, internet va boshqalar

Asosiy g‘oya

Alisa tasodifiy bitlarni foton polarizatsiyasiga kodlaydi. Bob tasodifiy o‘lchash bazalarini tanlaydi. Bazalar mos tushganda to‘g‘ri bitlar hosil bo‘ladi.

BB84 xavfsizligining asosi — tasodifiy sonlarning oldindan aytib bo‘lmasligi:

- Alisaning polarizatsiya tanlovlari
- Bobning o‘lchash bazalari

Agar Eva tasodifiy sonlarni oldindan bilsa, butun kalitni tiklay oladi [19].

Shu sababli, BB84 yuqori entropiyali, ishonchli, lokal RNG talab qiladi.

Qo‘shimcha bosqichlar

1. Ma’lumotlarni muvofiqlashtirish (reconciliation)
2. Maxfiylikni kuchaytirish (privacy amplification)

Amaliy hujumlar

Nazariy jihatdan mukammal bo‘lsa-da, real BB84 tizimlari zaifliklarga ega:

- 2007 (MIT): Bob detektorlarining xususiyatlari ma’lum bo‘lsa, to‘liq kalitni tiklash mumkin [22]
- 2010: ID Quantique va MagiQ kompaniyalari qurilmalariga hujumlar [23]

- Tamoyil: foton detektorlarini manipulyatsiya qilish orqali tasodifiylikni buzish

Bu shuni ko‘rsatadiki, amaliy kvant tizimlarining xavfsizligi tasodifiylik sifatiga bevosita bog‘liq.

Statistik kriptografiyada tasodifiy sonlar

Statistik kriptografiya (Maurer, 1991) kvant kriptografiyaga o‘xshash bo‘lib, SKAPD protokoliga asoslanadi:

1. Afzallikni oshirish (Advantage Distillation)
2. Ma’lumotlarni muvofiqlashtirish
3. Maxfiylikni kuchaytirish

Xavfsizlik faqat Alisa va Bob o‘rtasidagi umumiy axborot Evadagidan ko‘p bo‘lgandagina ta’minlanadi. Bu esa RNGning ishonchliligi bilan uzviy bog‘liq.

Deterministik (matematik) kriptografiyada tasodifiy sonlar

Matematik (klassik) kriptografiya quyidagi murakkab masalalarga tayanadi:

- Diskret logarifm
- Elliptik egrilik logarifmlari
- Ko‘paytuvchilarga ajratish

Biroq bu tizimlarning o‘zi deterministik bo‘lsa-da, quyidagilar uchun tasodifiylikning sifati juda muhim:

- Kalitlar
- Nonce’lar
- Seans kalitlari
- Paddiing
- Eliptik egri parametrlar

Tasodifiylik sifati past bo‘lsa, butun protokol zaiflashadi.

**Xulosa**

Tasodifiy sonlar kriptografiya, axborot xavfsizligi, statistik modellash va turli hisoblash jarayonlarida hal qiluvchi ahamiyatga ega. Biroq kompyuter tizimlarining deterministik tabiati sababli, haqiqiy tasodifiylikni faqat oldindan aytib bo‘lmaydigan fizik jarayonlar orqali yaratish mumkin. Shu bois, yuqori darajadagi ishonchlilik talab qilinadigan kriptografik tizimlarda fizik jarayonlarga asoslangan tasodifiy sonlar generatorlaridan (TRNG) foydalanish zarur hisoblanadi.

Hozirda TRNGlarning ishlab chiqarayotgan bit oqimining tasodifiyligini nazariy jihatdan to‘liq asoslash va amaliy jihatdan uzluksiz verifikatsiya qilish masalasi ochiq muammo bo‘lib qolmoqda. Bu omil TRNGlarning keng miqyosda joriy etilishiga to‘sqinlik qilayotgan asosiy ilmiy-texnik muammolardan biridir. Shuningdek, TRNG qurilmalarining yuqori narxi, ularning ishlash mexanizmlarini sertifikatlashdagi murakkabliklar va apparat darajasidagi nosozliklarni real vaqt rejimida aniqlash zarurati ham qo‘shimcha qiyinchiliklar tug‘diradi.

**Adabiyotlar/Литература/References:**

1. Carlet, C. (2010). Boolean Functions for Cryptography and Error Correcting Codes. In Y. Crama & P. L. Hammer (Eds.), Boolean Models and Methods in Mathematics, Computer Science, and Engineering (pp. 257–397). Cambridge University Press.

2. Maitra, S., & Pasalic, E. (2004). Further Constructions of Resilient Boolean Functions with Very High Nonlinearity. IEEE Transactions on Information Theory, 50(2), 379–386. https://doi.org/10.1109/TIT.2003.821971
3. Youssef, A. M., & Tavares, S. E. (1993). Resistance of balanced S-boxes to linear and differential cryptanalysis. Information Processing Letters, 56(5), 249–252. https://doi.org/10.1016/0020-0190(95)00119-N
4. Tokareva, N. (2015). Bent Functions: Results and Applications to Cryptography. Academic Press. https://doi.org/10.1016/C2014-0-04255-1
5. Cusick, T. W., & Stănică, P. (2009). Cryptographic Boolean Functions and Applications. Academic Press. https://doi.org/10.1016/B978-0-12-374890-4.00001-0
6. Daemen, J., & Rijmen, V. (2002). The Design of Rijndael: AES - The Advanced Encryption Standard. Springer. https://doi.org/10.1007/978-3-662-04722-4
7. Carlet, C., & Preneel, B. (2008). Boolean functions in cryptology and information security. In Handbook of Boolean Functions. CRC Press.
8. Rothaus, O. S. (1976). On "Bent" Functions. Journal of Combinatorial Theory, Series A, 20(3), 300–305. https://doi.org/10.1016/0097-3165(76)90031-0
9. Nyberg, K. (1993). Differentially uniform mappings for cryptography. In Advances in Cryptology — EUROCRYPT '93 (pp. 55–64). Lecture Notes in Computer Science, vol 765. Springer. https://doi.org/10.1007/3-540-48285-7_6
10. Zhang, X., & Zheng, Y. (2000). GAC - the Criterion for Global Avalanche Characteristics of Cryptographic Functions. Journal of Universal Computer Science, 6(1), 307–328. https://doi.org/10.3217/jucs-006-01-0307
11. Millan, W., Clark, J., & Dawson, E. (1998). Heuristic Design of Cryptographically Strong Balanced Boolean Functions. In Advances in Cryptology — EUROCRYPT '98 (pp. 489–499). Lecture Notes in Computer Science, vol 1403. Springer. https://doi.org/10.1007/BFb0054143
12. Zhang, X., Liu, Z., & Wu, X. (2013). A Study of the Cryptographic Properties of Balanced Boolean Functions. Cryptography and Communications, 5(3), 171–190. https://doi.org/10.1007/s12095-012-0064-6
13. Preneel, B., Govaerts, R., & Vandewalle, J. (1990). Boolean Functions Satisfying Higher Order Strict Avalanche Criterion. In Advances in Cryptology — EUROCRYPT '90 (pp. 49–60). Lecture Notes in Computer Science, vol 473. Springer. https://doi.org/10.1007/3-540-46877-3_5
14. Ding, J., & Liu, J. (2009). On the Algebraic Degree of Boolean Functions and its Applications to Cryptography. Information and Computation, 207(5), 505–513. https://doi.org/10.1016/j.ic.2008.09.012
15. Canteaut, A., & Charpin, P. (2001). The nonlinearity of Boolean functions and their algebraic immunity. Designs, Codes and Cryptography, 24(3), 257–269. https://doi.org/10.1023/A:1010685126671
16. Kavut, M., & Yılmaz, İ. (2013). Boolean Functions and their Cryptographic Properties. In Proceedings of the 2013 International Conference on Security and Cryptography (pp. 207–211). IARIA. https://www.thinkmind.org/index.php?view=article&articleid=securrity_2013_4_10_30026
17. Kasami, T. (1985). The Properties of 2k-1 Functions on GF(2n). In Advances in Cryptology — CRYPTO '84 (pp. 211–217). Lecture Notes in Computer Science, vol 196. Springer. https://doi.org/10.1007/3-540-39568-7_15
18. Oruç, E., & Yılmaz, İ. (2009). On the correlation immunity of Boolean functions. Journal of the Franklin Institute, 346(3), 256–265. https://doi.org/10.1016/j.jfranklin.2008.10.005

19. Liu, Z., & Zhang, X. (2011). A survey on the design of cryptographically strong Boolean functions. Cryptography and Communications, 3(1), 1–19. https://doi.org/10.1007/s12095-011-0033-0
20. Carlet, C. (2003). Boolean Functions and the Design of Cryptographic Systems. In Proceedings of the International Conference on Information Security (pp. 104–113). Springer. https://doi.org/10.1007/978-3-540-36025-5_10
21. Tavares, S. E. (1996). On the construction of S-boxes with high nonlinearity. Advances in Cryptology — CRYPTO '96 (pp. 205–216). Lecture Notes in Computer Science, vol 1109. Springer. https://doi.org/10.1007/3-540-68697-5_16
22. Yang, Y. (2015). Correlation immunity of Boolean functions: A survey. Cryptography and Communications, 7(2), 141–155. https://doi.org/10.1007/s12095-014-0135-y
23. 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.
24. W. Zhang, E. Pasalic, Highly nonlinear balanced S-boxes with good differential properties, IEEE Trans. Inf. Theory 60 (12) (2014) 7970–7979.
25. Yong Wang, Zhiqiang Zhang, Leo Yu Zhang, Jun Feng, Jerry Gao, Peng Lei, A genetic algorithm for constructing bijective substitution boxes with high nonlinearity, Information Sciences, Volume 523, 2020, Pages 152-166,ISSN 0020- 0255, https://doi.org/10.1016/j.ins.2020.03.025
26. H. Zahid et al., "Efficient Dynamic S-Box Generation Using Linear Trigonometric Transformation for Security Applications," in IEEE Access, vol. 9, pp. 98460-98475, 2021, doi: 10.1109/ACCESS.2021.3095618.

KONFERENSIYALAR.COM
ANJUMANLAR PLATFORMASI

# O‘ZBEKISTON — 2030: INNOVATSIYA, FAN VA TA’LIM ISTIQBOLLARI

## IX RESPUBLIKA ILMIY-AMALIY KONFERENSIYASI MATERIALLARI

2025-yil, 1-dekabr


**Mas’ul muharrir:** *F.T.Isanova*
**Texnik muharrir:** *N.Bahodirova*
**Diszayner:** *I.Abdihakimov*

O‘ZBEKISTON — 2030: INNOVATSIYA, FAN VA TA’LIM ISTIQBOLLARI. IX Respublika ilmiy-amaliy konferensiyasi materiallari. – Toshkent: Scienceproblems team, 2025. – 69 bet.

**Elektron nashr**: https://konferensiyalar.com

**Konferensiya tashkilotchisi:** Scienceproblems Team

**Konferensiya o‘tkazilgan sana:** 2025-yil, 29-noyabr

**ISBN 978-9910-8337-4-8**