KVANT TEXNOLOGIYALARIDA TASODIFIY SONLAR GENERATORLARINING KRIPTOGRAFIK AHAMIYATI

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

Annotatsiya: *Tasodifiy sonlar kriptografiya, modellashtirish, xavf tahlili va boshqa ko‘plab texnologik jarayonlarning asosiy komponentidir. Kompyuterlarning deterministik tabiatiga ko‘ra, haqiqiy tasodifiylikni faqat fizik jarayonlarga asoslangan True Random Number Generator (TRNG)lar orqali olish mumkin. Amaliyotda keng qo‘llaniladigan Free-Running Oscillator (FRO) yondashuvi elektron shovqindan foydalanadi, biroq uning to‘liq tasodifiyligi ilmiy jihatdan isbotlanmagan. Ushbu maqolada TRNG va FRO generatorlarining ishlash prinsiplari, ustun jihatlari va cheklovlari taqqoslanadi. Shuningdek, TRNGlardan kriptografik xavfsizlikda foydalanishning dolzarbligi hamda ularning keng miqyosda joriy etilishiga halaqit qilayotgan ilmiy va texnik masalalar tahlil qilinadi.*

Kalit so‘zlar: *fizik tasodifiylik, kriptografik xavfsizlik, Free-Running Oscillator (FRO), deterministik tizimlar, kvant tizimlari, RNG integratsiyasi, apparat xavfsizligi.*

KIRISH

Haqiqiy tasodifiy son generatorlari (TRNG) zamonaviy axborot texnologiyalarining deyarli barcha xavfsizlikka oid sohalarida markaziy o‘rin tutadi. Tasodifiylik kriptografiya (klassik, statistik, kvant), Monte-Karlo simulyatsiyalari, stoxastik modellar, raqamli testlar, kompyuter tajribalari, lotereyalar va bir qator kritik tizimlar uchun zarurdir. Bugungi kunda haqiqiy tasodifiy sonlarga bo‘lgan ehtiyoj ayniqsa quyidagi yo‘nalishlarda keskin ortgan:

- mobil aloqa tizimlari
- elektron pochta va messenjyerlar xavfsizligi
- onlayn to‘lovlar va banking
- bankomat va POS-terminallar
- e-commerce platformalari
- simsiz avtentifikatsiya tizimlari
- umumiy kiberxavfsizlik infratuzilmalari
- SCADA va taqsimlangan elektr tarmoqlari

Kriptografik tizimlarda tasodifiylik manbai yetarlicha ishonchlilikka ega bo‘lmasa, xavfsizlikning butun mexanizmi izdan chiqishi mumkin. Kerxoffs printsipiga ko‘ra, tizimning yagona maxfiy qismi — bu kriptografik kalitdir; agar raqib kalitni tasodifiylik nuqsonlari orqali oldindan bilsa, barcha xavfsizlik xususiyatlari bekor bo‘ladi. Masalan, BB84 kvant kalit almashuv protokoli faqat Alisa va Bobning tasodifiy tanlovlari oldindan bashorat qilib bo‘lmasagina xavfsiz ishlaydi.

Bundan tashqari, RNGlar qimor va lotereya sanoati uchun ham cheklovchi omil bo‘lib, ba’zi davlatlar RNG dizaynini sertifikatlashni majburiy qilgan (misol: Malta Gaming Authority). Bu adolatli o‘yin, shaffoflik va firibgarlikning oldini olish uchun zarur. Tarixan tasodifiy sonlar generatorlari ikki asosiy yondashuvga bo‘lingan:

1. Psevdotasodifiy generatorlar (PRNG) — deterministik ketma-ketliklar;
2. Fizik RNGlar (TRNG) — aniqsiz fizik jarayonlarga asoslangan.

Fon Neyman 1970-yillarda kompyuterlarning deterministik tabiatiga ishora qilib, haqiqiy tasodifiylik faqat fizik jarayonlardan kelib chiqishini ta’kidlagan. So‘nggi o‘n yilliklarda TRNGlar bo‘yicha tadqiqotlar sezilarli oshgan bo‘lsa-da, amaliyotda ularning ishlab chiqarilishi murakkab, sertifikatlash va ishonchlilikni nazariy asoslash esa hali ham dolzarb bo‘lib qolmoqda.

TASODIFIY SONLAR GENERATORLARI

Tarixiy jihatdan tasodifiy sonlar yaratishning ikkita asosiy usuli mavjud: algoritmik (psevdotasodifiy) usul va fizik (haqiqiy yoki nodeterministik) usul. Ilmiy adabiyotlarda psevdotasodifiy son generatorlari (PRNG) atroflicha o‘rganilganligi sababli, bu yerda ularga chuqur to‘xtalib o‘tmaymiz. Buning o‘rniga, [1] va [2] manbalarida batafsil tahlillar va amaliy misollarni topish mumkin.

PRNG aslida boshlang’ich qiymat (urug’) bilan belgilanadigan, deterministik va davriy sonlar ketma-ketligini yaratadigan matematik algoritmdir. Muhimi, bunday generatorlar tomonidan hosil qilingan ketma-ketliklarning haqiqiy tasodifiyligi matematik jihatdan isbotlanmaydi. Ular qisqa muddatda nol va birlarning muvozanatligini ta’minlashi mumkin bo‘lsa-da, ko‘pincha uzoq masofali korrelyatsiyaga ega bo‘ladi. Bu xususiyat kriptografik tizimlarda zaiflik yuzaga keltirishi, Monte-Karlo simulatsiyalarida yoki raqamli hisob-kitoblarda sezilmaydigan, ammo jiddiy xatoliklarni keltirib chiqarishi mumkin.

Garchi ko‘plab zamonaviy PRNGlar statistik testlardan muvaffaqiyatli o‘tsa-da, ba’zi generatorlarning boshqalariga qaraganda “universal ravishda ustun” degan tushuncha noto‘g’ri hisoblanadi. Amaliyotda har qanday PRNGning o‘ziga xos kamchiliklari mavjud bo‘lib, ular faqat ma’lum shartlar ostida namoyon bo‘ladi. Adabiyotlarda PRNGlar tasodifiy jarayonlarni noto‘g’ri modellashtirishi yoki hisoblashlarda jiddiy xatoliklarga olib kelgan holatlar qayd etilgan [3], [4].

Shuningdek, barcha taniqli PRNG oilalari kriptografiya sohasida turli hujumlar yo‘li bilan ularning xavfsizligi sinchkovlik bilan tekshirilgan va ularning zaif tomonlari aniqlandi [5], [6]. Shu sababli, yuqori darajadagi oldindan aytib bo‘lmaslikni talab qiladigan kriptografik qurilmalarda PRNGlardan foydalanish potentsial xavf hisoblanadi.

Ularning deterministik tabiati tufayli, hech qanday PRNG tasodifiylikning ideal talablariga to‘liq javob bera olmaydi. Agar algoritm va boshlang’ich qiymat ma’lum bo‘lsa, butun sonlar ketma-ketligini qayta tiklash mumkin – bu esa "oldindan aytib bo‘lmaslik" prinsipiga asoslangan tizimlar uchun jiddiy tahlikdir.

Shu bilan birga, PRNGlarning aniq afzalliklari bor:

- Iqtisodiy va qulay – dasturlarga oson integratsiya qilinadi.
- Juda tez – katta hajmdagi ma’lumotlarni osongina yarata oladi.

• Protsessorlar va umuman shaxsiy kompyuterlar uchun juda mos keladi.

Ammo, ayniqsa xavfsizlik talablari yuqori bo‘lgan hollarda, iloji boricha fizik (haqiqiy) tasodifiy son generatorlaridan (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:

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

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

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

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:

• 1×10^9 bit ma’lumotni NIST STS orqali tekshirish ≈ 6 soat

- Shu miqdordagi ma’lumotni kvant RNG generatsiya qilishi 7–250 soniya

Tasodifiy son generatorlarining (RNG) ma’lum bir turi qanday xatolarga moyil ekanligi ma’lum bo‘lsa, uning zaif tomonlarini aniqlash uchun maxsus testlar ishlatish mumkin.

Kvant kriptografiyasida Alisa va Bob ochiq kanal orqali maxfiy kalit yarata olishadi. BB84 protokoli (1984-yilda ishlab chiqilgan va 1991-yilda eksperimental tasdiqlangan) asosiy vosita hisoblanadi [18]. Protokol kvant kanali (fotonlar orqali) va klassik kanaldan (Internet, radio) foydalanadi.

Alisa tasodifiy bitlarni foton polarizatsiyasiga kodlaydi, Bob esa tasodifiy o‘lchash bazasini tanlaydi. Agar bazalar mos tushsa, to‘g’ri bit olinadi. Protokolning xavfsizligi Alisa va Bobning tasodifiy tanlovlariga tayanadi. Agar Eva bu tasodifiylikni bashorat qila olsa, kalitni tiklay oladi. Shuning uchun BB84 yuqori sifatli tasodifiy sonlar talab qiladi [19].

Protokol ma’lumotlarni muvofiqlashtirish va maxfiylikni kuchaytirish bosqichlarini o‘z ichiga oladi. Amaliyotda esa kvant tizimlari zaifliklarga ega: 2007-yilda MIT tadqiqotchilari Bobning detektorlari ma’lum bo‘lsa, kalitni tiklash mumkinligini ko‘rsatdi. 2010-yilda esa tijorat kvant qurilmalariga muvaffaqiyatli hujumlar amalga oshirildi [20].

Statistik kriptografiya (Maurer, 1991) SKAPD protokoli asosida ishlaydi va uch bosqichdan iborat: afzallikni oshirish, ma’lumotlarni muvofiqlashtirish va maxfiylikni kuchaytirish. Xavfsizlik Alisa va Bobning Evaga nisbatan ko‘proq ma’lumotga ega ekanligiga bog’liq, bu esa tasodifiy sonlar sifatiga bog’liq [21-23].

Deterministik kriptografiya diskret logarifm yoki sonlarni faktorizatsiya qilish kabi qiyin masalalarga asoslansa ham, kalitlar, noncelar va seans kalitlarini yaratishda yuqori sifatli tasodifiy sonlar muhim ahamiyatga ega. Tasodifiylik sifati past bo‘lsa, butun tizim xavf ostida qoladi.

XULOSA

Tasodifiy sonlar zamonaviy kriptografiya va axborot xavfsizligi uchun asosiy tayanch hisoblanadi. Kompyuter tizimlarining deterministik tabiati haqiqiy tasodifiylikni yaratishga imkon bermaydi, shuning uchun fizik jarayonlarga asoslangan generatorlardan foydalanish talab qilinadi. Ammo amaliyotda fizik generatorlarni keng joriy etish bir qator qiyinchiliklar bilan bog’liq. Ularning ishlab chiqarayotgan tasodifiy sonlari nazariy jihatdan to‘liq isbotlangan emas va doimiy tekshirishni talab qiladi. Qurilmalarning qimmatligi, sertifikatlash muammolari va texnik nosozliklarni aniqlash qiyinligi qo‘shimcha to‘siqlar yaratadi.

FOYDALANILGAN ADABIYOTLAR:

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.