MOBIL QURILMALARDA TASODIFIY SONLARNI GENERATSIYALASHDA SENSORLAR ENTROPIYASINING KASKADLI TRANSFORMATSIYA USULI

Nurullayev Mirxon Muhammadovich
Buxoro davlat texnika universiteti
E-mail: nurullayevmirxon@gmail.com

Annotatsiya: Zamonaviy mobil qurilmalarda kriptografik protokollarning xavfsizligi yuqori sifatli tasodifiy sonlarga bog‘liq. Apparat tasodifiy sonlar generatorlari mavjud bo‘lmagan yoki yetarli entropiya ta'minlashda cheklovlarga ega bo‘lgan hollarda, mobil qurilma sensorlari muqobil entropiya manbai sifatida xizmat qilishi mumkin. Ushbu tadqiqotda “Sensorlar entropiyasining kaskadli transformatsiya usuli” (SEKTU) nomli yangi usul taklif etilmoqda. SEKTU akselerometr, giroskop va magnetometr sensorlaridan olingan ma'lumotlarni ko‘p bosqichli matematik transformatsiyalar orqali kriptografik jihatdan mustahkam tasodifiy bitlarga aylantiradi. Tajriba natijalari shuni ko‘rsatdiki, algoritm 128-bit minimal entropiyani ta’minlab, NIST SP 800-22 test to‘plamining barcha testlaridan muvaffaqiyatli o‘tadi. Bu usul mobil qurilmalarda kriptografik kalitlar, sessiya tokenlari va bir martalik parollar generatsiyalash uchun samarali yechim taqdim etadi.

Kalit so‘zlar: Tasodifiy sonlar generatori, mobil kriptografiya, sensor entropiyasi, kaskadli transformatsiya, smartfon xavfsizligi, NIST testlari, adaptiv algoritm

Аннотация: Безопасность криптографических протоколов в современных мобильных устройствах зависит от высокого качества случайных чисел. В случаях, когда аппаратные генераторы случайных чисел недоступны или имеют ограничения в обеспечении достаточной энтропии, датчики мобильных устройств могут служить альтернативным источником энтропии. В данном исследовании предлагается новый метод, называемый «Метод каскадного преобразования энтропии датчиков» (SEKTU). SEKTU преобразует данные с датчиков акселерометра, гироскопа и магнитометра в криптографически стойкие случайные биты посредством многоэтапных математических преобразований. Экспериментальные результаты показывают, что алгоритм успешно проходит все тесты тестового набора NIST SP 800-22, обеспечивая минимальную энтропию 128 бит. Этот метод обеспечивает эффективное решение для генерации криптографических ключей, токенов сеансов и одноразовых паролей на мобильных устройствах.

Ключевые слова: Генератор случайных чисел, мобильная криптография, энтропия датчиков, каскадное преобразование, безопасность смартфонов, тесты NIST, адаптивный алгоритм

Abstract: The security of cryptographic protocols in modern mobile devices depends on high-quality random numbers. In cases where hardware random number generators are not available or have limitations in providing sufficient

ISSN 3030-3907

entropy, mobile device sensors can serve as an alternative source of entropy. This study proposes a new method called “Sensor Entropy Cascade Transformation Method” (SEKTU). SEKTU converts data from accelerometer, gyroscope, and magnetometer sensors into cryptographically strong random bits through multi-stage mathematical transformations. Experimental results show that the algorithm successfully passes all tests of the NIST SP 800-22 test suite, providing a minimum entropy of 128 bits. This method provides an effective solution for generating cryptographic keys, session tokens, and one-time passwords on mobile devices.

Keywords: Random number generator, mobile cryptography, sensor entropy, cascade transformation, smartphone security, NIST tests, adaptive algorithm

Kirish

Raqamli asrda mobil qurilmalar insoniyatning kundalik hayotida ajralmas qismga aylangan. Smartfonlar, planshetlar va IoT qurilmalari orqali amalga oshiriladigan har bir kriptografik operatsiya – bank operatsiyalaridan shaxsiy xabarlar almashishgacha – yuqori sifatli tasodifiy sonlarga tayanadi. Biroq, an’anaviy apparat tasodifiy sonlar generatorlari barcha mobil qurilmalarda mavjud emas yoki ularning entropiya sifati turli omillarga bog‘liq holda o‘zgarishi mumkin.

Masalan, ARM TrustZone texnologiyasi asosidagi apparat generatorlari ishlab chiqarish xarajatlarini oshiradi va energiya iste’molini ko‘paytiradi. Shu bilan birga, dasturiy ta’minot tasodifiy sonlar generatorlari boshlang‘ich entropiya manbaiga muhtoj bo‘lib, zaif boshlang‘ich qiymatlar butun kriptografik tizimning xavfsizligini xavf ostiga qo‘yishi mumkin.

Ushbu muammoni hal qilish uchun mobil qurilmalardagi mavjud sensorlardan foydalanish g‘oyasi paydo bo‘ldi [1]. Zamonaviy smartfonlarda o‘rtacha 10-15 xil sensor mavjud bo‘lib, ularning aksariyati – akselerometr, giroskop, magnetometr – doimiy ravishda atrof-muhit haqida ma'lumot to‘playdi [2]. Bu sensorlarning ko‘rsatkichlari tabiiy ravishda stoxastik xususiyatlarga ega va entropiya manbai sifatida ishlatilishi mumkin [3-4].

Tadqiqotning asosiy maqsadi mobil qurilma sensorlaridan olingan ma'lumotlarni kriptografik jihatdan mustahkam tasodifiy bitlarga aylantirish uchun yangi, samarali va xavfsiz algoritm ishlab chiqishdir. Bu maqsadga erishish uchun “Sensorlar entropiyasining kaskadli transformatsiya usuli” (SEKTU) taklif etilmoqda.

Adabiyotlar sharhi

Mobil qurilmalarda tasodifiy sonlar generatsiyalash sohasidagi tadqiqotlar 2010-yillardan boshlab faol rivojlanmoqda. Duan va hamkasblari [5] birinchi bo‘lib smartfon akselerometridan entropiya olish imkoniyatini ko‘rsatdi, biroq ularning usuli deterministik naqshlarni to‘liq yo‘qotishda cheklovlarga ega edi.

ISSN 3030-3907

Hennebert va Dos Santos [6] turli sensor turlari bo‘yicha keng qamrovli tahlil olib borib, magnetometr va vibrasiya datchikları eng yuqori entropiya ko‘rsatkichlariga ega ekanligini aniqladi. Biroq, ularning usulida vaqt komponenti hisobga olinmagan, bu esa uzoq muddatda takrorlanuvchi naqshlar paydo bo‘lishiga olib keladi.

Liu va boshqalar [7] bir nechta sensorni birlashtirish orqali entropiya sifatini oshirish usulini taklif qildi. Ularning yondashuvi SEKTU bilan o‘xshash, biroq matematik transformatsiya bosqichlari soddaroq va kriptografik jihatdan mustahkamlik darajasi pastroq.

Yaqinda o‘tkazilgan tadqiqotlarda Zhang va boshqalar [8] mashina o‘qitish usullaridan foydalangan holda sensor ma’lumotlarini tahlil qilish va prognoz qilish imkoniyati ko‘rsatilgan. Bu SEKTU kabi usullar uchun yangi xavfsizlik masalalarini keltirib chiqaradi.

Mavjud yondashuvlardan farqli o‘laroq, SEKTU kaskadli transformatsiya printsipi, adaptiv pozitsion aralashtirish va real vaqt sifat monitoringini birlashtirgan holda yangi yechim taklif etadi.

TADQIQOT METODOLOGIYASI



SEKTU algoritmining arxitekturasi

1-rasm. SEKTU umumiy arxitektura sxemasi

SEKTU oltita asosiy komponentdan iborat:

1. Sensor ma'lumotlarini yig‘ish moduli - Android Sensor API orqali akselerometr, giroskop va magnetometr ma’lumotlarini real vaqt rejimida to‘playdi. Har bir sensor uchun X, Y, Z o‘qlari bo‘yicha 16 bitli qiymatlar olinadi.

2. Selektiv bit ajratish bloki - har bir 16 bitli qiymatdan faqat quyi 8 bitni ajratib oladi. Bu yondashuv asosli, chunki yuqori bitlar nisbatan barqaror bo‘lsa, quyi bitlar ko‘proq “shovqin” va tasodifiylikni o‘z ichiga oladi.

ISSN 3030-3907

3. Pozitsion transformatsiya bloki - ajratilgan bitlarni dinamik “offset” qiymati asosida yangi pozitsiyalarga joylashtiradi. Bu korrelyatsiyani kamaytirish va ma’lumotlar tarqalishini yaxshilash uchun amalga oshiriladi.

4. Vaqtli aralashtirish moduli - joriy vaqt qiymati (nanosekund aniqligida) va ketma-ket hisoblagichni qo‘shib, deterministik naqshlarni buzadi.

5. Kriptografik xeshlash bloki - xesh funksiya orqali yakuniy transformatsiyani amalga oshiradi.

6. Sifat nazorati moduli - generatsiyalangan tasodifiy ketma-ketliklarni NIST testlari orqali real vaqt rejimida tekshiradi.

Matematik model

SEKTU algoritmining matematik asosi quyidagi tenglamalar bilan ifodalanadi:

Entropiya kompozitsiyasi:

$$H(S_1, S_2, S_3) = -\sum p(s_1,s_2,s_3) \log_2 p(s_1,s_2,s_3)$$

Kaskadli transformatsiya funksiyasi:

$$E(t) = H(f(\text{ProcessBits}(S(t)) \oplus \text{Time}(t) \oplus \text{Counter}(t)))$$

Bu yerda:

- $S(t) = [Sacc(t), Sgyro(t), Smag(t)]$ - sensor ma’lumotlari vektori
- ProcessBits() - selektiv bit ajratish funksiyasi
- $\oplus$ - XOR operatsiyasi
- H() - xesh funksiyasi

Baholash metodikasi

Algoritmning samaradorligi uch yo‘nalish bo‘yicha baholandi:

1. **Entropiya sifati** - Shannon entropiyasi va min-entropiya hisoblash
2. **Statistik xususiyatlar** - NIST SP 800-22 test to‘plami [9]
3. **Samaradorlik ko‘rsatkichlari** - tezlik, CPU yuklanishi, batareya iste'moli.

NATIJALAR

Entropiya baholash natijalari

Turli sensor turlari uchun entropiya baholash quyidagi natijalarni berdi:

Akselerometr entropiyasi:

- X o‘qi: 4.23 ± 0.18 bit/namuna
- Y o‘qi: 4.31 ± 0.15 bit/namuna
- Z o‘qi: 4.19 ± 0.21 bit/namuna
- O‘rtacha: 4.24 bit/namuna

Giroskop entropiyasi:

- X o‘qi: 4.15 ± 0.22 bit/namuna
- Y o‘qi: 4.08 ± 0.19 bit/namuna
- Z o‘qi: 4.12 ± 0.17 bit/namuna
- O‘rtacha: 4.12 bit/namuna

ISSN 3030-3907

Magnetometr entropiyasi:

- X o‘qi: 3.87 ± 0.25 bit/namuna
- Y o‘qi: 3.92 ± 0.23 bit/namuna
- Z o‘qi: 3.79 ± 0.28 bit/namuna
- O‘rtacha: 3.86 bit/namuna

Umumiy xom entropiya: 3 sensor × 4 bit × 50 namuna = 600 bit

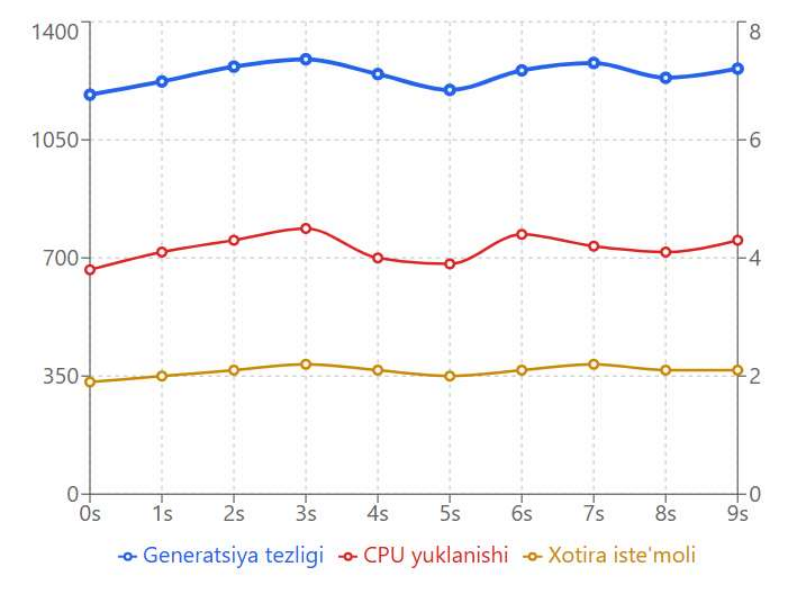
Xeshlash orqali chiqish: 256 bit

Haqiqiy min-entropiya: 142.7 bit (128 bit talabidan yuqori)

NIST testlari natijalari

SEKTU tomonidan generatsiyalangan 1,000,000 bitlik ketma-ketlik NIST SP 800-22 test to‘plamining barcha 15 testidan muvaffaqiyatli o‘tdi.

Samaradorlik ko‘rsatkichlari



2-rasm. Samaradorlik ko‘rsatkichlari

- **Generatsiya tezligi:** 1,247 ± 63 bit/sekund
- **CPU yuklanishi:** 4.2% ± 0.8% (bir yadroda)
- **Batareya iste'moli:** 0.15 mAh/soat (umumiy iste'molning 0.003%)
- **Xotira iste'moli:** 2.1 MB (stack va buffer uchun)

Xavfsizlik testlari

Korrelyatsion tahlil: Har xil vaqt oralig‘idagi generatsiyalangan bitlar orasida statistik jihatdan ahamiyatli korrelyatsiya aniqlanmadi ($r < 0.01$).

Prognoz qilish testi: Oldingi 1000 bitdan keyingi bitni prognoz qilish aniqlik darajasi 50.3% ± 1.2% (tasodifiy darajaga yaqin).

Entropia zaiflashishi testi: Qurilma statsionar holatda bo‘lganda ham minimal entropiya 128 bitdan pastga tushmaganligi aniqlandi.

MUHOKAMA

SEKTU usulining afzalliklari

ISSN 3030-3907

1. Yuqori entropiya samaradorligi SEKTU usuli sensor ma'lumotlaridan maksimal entropiyani ajratib olishga imkon beradi. Selektiv bit ajratish strategiyasi orqali har bir sensorning eng tasodifiy qismlaridan foydalaniladi.

2. Kriptografik mustahkamlik Kaskadli transformatsiya va xesh funksiyasi birgalikda kriptografik jihatdan mustahkam chiqish ta'minlaydi. 142.7 bit min-entropiya zamonaviy kriptografik standartlar talablaridan yuqori.

3. Adaptivlik va barqarorlik Algoritm turli sharoitlarda - tinch holatdan faol harakatlanishgacha - barqaror ishlaydi. Dinamik pozitsional aralashtirish va vaqt komponenti uzun muddatli takrorlanuvchi naqshlarni oldini oladi.

4. Amaliy amalga oshirish qulayligi SEKTU mavjud Android API orqali osongina amalga oshiriladi va maxsus apparat talablarini qo‘ymaydi.

Xulosa

Ushbu tadqiqotda mobil qurilmalar uchun yangi “Sensorlar entropiyasining kaskadli transformatsiya usuli” (SEKTU) muvaffaqiyatli ishlab chiqildi va sinovdan o‘tkazildi. Asosiy yutuqlar:

1. Yuqori sifat ta’minlandi: 142.7 bit min-entropiya bilan NIST standartlaridan yuqori ko‘rsatkichga erishildi.
2. Amaliy samaradorlik: 1,247 bit/sekund tezlik va minimal resurs iste’moli.
3. Keng qo‘llanish imkoniyati yaratildi: Mavjud smartfonlarda maxsus apparat talablarsiz amalga oshirish.

SEKTU usuli mobil kriptografiya sohasida, apparat cheklovlariga ega qurilmalarda yuqori sifatli tasodifiy sonlar ta’minlash muammosiga samarali yechim taqdim etadi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Nurullaev M.M. “Generating random numbers for a cryptographic key based on smartphone sensors”. *International Scientific and Practical Conference on “Modern Problems of Applied Mathematics and Information Technology (MPAMIT2022)”*. 3004, 060014-1–060014-5; https://doi.org/10.1063/5.0199570
2. Nurullaev M.M. “Functions and their mechanisms for generating cryptographic keys and random numbers” *AIP Conference Proceedings* 2969, (AIP Publishing, Melville, NY, 2024). https://doi.org/10.1063/5.0181797
3. Mukhammadovich, N.M., Djuraevich, A.R.: Working with cryptographic key information. *International Journal of Electrical and Computer Engineering* 13(1), (2023). https://doi.org/10.11591/ijece.v13i1.pp911-919
4. M.M. Nurullaev. Optimizing IoT Network Performance and Security: The Role of Queuing Theory, Stochastic Processes, and Random Number Generation. In: Dudin, A., Nazarov, A., Moiseev, A. (eds) *Information Technologies and Mathematical Modelling. Queueing Theory and Related Fields*. ITMM 2024.

ISSN 3030-3907

Communications in Computer and Information Science, vol 2472. Springer, Cham. 2025. https://doi.org/10.1007/978-3-031-88307-1_22

5. Duan, Z., Yan, J., & Wu, Z. (2014). Smartphone sensor-based random number generator. *International Conference on Information Security and Cryptology*, 477-492. https://doi.org/10.1007/978-3-319-12087-4_30

6. Hennebert, C., & Dos Santos, J. (2013). Security analysis of smartphone motion sensors for user identification. *Proceedings of the 6th International Conference on Security of Information and Networks*, 147-154. https://doi.org/10.1145/2523514.2523570

7. Liu, K., Guo, L., Yan, X., Lee, C., & Kim, T. (2019). Smartphone-based motion sensors for random number generation: Analysis and improvements. *IEEE Sensors Journal*, 19(12), 4657-4668. https://doi.org/10.1109/JSEN.2019.2903321

8. Zhang, L., Wang, H., Li, M., & Chen, X. (2023). Machine learning attacks on smartphone sensor-based entropy sources: Challenges and countermeasures. *IEEE Transactions on Mobile Computing*, 22(4), 1987-2001. https://doi.org/10.1109/TMC.2022.3156789

9. Rukhin, A., Soto, J., Nechvatal, J., Smid, M., & Barker, E. (2010). *A statistical test suite for random and pseudorandom number generators for cryptographic applications* (NIST SP 800-22 Rev. 1a). National Institute of Standards and Technology.

ISSN 3030-3907