KVANT MUHITIDA QUVVAT TAHLILI HUJUMLARI VA KRIPTOGRAFIK SXEMALARNI LOYIHALASH

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

Annotatsiya: *Quantum-dot Cellular Automata (QCA) — past energiya sarfi, yuqori zichlik va katta tezlikka ega bo‘lgan istiqbolli post-CMOS nanotexnologiya bo‘lib, uni kriptografik sxemalarni loyihalashda qo‘llash bo‘yicha izlanishlar kengayib bormoqda. Shunga qaramay, QCA asosidagi kriptoarxitekturalar quvvat tahlili hujumlari (Power Analysis Attacks, PAA)ga nisbatan sezilarli darajada zaif bo‘lib qolmoqda. Ushbu maqolada Serpent blok shifri, A5/1 oqim shifri hamda QCA asosida qurilgan haqiqiy tasodifiy sonlar generatorlarining (TRNG) barqarorligi baholanadi. Shuningdek, QCA qurilmalarida quvvat iste’moli modellari, xavfsizlik va samaradorlik o‘rtasidagi muvozanat, hamda nano va kvant kommunikatsiya tizimlarida qo‘llanishi mumkin bo‘lgan yangi himoya yondashuvlari ko‘rib chiqiladi.*

Kalit so‘zlar: *quvvat tahlili hujumi, tasodifiy sonlar generatsiyasi, psevdotasodifiy generator, entropiya, kriptografiya, simulyatsiya.*

KIRISH

Raqamli tizimlarning nanomasshtabga o‘tishi xavfsiz, energiya samarador va masshtablanadigan kriptografik qurilmalar zaruratini keskin oshirdi. CMOS texnologiyasining issiqlik tarqalishi, quvvat sizib chiqishi va fizika chegaralaridagi cheklovlari fonida Quantum-dot Cellular Automata (QCA) texnologiyasi zamonaviy alternativ sifatida e’tirof etilmoqda. QCA quyidagi afzalliklari bilan ajralib turadi:

- deyarli nol statik quvvat sarfi,
- juda yuqori integratsiya zichligi,
- yuqori soatlash chastotalari.

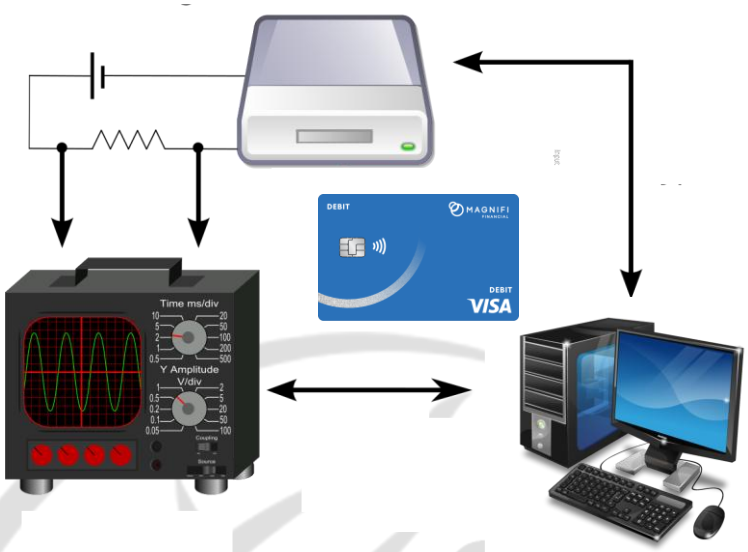
Bu xususiyatlar QCAni nano va kvant tarmoqlarida kriptografik algoritmlarni amalga oshirish uchun jozibador variantga aylantiradi. Biroq past energiya sarfi avtomatik ravishda yon kanal hujumlariga qarshi chidamlilikni kafolatlamaydi; aksincha, qutblanish almashinuvi asosidagi quvvat tebranishlari PAA orqali maxfiy kalit haqida ma’lumot sizib chiqishiga sabab bo‘lishi mumkin [1].

Maqolada QCA asosida loyihalashtirilgan Serpent shifri, A5/1 oqim shifri, reversiv autentifikatsiya sxemalari va TRNG qurilmalarining quvvat tahliliga nisbatan zaifliklari baholanadi. Bundan tashqari, reversible mantiq elementlari yordamida quvvat izini kamaytirish imkoniyatlari ham tahlil qilinadi [2].

QCA SXEMALARIDA QUVVAT TAHLILI HUJUMLARI

QCA uchun yuqori chegarali quvvat modeli. QCA sxemalarida PAAga qarshi zaiflikni baholash uchun [3] tomonidan yuqori chegarali (upper bound) quvvat modeli taklif

qilingan(1-rasm). Model signallar uzatilishi jarayonida sodir bo‘ladigan qutblanish almashinuvi (polarization switching) orqali dinamik quvvat sarfini baholaydi.



1-Rasm. Quvvat tahlili hujumlari

Tadqiqotda Serpent shifrining 4×4 kichik moduli QCA muhitida loyihalanib, juda kichik quvvat o‘zgarishlarining ham kalitni aniqlashda yetarli bo‘lishi ko‘rsatildi. Natijalar shuni anglatadiki, QCAning past quvvat iste’moli uni avtomatik ravishda yon kanal hujumlariga chidamli qilmaydi.

QCA asosidagi Serpent shifri. Serpent shifri 32 raundli SPN (Substitution–Permutation Network) tuzilmasi sababli yuqori kriptoturg‘unlikka ega. Ammo QCAda amalga oshirilgan Serpent varianti ham quvvat tahlili asosida kalit tiklash hujumlariga moyil ekanligi ko‘rsatildi [4].

Mualliflar [5] quyidagi xususiyatlarga ega to‘liq QCA-Serpent arxitekturasini yaratgan:

- 128-bit blok, 32 raund SPN,
- AND, NOT va chiziqli transformatsiyalardan tashkil topgan kalit aralashuvi,
- ~4 800 QCA hujayrali, 16:1 MUX asosidagi ixcham S-blok,
- har bir chiqish uchun 10 soat sikli.

Murakkabligi yuqori bo‘lishiga qaramay, S-blokdagi quvvat tebranishlari orqali kalit bitlarini tiklash imkoniyati mavjud.

QCA ASOSIDA KRIPTOGRAFIK ARXITEKTURALAR

Shifrlash va deshifrlash. Mualliflar [9] nanoaloqa uchun mos bo‘lgan XOR asosidagi shifrlash–deshifrlash (encoder–decoder) sxemasini taklif qilgan:

$$B_i = E_{K_i}(A_i) = A_i + K_i \; mod \; 2$$

$$A_i = D_{K_i}(B_i) = B_i + K_i \; mod \; 2$$

Sxema:

- 42 ta QCA hujayrasi,
- 3 ta majority gate va 2 ta invertordan iborat,
- umumiy maydon ~36 000 nm².

Model yaxshi masshtablanuvchi bo‘lib, istalgan uzunlikdagi kalitlarni qo‘llab-quvvatlaydi.

A5/1 oqim shifrining QCAdagi modellashtirilishi. A5/1 shifri GSM tizimlarida qo‘llaniladi. Uni QCAda amalga oshirish [6] da ko‘rsatildi. Asosiy element — majority gate asosida boshqariladigan ketma-ket registrlar. ENABLE signali orqali xotira blokining holatini yangilash yoki saqlash imkoniyati yaratildi. Bu real vaqt rejimida oqim shifrlashni qo‘llashga imkon beradi.

Reversiv autentifikatsiya sxemalari. [7] da Fredkin elementlari asosida reversiv autentifikatsiya sxemasi taklif etilgan. Ushbu yondashuv:

- energiya yo‘qotilishini kamaytiradi (axborot yo‘qolmaydi),
- kvant narxi 0.041,
- Hamming masofasi orqali issiqlik shovqiniga chidamliligi isbotlangan.

Kriptografik nano-router arxitekturasi. [8] tadqiqotida nanomasshtabli tarmoqlar uchun xavfsiz yo‘naltirish tizimi taklif etilgan. Tizim quyidagilardan iborat:

- XOR asosidagi shifrlash–deshifrlash moduli,
- 4:1 MUX asosidagi nano-router,
- 1:4 DEMUX asosidagi qabul moduli.

Bu tizim nanoaloqa kanallarida ma’lumot maxfiyligini saqlagan holda yo‘naltirish imkonini yaratadi.

TRNG yaratish. [9] da QCA asosida TRNG taklif etilgan, bunda entropiya:

- self-starved SRAM hujayrasi,
- floating clock mexanizmi

yordamida oshiriladi. TRNGlardagi haqiqiy tasodifiylik kriptografik kalitlar, nonce va IV generatsiyasida hal qiluvchi ahamiyatga ega.

Nosozlikka bardoshli dizaynlar. [10] da QCA asosida D-turdagi triggerning (D-FF) xatolarga chidamli varianti taklif qilingan. Simulyatsiya natijalari:

- energiya sarfining sezilarli kamayishini,
- uzoq muddatli barqarorlikni

ko‘rsatdi. Ushbu yondashuv yuqori ishonchlilik talab qilinadigan kriptoarxitekturalar uchun muhim.

XULOSA

Quantum-dot Cellular Automata (QCA) texnologiyasi kriptografik sxemalarni energiya samarali, zich va tezkor shaklda yaratish imkonini beradi. Ammo o‘tkazilgan tahlillar shuni ko‘rsatadiki, QCA sxemalari quvvat tahlili hujumlariga to‘liq barqaror emas. Kalitga bog‘liq bo‘lgan quvvat tebranishlari PAA orqali muvaffaqiyatli ekspluatatsiya qilinishi mumkin.

Kelajak tadqiqotlar quyidagilarga qaratilishi lozim:

- yanada aniqlashtirilgan quvvat modellari ishlab chiqish,
- S-bloklarning PAAga chidamli dizaynlarini yaratish,
- yuqori entropiyali TRNGlarga doir yangi arxitekturalar taklif qilish,
- reversiv mantiq elementlari asosida quvvat izini kamaytirish yondashuvlarini kengaytirish.

QCA texnologiyasi nano va kvant kommunikatsiyalarida xavfsiz kriptotizimlar uchun katta salohiyatga ega, biroq yon kanal hujumlari — ayniqsa quvvat tahlili — bu texnologiyada hal etilishi zarur bo‘lgan asosiy muammolardan biridir.

FOYDALANILGAN ADABIYOTLAR:

1. Chan, W. K. (2009). Random Number Generation in Simulation.
2. Gutterman, Z., Pinkas, B., & Reinman, T. (2006). Analysis of the Linux Random Number Generator.
3. Haahr, M. (2011). Introduction to Randomness and Random Numbers.
4. Marsaglia, G. (2005). Random Number Generators.
5. Schneier, B. (2007). Dual_EC_DRBG: A Case Study in Backdoors.
6. Sunar, B., Martin, W., & Stinson, D. (2006). A Provably Secure True Random Number Generator.
7. Eastlake, D., Schiller, J., & Crocker, S. (2005). Randomness Requirements for Security. RFC 4086. https://www.rfc-editor.org/rfc/rfc4086
8. Gutterman, Z., Pinkas, B., & Reinman, T. (2006). Analysis of the Linux Random Number Generator. IEEE Symposium on Security and Privacy. https://doi.org/10.1109/SP.2006.26
9. Dorrendorf, L., Gutterman, Z., & Pinkas, B. (2007). Cryptanalysis of the Random Number Generator of the Windows Operating System. ACM CCS. https://doi.org/10.1145/1315245.1315274
10. Lacharme, P. (2012). Security flaws in Linux's /dev/random. https://eprint.iacr.org/2012/251
11. Kelsey, J., Schneier, B., Ferguson, N. (1999). Yarrow-160: Notes on the Design and Analysis of the Yarrow Cryptographic Pseudorandom Number Generator. https://www.schneier.com/paper-yarrow.pdf
12. Dodis, Y., et al. (2013). Security Analysis of Pseudorandom Number Generators with Input: /dev/random is not Robust. ACM CCS. https://doi.org/10.1145/2508859.2516661
13. National Institute of Standards and Technology. (2012). A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST SP 800-22 Rev. 1a. https://doi.org/10.6028/NIST.SP.800-22r1a
14. Müller, T. (2013). Security of the OpenSSL PRNG. International Journal of Information Security, 12(4), 251–265. https://doi.org/10.1007/s10207-013-0213-7