

XOTIRA QURILMALARINING RIVOJLANISH TENDENSIYASI VA ULARDA AXBOROT XAVFSIZLIGINI TA'MINLASH BILAN BOG'LIQ MUAMMOLAR TAHLILI

DSc, professor Raximov Baxtiyorjon Ne'matovich

PhD, professor Yusupov Bahodir Karamatovich

O'zbekiston Respublikasi Harbiy xavfsizlik va mudofaa universitetining

Axborot-kommunikatsiya texnologiyalari va harbiy aloqa instituti

Tel: +998977180560, E-mail: bahodiryusupov1988@gmail.com

Annotatsiya: Ushbu maqolada yangi avlod xotira qurilmalarining rivojlanish tendensiyalari va ularda axborot xavfsizligini ta'minlashning zamonaviy muammolari tahlil qilingan. Shuningdek, maqolada tarmoqqa asoslangan disagregatsiyalangan xotira, bulutli ko'p birlamchi ma'lumotlar bazalari (GaussDB), golografik va molekulyar (DNK) xotira tizimlarining ishlash tamoyillari hamda ular bilan bog'liq axborot xavfsizligi zaifliklari 2024–2026-yillardagi xalqaro ilmiy natijalar asosida ko'rib chiqilgan. Ma'lumotlar hajmining 2026-yilga kelib 195 zettabaytga yetishi kutilayotgan sharoitda, an'anaviy saqlash vositalaridan voz kechib, kvant tahdidlariga bardoshli va yuqori zichlikdagi yangi arxitekturalarga o'tish zaruriyati asoslab berilgan.

Kalit so'zlar: yangi avlod xotira qurilmalari, axborot xavfsizligi, disagregatsiyalangan xotira, GaussDB, golografik xotira, molekulyar (DNK) xotira, post-kvant xavfsizlik, INDIGO, SARA hujumlari.

Annotation: This article analyzes the development trends of new generation memory devices and the contemporary challenges of ensuring information security within them. Furthermore, based on international scientific results from 2024-2026, the article examines the operating principles of network-based disaggregated memory, cloud multi-primary databases (GaussDB), holographic and molecular (DNA) memory systems, as well as their associated information security vulnerabilities. Given that the global data volume is expected to reach 195 zettabytes by 2026, the necessity of moving away from traditional storage media and transitioning to new, high-density architectures that are resilient to quantum threats is substantiated.

Keywords: next-generation memory devices, information security, disaggregated memory, GaussDB, holographic memory, molecular (DNA) memory, post-quantum security, INDIGO, SARA attacks.

XXI asrda umumjahon raqamlashtirish jarayoni fonida ma'lumotlarni saqlash usullari harbiy va strategik sohalarda hal qiluvchi ahamiyat kasb etib bormoqda. Bugungi kunning harbiy axborot tizimlari hamda sun'iy intellekt texnologiyalari katta hajmdagi ma'lumotlarni real vaqtda qabul qilish va saqlashni talab etmoqda. Hisob-kitoblarga ko'ra, 2026-yilga borib dunyodagi jami ma'lumotlar hajmi 195 zettabaytga yetishi kutilmoqda. Bu holat odatiy magnitli va yarimo'tkazgichli xotira qurilmalari sig'imini oxirgi chegarasiga yetib kelganini ko'rsatib, mutlaqo yangi fizik qonuniyatlarga asoslangan ma'lumot saqlash tizimlarni amaliyotga joriy etishni taqozo etmoqda [1, 2].

Tarmoqqa asoslangan tarkibiy ajratilgan xotira va INDIGO tizimi

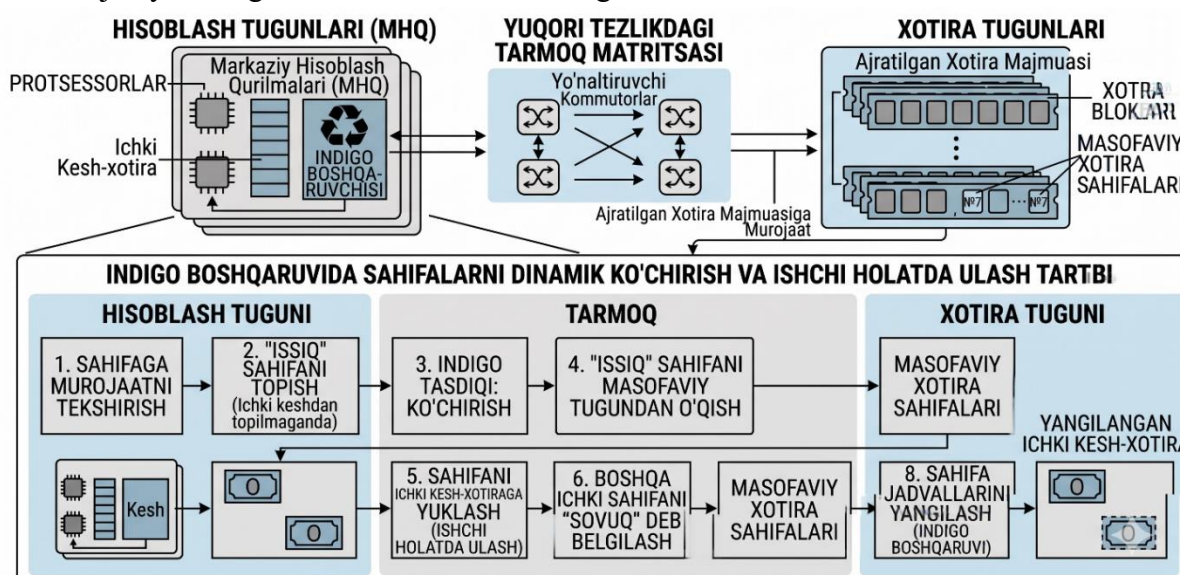
Ma'lumotlarni tarmoq orqali saqlash (Network Attached Storage-NAS) g'oyasi 1984-yilda "Sun Microsystems" kompaniyasi tomonidan taqdim etilgan tarmoq fayl tizimi bilan boshlangan bo'lsa, bugungi kunga kelib ushbu texnologiya apparat xotirani qismlarga ajratish darajasigacha

rivojlandi. 2025-yilda ishlab chiqilgan INDIGO tizim platformasi tarmoqdagi yuklamani hisobga oluvchi ma'lumotlar sahifasini ko'chirish uslubini joriy etdi. INDIGO (Intelligent Disaggregated Information Governance and Optimization-Tarkibiy ajratilgan ma'lumotlarni intellektual boshqarish va optimallashtirish) algoritmi mashinali o'qitish texnologiyasi yordamida tez-tez murojaat qilinadigan ma'lumotlarni markaziy hisoblash qurilmasiga yaqinroq joylashtiradi. Natijada tarmoqdagi ma'lumotlar oqimi ikki baravar kamayadi va ilovalarning ish unumdorligini 50-70% ga oshirishga erishilgan. Tarmoqqa asoslangan tarkibiy ajratilgan xotira va INDIGO tizimining qiyosiy tahlili 1-jadvalda keltirilgan [2, 3].

1-jadval. Tarmoqqa asoslangan tarkibiy ajratilgan xotira va INDIGO tizimining qiyosiy tahlili

№	Xususiyatlari	An'anaviy NAS tizimi (NFS)	Tarkibiy qismlarga ajratilgan xotira (CXL/INDIGO)
1.	Kirish darajasi	Fayl darajasida	Blok va kesh-xotira satri darajasida
2.	Kechikish vaqti	Millisoniyalarda	Mikrosoniyalarlar
3.	Uzatish protokollari	TCP/IP, Ethernet	CXL 3.0, RDMA
4.	Tizim manbalarini boshqarish	Statik (o'zgarmas) taqsimlash	O'zgaruvchan (dinamik) manbalar majmuasi

INDIGO tizimi yordamida tarkibiy ajratilgan xotira arxitekturasida sahifalarni dinamik ko'chirish jarayonining sxemasi 1-rasmda keltirilgan.



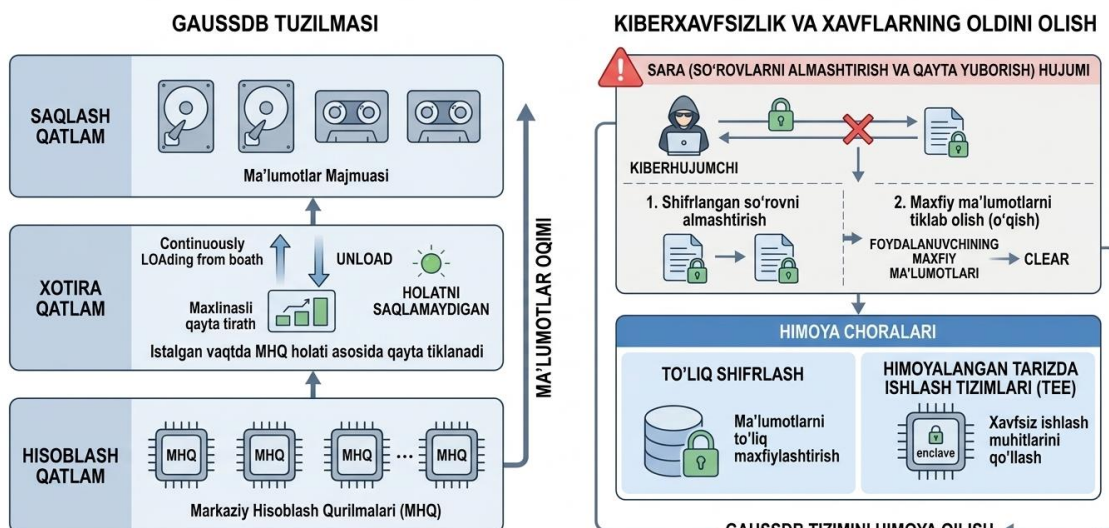
1-rasm. INDIGO tizimi yordamida tarkibiy ajratilgan xotira arxitekturasida sahifalarni dinamik ko'chirish jarayonining sxemasi

Bulutli ko'p markazli ma'lumotlar bazalari: GaussDB arxitekturasida va uning xavfsizligi

Bulutli xotira tizimlarida 2024-yilning eng muhim yangiligi GaussDB - uch qatlamli (hisoblash, xotira va saqlash kabi qismlarga ajratilgan) bulutli ma'lumotlar bazasining yaratilishi bo'ldi. GaussDB tizimida xotira qatlami holatni saqlamaydigan (stateless) xususiyatga ega bo'lib, u istalgan vaqtda markaziy hisoblash tugunlarining holati asosida qayta tiklanishi mumkin.

GaussDB markaziy hisoblash qurilmalari holatidan istalgan paytda qayta tiklanish xususiyatiga ega holatni saqlamaydigan xotira qatlamiga asoslangan, uch bosqichli ajratilgan arxitektura ega bulutli ma'lumotlar bazasidir. Biroq bunday murakkab xotira tizimi arxitekturasida yangi turdagi kiberhujumlarga nisbatan zaif hisoblanadi. Olib borilgan xalqaro tadqiqotlar

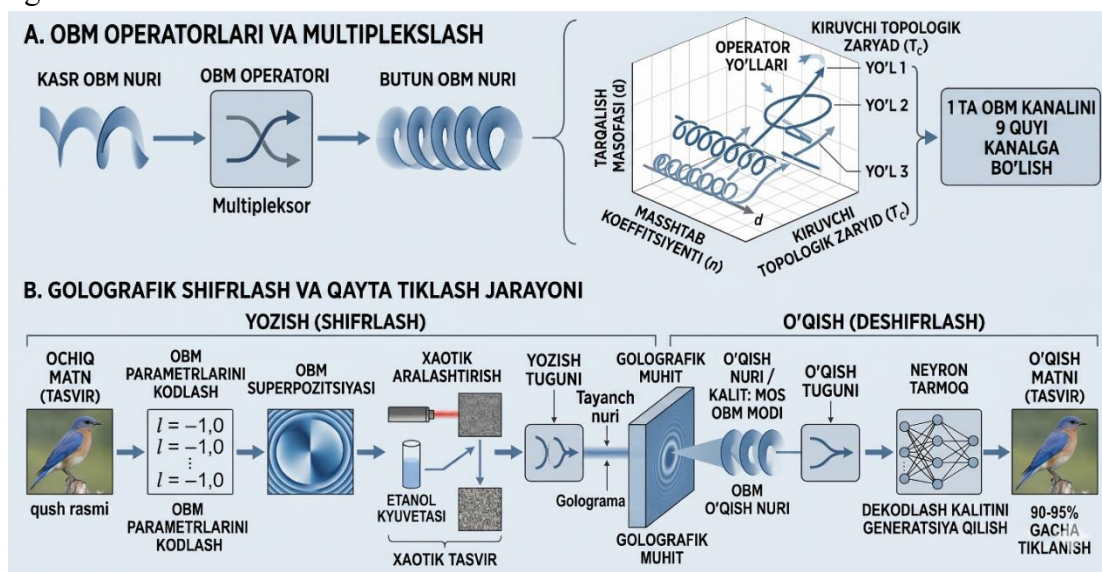
GaussDB kabi tizimlarning texnik xizmat ko'rsatish holatida so'rovlarni almashtirish va qayta yuborish (ing: Substitution and Replay Attacks-SARA) hujumlariga hisbatan zaifliklar borligini aniqlashgan. Ma'lumotlar bazasini boshqaruvchilar so'rovlarni o'zgartirish orqali foydalanuvchilarni konfidensial saqlanishi kerak bo'lgan ma'lumotlarini tiklab olish (o'qish) imkoniyatiga ega ekanligi isbotlangan. Ushbu xavfning oldini olish maqsadida to'liq shifrlash texnologiyasi hamda himoyalangan tarizda ishlash tizimlari amaliyotga joriy etilmoqda. Bulutli ko'p markazli ma'lumotlar bazasi arxitekturasi va uning xavfsizligi 2-rasmda keltirilgan.



2-rasm. Bulutli ko'p markazli ma'lumotlar bazasi arxitekturasi va uning xavfsizligi

Golografik xotira tizimlari: Yorug'likning orbital burchak momenti va optik shifrlash

Golografik xotira ma'lumotlarni uch o'lchamli muhitning to'liq hajmi bo'ylab yozish imkonini beradi. 2025-yilda o'tkazilgan tadqiqotlarga ko'ra, yorug'lik nurining orbital burchak momenti (OAM) xususiyatlaridan foydalanish orqali Golografik xotira sig'imini 9 baravarga oshirishga erishildi. Shu bilan birga, ushbu texnologiya yorug'likning faza va amplitudasini o'zgartirish orqali ma'lumotlarni fizik darajada optik shifrlash imkonini beradi, bu esa axborot xavfsizligini mutlaqo yangi bosqichga olib chiqadi [5]. Yorug'likning orbital burchak momenti (OBM) asosidagi multiplekslash va golografik shifrlash tizimining funksional sxemasi 3-rasmda keltirilgan.



3-rasm. Yorug'likning orbital burchak momenti (OBM) asosidagi multiplekslash va golografik

shifrlash tizimining funksional sxemasi

Golografik xotira tizimining barqaror shlashi va xafsizligi bilan bog'liq asosiy kamchiliklar quyidagilardan iborat:

- Fizik eskirish: Yorug'likka sezgir moddalar (fotopolimerlar) hajmining torayishi (qisqarishi) yozilgan ma'lumotlarning yo'qolishiga va yorug'lik nuri tushish burchagining buzilishiga olib keladi [6].

- Yuqori quvvat sarfi: Microsoft kompaniyasi tadqiqotlariga ko'ra, golografik xotira tizimlari bozorda raqobatbardosh bo'lishi uchun ularning energiya tejamkorligini 10 dan 100 baravargacha oshirish talab etiladi.

Kriptografik himoya vositalari bilan bog'liq zaifliklar quyidagilardan iborat:

- Tayanch nur parametrlarining o'g'irlanishi. Golografik xotiradagi ma'lumotni o'qish uchun uni yozishda foydalanilgan lazer nurining aniq burchagi, to'lqin uzunligi va fazasi talab qilinadi. Bu parametrlar o'ziga xos "ochiq kalit" vazifasini bajaradi. Agar buzg'unchi ushbu optik kalit parametrlarini qo'lga kiritisa, xotira muhitidagi barcha ma'lumotlarni to'siqsiz o'qib olishi mumkin.

- Fazoviy yorug'lik modulyatorlari zaifligi. Optik shifrlash jarayonida yorug'likning orbital burchak momenti yoki faza niqoblarini shakllantirish uchun maxsus dasturiy-apparat majmualari ishlatiladi. Agar hujumchi ushbu modulyatorlarni boshqaruvchi operatsion tizimga lokal tarmoq orqali buzib kirishga erishsa, optik shifrlash algoritmlarini to'liq aylanib o'tishi yoki ulardan nusxa ko'chirishi mumkin.

Ma'lumotlar yaxlitligiga qaratilgan fizik hujumlar turlari quyidagilardan iborat.

- Optik shovqin va modifikatsiya hujumlari. Golografik xotira muhiti yorug'likka o'ta sezgir bo'lganligi sababli, hujumchi xotira moduliga tashqaridan kuchli va tartibsiz lazer nurlarini yo'naltirishi mumkin. Bu jarayon asl ma'lumotlar ustiga yangi shovqinlarning yozilishiga va yorug'lik signallarining o'zaro aralashib ketishiga (crosstalk) olib keladi. Natijada axborot o'z yaxlitligini yo'qotib, tiklab bo'lmaydigan holatga keladi.

- Qisman o'chirish xavfi. An'anaviy xotira qurilmalari va tizimlaridan farqli o'laroq, golografik tizimlarda bitta nuqtaga qaratilgan noto'g'ri nur butun bir ma'lumotlar sahifasining ma'lum bir qismini qaytarib bo'lmas darajada yemirilishiga olib kelib qo'yishi mumkin.

- Mexanik tebranishlar xavfi. Gologrammani yozish va o'qish jarayoni nanometr aniqlikni talab etadi. Tizimga ataylab yo'naltirilgan kuchli akustik yoki mexanik tebranishlar uzluksiz ma'lumotlar oqimini to'xtatib qo'yishi mumkin [7].

Golografik xotira tizimlari an'anaviy dasturiy jumladan ko'ra ko'proq fizik, optik parametrlar o'g'irlanishi va atrof-muhit modifikatsiyasi qiish orqali qilinadigan maxsus hujumlarga nisbatan zaif hisoblanadi. Shu sababli bunday tizimlarni joriy etishda dasturiy himoya tizimlari bilan bir qatorda, qat'iy fizik himoya va optik ajartish (izolyatsiya) usullarini qo'llash talab etiladi.

DNK molekulasi asosidagi xotira tizimlari va "DNA Tails" innovatsion yechimi

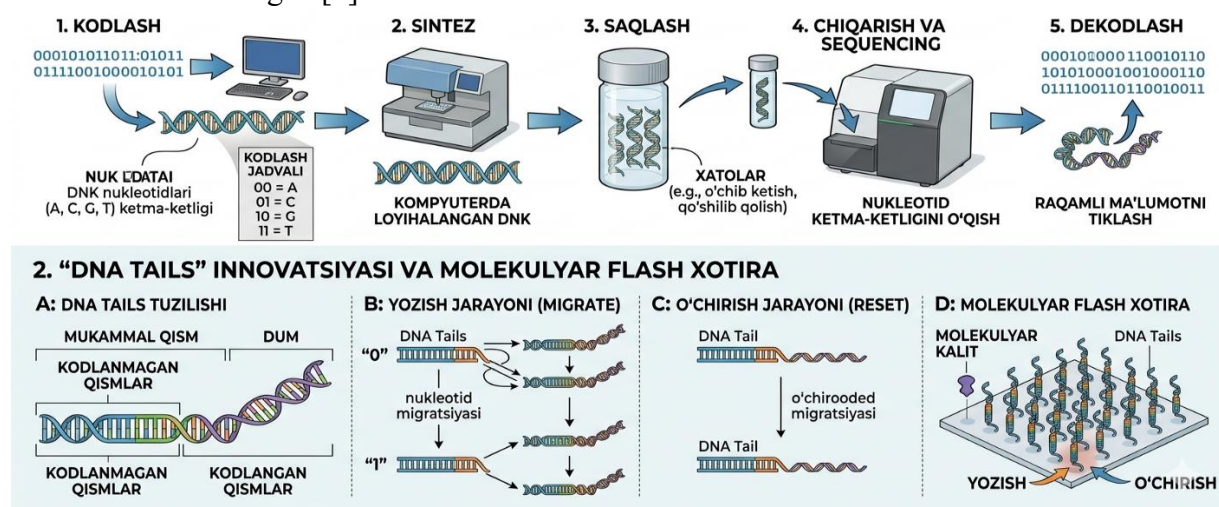
DNK molekulasi asoslangan xotira tizimlari o'ta yuqori zichlikka ega bo'lib, uning nazariy axborot sig'imi bugungi kunga kelib 1 gramm DNK massasida 215 dan 450 petabaytgacha (PB) yetishi isbotlangan. Bu yo'nalishda 2025-yilda taqdim etilgan eng muhim kashfiyotlardan biri "DNA Tails" (molekulyar flesh-xotira) texnologiyasi hisoblanadi. Mazkur innovatsiya DNK zanjiridagi maxsus uzilish joylarida sun'iy polinukleotid "dumlar" (tails) o'stirish orqali ma'lumotlarni ko'p bitli formatda va yuqori tezlikda kodlash imkonini beradi [8].

Tizimning xavfsizlik va sintez jarayoni bilan bog'liq zaifliklari quyidagilardan iborat:

- Biologik xatarlar. Ma'lumotlarni kodlashning ayrim sun'iy intellektga asoslangan algoritmlari (masalan, Movable-Type usuli) natijasida shakllangan DNK ketma-ketliklari tabiatdagi real patogen viruslar genomi bilan 5% gacha tasodifiy o'xshashlikni namoyon qilishi kuzatilgan. Bu holat axborot tashuvchi molekulalarga nisbatan kutilmagan biologik xavflarni yuzaga kelish ehtimolini oshiradi.

- Sintez jarayonidagi to'liq o'smay qolish xatolari. DNK zanjirni uzaytirish bosqichida sun'iy "dumlar"ning kutilmaganda o'smay (sintezlanmay) qolishi ma'lumotlar yo'qotilishiga va o'chirish xatolariga olib kelishi aniqlangan. Ushbu turdagi apparat va biokimyoviy xatoliklarni bartaraf etish hamda ma'lumotlar butunligini ta'minlash uchun yuqori aniqlikdagi Tenengolts va Lemer xatoliklarni tuzatish kodlari algoritmlaridan foydalanish tavsiya etiladi. DNK molekulasi asosidagi xotira tizimlari va "DNA Tails" innovatsion yechimining arxitekturasini

4-rasmda keltirilgan [9].



4-rasm. DNK molekulasi asosidagi xotira tizimlari va "DNA Tails" innovatsion yechimining arxitekturasini

DNK xotirasidagi ma'lumotlardan nusxa ko'cherish jarayoni

Ma'lumotlarni o'qish jarayonida DNK zanjiridan nusxa ko'chirish samaradorligi Polimeraza zanjir reaksiyasi (PCR) qonuniyatlariga asoslanadi va quyidagi 1 formula orqali ifodalanadi [10]:

$$N = N_0 \cdot (1 + E)^n \quad (1)$$

Bu yerda:

N - amaliyot yakunida hosil bo'lgan DNK nusxalarining yakuniy miqdori;

N_0 - boshlang'ich (shablon) DNK nusxalari soni;

E - har bir termik sikldagi ko'paytirish samaradorligi koeffitsiyenti (0 dan

1 gacha bo'lgan oraliqda);

n - jarayon davomida amalga oshirilgan sikllar soni.

Olib borilgan tahlil natijalariga tayangan holda shunday xulosa qilish mumkinki, yangi avlod xotira qurilmalari katta hajmdagi axborotni saqlash muammosini hal qilsada, ular fizik va kiberxavfsizlik nuqtai nazaridan yangi zaifliklarni yuzaga keltiradi. Xususan GaussDB kabi tizimlarda SARA hujumlari va DNK asosidagi xotira qurilmalarida bioxavfsizlik tahdidlari alohida e'tiborni talab etadi. Kelajakda ushbu tizimlarning xavfsizligini oshirish uchun post-kvant kriptografiyasi algoritmlarini, INDIGO kabi adaptiv tarmoq boshqaruv freymvorklarini hamda DNK ketma-ketligini tasodifiy generatsiya qilishning takomillashtirilgan yangi usullarini ishlab chiqish va amaliyotga joriy etish zarur hisoblanadi.

Foydalanilgan adabiyotlar ro'yxati:

1. Archit Patke, et al. INDIGO: Page Migration for Hardware Memory Disaggregation Across a Network. ICS 2025.
2. Guoliang Li, et al. GaussDB: A Cloud-Native Multi-Primary Database with Compute-Memory-Storage Disaggregation. VLDB 2024.
3. Jin Sima, et al. DNA Tails for Molecular Flash Memory. arXiv 2025.
4. Pallab Banerjee, et al. DNA Data Storage: A Novel Approach to High Density, Long Term Digital Storage. ECJSE 2026.
5. Hongjie Liu, et al. Application of Holography for Data Storage. Springer 2025.
6. Usman Ali, Sheikh Abdul Rasheed Sahni, and Omer Khan. 2023. Characterization of timing-based software sidechannel attacks and mitigations on network-on-chip hardware. ACM Journal on Emerging Technologies in Computing Systems 19, 3 (2023), pp. 10-19.
7. Guo Y., Zigerelli A., Zhang Y., Yang J. Adversarial Prefetch: New Cross-Core Cache Side Channel Attacks. In Proceedings of the 2022 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 23-26 May 2022. pp. 1458-1473.
8. Hongjie Liu, Ruixian Chen, Rupeng Yang, Dakui Lin. Application of Holography for Data Storage. Springer Proceedings in Physics, 2025. pp. 45-61.
9. K. Pandurangan. Quantum-inspired algorithms for AI and machine learning Integration of AI, Quantum Computing, and Semiconductor Technology, IGI Global (2025), pp. 79-92, 10.4018/979-8-3693-7076-6.ch004
10. Banerjee P., Hashim M., Mitra D., Upreti K., Jain R., Kumar A. DNA Data Storage: A Novel Approach to High Density, Long Term Digital Storage. El-Cezeri Journal of Science and Engineering. 2026, Vol. 13, No 1, pp. 59-70.