ISNN 3030-3907

2026
MAY
ISSUE - 5
VOLUME - 8

DEVELOPMENT OF SCIENCE

scientific journal



Development of science

Ilmiy jurnal

MAY 2026
Issue - 5, VOLUME – 8

ISSN 3030 -3907

Ilmiy jurnal OAK rayosatining 2024 yil 27 sentabrdagi 361-son qaroriga asosan 02.00.00 kimyo fanlari hamda 2025 yil 12 fevral 367- son qaroriga asosan 05.00.00 texnika fanlari bo‘yicha falsafa doktori (PhD) va fan doktori (DSc) ilmiy darajasiga talabgorlarning dissertatsiya ishlari yuzasidan dissertatsiyalari asosiy ilmiy natijalarini chop etish tavsiya etilgan milliy ilmiy nashrlar ro‘yxatiga kiritilgan.

BOSH MUHARRIR:
Temirov Alisher Hoshim o‘g‘li – texnika fanlari falsafa doktori (PhD),Dotsent.
TAHRIRIYAT KENGASH RAISI:
Fozilov Sadriddin Fayzullayevich – texnika fanlari doktori, professor
TAHRIRIYAT KENGASH A’ZOLARI

TEXNIKA FANLARI/ TECHNICAL SCIENCES/ ТЕХНИЧЕСКИЕ НАУКИ

Bozorov G‘ayrat Rashidovich
Buxoro Davlat Texnika Universiteti, professor
Abdurahmonov Olim Rustamovich
Buxoro Davlat Texnika Universiteti, professor
Adizov Bobur Zamirovich
O‘zbekiston Respublikasi Fanlar akademiyasi Umumiy va noorganik kimyo instituti, professor
Hayitov Ruslan Rustamjonovich
Buxoro Davlat Texnika Universiteti, professor
Jumayev Qayum Karimovich
Buxoro Davlat Texnika Universiteti, professor.
Berdiyev Dorob Murodovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor
Maxmudov Rafiq Amonovich
Buxoro Davlat Texnika Universiteti, professor.
Tilloyev Lochin Ismatilloyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Raxmonov Qahramon Sanakulovich
Buxoro Davlat Texnika Universiteti, dotsent.
Barakayev Nusratullo Rajabovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor.
Jo‘rayev Xayrullo Fayziyevich
Buxoro Davlat Texnika Universiteti, professor.
Panoyev Erali Rajabboyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Ataullayev Sherzod Nabiullyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Malik Negmurodovich
Buxoro Davlat Texnika Universiteti, dotsent.
Axmedova Ozoda Bahronovna
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti.
Safarov Bahri Jumayevich
Buxoro Davlat Texnika Universiteti, dotsent.
Xaydarov Axtam Amonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Safarov Jasur Alijon o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.

KIMYO FANLARI/ CHEMICAL SCIENCES/ ХИМИЧЕСКИЕ НАУКИ

Axmedov Voxid Nizomovich
Buxoro Davlat Texnika Universiteti, professor
Umarov Baqo Bafoyevich
Buxoro Davlat Universiteti, professor
Kodirov Abduaxad Abduraximovich
Qarshi davlat Universiteti, professor
Qurbonov Mingniqul Jumagulovich
Qarshi davlat Universiteti, dotsent
Turemuratov Sharibay Naurizbaevich
O‘zbekiston Respublikasi Fanlar akademiyasi Qoraqalpog‘iston bo‘limi Bosh ilmiy kotibi, professor
Tursunov Kaxor Shonazarovich
Qarshi davlat Universiteti, professor
Do‘stov Hamro
Buxoro Davlat Texnika Universiteti, professor
Panoyev Nodir Shavkatovich
Buxoro Davlat Texnika Universiteti, dotsent.
Olimov Bobur Bahodir o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.
Kasimov Sherzod Abduazimovich
Termiz Davlat Universiteti, professor.
Aliqulov Rustam Valiyevich
Termiz Davlat Universiteti, professor
Tropov Xamza Tursunovich
Samarqand Davlat Universiteti, professor

IQTISODIYOT FANLARI/ ECONOMICS/ ЭКОНОМИЧЕСКИЕ НАУКИ

Nizamov Aslitdin Badreddinovich
Buxoro Davlat Texnika Universiteti, professor.
Boboyev Akmal Choriyevich
Buxoro Davlat Texnika Universiteti, professor.
Ergashxojayeva Shaxnoza Djasurovna
Toshkent davlat iqtisodiyot universiteti, professor
Saidaxmedova Nodira Ilxomovna
Toshkent davlat iqtisodiyot universiteti, professor
Muxsinov Bekzod Toxirovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shakarov Qulmat Ashirovich
Renessans ta'lim universiteti,dotsent.
Jumaeva Zulfiya Qayumovna
Buxoro Davlat Texnika Universiteti, dotsent.
Norova Salomat Yusupovna
Buxoro Davlat Texnika Universiteti, dotsent.
Avezova Shaxnoza Maxmudjonovna
Buxoro Davlat Texnika Universiteti, dotsent.
Jalilov Jamshid G‘anijonovich
Toshkent davlat iqtisodiyot universiteti, dotsent
Xasanova Gulruh Djumanazarovna
Buxoro Davlat Texnika Universiteti, dotsent.

PEDAGOGIKA FANLARI/ PEDAGOGICAL SCIENCES / ПЕДАГОГИЧЕСКИЕ НАУКИ

Siddiqova Sadoqat G‘afforovna
Buxoro Davlat Texnika Universiteti, dotsent.
Zoyirov Erkin Xalilovich
Buxoro Davlat Texnika Universiteti, DSc, professor
Gaffarov Feruz Hasanovich
Puchon Universiteti, *professor*
Ruziyev Davron Yuldashevich
Buxoro Davlat Universiteti, professor
Muradova Firuza Rashidovna
Buxoro Davlat Texnika Universiteti, professor.
Yunusova Gulandon Samiyevna
Buxoro Davlat Texnika Universiteti, professor.
To‘xtayeva Zebo Sharifovna
Buxoro Davlat Texnika Universiteti, professor.
Navro‘zova Gulchixra Nigmatovna
Buxoro Davlat Texnika Universiteti, dotsent.
Uzoqova Laylo Polvonovna
Buxoro muhandislik – texnologiya instituti, dotsent.
To‘raqulova Marjona Qiyom qizi
Buxoro Davlat Texnika Universiteti, dotsent.
Muradova Zarina Rashidovna
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Sanjar Aslonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shodiyev Jahongir Jo‘raqulovich
Buxoro Davlat Texnika Universiteti, dotsent
Gaffarov Laziz Hasanovich
Buxoro muhandislik – texnologiya instituti, dotsent.

Tahririyat a’zolarning to‘liq ro‘yxati jurnalning www.devos.uz saytida keltirilgan.

Tahririyat hay’ati a’zolarining tarkibini o‘zgartirish hamda qo‘shimcha kiritish yoki tahririyat a’zoligidan chiqarish bosh muharrir tomonidan amalga oshiriladi.

ISSN 3030-3907

Development of science ilmiy jurnali 2024 yil 15 aprel kuni №256445 sonli guvohnoma bilan Davlat ro‘yxatidan o‘tgan.

To‘plam elektron ko‘rinishda (pdf formatida) mualliflarga taqdim etiladi. To‘plamga kiritiladigan maqolalarning mazmuni, ulardagi statistik ma’lumotlar va me’yoriy hujjatlarning to‘g‘riligiga hamda har qanday fikr - mulohazalarga mualliflarning o‘zlari mas’ul hisoblanadilar. Talablarga javob bermaydigan maqolalar to‘plamga kiritilmaydi. Tashkiliy qo‘mita maqola matnini qisqartirish, qisman tuzatish kiritish, seksiyalarga joylashtirish huquqiga ega.

ISSN 3030-3907

UDK 519.7:004.056.55

SONLAR NAZARIYASIGA ASOSLANGAN KRIPTOGRAFIK ALGORITMLARNING SAMARADORLIGINI EKSPERIMENTAL TAHLIL QILISH VA SEI INDEKSINI JORIY ETISH

Raximov Q. O.
Farg‘ona Davlat Universiteti, Farg‘ona, Uzbekiston
E-mail: quvvatali.rahimov@gmail.com
Ne’matova H. N.
Farg‘ona Davlat Universiteti, Farg‘ona, Uzbekiston
E-mail: nematovahayitxon@gmail.com

Annotatsiya. Ushbu maqolada RSA-2048, RSA-4096, ECC (P-256), ECC (P-384) va post-kvant Kyber-768 algoritmlarining hisoblash samaradorligi Google Colab muhitida NVIDIA Tesla T4 GPU bilan Python 3 yordamida 1000 ta iteratsiya asosida eksperimental o‘lchandi. Tadqiqotda har xil uzunlikdagi matnlar (qisqa — 44 belgi, o‘rta — 177 belgi va uzun — 256+ belgilar) shifrlash va deshifrlash uchun foydalanildi hamda har xil natijalar qayd etildi. Xususan, RSA-2048 algoritmi uzun matnni shifrlashda xato berdi — bu algoritmning kalit hajmi bilan bog‘liq cheklovini ko‘rsatdi. Xavfsizlik-Samaradorlik Indeksi (SEI) yordamida algoritmlar bir o‘lchovda taqqoslandi: Kyber-768 — 1 875–2 065 bit/ms, ECC P-256 — 30–42 bit/ms, RSA-2048 esa atigi 0.16–0.17 bit/ms SEI qiymatini ko‘rsatdi. Natijalar O‘zbekistonda axborot xavfsizligi tizimlarini modernizatsiya qilishda ECC va post-kvant algoritmlariga o‘tishning texnik asosini isbotlaydi.

Kalit so‘zlar: kriptografiya, RSA, ECC, Kyber-768, sonlar nazariyasi, SEI indeksi, samaradorlik tahlili, matn uzunligi ta’siri, post-kvant kriptografiya.

Аннотация. В данной статье экспериментально измерена вычислительная эффективность алгоритмов RSA-2048, RSA-4096, ECC (P-256), ECC (P-384) и постквантового алгоритма Kyber-768 в среде Google Colab с использованием GPU NVIDIA Tesla T4 на языке Python 3 на основе 1000 итераций. В исследовании применялись тексты различной длины (короткий — 44 символа, средний — 177 символов и длинный — свыше 256 символов) для шифрования и дешифрования, при этом были зафиксированы различные результаты. В частности, алгоритм RSA-2048 выдал ошибку при шифровании длинного текста, что наглядно демонстрирует его ограничение, связанное с размером ключа. С помощью индекса безопасности-эффективности (SEI) алгоритмы были сопоставлены в единой метрике: Kyber-768 показал 1 875–2 065 бит/мс, ECC P-256 — 30–42 бит/мс, тогда как RSA-2048 — лишь 0,16–0,17 бит/мс. Полученные результаты подтверждают техническое обоснование перехода на алгоритмы ECC и

ISSN 3030-3907

постквантовой криптографии при модернизации систем информационной безопасности в Узбекистане.

Ключевые слова. Криптография, RSA, ECC, Kyber-768, теория чисел, индекс SEI, анализ эффективности, влияние длины текста, постквантовая криптография

Abstract. This paper experimentally measures the computational performance of RSA-2048, RSA-4096, ECC (P-256), ECC (P-384), and the post-quantum algorithm Kyber-768 in a Google Colab environment with an NVIDIA Tesla T4 GPU, using Python 3 over 1,000 iterations. The study employs texts of varying lengths — short (44 characters), medium (177 characters), and long (256+ characters) — for encryption and decryption, yielding distinct results across cases. Notably, RSA-2048 produced an error when encrypting the long text, exposing a key-size limitation inherent to the algorithm. Using the Security-Efficiency Index (SEI), the algorithms were compared on a unified scale: Kyber-768 achieved 1,875–2,065 bit/ms, ECC P-256 achieved 30–42 bit/ms, while RSA-2048 reached only 0.16–0.17 bit/ms. The findings provide a technical foundation supporting the transition to ECC and post-quantum algorithms in the modernisation of information security systems in Uzbekistan.

Keywords. Cryptography, RSA, ECC, Kyber-768, number theory, SEI index, performance analysis, text length effect, post-quantum cryptography

KIRISH.

Axborot texnologiyalari jadal rivojlanayotgan davrda kriptografik algoritmlarning xavfsizligi va samaradorligi birgalikda ta’minlanishi zarur. Sonlar nazariyasiga asoslangan algoritmlar — RSA, ECC va zamonaviy post-kvant tizimlari — bugungi axborot xavfsizligi infratuzilmasining asosini tashkil etadi [1, 2]. Amaliyotda muhim savol tug‘iladi: bir xil xavfsizlik darajasini ta’minlashda bu algoritmlar qanchalik turli hisoblash xarajatlarini talab qiladi va shifrlash ishlovi matn uzunligiga qanday bog‘liq?

Mavjud adabiyotlarda RSA va ECC ni nazariy jihatdan taqqoslovchi ishlar ko‘p bo‘lsada [3, 4], ular kamida ma’lum jihatdan cheklangan: (a) o‘zbek tilida mavjud emas; (b) algoritmlarni bir integral ko‘rsatkich orqali baholash metodikasi ishlab chiqilmagan. Ushbu bo‘shliqlarni to‘ldirish maqolaning asosiy maqsadini tashkil etadi.

Tadqiqotning ilmiy yangiligi ikki qatlamdan iborat. Birinchi qatlam — eksperimental: RSA-2048, RSA-4096, ECC P-256, ECC P-384 va Kyber-768 algoritmlari Google Colab muhitida NVIDIA Tesla T4 GPU bilan, Python yordamida, 1000 ta iteratsiya asosida o‘lchandi — bu konfiguratsiya adabiyotda avval e’lon qilinmagan. Ikkinchi qatlam — metodologik: algoritmlarning xavfsizlik darajasi va bajarilish vaqtini birlashtiruvchi Xavfsizlik-Samaradorlik

ISSN 3030-3907

Indeksi (SEI) taklif etildi va algoritmlarni qiyosiy baholashda qo‘llash usuli ko‘rsatildi.

Tadqiqot gipotezasi: ECC algoritmlari RSA ga nisbatan sezilarli samaradorlik ustunligini namoyon etadi; Kyber-768 esa SEI bo‘yicha an’anaviy algoritmlarning ikkalasini ham ustib o‘tadi. Shuningdek, matn uzunligi RSA uchun amaliy cheklov yaratadi, ECC va Kyber-768 esa matn hajmidan mustaqil ravishda barqaror ishlaydi.

Tadqiqot doirasida beshta kriptografik algoritm o‘rganildi. RSA-2048 — 2048 bitli kalit uzunligiga ega bo‘lib, taxminan 112 bit xavfsizlik darajasini ta’minlaydi va PKCS#1 v2.2 standarti asosida ishlaydi. RSA-4096 esa 4096 bitli kalit bilan ~140 bit xavfsizlikni kafolatlaydi. ECC (P-256) elliptik egri chiziqlar kriptografiyasiga asoslangan bo‘lib, 256 bitli kalit bilan 128 bit xavfsizlik darajasini ta’minlaydi (NIST FIPS 186-4). ECC (P-384) — 384 bitli kalit, 192 bit xavfsizlik. Kyber-768 post-kvant panjara asosidagi algoritm bo‘lib, 1184 bitli ochiq kalit va ~178 bit xavfsizlik darajasini ta’minlaydi (NIST FIPS 203).

Adabiyotda algoritmlarni xavfsizlik va samaradorlik bo‘yicha bitta skalyar ko‘rsatkich orqali baholash metodikasi taklif etilmagan. Shu sababli ushbu tadqiqotda quyidagi formula ishlab chiqildi:

$$SEI = \frac{S}{T_{Jami}},\ T_{Jami} = T_{keygen} + T_{enc} + T_{dec}$$

bu yerda S — algoritmning xavfsizlik darajasi (bit), T_{jami} — kalit generatsiyasi, shifrlash va deshifrlash operatsiyalarining yig‘indi bajarilish vaqti (ms). SEI qiymati qanchalik yuqori bo‘lsa, algoritm shunchalik ko‘p xavfsizlikni kam vaqt sarflab ta’minlaydi. Kalit hajmi formuladan ataylab ajratilgan, chunki u alohida resurs kategoriyasi hisoblanib, xotira cheklangan qurilmalar uchun mustaqil baholash mezoni sifatida muhimdir.

Google Colab muhitida NVIDIA Tesla T4 GPU bilan har bir operatsiya 1000 marta mustaqil ravishda bajarildi va o‘rtacha qiymat hamda standart og‘ish hisoblandi. RSA kalit generatsiyasi hisoblash murakkabligi sababli n=50 takrorlash ishlatildi, so‘ng natija n=1000 uchun ekstrapolatsiya qilindi. Tadqiqotning muhim xususiyati — uch xil uzunlikdagi matnlardan foydalanilganligi bo‘ldi: Matn 1 (qisqa, ~44 belgi): “Bugun havo juda yaxshi va quyosh yorqin nur sochmoqda”; Matn 2 (o‘rta, ~177 belgi): kundalik voqealarni tasvirlovchi kichik parcha; Matn 3 (uzun, 256+ belgi): kengaytirilgan matn. Ushbu yondashuv algoritmlarning real sharoitdagi xatti-harakatini yanada to‘liq aks ettirdi.

ISSN 3030-3907

1-jadval.

Eksperimental o‘lchash natijalari — Matn 1 (qisqa, ms)

Algoritm	Kalit gen.	Shifr.	Deshifr.	Imzo	Teksh.	SEI (bit/ms)
RSA-2048	706.40	0.726	1.867	2.096	0.606	0.16
RSA-4096	6598.46	1.409	10.130	10.086	1.950	0.02
ECC (P-256)	0.106	1.996	1.617	0.999	2.144	**34.42**
ECC (P-384)	0.058	3.350	4.489	1.680	4.643	24.31
Kyber-768	0.033	0.034	0.020	—	—	**2052.87**

2-jadval.

Eksperimental o‘lchash natijalari — Matn 2 (o‘rta uzunlik, ms)

Algoritm	Kalit gen.	Shifr.	Deshifr.	Imzo	Teksh.	SEI (bit/ms)
RSA-2048	646.69	0.831	1.842	2.094	0.646	0.17
RSA-4096	6550.99	1.856	8.886	11.073	1.218	0.02
ECC (P-256)	0.056	1.956	2.199	0.959	2.105	**30.40**
ECC (P-384)	0.059	3.230	3.377	2.705	4.478	28.81
Kyber-768	0.032	0.034	0.020	—	—	**2064.23**

3-jadval.

Eksperimental o‘lchash natijalari — Matn 3 (uzun, ms)

Algoritm	Kalit gen.	Shifr.	Deshifr.	Imzo	Teksh.	SEI (bit/ms)
RSA-2048	—	**XATO***	—	—	—	—
RSA-4096	6729.14	1.386	10.191	11.165	1.224	0.02
ECC (P-256)	0.065	1.470	1.503	1.025	3.266	**42.13**
ECC (P-384)	0.061	3.282	3.286	1.672	5.729	28.96
Kyber-768	0.036	0.039	0.020	—	—	**1875.56**

* RSA-2048 uchun “Plaintext is too long” xatosi — OAEP padding bilan maksimal (256−42)=214 bayt shifrlash chegarasidan oshib ketdi.

4-jadval.

SEI qiymatlarining matn uzunligiga ko‘ra umumlashtirmasi

Algoritm	SEI (Matn 1)	SEI (Matn 2)	SEI (Matn 3)	O‘rtacha SEI
RSA-2048	0.16	0.17	—	~0.165
RSA-4096	0.02	0.02	0.02	0.02
ECC (P-256)	**34.42**	**30.40**	**42.13**	**35.65**

ISSN 3030-3907

ECC (P-384)	24.31	28.81	28.96	27.36
Kyber-768	**2052.87**	**2064.23**	**1875.56**	**1997.55**

Olingan natijalar bir necha muhim xulosaga olib keldi. Birinchi va eng ko‘zga tashlanarli holat — RSA-2048 algoritmi uzun matn (Matn 3) ni shifrlashda muvaffaqiyatsizlikka uchradi. Bu algoritmning OAEP padding sxemasi bilan bog‘liq: RSA-2048 maksimal 214 bayt, RSA-4096 esa 470 bayt gacha matnni to‘g‘ridan-to‘g‘ri shifrlashi mumkin. Katta hajmdagi ma’lumotlarni shifrlashda RSA gibrid sxemada ishlatilishi zarur. ECC va Kyber-768 algoritmlari uchun esa matn uzunligi shifrlash vaqtiga sezilarli ta’sir qilmadi.

Kalit generatsiyasida ECC P-256 (~0.056–0.106 ms) RSA-2048 (~646–706 ms) dan o‘rtacha 10 000 marta tezroq ishladi. Bu farqning matematik asosi quyidagicha: RSA kalit generatsiyasida probabilistik Miller-Rabin sinovidan o‘tkaziluvchi katta tub sonlar izlanadi (bit uzunligiga bog‘liq eksponensial murakkablik), ECC da esa oddiy tasodifiy son tanlanadi — bu O(1) murakkablikdagi operatsiya. RSA ning yuqori standart og‘ishi (±70–120%) tekshirilayotgan sonning tub yoki tub emasligiga bog‘liq bo‘lib, kriptografik jihatdan to‘g‘ri xatti-harakat hisoblanadi.

Kyber-768 ning o‘rtacha SEI ko‘rsatkichi (1997.55 bit/ms) ECC P-256 (35.65 bit/ms) dan 56 marta, RSA-2048 (0.165 bit/ms) dan esa taxminan 12 000 marta yuqori. Bu g‘ayritabiiy yuqori ko‘rsatkich panjara asosidagi matematikaning zamonaviy protsessorlar arxitekturasi bilan uyg‘unligidan kelib chiqadi: matritsaviy ko‘paytirish va modul qo‘shish operatsiyalari CPU ning SIMD ko‘rsatmalari bilan parallel bajariladi. Qo‘shimcha ravishda, Kyber-768 ning shifrlash va deshifrlash vaqtlari (0.020–0.039 ms) barcha sinov matnlarida o‘zgarmasligi algoritmning matn uzunligidan mustaqilligi va barqarorligini tasdiqlaydi.

Tadqiqotning bir necha cheklovi mavjud. Birinchisi: RSA-2048 ning uzun matn uchun xatosi faqat sof (raw) shifrlash rejimida yuzaga keladi; gibrid sxemada bu cheklov amalda muhim emas. Ikkinchisi: Kyber-768 natijalari Google Colab T4 muhitida liboqs kutubxonasi orqali o‘lchandi; keyingi tadqiqotda boshqa apparat platformalarida ham solishtirma o‘lchashlar o‘tkazilishi maqsadga muvofiq. Uchinchisi: SEI formulasi kalit hajmini hisobga olmaydi; kelajakda resurs cheklangan qurilmalar uchun kalit hajmi koeffisiyentini kiritish ko‘zda tutilmoqda.

Olingan natijalar asosida quyidagi amaliy tavsiyalar shakllantirildi. O‘zbekiston korxonalari va davlat tashkilotlarining kriptografik infratuzilmasida RSA o‘rniga ECC P-256 yoki P-384 ga o‘tish zarur — bu o‘rtacha 10 000 marta tezroq kalit generatsiyasini, tezroq deshifrlash va raqamli imzoni ta’minlaydi. Katta hajmdagi ma’lumotlarni shifrlashda RSA ni to‘g‘ridan-to‘g‘ri ishlatmaslik

ISSN 3030-3907

kerak — gibrid sxema (AES + RSA) yoki ECC ishlatilishi lozim. Yangi axborot tizimlari loyihalashda, ayniqsa ma'lumotlarning 10 yildan ortiq maxfiyligi talab etilganda, post-kvant algoritmlarini (Kyber-768) tatbiq etish ko'zda tutilishi lozim. O'zbekiston axborot xavfsizligi sohasida standartlashtirish bo'yicha vakolatli idoralar NIST FIPS 203 (Kyber) standartini milliy hujjatlarga kiritish masalasini ko'rib chiqishi tavsiya etiladi.

Ushbu tadqiqotda sonlar nazariyasiga asoslangan beshta kriptografik algoritmning samaradorligi Google Colab muhitida NVIDIA Tesla T4 GPU bilan, Python yordamida, 1000 ta iteratsiya asosida eksperimental o'lchandi va taqqoslandi. Har xil uzunlikdagi uchta matn bilan o'tkazilgan tajribalar algoritmlar xatti-harakatidagi farqlarni yanada aniqroq ko'rsatdi. Matn uzunligi RSA uchun amaliy cheklov yaratdi: RSA-2048 uzun matnni shifrlashda "Plaintext is too long" xatosini berdi, ECC va Kyber-768 esa barcha matnlarni muammosiz shifrladi. Kalit generatsiyasida ECC P-256 RSA-2048 dan o'rtacha ~10 000 marta tezroq ishladi. Taklif etilgan SEI indeksi (S / T_jami) algoritmlarni bir o'lchovda qiyosiy baholash uchun yangi metodologik vosita sifatida joriy etildi va uch xil matn o'lchovi bo'yicha tasdiqlandi. O'rtacha SEI bo'yicha: Kyber-768 — 1997.55 bit/ms, ECC P-256 — 35.65 bit/ms, ECC P-384 — 27.36 bit/ms, RSA-2048 — 0.165 bit/ms, RSA-4096 — 0.02 bit/ms. Natijalar tadqiqot gipotezasini to'liq tasdiqladi va O'zbekistonda ECC hamda post-kvant algoritmlariga o'tishning texnik asosini ilmiy jihatdan isbotladi. Kelajak tadqiqotlarda SEI formulasiga kalit hajmi koeffisiyentini kiritish, ARM Cortex-M (IoT) platformasida takror o'lchash va Kyber-768 ni boshqa muhitda real o'rnatib sinash ko'zda tutilmoqda.

ADABIYOTLAR

1. Rivest R.L., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems // Communications of the ACM. — 1978. — Vol. 21, No. 2. — P. 120–126.
2. Diffie W., Hellman M. New Directions in Cryptography // IEEE Transactions on Information Theory. — 1976. — Vol. 22, No. 6. — P. 644–654.
3. Koblitz N. Elliptic curve cryptosystems // Mathematics of Computation. — 1987. — Vol. 48, No. 177. — P. 203–209.
4. Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography. — CRC Press, 1996. — 816 p.
5. Stinson D.R. Cryptography: Theory and Practice. — 3rd ed. — CRC Press, 2006. — 616 p.
6. Avanzi R. et al. CRYSTALS-Kyber Algorithm Specifications and Supporting Documentation (v3.02). — NIST PQC Round 3, 2021. — 43 p.

ISSN 3030-3907

7. Bernstein D.J., Lange T. Post-quantum cryptography // Nature. — 2017. — Vol. 549. — P. 188–194.
9. NIST FIPS 186-4. Digital Signature Standard (DSS). — National Institute of Standards and Technology, 2013.
10. NIST FIPS 203. Module-Lattice-Based Key-Encapsulation Mechanism Standard. — NIST, 2024.
11. PyCryptodome. Cryptographic library for Python. — URL: https://pycryptodome.readthedocs.io (murojaat: 2026).