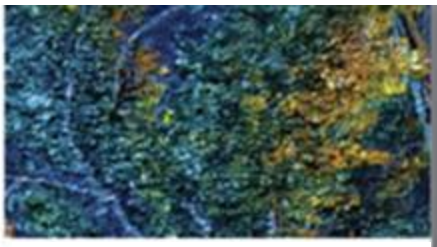


№1 (7) 2025

INTERNATIONAL SCIENCE REVIEWS

AIU

Natural Sciences and Technologies series

www.aiu.kz

ISSN: 2707-4862

ASTANA INTERNATIONAL UNIVERSITY

INTERNATIONAL SCIENCE REVIEWS
Natural Sciences and Technologies series

Has been published since 2020

№1 (7) 2025

Astana

Editorial address: 8, Kabanbay Batyr avenue, of.316, Nur-Sultan,
Kazakhstan, 010000
Tel.: (7172) 24-18-52 (ext. 316)
E-mail: natural-sciences@aiu.kz

International Sciense Reviews NST - 76153
International Science Reviews
Natural Sciences and Technologies series
Owner: Astana International University
Periodicity: quarterly
Circulation: 500 copies

CONTENT

МРНТИ: 20.53.15

Постквanттық криптографиялық алгоритмдерді қауіпсіздік пен стандарттауға қолдану және бағалау критерийлері

Н.Ж. Жарасхан*, С.А. Наурызбаева

Ақпараттық технологиялар және инженерия жоғары мектебі, Астана халықаралық университеті, Астана, Қазақстан
*Автор-корреспондент

Аннотация. Бұл мақалада постквanттық криптография саласындағы заманауи алгоритмдерге теориялық және салыстырмалы талдау жүргізіледі. Қазіргі таңда кеңінен қолданылатын RSA және ECC сияқты классикалық криптографиялық әдістер кванттық компьютерлердің дамуы нәтижесінде қауіпсіздігін жоғалту қаупіне ұшырап отыр. Осыған байланысты АҚШ Ұлттық стандарттар және технологиялар институты (NIST) бастамасымен жаңа постквanттық алгоритмдерді таңдау және стандарттау үдерісі басталды. Мақалада CRYSTALS-Kyber, CRYSTALS-Dilithium, Falcon, SPHINCS+, BIKE, HQC және басқа алгоритмдердің құрылымы, қауіпсіздік сипаттамалары, тиімділігі мен қолдану аймақтары қарастырылады. Әр алгоритмнің артықшылықтары мен шектеулері көрсетіліп, олардың ресурсы шектеулі құрылғыларда қолдану мүмкіндігі бағаланады. Негізгі әдістер ретінде жүйелік шолу, салыстырмалы және классификациялық сараптама пайдаланылды. Зерттеу нәтижелері постквanттық криптографиялық шешімдердің ұзақ мерзімді ақпараттық қауіпсіздікті қамтамасыз етудегі рөлін негіздейді және болашақта қолданылатын стандарттарды таңдауда бағыт береді.

Кілттік сөздер: Постквanттық криптография, CRYSTALS-Kyber, Қауіпсіздік алгоритмдері, Кванттық шабуыл, Торлық криптография, Кодтық криптография, NIST стандарты

Кіріспе

Қазіргі заманғы ақпараттық жүйелер мен коммуникациялық инфрақұрылымдар негізінен классикалық криптографиялық әдістерге сүйенеді. Бұл жүйелердің қауіпсіздігі көбіне факторизациялау мен дискреттік логарифм сияқты математикалық есептердің күрделілігіне негізделеді. Алайда, кванттық есептеудің дамуымен бұл криптографиялық жүйелердің қауіпсіздігіне елеулі қауіп төнуде. Кванттық есептеудің ең танымал алгоритмдерінің бірі — Шор алгоритмі [1], үлкен сандарды өте жылдам көбейткіштерге жіктей алады. Бұл RSA және эллиптикалық қисық криптографиясы (ECC) сияқты кең таралған криптожүйелер үшін қауіпсіздік қаупін тудырады.

Мұндай шабуыл мүмкіндігін болдырмау үшін жаңа криптографиялық әдістерді әзірлеу қажет. Қазіргі таңда криптография саласындағы зерттеулердің екі негізгі бағыты бар: кванттық кілттерді тарату (Quantum Key Distribution, QKD) [2] және постквanттық криптография (Post-Quantum Cryptography, PQC) [3]. QKD — кванттық механикаға негізделген, физикалық принциптермен қамтамасыз етілетін қауіпсіз кілт алмасу әдісі болса, PQC — классикалық есептеу құрылымына негізделіп, кванттық шабуылдарға төтеп бере алатын жаңа криптографиялық алгоритмдердің жиынтығы болып табылады.

PQC-ның артықшылығы — оның практикалық түрде қазіргі криптожүйелерді алмастыра алуы. Ол сандық қолтаңба, деректерді шифрлау және кілт алмасу сияқты негізгі тетіктерді қамтамасыз етуге бағытталған. Бұл алгоритмдердің көбі Шор мен Гровер алгоритмдеріне төтеп бере алатын күрделі математикалық мәселелерге негізделеді. Осы бағытта 2016 жылы АҚШ Ұлттық стандарттар және технологиялар институты (NIST) постквanттық криптография алгоритмдерін бағалау және стандарттау процесін бастады. Осы конкурс нәтижесінде бірнеше

перспективалы алгоритмдер, соның ішінде CRYSTALS-Kyber және CRYSTALS-Dilithium стандарттарға енді [4].

Осы зерттеудің мақсаты — постквантты криптографияның негізін, заманауи алгоритмдердің артықшылықтары мен шектеулерін зерделеу, сондай-ақ олардың нақты құрылғыларда қолдану әлеуетін бағалау.

Материалдар мен әдістер

Зерттеу барысында постквантты криптографияның теориялық негіздері мен практикалық аспектілері аралас әдіснама негізінде талданды. Жүйелі шолу әдісі арқылы NIST бастамасымен іске асқан постквантты криптографияны стандарттау үдерісінің төрт кезеңі мұқият зерделенді. Әр кезеңде іріктелген, қабылданған немесе жойылған алгоритмдер сандық және сапалық тұрғыдан талданды.

Салыстырмалы талдау әдісі арқылы алгоритмдердің математикалық негіздері, қауіпсіздік сипаттамалары мен өнімділік параметрлері қарастырылып, олардың қолдану контекстіндегі артықшылықтары мен шектеулері анықталды. Ал классификациялық сараптама тәсілі арқылы алгоритмдер торлық, кодтық және хэшке негізделген топтарға бөлініп, олардың криптографиялық мақсаттағы қолдану аймақтары жүйелендірілді.

Постквантты криптографияны стандарттау үдерісі

2016 жылғы желтоқсанда АҚШ Ұлттық стандарттар және технологиялар институты (NIST) кванттық және классикалық компьютерлерге төзімді криптографиялық алгоритмдерді жинақтау, бағалау және стандарттау үдерісін бастады. Бұл бастама постквантты криптографияны (PQC) әзірлеудің халықаралық кезеңі ретінде танылып, қазіргі байланыс хаттамалары мен желілік инфрақұрылыммен үйлесімді алгоритмдерді таңдауға бағытталды [4].

Бірінші кезеңде (2017–2019 ж. қаңтар) NIST әртүрлі криптографиялық тәсілдерге негізделген 82 алгоритм қабылдады, бірақ олардың тек 69-ы қойылған талаптарға сәйкес келіп, келесі кезеңге өтті. Ұсынылған алгоритмдерге торлық (lattice-based), хэшке негізделген (hash-based), көпмүшелікке негізделген (multivariate) және кодтық (code-based) жүйелер жатады. Қауіпсіздік пен өнімділік сипаттамаларына жүргізілген алдын ала талдау нәтижесінде 43 алгоритм алынып тасталды да, 26 алгоритм келесі кезеңге өтті.

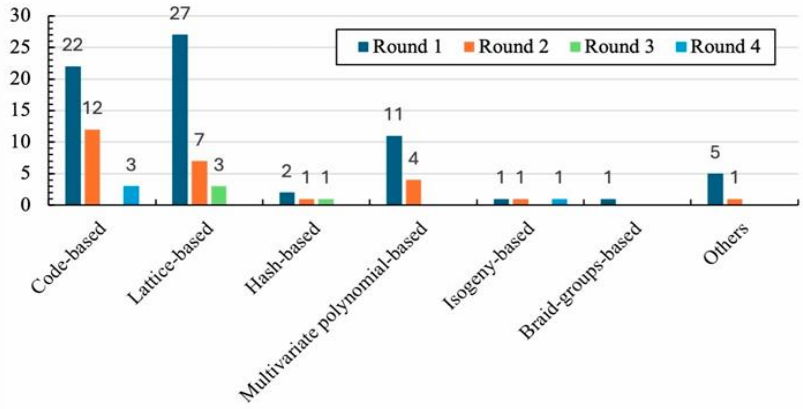
Екінші кезең (2019 ж. қаңтар – шілде) барысында қалған 26 алгоритмге терең талдау жүргізілді. Олардың ішінен 11 алгоритм алынып тасталды, ал 15 алгоритм үшінші кезеңге өтті.

Үшінші кезең (2020–2022 ж. шілде) – 15 финалист алгоритм жан-жақты зерттелген кезең. Олардың арасында CRYSTALS-Kyber (KEM), CRYSTALS-Dilithium, Falcon және SPHINCS+ (сандық қолтаңба алгоритмдері) финалист ретінде таңдалды.

*Төртінші кезең (*2022 ж. шілде – 2024 ж. тамыз) кезінде BIKE, Classic McEliece, HQC және SIKE алгоритмдері қосымша бағалау үшін қарастырылды. Алайда SIKE алгоритміне қарсы тиімді шабуыл анықталғандықтан, ол үдерістен шығарылды.

1-суретте әрбір кезеңнен (1-раундтан 4-раундқа дейін) өткен криптографиялық алгоритмдердің түрлер бойынша үлестірімі көрсетілген.

Бұл суреттен торлық (lattice-based) және кодтық (code-based) тәсілдердің басымдығы айқын байқалады [5].



Сурет 1 – NIST стандартизациялау процесінің раундтары бойынша постквантық алгоритмдер түрлерінің үлестірілуі

Постквантық алгоритмдерге шолу

Бұл бөлімде постквантық криптографияның (PQC) заманауи алгоритмдері жан-жақты қарастырылады. NIST (Ұлттық стандарттар және технологиялар институты) ұйымдастырған стандарттау үдерісінің нәтижесінде іріктелген және қосымша зерттеліп жатқан алгоритмдерге назар аударылады [4]. Талдау барысында әртүрлі математикалық негіздерге сүйенетін алгоритмдер сипатталып, олардың қолданылу аясы, артықшылықтары мен шектеулері ашып көрсетіледі.

Қазіргі ақпараттық қауіпсіздік шешімдерінде симметриялық және асимметриялық криптография негізгі рөл атқарады.

Симметриялық криптография бір ғана құпия кілтті қолдана отырып шифрлау және шифрды шешуді жүзеге асырады. AES және Triple DES алгоритмдері кең таралған [6]. Дегенмен, кванттық шабуылдарға, әсіресе Гровер алгоритміне қатысты, бұл әдістердің қауіпсіздігі екі есеге дейін төмендейтіні дәлелденген. Осы себепті AES-256 сияқты ұзын кілттер ұсынылады.

Асимметриялық криптография екі түрлі кілт жұбына негізделеді: ашық және жабық кілт. RSA, DSA және ECC алгоритмдері көбейткішке жіктеу мен дискреттік логарифм есептерінің күрделілігіне сүйенеді. Алайда Шор алгоритмі бұл есептерді кванттық компьютерлерде тиімді шешуге мүмкіндік беретіндіктен, дәстүрлі асимметриялық криптожүйелердің қауіпсіздігіне үлкен қауіп төндіреді. Бұл мәселені тереңірек түсіну үшін классикалық және кванттық есептеу жағдайындағы криптографиялық алгоритмдердің қауіпсіздік деңгейін салыстырмалы түрде қарастыру маңызды. 1-кестеде кеңінен қолданылатын симметриялық және асимметриялық алгоритмдердің кілт өлшемі мен олардың классикалық және кванттық ортадағы қауіпсіздік биттері көрсетілген [7]. Бұл деректерден байқауға болады: RSA және ECC сияқты жүйелер кванттық компьютерлерге мүлде төтеп бере алмайды (қауіпсіздік деңгейі — 0 бит), ал AES секілді симметриялық жүйелердің қауіпсіздігі екі есеге дейін төмендейді. Мұндай ахуал постквантық криптографияны дамытудың маңыздылығын айқын дәлелдейді.

Кесте-1. Классикалық және кванттық ортадағы алгоритмдердің салыстырмалы қауіпсіздігі.

Cryptography Method	Key Size	Key Strength	
		Classical Computing (bits)	Quantum Computing (bits)
AES-128	128 bits	128	64
AES-256	256 bits	256	128
RSA-1024	1024 bits	80	0
RSA-2048	2048 bits	112	0
ECC-256	256 bits	128	0
ECC-384	384 bits	256	0

Осылайша, сандық қолтаңба және кілт алмасу тетіктерін кванттық қауіпсіз нұсқалармен алмастыру мәселесі туындайды. Сандық қолтаңбаның түпнұсқалық пен бүтіндікті растаудағы рөлі аса маңызды. Ал кілт алмасу – сенімсіз ортада қауіпсіз байланыс орнатудың іргетасы. Бұл екеуі де постквантық шифрлау жүйелерінің негізгі құрамдас бөліктері болып табылады.

Кодтық постквантық криптографиялық алгоритмдерге шолу

McEliece – қатені түзейтін кодтарға негізделген асимметриялық шифрлау алгоритмі. Ашық кілтті алу үшін код матрицасына әдейі енгізілген қателер қолданылады. Шифрлау мен дешифрлау жылдамдығы жоғары болғанымен, ашық кілттің өлшемі өте үлкен, бұл оны практикалық қолдануда шектейді [8]. McEliece қолтаңба схемасына тікелей бейімделмеген, бірақ оның баламасы ретінде **Niederreiter** схемасы қарастырылған.

BIKE алгоритмі орташа тығыздықтағы паритеттік тексеру кодтарын (MDPC) пайдалана отырып, биттерді аудару арқылы қатені түзетеді. Кілттердің өлшемі салыстырмалы түрде шағын, ал шифрлау мен кілт генерациясы жылдам [9].

HQC (Hamming Quasi-Cyclic) — Хэмминг кодтарына негізделген және IND-CCA2 қауіпсіздік моделіне сәйкес келетін KEM алгоритмі. Артықшылықтары қатені түзету қасиетінің мықтылығы, салыстырмалы түрде шағын кілт өлшемі және платформаларға бейімділігімен ерекшеленеді [10].

Торлық постквантық криптографиялық алгоритмдерге шолу

Торлық криптография шифрлау, кілт алмасу, хэш-функциялар мен сандық қолтаңба сияқты міндеттер үшін торлар (lattices) деп аталатын көпөлшемді құрылымдарды қолданады. Бұл құрылымдар ақпаратты күрделі геометриялық кеңістікте шифрлауға мүмкіндік береді және кванттық шабуылдарға төтеп бере алады.

Гомоморфты шифрлау — шифрланған деректерге арифметикалық амалдарды тікелей қолдануға мүмкіндік береді. Үш түрі ажыратылады [11]:

- Шектеулі (Somewhat)
- Жартылай (Partially)
- Толық (Fully)

Гомоморфты схемалар анонимді дерекқорлар, электронды денсаулық сақтау жүйелері және бұлттық есептеулерде қолданылады.

Торлық негізде жасалған алгоритмдер қатарына GGH, NTRU, CRYSTALS-Kyber, FrodoKEM, SABER, NTRU Prime және басқалары жатады [12]. Олардың кейбірі кілт алмасу үшін, ал басқалары сандық қолтаңба үшін қолданылады.

- **GGH** – ең алғашқы торлық шифрлау схемасы, бірақ белгілі шабуылдарға осалдығы анықталған.
- **NTRU** – жеңіл құрылғыларға бейімделген, бірақ кілт пен шифрмәтін көлемі үлкен.
- CRYSTALS-Kyber және ML-KEM

CRYSTALS–Kyber – кілт алмасуға арналған негізгі алгоритм ретінде NIST тарапынан стандартталды. Ол Module Learning-With-Errors (MLWE) есебіне негізделген және IND-CCA2 моделіне сай келеді [12]. Артықшылықтары:

- кілттердің шағын көлемі,
- жоғары өнімділік,
- жақсы өткізу қабілеті.

Kyber-512, Kyber-768 және Kyber-1024 деген үш деңгейі бар, олар сәйкесінше AES-128, AES-192 және AES-256 қауіпсіздік деңгейіне теңестірілген.

Осы алгоритмнің стандарты 2024 жылы FIPS 203 – ML-KEM атауымен ресми түрде қабылданды. ML-KEM схемасы CRYSTALS-Kyber-ден құпия кілтті басқару, инкапсуляция алгоритмдері мен кездейсоқтық генерациясында айырмашылықтарымен ерекшеленеді. ML-KEM-де құпия кілт ұзындығы – 256 бит және ол бірден симметриялық кілт ретінде пайдалануға болады [4].

Сандық қолтаңба үшін NIST үш алгоритмді стандарттауды бастады:

- **CRYSTALS–Dilithium** – негізгі ұсынылатын алгоритм;
- **Falcon** – қолтаңба көлемі шағын болғанымен, жад талаптары жоғары;
- **SPHINCS+** – хэшке негізделген, баяу, бірақ ерекше математикалық негізге сүйенетін балама алгоритм.

Нәтижелер

Зерттеу нәтижесінде постквантық криптографияны стандарттау үдерісінің төрт кезеңі жүйелі түрде талданып, олардың әрқайсысында қарастырылған алгоритмдердің (торлық, кодтық, хэшке негізделген және басқа) іріктелу логикасы мен бағалау критерийлері сараланды. Анализ барысында CRYSTALS-Kyber және CRYSTALS-Dilithium алгоритмдері қауіпсіздік пен өнімділік көрсеткіштері бойынша стандарт ретінде бекітілгені расталды. Сонымен қатар, Falcon, SPHINCS+, BIKE, HQC, McEliece және басқа алгоритмдердің құрылымдық ерекшеліктері мен қолдану салалары, соның ішінде ресурсы шектеулі құрылғылардағы (мысалы, IoT) әлеуеті бағаланды. Салыстырмалы және классификациялық сараптама нәтижесінде әр алгоритмнің криптографиялық қолдану саласындағы орны анықталды, ал олардың қауіпсіздік параметрлері кванттық шабуылдарға қарсы төзімділік деңгейіне сәйкес жіктелді.

Талқылау

Жоғарыда қарастырылған постквантық криптографиялық алгоритмдер әртүрлі математикалық негіздерге сүйенеді және кванттық шабуылдарға қарсы тұра алатын түрлі әдістерді ұсынады. Алайда олардың әрқайсысының артықшылықтары мен шектеулері бар, бұл оларды нақты қолдану контекстінде бағалауды қажет етеді.

Кодтық алгоритмдерге келсек (McEliece, BIKE, HQC), олар криптоанализге қарсы тұрақты болып есептеледі және Шор алгоритміне төзімділігімен ерекшеленеді. McEliece шифрлауы жылдам болғанымен, ашық кілттің өте үлкен өлшемі және шифрланған хабарламаның ұзақтығы бұл алгоритмнің практикалық қолданысын шектейді [8]. HQC

салыстырмалы түрде шағын кілттерді ұсынады және жақсы бейімделетін құрылымға ие, бірақ күрделі декодтау процедурасы ресурсы шектеулі құрылғыларда қолдануды қиындатады. BIKE өнімділігі жоғары болғанымен, криптографиялық шабуылдарға тұрақтылығы тұрғысынан қосымша талдау қажет.

Торлық алгоритмдер (Kyber, SABER, Dilithium, Falcon, т.б.) — қазіргі таңда ең перспективалы бағыттардың бірі. CRYSTALS–Kyber және CRYSTALS–Dilithium алгоритмдерінің стандарт ретінде қабылдануы олардың қауіпсіздік пен өнімділік тұрғысынан теңгерімді ұсынатынын көрсетеді [12].

Kyber алгоритмі жоғары тиімділікке ие және кішігірім кілт өлшемдерін қамтамасыз етеді, сондықтан ол шектеулі ресурсты құрылғылар үшін де қолайлы. Falcon алгоритмі шағын қолтаңба өлшемдерімен ерекшеленсе де, көп жадты қажет ететіндіктен оның қолданысы шектеулі болуы мүмкін. SABER алгоритмі қарапайым әрі қуат үнемдейтін құрылғылар үшін тиімді, бірақ ол ресми стандартталмаған.

Хэшке негізделген алгоритмдер (SPHINCS+) ерекше сенімділік деңгейін қамтамасыз етеді, себебі олардың қауіпсіздігі тек хэш функциясына негізделеді. Бұл – математикалық тұрғыдан айқын және түсінікті қауіпсіздік моделі. Алайда, SPHINCS+ алгоритмінің негізгі кемшілігі – қолтаңба өлшемдерінің үлкен болуы мен операциялық жылдамдықтың төмендігі. Сондықтан бұл алгоритм резервтік немесе балама шешім ретінде қарастырылады [10].

Зерттеу барысында байқалған тағы бір маңызды аспект — алгоритмдердің әртүрлі платформаға бейімделу мүмкіндігі.

Жоғары өнімді серверлік жүйелер үшін CRYSTALS–Kyber мен Dilithium секілді алгоритмдер тиімді болса, IoT құрылғылар сияқты шектеулі ресурсты орта үшін Falcon немесе SABER сияқты жеңілдетілген құрылымдар орынды. Ал қауіпсіздікке барынша сенімділік қажет болатын жүйелер үшін SPHINCS+ немесе FrodoKEM сынды шешімдер тиімді болуы мүмкін, бірақ оларды қолдану өнімділік есебінен жүргізіледі [8, 12].

Сондай-ақ, NIST таңдауының өзі талқылауға тұрарлық**.** Kyber мен Dilithium-ның стандартталуы – олардың криптоанализге тұрақтылығы, өнімділігі және нақты жүйелерде сәтті іске асырылғандығын көрсетеді [4]. Ал BIKE және HQC секілді алгоритмдердің балама ретінде сақталуы, криптографиялық әртүрлілікті қамтамасыз етуге және әртүрлі шабуыл модельдеріне қарсы қорғаныс құруға мүмкіндік береді.

Жалпы, постквантық алгоритмдер — қауіпсіздік пен өнімділік, әмбебаптылық пен мамандандыру арасындағы тепе-теңдікті табуға бағытталған. Бұл саланың үнемі дамуы – болашақта стандарттардың толыққанды және икемді болуына негіз қалайды.

Қорытынды

Қазіргі заманда кванттық есептеудің қарқынды дамуы классикалық криптографиялық жүйелерге елеулі қауіп төндіріп отыр. Бұл жағдай, әсіресе факторизациялау мен дискреттік логарифм есептеріне негізделген RSA және ECC сияқты кең таралған алгоритмдерге қатысты өзекті. Осыған байланысты постквантық криптография саласындағы зерттеулер мен стандарттау үдерістері жаһандық деңгейде маңызды ғылыми және практикалық мәселе ретінде алға шықты.

Зерттеу нәтижесінде постквантық криптографияға негізделген әртүрлі алгоритмдердің (торлық, кодтық, хэшке негізделген) артықшылықтары мен шектеулері салыстырмалы түрде талданып, олардың қауіпсіздік деңгейі, өнімділігі және қолдану салалары жіктеліп көрсетілді. CRYSTALS–Kyber және CRYSTALS–Dilithium алгоритмдерінің стандарт ретінде бекітілуі олардың практикалық тиімділігін дәлелдейді. Ал SPHINCS+, BIKE және HQC сынды баламалар әртүрлі сценарийлер мен қауіп-қатер модельдеріне қарсы қосымша қорғаныс ретінде қарастырылады. Сонымен қатар, постквантық алгоритмдерді ресурсы шектеулі

құрылғыларда (мысалы, IoT немесе кірістірілген жүйелер) қолдану мәселесі де маңызды болып қала береді. Бұл тұрғыда шағын кілттер мен тиімді есептеу сипаттамалары бар жеңілдетілген схемалар өзекті. Осыған орай, болашақ зерттеулер алгоритмдерді оңтайландыру, стандарттау, нақты платформаларда бейімдеу және гибридті криптожүйелерді құру бағытында жалғасуы тиіс.

Жалпы алғанда, постквanттық криптография саласындағы ғылыми ізденістер мен стандарттау әрекеттері ақпараттық қауіпсіздікті жаңа деңгейге көтеріп, цифрлық инфрақұрылымды ұзақ мерзімді қорғауға бағытталған маңызды қадам болып табылады. Бұл зерттеу — осы жаһандық бастамаларға үлес қосатын практикалық әрі теориялық негіз қалыптастыруға бағытталған.

Әдебиеттер тізімі

[1] Shor, P.W. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 20–22 November 1994; pp. 124–134.

[2] Gottesman, D.; Lo, H.K. Proof of Security of Quantum Key Distribution with Two-Way Classical Communications. IEEE Trans. Inf. Theory 2003, 49, 457–475. [CrossRef]

[3] Mailloux,L.O.; Lewis, C.D.; Riggs, C.; Grimaila, M.R.Post-QuantumCryptography: WhatAdvancementsinQuantumComputing Meanfor IT Professionals. IT Prof. 2016, 18, 42–47. [CrossRef]

[4] Cherkaoui Dekkaki, K.; Tasic, I.; Cano, M.-D. Exploring Post-Quantum Cryptography: Review and Directions for the Transition Process. Technologies 2024, 12, 241. https://doi.org/10.3390/ technologies12120241

[5] Imai, H.; Hagiwara, M. Error-Correcting Codes and Cryptography. Appl. Algebra Eng. Commun. Comput. 2008, 19, 213–228. [CrossRef]

[6] Abusultanov, R., Buqekov, A., & Seilov, T. (2023). Post-Quantum Cryptographic Algorithms and Their Implementation in Computer Systems. 2023 IEEE 5th International Conference on Advanced Information and Communications Technologies (AICT), 312–317. https://doi.org/10.1109/AICT58444.2023.10810828

[7] Bulatova, K. A., & Khalymon, D. M. (2024). Methods of post-quantum cryptography. *Radiotekhnika*, (215), 76–85. Retrieved from http://rt.nure.ua/article/view/229327

[8] https://bikesuite.org/

[9] https://pqc-hqc.org/

[10] Cheon, J.H.; Kim, J. A Hybrid Scheme of Public-Key Encryption and Somewhat Homomorphic Encryption. IEEE Trans. Inf. Forensics Secur. 2015, 10, 1052–1063. [CrossRef]

[11] Bos, J.; Ducas, L.; Kiltz, E.; Lepoint, T.; Lyubashevsky, V.; Schanck, J.M.; Schwabe, P.; Seiler, G.; Stehle, D. CRYSTALS—Kyber: ACCA-Secure Module-Lattice-Based KEM. In Proceedings of the 2018 IEEE European Symposium on Security and Privacy (EuroS&P), London, UK, 24–26 April 2018; pp. 353–367.

[12] Bernstein, D. J., Lange, T., & Peters, C. (2008). Attacking and defending the McEliece cryptosystem. In Post-Quantum Cryptography (pp. 31–46). Springer.

References

[1] Shor, P.W. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 20–22 November 1994; pp. 124–134.

[2] Gottesman, D.; Lo, H.K. Proof of Security of Quantum Key Distribution with Two-Way Classical Communications. IEEE Trans. Inf. Theory 2003, 49, 457–475. [CrossRef]

[3] Mailloux,L.O.; Lewis, C.D.; Riggs, C.; Grimaila, M.R.Post-QuantumCryptography: WhatAdvancementsinQuantumComputing Meanfor IT Professionals. IT Prof. 2016, 18, 42–47. [CrossRef]
[4] Cherkaoui Dekkaki, K.; Tasic, I.; Cano, M.-D. Exploring Post-Quantum Cryptography: Review and Directions for the Transition Process. Technologies 2024, 12, 241. https://doi.org/10.3390/ technologies12120241
[5] Imai, H.; Hagiwara, M. Error-Correcting Codes and Cryptography. Appl. Algebra Eng. Commun. Comput. 2008, 19, 213–228. [CrossRef]
[6] Abusultanov, R., Buqekov, A., & Seilov, T. (2023). Post-Quantum Cryptographic Algorithms and Their Implementation in Computer Systems. 2023 IEEE 5th International Conference on Advanced Information and Communications Technologies (AICT), 312–317. https://doi.org/10.1109/AICT58444.2023.10810828
[7] Bulatova, K. A., & Khalymon, D. M. (2024). Methods of post-quantum cryptography. *Radiotekhnika*, (215), 76–85. Retrieved from http://rt.nure.ua/article/view/229327
[8] https://bikesuite.org/
[9] https://pqc-hqc.org/
[10] Cheon, J.H.; Kim, J. A Hybrid Scheme of Public-Key Encryption and Somewhat Homomorphic Encryption. IEEE Trans. Inf. Forensics Secur. 2015, 10, 1052–1063. [CrossRef]
[11] Bos, J.; Ducas, L.; Kiltz, E.; Lepoint, T.; Lyubashevsky, V.; Schanck, J.M.; Schwabe, P.; Seiler, G.; Stehle, D. CRYSTALS—Kyber: ACCA-Secure Module-Lattice-Based KEM. In Proceedings of the 2018 IEEE European Symposium on Security and Privacy (EuroS&P), London, UK, 24–26 April 2018; pp. 353–367.
[12] Bernstein, D. J., Lange, T., & Peters, C. (2008). Attacking and defending the McEliece cryptosystem. In Post-Quantum Cryptography (pp. 31–46). Springer.

Применение и критерии оценки постквантовых криптографических алгоритмов для безопасности и стандартизации

Н.Ж. Жарасхан *, С.А.Наурызбаева

Высшая школа информационных технологий и инженерии, Международный университет Астана, Астана, Казахстан

Аннотация. В статье представлено теоретическое и сравнительное исследование современных алгоритмов постквантовой криптографии. Классические криптографические методы, такие как RSA и ECC, теряют свою устойчивость в условиях развития квантовых вычислений, что вызывает необходимость в разработке новых алгоритмов. В связи с этим Национальный институт стандартов и технологий США (NIST) инициировал процесс выбора и стандартизации постквантовых алгоритмов. В работе рассмотрены архитектура, безопасность, производительность и области применения алгоритмов CRYSTALS-Kyber, CRYSTALS-Dilithium, Falcon, SPHINCS+, BIKE, HQC и других. Отражены их преимущества и ограничения, а также возможности использования в устройствах с ограниченными ресурсами. Методология включает системный обзор, сравнительный анализ и классификационную экспертизу. Полученные результаты подчеркивают значимость постквантовых алгоритмов в обеспечении долгосрочной кибербезопасности и служат ориентиром при выборе будущих криптографических стандартов.
Ключевые слова: Постквантовая криптография, CRYSTALS-Kyber, Алгоритмы безопасности, Квантовые атаки, Решеточная криптография, Кодовая криптография, Стандартизация NIST

Application and Evaluation Criteria of Post-Quantum Cryptographic Algorithms for Security and Standardization

N. Zharaskhan *, S.A. Nauryzbaeva

Highe School of Information Technology and Engineering, Astana International University, 010000, Astana, Kazakhstan

Abstract. This article provides a theoretical and comparative analysis of modern post-quantum cryptographic algorithms. Classical cryptographic schemes such as RSA and ECC are vulnerable to quantum attacks, prompting the urgent need for quantum-resistant alternatives. In response, the U.S. National Institute of Standards and Technology (NIST) initiated a global effort to evaluate and standardize post-quantum algorithms. The paper explores the architecture, security characteristics, performance, and application areas of algorithms including CRYSTALS-Kyber, CRYSTALS-Dilithium, Falcon, SPHINCS+, BIKE, and HQC. Each algorithm's strengths and limitations are highlighted, with particular attention to their feasibility for resource-constrained devices. The research methodology involves a systematic review, comparative assessment, and classification analysis. The findings demonstrate the critical role of post-quantum cryptography in achieving long-term cybersecurity and offer insights to guide the adoption of future cryptographic standards.

Keywords: Post-Quantum Cryptography, CRYSTALS-Kyber, Security Algorithms, Quantum Attacks, Lattice-based Cryptography, Code-based Cryptography, NIST Standardization