АҢДАТПА

8D06301 – «Ақпараттық қауіпсіздік жүйелері» білім беру бағдарламасы бойынша PhD докторанты Әмірханова Дана Сайранғажықызының «Эль-Гамаль принциптерін пайдалана отырып, торға негізделген постквантық ашық кілтті шифрлау схемасы» тақырыбындағы диссертациялық жұмысы.

Зерттеу тақырыбының өзектілігі. Қазіргі заманғы технологиялар, мысалы, кванттық және бұлтты есептеу, есептеу техникасының бейнесін өзгертіп, теңдессіз есептеу қуатын және масштабталуын ұсынады. Әрине, бұл жетістіктер елеулі артықшылықтарды уәде етсе де, олар классикалық криптографиялық құрылымдардың қауіпсіздігіне қиындықтар туғызады. Кванттық есептеу есептеулерді экспоненциалды жылдамдату мүмкіндігіне ие болғандықтан, Шор алгоритмі сияқты алгоритмдер арқылы үлкен сандарды факторизациялау және дискретті логарифмдерді шешу арқылы кеңінен қолданылатын RSA және ECC және де Эль-Гамаль сияқты ашық кілт криптосистемаларының қауіпсіздігіне қауіп төндіреді. Кванттық компьютерлердің дамуы барысында цифрлық қауіпсіздігімізді қорғайтын криптографиялық алгоритмдер шабуылдарға осал болуы мүмкін, сондықтан кванттыққа төзімді криптографиялық примитивтерді әзірлеу қажеттілігі туындайды. Бұлтты есептеу, екінші жағынан, деректердің құпиялылығы, тұтастығы және жеке өмірі мәселелеріне жаңа қауіпсіздік проблемаларын тудырады. Ол кең көлемдегі есептеу ресурстарына және сақтау орындарына ыңғайлы қол жеткізуді ұсынса да, сондай-ақ авторланбаған деректерге қол жеткізу, ақпардың ағып кетуі және ішкі қауіптер сияқты мәселелерді көтереді. Бұлттағы деректердің қауіпсіздігін қамтамасыз ету сенімді криптографиялық механизмдер, қорғалған байланыс протоколдары және қатаң қол жеткізу бақылауларын талап етеді. Кванттық есептеу және дамып келе жатқан есептеу технологияларының туғызған қиындықтарына жауап ретінде, решеткалық криптография, мысалы, қысқа бүтін санды шешім (SIS) мәселесіне негізделген қиындықты пайдалану арқылы қызықты шешім ретінде кеңінен тарала бастады. Бұл жұмыста жаңа кванттыққа төзімді ашық кілтпен шифрлау схемасы ұсынылған, ол решеткаларға негізделіп, Эль-Гамаль принциптерін пайдаланады. Схема SIS проблемасына негізделген және осы мәселе бойынша кілт алмасу протоколын қамтиды, бұл кванттық және классикалық шабуылшылардан қорғауды қамтамасыз етеді. Схеманың құрылысы қарапайым болып табылады және қазіргі замандағы криптографиялық орталарда деректерді қауіпсіз жіберу үшін шешім ұсынады. Бұл жетістік кванттық есептеулер мен жаңа технологиялардың туғызған қиындықтарына жауап ретінде криптографияның үздіксіз дамуын көрсетеді. Жоғарыда айтылғандарды ескере отырып, қазіргі уақытта

торларға негізделген Эль-Гамаль әдісін пайдаланып, кванттық шабуылдарға қарсы қорғанысты жетілдіруге арналған тиімді әдістер мен алгоритмдерге деген қажеттілік өзекті болып отыр.

Зерттеудің мақсаты: Эль-Гамаль принциптерін пайдалана отырып, торға негізделген постквантық ашық кілтті шифрлау схемасын құру әдісін әзірлеу.

Міндеттері:

1) Дәстүрлі криптографияның танымал әдістері мен алгоритмдерін және олардың постквантық криптография жағдайындағы төзімділігін талдау.

2) Торларға негізделген кілттерді бөлу схемаларын зерттеу.

3) Эль-Гамаль қағидаттарын пайдалана отырып, торларға негізделген тиімді әрі қауіпсіз постквантық кілт алмасу схемасының моделін әзірлеу.

4) Торларға негізделген және Эль-Гамаль қағидаттарын пайдаланатын ашық кілтті постквантық криптожүйенің алгоритмі мен прототипін әзірлеу.

5) Ұсынылған постквантық криптожүйенің тиімділігін зерттеу және сынақтан өткізу.

Зерттеу нысандары: ашық кілтті схемаларды қолдана отырып, классикалық және кванттық шабуылдардан деректерді криптографиялық қорғау процесі.

Зерттеу әдістері: Классикалық криптография, параметрлердің өлшемдері, торлар теориясы, алгоритмдердің тиімділігін бағалау, тәжірибелік тестілеу.

Ғылыми жаңалығы:

- Эль-Гамаль принциптерін қолдана отырып, решеткаларға негізделген тиімді және қауіпсіз постквантық кілт алмасу схемасының математикалық моделін әзірлеу жүзеге асырылды, ол постквантық ашық кілт схемаларын тиімді түрде құруға мүмкіндік береді.
- Эль-Гамаль принциптерін қолданатын, решеткаларға негізделген постквантық ашық кілт схемасының алгоритмі мен прототипі әзірленді, ол шифрлау кілттерін генерациялау жылдамдығын 240-583 есе (аналогтарымен салыстырғанда – LWE, Ring-LWE) арттырып, кванттық шабуылдарға төзімділікті қамтамасыз етті(классикалық Эль-Гамаль схемасымен салыстырғанда).

Жұмыстың теориялық және практикалық маңыздылығы. Зерттеу жұмысының теориялық маңыздылығы кванттық шабуылдарға төзімді криптографиялық жүйелерді әзірлеуді дамытуға және ақпараттық қауіпсіздік саласында математикалық әдістерді қолдану мүмкіндіктерін кеңейтуге қосқан үлесімен айқындалады. Жұмыстың практикалық маңыздылығы әзірленген алгоритм мен бағдарламалық қамтамасыз етуді кванттық және классикалық қауіптерден қорғайтын басқа технологияларды дамытуда әрі қарай қолдануға негізделген. Әзірленген схема қарапайым әрі

жылдамдығы тиімді, қазіргі криптографиялық ортада қауіпсіз деректерді тасымалдау мәселесін шешуге мүмкіндік береді. Бұл жетістік кванттық есептеу және бұлттық есептеу технологияларымен байланысты мәселелерді шешуде криптографияның үздіксіз дамуын көрсетеді.

Қорғауға шығарылатын негізгі тұжырымдар:

1. Эль-Гамаль принциптерін қолдана отырып, торлар негізінде тиімді және қауіпсіз постквантық кілт алмасу сұлбасының математикалық моделі әзірленді. Бұл модель криптографиялық протоколдарда, аутентификация жүйелерінде, қаржы жүйелерінде, блокчейн және IoT технологияларында қолдануға болатын тиімді ашық кілтті постквантық сұлбаларды құруға мүмкіндік береді.
2. Эль-Гамаль шифрлеу принциптерін қолданатын, торлар негізіндегі постквантық ашық кілтті шифрлеу сұлбасының алгоритмі мен прототипі әзірленді. Бұл шешім шифрлеу кілттерін генерациялау жылдамдығын 240–583 есеге арттыруға (LWE, Ring-LWE сұлбаларымен салыстырғанда) және классикалық Эль-Гамаль сұлбасымен салыстырғанда кванттық шабуылдарға төзімділікті қамтамасыз етуге мүмкіндік берді.
3. Кванттық қолжетімді кездейсоқ оракул үлгісінде (QROM) SIS есебіне редукциялау арқылы IND-CCA стандартына сәйкес криптожүйенің теориялық қауіпсіздік моделі ұсынылды және негізделді. Бұл шифрлеу схемасының кванттық шабуылдарға формалды төзімділігін қамтамасыз етеді.

Жұмыстың апробациясы. Диссертациялық зерттеудің негізгі ережелері мен нәтижелері «Киберқауіпсіздік, ақпаратты өңдеу және сақтау» кафедрасының ғылыми семинарларында, ИИВТ зертханасында, сондай-ақ SCSA және Кавказ университетінде (Caucasus University) баяндалып, талқыланды.

Нәтижелердің дұрыстығы. Диссертациялық жұмыстың нәтижелерінің дұрыстығы мен негізділігі Қазақстан Республикасы Ғылым және жоғары білім министрлігінің Білім және ғылым саласындағы сапаны қамтамасыз ету комитеті ұсынған басылымдардағы, сондай-ақ Web of Science және Scopus (MDPI, Швейцария) халықаралық ақпараттық дерекқорларына кіретін журналдардағы және халықаралық ғылыми конференцияларда жарияланған мақалалармен, сондай-ақ басқа авторлардың алған нәтижелерімен расталады.

Мемлекеттік бағдарламалармен байланысы. Диссертациялық жұмыстың тақырыбы Қазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы № 407 қаулысымен (2023 жылғы 17 наурыздағы № 236 Қазақстан Республикасы Ғылым және жоғары білім министрінің бұйрығына сәйкес өзгерістерімен және толықтыруларымен) бекітілген «Киберқалқан Қазақстан» киберқауіпсіздік тұжырымдамасында белгіленген басымдықтармен тікелей байланысты. «Киберқалқан Қазақстан» тұжырымдамасында орнықты және қорғалған цифрлық ортаны

қалыптастыру ұлттық қауіпсіздік саласындағы мемлекеттік саясаттың негізгі бағыты ретінде анықталған. Тұжырымдаманың стратегиялық бағыттарының бірі – кванттық технологиялардың дамуымен байланысты қауіп-қатерлерді қоса алғанда, болашақтағы қауіптерге төтеп бере алатын ақпараттық қауіпсіздікті дамыту. Осы тұрғыдан алғанда, диссертацияда ұсынылған шифрлеу схемасы сияқты постквантық криптографиялық шешімдерді әзірлеу тұжырымдамада көзделген мақсаттар мен міндеттерге толық сәйкес келеді. Ұсынылған жұмыс кванттық шабуылдарға төзімді отандық криптографиялық технологияны әзірлеуге бағытталған және оны ақпараттық-коммуникациялық инфрақұрылымды, маңызды нысандарды, қаржылық жүйелерді қорғау үшін, сондай-ақ цифрлық трансформация мен ұлттық деректердің қауіпсіздігін қамтамасыз ету аясында қолдануға болады.

Жарияланымдар

1) Әмірханова Д.С, Максим Явич және Мамырбаев Ө.Ж.*Cryptography* 2024, *8*(3),31. https://doi.org/10.3390/cryptography8030031 (Scopus, процентиль 66, Web of Science – Q2). “Lattice- based Post-Quantum Public Key Encryption Scheme Using ElGamal’s Principles”.

2) Әмірханова Д.С., Мамырбаев Ө.Ж., Хабаршысы Абай атындағы ҚазҰПУ. Серия: Физика – Математика ғылымдары Том 83 № 3(2023). “Cryptographic analysis of the scheme of polylinear cryptography”.

3) Әмірханова Д.С., Мамырбаев Ө.Ж., Хабаршысы ҚР ҰҒА: Серия: Физика – Математика ғылымдары ISSN 1991-346X Том 3. № 351 (2024).“El-Gamal’s Cryptographic Algorithm: Mathematical Foundations, Applications And Analysis”.

4) Әмірханова Д.С., Мамырбаев Ө.Ж.,Хабаршысы ШҚТУ: Серия: Ақпараттық және коммуникациялық технологиялар ISSN 1561-4212 № 1(2025))“Research And Development of a Cryptography Algorithm Based on Polylinear Algebra Using Blockchain Methodology”.

Диссертацияның құрылымы мен көлемі: Диссертация нормативтік сілтемелерден, белгілер мен қысқартулардан, кіріспеден, 3 тараудан, қорытындыдан және пайдаланылған әдебиеттер тізімінен тұрады. Жұмыс 96 беттен, 1 кестеден және 39 суреттен тұрады. Пайдаланылған әдебиеттер тізімі 85 атаудан тұрады.

Кіріспеде тақырыптың өзектілігі ашылып көрсетіліп, зерттелетін мәселе нақты анықталған. Зерттеу мақсаты мен міндеттері, жұмыстың ғылыми жаңалығы мен практикалық құндылығы, сондай-ақ зерттеу әдістері берілген.

Диссертацияның бірінші тарауында дәстүрлі криптографияның танымал әдістері мен алгоритмдерін талдау ұсынылып, олардың кванттық шабуылдарға осалдығы анықталды, себебі кванттық алгоритмдер мұндай жүйелерді тиімді бұза алады. Сондай-ақ постквантық криптография және оның қазіргі заманғы криптографиядағы маңызы талданады, өйткені ол

кванттық компьютерлердің шабуылына төтеп бере алатын әдістер мен алгоритмдерді ұсынады.

Диссертацияның екінші тарауында решеткаларға негізделген кілт тарату схемалары талданып, олардың негізгі есептердің күрделілігіне байланысты кванттық шабуылдарға жоғары төзімділігі расталды. Осы талдау негізінде решеткалық әдістер мен Эль-Гамаль қағидаттарын қолданатын тиімді әрі қауіпсіз кілт алмасу схемасының моделі әзірленді. Мұндай үйлесім криптографиялық беріктіктің және өнімділіктің жоғары деңгейін қамтамасыз етіп, ұсынылған шешімді қазіргі заманғы ақпараттық қауіпсіздік жүйелерінде іс жүзінде пайдалануға мүмкіндік береді.

Үшінші тарауда бағдарламалық іске асыру негізінде Эль-Гамаль принциптерін қолданатын, решеткелерге негізделген постквантық ашық кілт схемасының алгоритмі мен прототипі әзірленді. Сондай-ақ ұсынылған криптожүйенің тиімділігіне жүргізілген зерттеу және тестілеу нәтижелері көрсетілген, криптожүйенің қауіпсіздік теориялық моделі IND-CCA стандартына сәйкес негізделіп, кванттық қолжетімді кездейсоқ оракул үлгісінде (QROM) SIS есебіне редукциялау арқылы құрылды, бұл схеманың кванттық шабуылдарға формалды төзімділігін қамтамасыз етеді. Сонымен қатар, жүйе жоғары жұмыс жылдамдығын көрсетіп, оны практикалық қолдануға болашағы зор етеді.

Қорытынды бөлімде диссертациялық жұмыстың негізгі нәтижелері мен тұжырымдары көрсетілген.