«8D06301 – Ақпараттық қауіпсіздік жүйелері» білім беру бағдарламасының PhD докторанты Сақан Қайрат Сақанұлының «Итерациялық блоктық шифрларға негізделген хеш алгоритмдерін құру және олардың криптоберіктілігін зерттеу» тақырыбындағы диссертациялық жұмысына

АҢДАТПА

Зерттеу тақырыбының өзектілігі. Қазіргі таңдағы электрондық құрылғылардың, байланыс құралдарының және интернет-технологиялардың қарқынды дамуы кезеңінде ақпараттың қауіпсіздігін қамтамасыз ету мақсатында, негізінен, криптографиялық әдістер – шифрлау және хештеу жүйелері пайдаланылады.

Хеш функциялар электрондық жүйелерде парольдар мен кілттерді қорғаудан бастап, ақпараттың тұтастығын және авторлықты растау мен одан бас тарта алмау құқығын тексеруде, блокчейн технологиясында, сондай-ақ постквантты криптография саласында да кеңінен қолданылуда. Кванттық компьютер хеш функциялардағы түпбейнені табу мәселесін шешуді квадраттық үдеумен шешетіндіктен, хеш функцияларға негізделген криптографиялық хештеу алгоритмдерін постквантты криптографияда да сәтті қолдануға болады.

Бүгінгі күні жаңа конструкциялар мен оларды құрастыру тәсілдері арқылы көптеген жаңа хеш-функциялар жасалуда. Алайда, ақпараттық технологиялардың мүмкіндіктерінің артуы және есептеу қуатының қарқынды дамуы ақпараттық қорғаудың криптографиялық әдістеріне бағытталған жаңа шабуылдардың пайда болуына және бар шабуылдардың жаңа нұсқалары құрылуына әкелуде. Сол себепті, ақпараттың қорғаныс жүйелерін, соның ішінде хештеу жүйесінің қолданыстағы моделдерін үнемі дамытып және жаңартып отыру қажеттілігін туындатады. Яғни, әзірленетін хеш функциялар қауіпсіздік қасиеттері бойынша қатаң тексерулерінен өтуі тиіс.

Блоктық шифрға негізделген хеш-функцияның негізгі артықшылығы болып оны жобалау барысында қолданылатын шифрлау алгоритмінде жақсы зерттелген криптографиялық примитивтер мен конструкцияларды пайдалану саналады. Сонымен бірге, блоктық шифрдағы блок пен кілт ұзындығы, раунд саны сияқты параметрлерді өзгерте отырып, хеш функциялардың қауіпсіздік деңгейі мен жұмыс өнімділігін қажеттегідей таңдай алуға мүмкіндік береді. Сызықтық пен дифференциалдық криптоталдау және «Толық теру» әдістеріне беріктілігі жоғары блоктық шифрды пайдалану – құрылған хеш функциядағы коллизияларды, түпбейнені және екінші түпбейнені табу мүмкіндіктерін қиындатады. Хеш функцияларды әзірлеуде қолданылатын блоктық шифр компоненттерін жан-жақты талдау, сондай-ақ хеш функциялардың заманауи технологиялардағы маңыздылығы үздіксіз және серпінді ғылыми зерттеулерді қажет етеді.

Диссертациялық жұмыстың негізгі бағыты болып қауіпсіздік қасиеттердің жоғарғы деңгейін қамтамасыз ете отырып, есептеу өнімділігі

жағынан тиімді блоктық шифрға негізделген жаңа хештеу алгоритмін құру және оны сенімділікке зерттеу саналады.

Сонымен бірге, қазір Қазақстанның электрондық жүйелерінде ақпаратты қорғау үшін негізінен халықаралық стандарттар және шетелдік криптографиялық құралдар мен бағдарламалық жасақтамалар қолданылатынын ескергенде, мәліметтерді хештеу жүйесі бойынша отандық өнімдерді жасау – сөзсіз өзекті және қажетті мәселе.

Диссертациялық жұмыстың мақсаты. Симметриялы блоктық шифрлау алгоритмі негізінде қауіпсіздігі мен өнімділігі жағынан жоғары, бағдарламалы-аппараттық жүзеге асыруға және параллелдік есептеуге икемделген хештеу алгоритмін құру және оның қауіпсіздік қасиеттері мен тиімділігін зерттеу.

Зерттеу міндеттері:

– Заманауи хеш функцияларға сараптама жүргізу, коллизияларды зерттеу әдістерін талдау, шабуыл үлгілері мен криптоталдау әдістерін зерделеу;

– блоктық шифрға негізделген жаңа хеш алгоритмін құру;

– қысу функциясы ретінде қолданылатын жаңа блоктық шифрлау алгоритмін құру;

– құрылған хештеу алгоритмінің қауіпсіздік қасиеттерін статистикалық сынақтар және криптоталдау әдістері арқылы зерттеу;

– құрылған хештеу алгоритмін бағдарламалық және бағдарламалы-аппараттық жүзеге асыру, сондай-ақ тиімділігін талдау.

Зерттеу нысаны: Криптографиялық хеш-функциялар және шифрлау жүйелері.

Зерттеу пәні:

– Аз өлшемді S-блок ауыстыру түйіндерінің ерекше архитектурасы негізінде жасалынған симметриялық блоктық шифрлау алгоритмі;

– қысу функциясы ретінде симметриялық блоктық шифрлау алгоритмі пайдаланатын хештеу алгоритмі.

Зерттеу құралы мен әдісі: Бульдік функция теориясы, сызықтық алгебра, ықтималдықтар теориясы және математикалық статистика, хеш алгоритмге жүргізілетін криптографиялық талдау әдістері мен шабуылдар түрлері, лавиндік әсерлер.

Жұмыстың ғылыми жаңалығы:

– жаңа хештеу алгоритмін жасау үшін қажетті жаңа симметриялық блоктық шифрлау алгоритмі құрылды;

– блоктық шифрларға негізделіп, паралелльді есептеуге және бағдарламалы-аппараттық жүзеге асыруға икемделген жаңа хештеу алгоритмі құрылды;

– төрт 4-биттік S-блок ауыстыру түйіндерін элементтің индекстеріне қатысты жұптастырып қолданудың жаңа сұлбасы ұсынылды, оны қолдану

алгоритмнің қауіпсіздігін арттыруға және аппараттық жүзеге асыруда микросхеманың жадын тиімді пайдалануға мүмкіндік береді;

– қысу функциясындағы сызықты емес түрлендіруді қолданудың жаңа сұлбасы ұсынылып, оның раундтар санын азайтуға мүмкіндік беретіні көрсетілді;

– хабарлама блогының ұзындығын оның көлеміне байланысты k бөліктер санын өзгерту мүмкіндігі ұсынылды, ол өз кезегінде есептеу өнімділігін арттыратыны анықталды (k=3,…, 8, k - бөліктер саны).

Зерттеудің теориялық және практикалық құндылығы. Жүргізілген ғылыми зерттеулердің теориялық және алынған нәтижелердің практикалық құндылығы электрондық құрылғыларда, деректерді тасымалдаудың және сақтаудың арнайы жүйелерінде ақпаратты қорғаудың криптографиялық құралдарын пайдалану мүмкіндігін арттырады және нәтижесінде отандық ақпараттық жүйелерді дамыту үшін жаңа мүмкіндіктер ашады.

Жасалған HBC-256 хештеу алгоритмі 2022 жылы Алматы қаласындағы «Guppyprint» баспасынан шыққан «Разработка и исследование алгоритмов хеширования произвольной длины» монографиясында жеке бөлім ретінде енгізілді (ISBN 978-601-08-2549-9, 95 бет).

Зерттеу жұмысы нәтижелері SCOPUS және Web of Science халықаралық деректер қорына кірген журналдарда, сондай-ақ ҚР ҒЖБМ-нің Білім және ғылым саласы бойынша бақылау комитетімен ұсынылған басылымдарда ғылыми мақалалар болып жарияланды (Қосымша А).

Аталған хештеу алгоритмнің тәуелсіз зерттеулері нәтижелері Новосибирск мемлекеттік университеті және «Криптографиялық Орталық» (Новосибирск қ.) ұйымдастыруымен өткен «Криптография и информационная безопасность» жаздық мектеп-конференцияның еңбектері жинағына «Исследование криптографических свойств новых функций хэширования HBC и HAS01» тақырыбында енді.

ҚР ӘМ Ұлттық зияткерлік меншік институтынан ғылыми туынды ретінде 1 авторлық куәлік және алгоритмнің бағдарламалық жасақтамасы бойынша 3 авторлық куәлік алынды (Қосымша Ә).

Қорғауға шығарылған негізгі тұжырым. Блоктық шифр негізде бағдарламалы-аппараттық жүзеге асыруға және параллелді есептеуге икемделген жаңа хештеу алгоритмі құрылды. Құрылған хештеу алгоритмінің қауіпсіздігі қасиеттерін статистикалық сынақтары, лавиндік әсер критерийі, «жақын коллизиялар» әдісі, сондай-ақ дифференциалдық, сызықтық және алгебралық криптоталдау әдістері арқылы зерттелді. Әзірленген хештеу алгоритмі заманауи технологиялық дамудың жетістіктері жағдайында оның криптографиялық беріктігі мен қолдану тиімділігін арттыруға мүмкіндік береді.

Сенімділік дәрежесі мен апробациялау нәтижелері. Диссертациялық жұмыс бойынша жүргізілген зерттеулер мен алынған нәтижелердің сенімділігі екінші, үшінші және төртінші бөлімдерде келтірілген.

Зерттеулер нәтижесі төмендегі ғылыми-практикалық конференцияларда, сондай-ақ отандық және шетелдік ғылыми-зерттеу институттары мен оқу орындарындағы ғылыми семинарларда баяндалған (Қосымша Б):

– «Информатика және қолданбалы математика» V, VI және VII халықаралық ғылыми-тәжірибелік конференцияларында (Алматы, 2020-2022 жж.);

– «Қазақстандағы ақпараттық қауіпсіздіктің өзекті мәселелері» халықаралық ғылыми-тәжірибелік конференциясында (АПБИК-2021, Алматы, 2021 ж. 11 маусым);

– Әл-Фараби атындағы ҚазҰУ профессорі У.А. Тукеевтің 75 жылдық мерейтойына арналған ақпараттық технологиялар саласындағы Халықаралық ғылыми конференцияда (Алматы, 2021 ж. 8 қазан);

– IV халықаралық «Минские научные чтения-2021. Передовые технологии и материалы будущего» ғылыми-техникалық конференциясында (Минск, Беларусь, 2021 ж. 9-10 желтоқсан);

– “Computer Data Analysis and Modeling: Stochastics & data Science” (CDAM-2022) халықаралық конференцияда (Минск, Беларусь, 2022 ж. 6-9 қыркүйек);

– Украина Ұлттық авиациялық университеті «Киберқауіпсіздік, компьютерлік және бағдарламалық инженерия» факультетінің (ФКбКПИ НАУ) ғылыми семинарында (Киев, Украина, 2021 ж.3 желтоқсан);

– Беларусь мемлекеттік университеті «Математика және информатиканың қолданбалы мәселелері» ғылыми зерттеу институты ғылыми семинарында (НИИ ППМИ БГУ) (Минск, Беларусь, 2022 ж. 6 қыркүйек);

– Electrical Engineering and Computer Science Department of Khalifa University ғылыми семинарында (Абу-Даби, БАӘ, 2022 ж. 13 желтоқсан);

– «Ақпараттық және есептеуіш технологиялар» институты және Әл-Фараби атындағы ҚазҰУ «Ақпараттық технологиялар» факультеті ғылыми семинарларында (2020 – 2023жж., Алматы).

Диссертациялық тақырыптың ғылыми бағдарламалармен байланысы. Диссертациялық жұмыс Қазақстан Республикасының Ғылым және жоғарғы білім министірлігі Ғылым комитетінің Ақпараттық және есептеуіш технологиялар институтында бекітілген PhD докторлық диссертациялар жоспары және ЖТН – OR11465439 «Электрондық цифрлы қолтаңба үшін еркін ұзындықтағы хештеу алгоритмін құру мен зерттеу және олардың беріктілігін бағалау» бағдарламалық-нысаналы қаржыландыру жобасының ғылыми-зерттеу жұмыстарының аясында орындалды. Диссертациялық жұмыс бойынша жүргізілген зерттеу жұмыстарының нәтижесі аталған БНҚ жобасының 2021-2022 жылдарындағы есебіне енгізіліп, «Енгізу актісі» алынды (Қосымша В).

Жұмыс көлемі мен құрылымы. Диссертациялық жұмыс кіріспе, 4 бөлім, қорытынды, пайдаланылған әдебиеттер тізімі мен қосымшалардан тұрады. Диссертацияның толық көлемі: 103 бет жазба мәтіні, оның ішінде 30 сурет, 28 кесте, 99 пайдаланылған әдебиеттер тізімінен, 6 қосымшадан тұрады.

Нәтижелердің жарияланымдары. Ғылыми зерттеу жұмыстарын жүргізу барысында 24 ғылыми еңбек жарық көрді. Оның ішінде 7 мақала Scopus және Web of Science базаларында индекстелген журналдарда, 1 отандық монография, 7 мақала Қазақстан Республикасы ғылым және жоғарғы білім министрлігінің білім және ғылым саласы бойынша бақылау комитетімен ұсынылған басылымдарда, 10 мақала халықаралық және отандық ғылыми-практикалық конференциялар жинақтарында және басқа да ғылыми журналдарда жарияланды.

Кіріспеде диссертациялық жұмыс тақырыбы бойынша алғысөз және тақырып өзектілігінің негіздемесі баяндалады. Осы бөлімде ғылыми-зерттеу жұмысының мақсаттары, нысаны және зерттеу пәні көрсетілді. Сондай-ақ, жұмыстың ғылыми жаңалығы, тәжірибелік маңызы, жұмыс–нәтижелерінің апробациясымен қоса жарияланымдары туралы мағлұматтар беріледі.

Бірінші бөлімде хештеу алгоритмдерінің түрлері және хеш функцияларға қатысты пайдаланылатын негізгі ұғымдар келтірілген. Хеш функцияларға қойылатын талаптар сипатталып, олардың негізгі қасиеттері сараланады. Бөлімнің соңында хеш алгоритмдердің сапасын бағалау критерийлері мен оларға жасалатын шабуылдарға жіктеу жасалып, сараптама жүргізілген.

Екінші бөлімде хеш функцияларға қойылатын талаптарды ескере отырып, оның негізгі қасиеттеріне ие бола алатындай етіп, итерациялы симметриялы блоктық шифрлау алгоритмі негізінде HBC-256 хештеу алгоритмі ұсынылады. Блоктық шифрлау алгоритмі ретінде SP-желісі негізінде құрылған CF алгоритмі қарастырылады. Құрылған CF шифрлау алгоритмде қолданылған криптографиялық примитивтер мен түрлендірулерге жеке-жеке сипаттамалар беріледі. Есептеу өнімділігін арттыру мақсатында раундтар санын неғұрым минималды ету үшін жаңа сұлба ұсынылады. Жадыдағы орынды үнемдеу үшін төрт 4-биттік S-блок ауыстыру кестесі қолданылды және оларды тиімді пайдалану қағидасы көрсетіледі.

Үшінші бөлімде құрылған HBC-256 хештеу алгоритмінің қауіпсіздік қасиеттеріне зерттеулер жүргізіледі. Атап айтқанда, алгоритмнің қауіпсіздік қасиеттері теориялық тұрғыдан бағаланып, одан әрі NIST және Д.Кнут сатистикалық сынақтар жиынтығы бойынша хеш-мәннің псевдокездейсоқтық қасиетке ие болу деңгейіне баға беріледі. Хабарлама мен хеш-мән арасындағы қатынасты сипаттайтын талап – лавиндік және қатаң лавиндік әсері зерттеледі. Сондай-ақ, «жақын коллизияларға», дифференциалдық, сызықтық және алгебралық криптоталдау әдістері бойынша коллизияларды табу мүмкіндіктері бағаланады.

Төртінші бөлімде құрылған хештеу алгоритмі бағдарламалық және бағдарламалы-аппараттық жасақтамалары жайлы мәліметтер көрсетіледі. HBC-256 алгоритмін жүзеге асыру түрлеріне байланысты ерекшеліктеріне сипаттамалар беріліп, олардың есептеу өнімділігіне баға беріледі және осы бағытта басқа хештеу алгоритмдеріне қатысты салыстырмалық талдаулар нәтижелері келтірілген.

Қорытындыда ғылыми жұмыстың зерттеу нәтижелері көрсетіліп, оларға қысқаша баға берілді.