«6D100200 – Ақпараттық қауіпсіздік жүйелері» мамандығының PhD докторанты Алғазы Күнболат Тілеуханұлының «Әртүрлі әдістерге негізделген шифрлау алгоритмдерін құру және зерттеу» тақырыбындағы диссертациялық жұмысына

АҢДАТПА

Зерттеу тақырыбының өзектілігі ақпараттық қауіпсіздікті қамтамасыз ету мақсатында ақпараттық-коммуникациялық технологиялардың қарқынды дамуы мен ақпараттық қауіпсіздіктің қолданыстағы түрлерін жетілдіру қажеттілігіне байланысты. Ақпаратты өңдеу, сақтау, беру және пайдалану үдерістері заманауи қоғам өмірінің басым бағытына айналды және көбінесе байланыс құралдары мен ақпарат беру тәсілдерінің дамуы мен қолданылу деңгейіне тәуелді. Қазіргі жағдайда ақпараттың қорғалуы тек мемлекеттік сектор тарапынан ғана емес, сондай-ақ қарапайым тұтынушылар мен үкіметтік емес ұйымдардың қажеттілігі болып табылады. Ақпаратты қорғаудың заманауи құралдарын құру арқылы оны қорғаудың қажетті деңгейін қамтамасыз ету, ақпараттың қауіпсіздігін қамтамасыз етудің өзекті мәселелерінің бірі.

Тәуелсіз мемлекет үшін де ақпараттық және коммуникациялық технологиялар дамуында үлкен рөл атқарады. Қазақстанда 2017 жылы Киберқауіпсіздік тұжырымдамасы («Қазақстанның киберқалқаны») қабылданды. Тұжырымдаманың мақсаты – жаһандық бәсекелестік жағдайда Қазақстан Республикасының орнықты дамуын қамтамасыз ету үшін, электрондық ақпараттық ресурстарды, ақпараттық жүйелер мен ақпараттық-коммуникациялық инфрақұрылымдарды сыртқы және ішкі қатерлерден қорғау деңгейіне қол жеткізу және ұстап тұру болып табылады. Осыған байланысты халықаралық ақпаратты қорғауға қойылатын заманауи талаптарды қанағаттандыратын отандық ақпаратты қорғау жүйелерін құру өзекті болып табылады.

ҚР БҒМ ҒК Ақпараттық және есептеуіш технологиялар институтының Ақпараттық қауіпсіздік зертханасында отандық ақпаратты криптографиялық қорғау құралдарын құру саласында ғылыми-зерттеу жұмыстары жүргізілуде. Атап айтқанда, электронды хабарламаларды симметриялы блоктық шифрлау жүйелерін, соның ішінде позициялық емес полиномдық санау жүйелеріне негізделген модификациялар әзірленді.

Бүгінгі күні блоктық шифрлау алгоритмдері компьютерлерде сақталған немесе жалпыға ортақ ақпаратты-коммуникациялық желісі арқылы берілетін ақпаратты криптографиялық қорғаудың негізгі құралы болып отыр. Шифрлау алгоритмінің бұл түріне деген сұраныс оның практикалық қолданылуының артықшылықтарына байланысты. Заманауи аппаратты-бағдарламалық құрылғыларда тиімді бағдарламалық іске асыру мүмкіндігі мол, шифрлау жылдамдығының жоғарылығы және жоғары деңгейде беріктілікке кепілдік береді. Симметриялы блоктық шифрлар тек жеке криптографиялық алгоритм ретінде ғана қолданылмайды, сонымен бірге басқа да криптографиялық

алгоритмдер мен хаттамалардың құрамына кіретін маңызды криптографиялық механизм. Оларды псевдокездейсоқ тізбек генераторының және криптографиялық хэш алгоритмдерінің құрамының негізгі бөлігі ретінде қолдану практикада жиі кездеседі.

Блоктық шифрлардың тағы бір артықшылығы – кілтінің қысқалығында. Ұзындығы көп жағдайда 128 – 256 бит аралығында жататын бір ғана қысқа кілтпен үлкен бірнеше файлды немесе деректерді шифрлауға болады. Бұл ағындық шифрлардан қарағандағы ең негізгі артықшылығы. Себебі, ағындық шифрларда кілтті бір реттен артық қолданбау ұсынылады. Ұзын кілттерді сақтау және қолданушылар арасында оларды алмасуда тағы да қосымша қорғаныста талап етеді. Жоғарыда аталғандарды ескере отырып, шифрлардың ішінде қолданысқа ең тиімдісі және лайықтысы блоктық шифрлар. Сондықтан симметриялы блоктық шифрлау алгоритмдері қазіргі уақытта, ақпаратты өңдеудегі құпиялылықты қамтамасыз етудің негізгі криптографиялық құралы болып табылады.

Криптографияның жетілуімен қатар криптографиялық шабуылдар және криптоталдау әдістері дамып отырды. Криптография және криптоталдау бір-бірінен ажырамастай ұғымдарға айналды: олар криптологияның екі құрамдас бөлігі. Берік криптографиялық жүйені құру үшін оған жасалынатын шабуылдың барлық мүмкін жолдарын ескеру қажет. Криптография мен криптоталдаудың құны уақыт өткен сайын тек қана өседі. Сондықтан, криптографиялық алгоритмдер құру, ғылыми зерттеу жұмыстарында да және практикада да та **өзекті** болып табылады.

Қазақстанда электрондық ақпаратты қорғау үшін негізінен шетелдік криптографиялық құралдар және бағдарламалық жасақтамалар қолданылады, сондықтан отандық криптографиялық қорғау құралдарын құру сөзсіз өзекті және қажет.

Диссертациялық жұмыстың мақсаты. Итеративті блоктық шифрлау алгоритмін және позициялық емес полиномдық санау жүйесін пайдаланып раундтық кілттер алгоритмін құру. Құрылған алгоритмдердің криптоберіктілігін зерттеу.

Зерттелу міндеттері:

- ақпаратты криптографиялық қорғаудың қолданыстағы симметриялы блоктық алгоритмдеріне сараптау жүргізу;
- криптографиялық шабуылдардың және криптоталдаудың белгілі әдістерін қарастыру және талдау;
- позициялық емес полиномдық санау жүйесін пайдаланып раундтық кілттер алу және ауыстыру-алмастыру желісі негізінде симметриялы блоктық шифрлау алгоритмдерін құру;
- құрылған шифрлау алгоритмдерінің беріктілігін криптоталдау әдістері арқылы зерттеу;
- құрылған итеративті шифрлау алгоритмдерін бағдарламалық жүзеге асыру.

Зерттелу нысаны. Шифрлау жүйелері, позициялық емес полиномдық санау жүйесі, криптографиялық шабуылдар, криптоталдау әдістері.

Зерттеудің пәні. Симметриялы блоктық шифрлау алгоритмдері, оның ішінде позициялық емес полиномды санау жүйесі негізінде құрылған алгоритмдер.

Зерттелу құралы мен әдісі. Жұмыста бульдік функция теориясы, сызықтық алгебра, ықтималдықтар теориясы және математикалық статистика, сондай-ақ әртүрлі криптографиялық алгоритмдер және криптоталдау әдістері қолданылды.

Жұмыстың ғылыми жаңалығы:

- шифрлау алгоритмдеріне қойылатын жалпы талаптарға жауап беретін, ауыстыру-алмастыру жүйесі құрылымындағы жаңа симметриялы блоктық шифрлау алгоритмі құрылды;
- дәстүрлі емес әдіске (ПЕПСЖ) негізделген симметриялы блоктық шифрлау алгоритмі құрылды, оны қолдану алгоритмнің криптографиялық беріктігін арттыруға мүмкіндік береді;
- дифференциалдық және сызықтық криптоталдауларға беріктілік көрсеткіштері жоғары, сызықты емес (S-блок) ауыстыру түйіндері құрылды.

Зерттеудің теориялық және практикалық құндылығы. Жүргізілген ғылыми зерттеулердің және алынған нәтижелердің практикалық мүмкіндігі жоғары және ақпараттық-коммуникациялық жүйелер мен желілерде құпия ақпараттарды сақтауға және алмасуда оларды қорғауға пайдалануға болады. Сонымен қатар, осы нәтижелер отандық ақпаратты қорғау құралдарын құруға, дамытуға ықпал етеді және ақпаратты шифрлаудың тиімді алгоритмдерін құру теориясын кеңейтеді. Әзірленген итеративті блоктық шифрлау алгоритмінің бағдарламалық жасақтамасы іске асырылып, ҚР Әділет министрлігі Ұлттық зияткерлік меншік институтынан «Qamal v 1.0.1» 2019 жылғы 6 қыркүйектегі № 5200 авторлық куәлігі алынды.

Қорғауға шығарылған негізгі тұжырым. Шифрлау алгоритміне қойылатын жалпы талаптарға жауап беретін жаңа симметриялық блоктық шифрлау алгоритмі құрылды. Алгоритмнің позициялық емес полиномдық санау жүйесінде әзірленген екінші нұсқасы ұсынылды. Құрылған алгоритмдердің беріктілігі криптоталдаудың дифференциалдық, сызықтық, алгебралық және т.б. түрлері бойынша зерттелді.

Сенімділік дәрежесі мен апробациялау нәтижелері. Диссертациялық жұмыс бойынша жүргізілген зерттеулер мен нәтижелерінің сенімділігі үшінші бөлімде көрсетілген.

Зерттеулер нәтижесі төменде көрсетілген ғылыми-практикалық конференцияларда баяндалды және талқыланды.

1) «Информатика және қолданбалы математика» атты III Халықаралық ғылыми-тәжірибелік конференциясында (Алматы, 26-29 қыркүйек 2018).

2) International Conference on Wireless Communication, Network and Multimedia Engineering, WCNME-2019 (Гуйлин, Китай, 2019).

3) «Информатика және қолданбалы математика» атты IV Халықаралық ғылыми-тәжірибелік конференциясында (Алматы, 25-29 қыркүйек 2019).

4) International Conference on Security of Information and Networks (Sochi, Russia September, 2019).

5) «Қазақстандағы Ақпараттық қауіпсіздіктің өзекті мәселелері» атты Халықаралық ғылыми-тәжірибелік конференциясында (Алматы, 15 қаңтар 2020).

6) «Информатика және қолданбалы математика» атты V Халықаралық ғылыми-тәжірибелік конференциясында (Алматы, 29 қыркүйек – 1 қазан 2020).

Диссертациялық тақырыптың ғылыми бағдарламалармен байланысы. Диссертациялық жұмыс Қазақстан Республикасының Білім және Ғылым министірлігі Ғылым комитетінің Ақпараттық және есептеуіш технологиялар институтында бекітілген PhD докторлық диссертациялар жоспарына және ЖТН – BR05236757-ОТ-20 «Жалпы мақсаттағы желілер мен инфокоммуникациялық жүйелерде ақпаратты жіберу және сақтау кезінде оны криптографиялық қорғау үшін бағдарламалық және бағдарламалық-аппараттық кешендерді құрастыру» бағдарламалық – нысаналы қаржыландыру жобасының ғылыми-зерттеу жұмыстарының аясында орындалды. Диссертациялық жұмыс бойынша жүргізілген зерттеу жұмыстарының нәтижесі аталған БНҚ жобасының 2018-2020 жылдарындағы есебіне енгізілген.

Жұмыс көлемі мен құрылымы. Диссертациялық жұмыс кіріспе, 4 бөлім, қорытынды және пайдаланылған әдебиеттерден тұрады. Диссертацияның толық көлемі: 118 бет жазба мәтіні, соның ішінде 23 сурет, 42 кесте, 94 пайдаланылған әдебиеттер тізімінен және 4 қосымшадан тұрады.

Нәтижелердің жарияланымдары. Ғылыми зерттеу жұмыстарын орындау барысында 21 ғылыми жұмыстар жазылды. Оның ішінде 3 мақала Scopus және Thomson Reuters базаларында индекстелінетін «Cogent Engineering» және «International journal of electronics and telecommunications» журналдарында, 8 мақала Қазақстан Республикасы Білім және ғылым министрлігінің білім және ғылым саласы бойынша бақылау комитетімен ұсынылған басылымдарда, 10 мақала халықаралық ғылыми-практикалық конференциялар жинақтарында жарық көрді.

Кіріспеде диссертациялық жұмыст тақырыбының өзектілігінің негіздемесі берілген. Ғылыми-зерттеу жұмысының мақсаты, нысаны және пәні тұжырымдалған. Сонымен бірге, ғылыми жаңалығы және тәжірибелік маңызы көрсетілген. Зерттеу жұмысттарының нәтижелерінің апробациясы және жарияланымдары туралы мәліметтер келтірілген.

Бірінші бөлімде ақпаратты қорғауда қолданылатын алгоритмдердің түрлері және негізгі бағыттары сипатталған. Сонымен бірге, жалпы криптографияда және диссертациялық жұмыста пайдаланылған терминдерге түсініктеме берілген. Криптоалгоритмдердің қауіпсіздігінің дәрежесі бойынша бөлінген топтарына сипаттама беріліп, симметриялы блоктық шифрларға қойылатын талаптар аталған және шифрлауда қолданылатын режимдер сипатталған. Сондай-ақ заманауи симметриялы шифрлау алгоритмдеріне жүргізілетін криптоталдаулардың негізгі түрлері келтірілген.

Екінші бөлімде SP-жүйесі негізінде құрылған жаңа «Qamal» симметриялы блоктық шифрлау алгоритмі сипатталады және кілтті

пайдаланудағы ерекшелігіне байланысты осы алгоритмнің «Qamal NPNS» екінші нұсқасы да ұсынылды. Әзірленген алгоритмде қолданылған түрлендірулер жеке-жеке сипатталған. Әртүрлі қауіпсіздік деңгейлеріне сәйкес алгоритмнің шифрлау блогының және кілтінің ұзындықтары да әртүрлі үш мән қабылдай алады. Әзірленген шифрлау алгоритмі үшін құрылған S-блок ауыстыруының құрылысы сипаттталған. Сонымен бірге, «Qamal NPNS» алгоритмі ПЕПСЖ негізделген алгоритм болғандықтан, позициялық емес полиномдық санау жүйелерінің құрылуы және оны шифрлауда, шифрды кері ашуда қалай қолданылатыны туралы мәліметтер берілген. Әзірленген алгоритм бойынша деректерді шифрлау мысалы келтірілген.

Үшінші бөлімде құрылған шифрлау алгоритмінің сенімділігі зерттеліп, оның нәтижелері берілген. Зерттеу жұмыстары шифрлау алгоритмінің көмегімен алынған шифрмәтіндердің статистикалық қауіпсіздігін тексеру жұмыстарымен басталады. Одан кейін, криптографияда қажетті шарттардың бірі – шифрдың лавиндік әсері тексерілген. Алгоритмнің беріктілігін бағалау үшін криптоталдаудың алгебралық, дифференциалдық, сызықтық және тағы басқа да әдістерімен тексерілген. Жүргізілген криптошабуылдардың теориялық бағасы ғана емес, нәтижелері нақты мысалдар арқылы да көрініс табады. Сонымен қатар, кілтті ПЕПСЖ-де пайдаланғанда алгоритмнің беріктілігіне әсері зерттелді және анықталды.

Төртінші бөлімде әзірленген шифрлау алгоритмі үшін құрылған бағдарламалық жасақтама туралы ақпараттар берілген. Мысалы, бағдарламалық тілі, жүйелік талаптар, жұмыс істеу түсіндірілімдемелері және т.б. Бағдарламаның есептеу істеу жылдамдығын арттыру мақсатында шифрлау алгоритмінде қолданылған Mixer2 түрлендіруін үш тәсіл бойынша жүзеге асырылуы қарастырылды. Алынған нәтижелерге салыстыру жүргізілді.

Қорытындыда жұмыстың негізгі қорытындылары мен нәтижелері тұжырымдалды.