"Халықаралық ақпараттық технологиялар университеті" АҚ

АО "Международный университет информационных технологий"

JSC "International Information Technology University"

19.01.2021 № 125

Алматы қ. г.Алматы

«6D100200 – Ақпараттық қауіпсіздік жүйелері» мамандығы бойынша философия докторы (PhD) дәрежесін алу үшін ұсынылған ізденуші **Хомпыш Ардабектің «Позициялық емес санау жүйесін қолдану арқылы ақпаратты қорғау алгоритмін құру және зерттеу»** тақырыбы бойынша диссертациялық жұмысына ресми пікір берушінің

ПІКІРІ

1. Зерттеу тақырыбының өзектілігі және жалпы ғылыми, жалпы мемлекеттік бағдарламамен (практикалық және ғылым мен техника дамуының сұраныстарымен) байланысы.

Ақпараттық-коммуникациялық жүйелердегі ақпаратты қорғаудың отандық криптографиялық құралдарын дамыту біздің мемлекетіміз үшін өте маңызды және қажетті, себебі көптеген ұйымдардың құпия ақпараттар сақталатын және өңделетін компьютерлік жүйелеріне күнделікті шабуылдар жасалынып жатады.

Сондықтан қазіргі заманғы ақпараттық қауіпсіздік құралдарын құру өзекті мәселелердің бірі болып табылады. Осы мәселелерді шешудің ең тиімді әдістерінің бірі - криптографиялық әдістерді пайдалану. Ақпаратты криптографиялық қорғау әдістері олардың қызметіне байланысты әр түрлі болуы мүмкін. Сонымен қатар, ақпаратты криптографиялық қорғау ақпаратқа рұқсатсыз қол жеткізуден қорғаудың негізгі құралы болып табылады.

Бүгінгі таңда әлемде цифрлық технологиялардың белсенді өсуіне байланысты ақпаратты қорғаудың криптографиялық әдістерімен байланысты ғылым саласы да қарқынды дамып келеді. Осыған байланысты шетелдік және отандық ғалымдар жыл сайын өз жұмыстарын жетілдіреді, тиімді шешімдер қабылдай отырып өз нәтижелерімен бөліседі.

2. Диссертацияға қойылатын талап деңгейіндегі ғылыми нәтижелері.

А. Хомпыш «Позициялық емес санау жүйесін қолдану арқылы ақпаратты қорғау алгоритмін құру және зерттеу» тақырыбындағы диссертациялық жұмысының зерттеу қорытындысында келесі нәтижелер алынды:

- ЕМ түрлендіру әдісін қолдану арқылы жаңа симметриялық блокты шифрлау алгоритмі құрылды;

- криптоталдау талаптарына жауап беретін S-блок ауыстыру кестесі жасалынды;

- раундттық кілттерді генерациялау алгоритмі жасалды;

- шифрлау жылдамдығын оңтайландыру үшін таңдалған жұмыс негіздерінің индекс кестесі құрылды.

3. Ізденуші диссертациясында тұжырымдалған әрбір нәтиженің, тұжырымдары мен қорытындыларының негізделуі және шынайылық дәрежесі.

Ғылыми тұжырымдардың негіздемелері отандық және шетелдік авторлардың зерттеу тақырыбы бойынша көптеген ғылыми басылымдарын талдау арқылы расталған. Диссертацияда тұжырымдалған әрбір ғылыми нәтиже (ғылыми ережелер), ізденушінің тұжырымдары мен қорытындыларының дұрыстығы статистикалық тестілер мен криптографиялық талдау әдістері, сондай-ақ биттік шашырау критерийі, сандық тәжірибелер нәтижелері мен теориялық мәліметтер арасындағы қанағаттанарлық келісім арқылы анықталады.

Әр тапсырманың шешімі зерттеудің алдыңғы кезеңдерінен алынған нәтижелерге негізделеді, олардың өзара байланысы мен тәуелділігін, сондай-ақ алынған нәтижелердің ішкі тұтастығын негіздейді.

4. Ізденушінің диссертациясында тұжырымдалған әрбір ғылыми нәтиже (қағида) мен қорытындының жаңашылдық деңгейі.

Ізденуші келесі нәтижелерге қол жеткізді:

1) позициялық емес полиномды санау жүйелеріне негізделген ЕМ түрлендіру әдісін қолдана отырып, симметриялы блок шифрлау алгоритмі құрылды;

2) S блоктарға қойылатын талаптарға жауап беретін алмастыру кестесі жасалды;

3) раундттық кілттерді генерациялау алгоритмі құрылды;

4) шифрлау жылдамдығын оңтайландыру үшін позициялық емес полиномды санау жүйелерінің таңдалған жұмыс негіздерінің индекс кестесі жасалды.

5. Алынған нәтижелердің практикалық және теориялық маңыздылығы.

Диссертациялық жұмыс барысында алынған ғылыми нәтижелер тәжірибелік және теориялық маңызға ие.

Диссертациялық зерттеудің тәжірибелік маңызы мәліметтерді тиімді криптографиялық қорғау үшін ақпараттық-коммуникациялық жүйелер мен желілерде электрондық мәліметтерді қорғау үшін құрылған симметриялы блокты шифрлау алгоритмін қолдану мүмкіндігінен тұрады.

Бұл жұмыстың теориялық маңыздылығы позициялық емес полиномды санау жүйесіне негізделген ЕМ түрлендіру әдісін қолдана отырып, симметриялы блокты шифрлаудың жаңа алгоритмін құру болып табылады.

6. Диссертацияның негізгі қағидасының, нәтижесінің, тұжырымдары мен қорытындыларының жариялануының жеткіліктілігіне растама.

Ізденушінің ұсынылған диссертациялық жұмысы өзінің және ғылыми тәжірибелік маңызы бар зерттеу болып табылады. Жұмыс авторының негізгі алынған нәтижелері халықаралық конференцияларда баяндалып, ғылыми журналдарда жарияланды, оның ішінде: ҚР БҒМ ҒК ұсынған ғылыми басылымдарда 6 мақала, Scopus деректер базасына кіретін Халықаралық ғылыми басылымдарда 1 мақала, Халықаралық ғылыми-практикалық конференциялар материалдарында 7 мақала.

7. Диссертация мазмұнындағы және рәсімдеуіндегі кемшіліктер мен ұсыныстар.

Диссертацияны тұтастай алғанда оң бағалай отырып, онда жеке даулы ережелер мен ескертулерді атап өтеміз.

Бұл жұмыста толық көрінісін беретін позициялық емес полиномды санау жүйесінің (ПЕПСЖ) негізінде бұрын құрылған алгоритмдер егжей-тегжейлі сипаттауға болар еді, себебі ЕМ түрлендірудің негізінде де ПЕПСЖ жатыр.

Диссертацияда ұсынылған S-блок сызықты және дифференциалды криптоталдау әдістерімен зерттелді, ал оның нәтижелері белгілі алгоритмдермен салыстырылды. Сондай-ақ, Калин блокты симметриялы шифрінің S-блогын да қарастыруға болар еді.

Бұл ескертулер мен ұсынытар орындалған зерттеулердің және оның нәтижелерінің өзектілігі мен сапасын төмендетпейді, сонымен қатар бұл тақырыптағы одан әрі зерттеулер аясындағы міндеттерді қою үшін нұсқаулық бола алады.

8. Диссертация мазмұнының Ғылыми дәреже беру ережелерінің талаптарына сәйкестегі.

Хомпыш Ардабектің «Позициялық емес санау жүйесін қолдану арқылы ақпаратты қорғау алгоритмін құру және зерттеу» тақырыбына жазылған диссертациялық жұмысы ҚР БҒМ білім және ғылым саласындағы бақылау комитетінің «Ғылыми дәрежесін беру ережелері» (PhD) докторлық диссертацияларға қойылатын барлық талаптарына толық сәйкес келеді, ал зерттеу жұмысының авторы Хомпыш Ардабекті «6D100200 – Ақпараттық қауіпсіздік жүйелері» мамандығы бойынша PhD философия докторы ғылыми дәрежесін алуға лайықты деп есептеймін.

Ресми рецензент:
Халықаралық ақпараттық
технологиялар университетінің
т.ғ.к., ассистент-профессор С.Т.Аманжолова

Халықаралық ақпараттық технологиялар университеті АҚ «Международный университет информационных технологий» Ақпараттық және компьютерлік технологиялар факультеті Факультет информационные и компьютерные технологии