«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 рецезенттің

ПІКІРІ

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

Электронды құжат айналым барысында ақпараттарды қорғау мәселесінің өзекті екендігін ескерсек, қазіргі уақытта криптографиялық әдістер ақпараттарды қорғаудың ең сенімді әдістері екендігі айқындалған.

Ақпаратты қорғаудың криптографиялық әдістері қазіргі өмірде ақпаратты сақтау, өңдеу және жіберу үшін коммуникациялық желілерде және әр түрлі тасымалдаушыларда белсенді қолданылады. Компьютерлік технология мүмкіндіктерінің қарқынды дамыу оларға қойылатын талаптарды да күрделендіреді. Криптографиялық әдістердің ішінде симметриялы блокты шифрлау алгоритмдері қауіпсіздіктің қатаң талаптарын қанағаттандыратын, шифрлау жылдамдығы жоғары, бағдарламалық және аппаратты түрде жүзеге асырылатын алгоритмдер болып саналады. Сондықтан симметриялы блокты шифрлау алгоритмдеріне қойылатын талаптарды қанағаттандыратын әр түрлі криптоталдауларға берік тиімді алгоритмдер құру өзекті. Қазіргі уақытта шетелдік және отандық ғалымдар осы бағыттағы есептерді оңтайлы шешумен айналысып, нәтижелерін жариялауда. Осыған байланысты отандық криптографиялық құралдар құру бойынша ғылыми зерттеу жұмыстарын жүргізу өзекті болып табылады.

2. Диссертацияға қойылатын талап деңгейіндегі ғылыми нәтижелері.

Диссертациялық жұмыстың мақсатын жүзеге асыру барысында келесі нәтижелер алынды:

- ЕМ түрлендіру әдісі қолдану арқылы жаңа симметриялық блокты шифрлау алгоритмі құрылды;
- криптоталдау талаптарын қанағаттандыратын жаңа S-блок алмастыру кестесі құрылды;
- раундттық кілттерді жасау алгоритмі құрылды;
- шифрлау алгоритмінің жылдамдығын арттыру мақсатында таңдап алған жұмыс негіздерінің индекс кестесі қолданылды.

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

Диссертациялық жұмыста тұжырымдалған зерттеудің әрбір нәтижесі ғылыми негізделген және шынайы. Зерттеудің әдіснамалық негіздері мемлекеттік бағдарламаларға, заңнамаларға, стандарттарға және ғылыми

теорияларға негізделіп, сонымен қатар отандық және шетелдік ғалымдардың нәтижелерін саралау арқылы қол жеткізген.

Зерттеу жұмысында қойылған мақсаттар мен есептер толығымен шешілген және позициялық емес полиномды санау жүйесінің мүмкіндіктерін пайдалана отырып ақпаратты қорғау алгоритмі құрылған. Алынған нәтижелерге, яғни биттік шашырау критерийлері, графикалық және бағалау тесттер, сызықты және дифференциалды криптоталдау нәтижелеріне саралау жұмыстары жүргізілген, саралау барысында құрылған алгоритмнің криптоберіктілігі осы қарастырған талдауларға тұрақты екендігі көрсетілген. Талдау жүргізу барысында, құрылған алгоритмдер мен модельдердің ғылыми маңыздылығы тұжырымдалған.

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

Ізденуші диссертацияны орындау кезінде келесі нәтижелерге қол жеткізді:

1) Жаңа симметриялық блокты EMCipher шифрлау алгоритмі құрылды. Құрылған алгоритмге келесі криптографиялық түрлендірулер (EM түрлендіру әдісі, S-блок алмастыру кестесі, биттік қосу операциясы, цикльдік жылжыту операциясы және P блок орын ауыстырулары) қолданылды.

2) Криптоталдау талаптарын қанағаттандыратын жаңа S-блок алмастыру кестесі құрылды. S-блок алмастыру кестесі сызықты емес және математикалық әдіс арқылы кездейсоқ алынғандығы анықталып, сызықты және дифференциалды криптоталдау әдістері бойынша талдау жүргізілген.

3) Раундттық кілттерді жасау алгоритмі құрылды. Онда S-блок алмастыру кестесі және RNS түрлендіру әдісі сипатталған.

4) EMCipher алгоримінің жылдамдығын арттыру үшін позициялық емес полиномды санау жүйесі және таңдап алған жұмыс негіздерінің индекс кестесі қолданылды. Ұсынылған алгоритмнің компьютерлік бағдарламасы құрылып, статистикалық қауіпсіздігі, биттік шашырау критерийі, дифференциалды криптоталдау бойынша зерттелінді.

5. Алынған нәтижелердің практикалық және теориялық маңыздылығы.

Диссертациялық жұмыс нәтижесінде келтірілген тұжырымдар жекелеген бөлімдердің және жалпы мазмұнға сай сабақтаса жасалған, олардың арасында мағыналық байланыс сақталған, бірінен бірі туындап отырады.

Жұмыстың практикалық маңыздылығы келесідей, диссертациялық зерттеуде алынған нәтижелер телекоммуникациялық және ақпараттық жүйелер мен желілердегі, электрондық құжат айналым жүйелеріндегі ақпараттарды қорғау үшін қолдануға болады.

Бұл жұмыстың теориялық маңызы криптографиялық примитивтерді әзірлеуде: EM түрлендіру әдісі, жаңа алмастыру кестесі (S-блок) және раундттық кілт генераторы. Бұлардың көмегімен жаңа симметриялық блокты шифрлау алгоритмі құрылды, ол қазіргі заманғы симметриялы блокты шифрлау алгоритмдерінің негізгі талаптарына жауап береді.

Докторанттың материалды жүйелі беруі, зерттеу әдістері мен алынған нәтижелері, қорытындылары мен ғылыми тұжырымдамалары толық аяқталған дербес ғылыми еңбек екендігін дәлелдейді.

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

Диссертациялық жұмыстың негізгі нәтижелері 14 басылымдарда баяндалған, олардың ішінде ҚР Білім және ғылым саласы бойынша бақылау Комитеті ұсынған ғылыми басылымдарда 6 мақала, Scopus және Thomson Reuters халықаралық деректер қорына кірген журналдарда 1 мақала, Қазақстан мен шетелдердегі халықаралық ғылыми конференцияларда 7 мақала жарияланған. Зерттеу нәтижесі жүзеге асырылған бағдарламалық кешенге 1 авторлық құқық куәлігі алынған. Жарияланған ғылыми еңбектер көлемінен зерттеу нәтижелерін жеткілікті деңгейде баяндалып, талқыланғандығын көруге болады.

7. Диссертация мазмұнындағы және рәсімдеуіндегі кемшіліктер мен ұсыныстар.

- Жұмыстың мазмұнында диссертантың өзі қолжеткізген нәтижелері мен белгілі нәтижелер арасындағы айырмашылыққа көбірек назар аударған жөн еді.
- Ұсынылған алгоритмнің құрама бөлігі болып саналатын S-блокқа жүргізілген дифференциалды және сызықты криптоталдау нәтижесін сипатау кезінде максималды және минималды мәндері көрсетілген, бірақ бұл мәндердің не екендігін диссертацияда ашып көрсеткен дұрыс.
- Диссертацияның бірінші бөлімінде криптоталдау әдістері туралы ақпараттар келтірсе артық болмас еді.

Алайда бұл ескертулер мен ұсынытар орындалған зерттеулердің және оның нәтижелерінің өзектілігі мен сапасын төмендетпейді.

8. Диссертация мазмұнының Ғылыми дәреже беру ережелерінің талаптарына сәйкестегі.

Хомпыш Ардабектің «Позициялық емес санау жүйесін қолдану арқылы ақпаратты қорғау алгоритмін құру және зерттеу» тақырыбында жазылған диссертациясы толық аяқталған ғылыми зерттеу жұмыс және ҚР БҒМ білім және ғылым саласындағы бақылау комитетінің «Ғылыми дәрежесін беру ережелері» талаптарына сәйкес келеді.

Жоғарыда айтылғандарды ескере отырып, А.Хомпыштың диссертациялық жұмысы «6D100200 - Ақпараттық қауіпсіздік жүйелері» мамандығы бойынша (PhD) философия докторы дәрежесін алуға лайықты деп есептеймін.

Ресми рецензент:
Ақпараттық және есептеуіш
технологиялар институтының
бас ғылыми қызметкері,
ф-м.ғ.д.,профессор Т.Ж. Мазаков

КУӘЛАНДЫРАМЫН
КБ АҒА ИНСПЕКТОРЫ
УДОСТОВЕРЯЮ
СТ. ИНСПЕКТОР ОК