«8D06201 – Радиотехника, электроника және телекоммуникациялар» білім беру бағдарламасы бойынша философия докторы (PhD) дәрежесін алу үшін диссертациялық жұмысқа

АҢДАТПА

СҚАБЫЛОВ ӘЛІШЕР ӘЛИҰЛЫ

ПЛИС НЕГІЗІНДЕ ШИФРЛЕУГЕ АРНАЛҒАН АППАРАТТЫҚ БАҒДАРЛАМАЛЫҚ ҚАМТАМАСЫЗДАНДЫРУ

Жұмыстың жалпы сипаттамасы

Осы зерттеуде талқыланған докторлық диссертация телекоммуникациялық желілерде, соның ішінде заттар интернеті мен қауіпсіз байланыс жүйелерінде деректерді шифрлауға арналған аппараттық және бағдарламалық жасақтаманы әзірлеуге бағытталған. Зерттеу параллельді және конвейерлі деректерді өңдеу арқылы жоғары жылдамдықты және сенімді шифрлауға қол жеткізу үшін программаланатын логикалық интегралды схемаларды (ПЛИС) пайдалануға негізделген тәсілді ұсынады. Жұмыстың негізгі аспектісі шифрланған ақпараттың қауіпсіздігін едәуір жақсартатын кілт ретінде пайдаланылатын жалған кездейсоқ сандарды құру үшін хаос генераторларын қолдануды қамтиды. Диссертацияда ұсынылған шифрлау алгоритмі позициялық емес көпмүшелік санау жүйесіне (ПЕКСЖ) негізделген және дәстүрлі шифрлау әдістерінен ерекшеленетін деректерді қорғаудың жаңа шешімдерін ұсынады. Бұл алгоритмді ПЛИС-ке енгізу арқылы зерттеу технологиялық тәуелсіздік пен қауіпсіздікті қамтамасыз ететін ақпараттық қауіпсіздіктің заманауи стандарттарына сәйкес келетін отандық шифрлау құрылғысын құруға бағытталған. Тұтастай алғанда, бұл зерттеу ақпараттық-коммуникация технологияларға (АКТ) негізделген қауіпсіздікті жақсарту үшін деректерді шифрлау технологиялары мен сенімділік шешімдерін дамытуға айтарлықтай үлес қосады. Бұл үлес қазіргі байланыс жүйелеріндегі деректерді қорғаудың негізгі аспектілеріне әсер ететін ақпараттық қауіпсіздік пен технологиялық құпиялылық саласында өте маңызды.

Зерттеудің өзектілігі

Бұл зерттеудің өзектілігі электрондық ақпараттық ресурстарды, ақпараттық жүйелерді және байланыс инфрақұрылымын қорғауды қамтамасыз етуге қойылатын талаптардың артуына және құпия байланыс пен бейне байланыс сияқты мамандандырылған жүйелерге байланысты. Цифрлық ақпараттың көлемі үнемі өсіп келе жатқан сайын және оның стратегиялық маңыздылығы жағдайында, деректерді тиімді шифрлау мәселелері бірінші кезектегі маңызға ие болуда.

ПЛИС икемділігі, ауқымдылығы және өнімділігі жоғары параллельді деректерді өңдеу қабілетінің арқасында осы мәселелерді шешудің бірегей мүмкіндіктерін ұсынады. Ақпаратты қорғау жүйелеріне ПЛИС деректерді шифрлау жылдамдығын айтарлықтай жақсартуға мүмкіндік береді, сонымен бірге олардың құпиялылығы мен тұтастығының жоғары дәрежесін қамтамасыз

етеді. Бұл ПЛИС-ті әсіресе қауіпсіздік пен өнімділікке қойылатын талаптар жоғары болатын арнайы байланыс және бейне байланыс жүйелері үшін де таңдау шешімі етеді.

Бұл зерттеудің негізгі аспектілерінің бірі-шифрлау кілттерін жасау үшін жалған кездейсоқ сандардың көзі ретінде хаос генераторларын пайдалану. Бұл тәсіл деректердің қауіпсіздігін едәуір арттырады, өйткені хаостық тізбектерді болжау және талдау қиын, бұл тиісті кілтсіз шифрды ашу процесін өте күрделі етеді.

Осы зерттеу аясында жасалған және ПЕКСЖ негізделген шифрлау алгоритмі дәстүрлі шифрлау әдістерінен айтарлықтай ерекшеленетін шешім болып табылады. Бұл шифрлаудың қауіпсіздік деңгейін арттырып қана қоймайды, сонымен қатар деректерді өңдеу процестерін оңтайландыру арқылы оның тиімділігін арттырады.

Шифрлаудың бұл тәсілі ақпаратты қорғаудың заманауи талаптарына жауап беретін отандық шифрлау құрылғысын жасауға мүмкіндік береді. Қазіргі әлемде технологиялық егемендік ұлттық қауіпсіздікті қамтамасыз ету үшін барған сайын өзекті бола бастаған кезде, әр ел үшін өзінің шифрлау алгоритмдері мен технологияларын құру мүмкіндігі стратегиялық артықшылықты білдіреді. Деректерді шифрлау саласында өз шешімдерін әзірлеу және енгізу ақпараттың сенімді қорғалуын қамтамасыз етіп қана қоймай, сонымен қатар елдің технологиялық тәуелсіздігі мен қауіпсіздігін нығайта отырып, ұлттық технологиялық және ғылыми құзыреттердің дамуына ықпал етеді.

Осылайша, бұл зерттеудің өзектілігі деректерді шифрлаудың тиімді және сенімді әдістерін әзірлеудің техникалық аспектілеріне ғана емес, сонымен қатар ақпараттық қауіпсіздік саласындағы технологиялық егемендікті қамтамасыз етудің стратегиялық қажеттілігіне байланысты.

Диссертациялық жұмыстың мақсаты ПЛИС негізінде деректерді шифрлаудың кешенді ақпараттық-бағдарламалық жасақтаманы әзірлеу және енгізу болып табылады.

Зерттеу пәні телекоммуникациялық жүйелер және арнайы байланыс жүйелері.

- программаланатын логикалық интегралдық схемалар (ПЛИС);
- позициялық емес көпмүшелік санау жүйелері;
- псевдокездейсоқ сандар генераторы.

Зерттеу міндеттері

1. Деректерді шифрлау алгоритмдерін зерттеу: деректерді шифрлау үшін қолданылатын дәстүрлі және заманауи шифрлау әдістерін зерттеу және салыстыру;
2. Бағдарламалық және аппараттық құралдарды әзірлеу: деректерді шифрлау жүйелерінің негізі ретінде ПЛИС пайдалану потенциалын бағалау. ПЛИС негізінде аппараттық архитектураны құру, шифрлау алгоритмдерін оңтайландыру және бағдарламалық және аппараттық құрамдас бөліктерді біріктіру;
3. Шифрлау алгоритмін әзірлеу: позициялық емес көпмүшелік санау жүйесіне негізделген және ПЛИС-те іске асыруға бейімделген деректерді шифрлаудың тиімді алгоритмін құру;

4. Хаос генераторларын қолдану: сенімді шифрлау кілттері ретінде қызмет ететін жалған кездейсоқ сандарды құру үшін хаос генераторларын қолдану әдістемесін әзірлеу;

5. Қауіпсіздік пен тиімділікті бағалау: ақпараттық-коммуникациялық технологиялардағы деректерді шифрлаудың басқа әдістерімен салыстырғанда әзірленген құралдардың өнімділігін, күші мен тиімділігін талдау;

6. ПЛИС-ке алгоритмді енгізу және тестілеу: оның практикалық қолданылуы мен өнімділігін бағалау үшін ПЛИС-та әзірленген шифрлау алгоритмін енгізу және тестілеу.

Диссертациялық жұмыстың жаңалығы мен ерекшелігі, алғаш рет:

1. ПЕКСЖ негізінде ПЛИС арқылы шифрлау алгоритмі енгізілді және тексерілді;

2. Шифрлау кілттері ретінде қызмет ететін жоғары энтропиялық жалған кездейсоқ сандарды жасау үшін хаос генераторларын тікелей ПЛИС-та қолдану алғаш рет жүзеге асырылды, бұл жүйенің қауіпсіздік деңгейін едәуір арттырады;

3. Алғаш рет қарапайым телекоммуникациялық жүйелерде деректерді жоғары өнімді және қауіпсіз шифрлауды қамтамасыз етуге қабілетті ПЛИС аппараттық құралдары мен мамандандырылған бағдарламалық жасақтаманы біріктіретін кешенді шешім ұсынылды;

4. Шифрлау алгоритмдерінде қолдануға арналған келтірілмейтін көпмүшелік мәліметтер базасы ПЛИС-те алғаш рет құрылды және жүйеленді, бұл шифрлау кілттерін құру үшін көпмүшелерді таңдаудың негізгі процесі. Көпмүшелердің келтірілмейтіндігін аппараттық тексеру алғаш рет ПЛИС-ке тікелей енгізілді, бұл көпмүшелерді тексеру процесін автоматтандыруға және жеделдетуге мүмкіндік береді, соның ішінде деректерді шифрлау үшін кілттерді таңдаудың жоғары сенімділігі мен жеделдігін қамтамасыз етеді.

Қорғауға ұсынылатын негізгі тұжырымдамалар:

1. Аппараттық қорғаныста қолдануға арналған келтірілмейтін көпмүшелер генераторы ПЛИС Artix-7 құрылғысы арқылы 16 биттік кілтті жасауды қамтамасыз етеді;

2. ПЛИС негізінде жүзеге асырылатын хаостық сигналдар мен псевдокездейсоқ сандар генераторлары жіберуші және қабылдаушы құрылғылардағы ақпараттық блоктардың ұзындығын кездейсоқ бөлу арқылы шифрланған ақпараттың крипто-төзімділігін арттырады;

3. Паралельді және конвейерлі есептеу әдістерінің арқасында ПЛИС негізіндегі ашық кілтті шифрлау алгоритмін аппараттық іске асырудың жылдамдығы бір тактыні 6,239 нс. дейін жеткізуге болады.

Жұмыстың теориялық және практикалық маңыздылығы

Бұл зерттеудің теориялық маңыздылығы ақпараттық-коммуникациялық технологиялар (АКТ) және олардың мәліметтерді шифрлау мен шифрын шешуде, сондай-ақ ақпараттық қауіпсіздікте қолдану саласындағы теориялық негіздері мен түсінігін дамытуда жатыр. Зерттеу АКТ жұмысының принциптерін, деректерді шифрлау және шифрын ашу ерекшеліктерін тереңірек зерттеуге, сондай-ақ ақпараттық қауіпсіздікті қамтамасыз етудің жаңа әдістері мен алгоритмдерін әзірлеуге мүмкіндік береді.

Зерттеудің тәжірибелік маңыздылығы тиімді және сенімді деректерді шифрлау және дешифрлеу жүйелерін енгізу үшін ПЛИС негізінде аппараттық және бағдарламалық қамтамасыз етуді құруда жатыр. Бұл ақпаратты рұқсат

етілмеген қол жеткізуден қорғауды қамтамасыз етеді және берілетін және сақталған деректердің құпиялылығын қамтамасыз етеді.

Бұл ғылыми зерттеудің нәтижелері әртүрлі салаларда, соның ішінде телекоммуникация, электроника, ақпараттық жүйелер және т.б. ПЛИС негізіндегі аппараттық және бағдарламалық шешімдер, деректер қауіпсіздігі мен ақпаратты қорғауды қамтамасыз ету үшін әртүрлі АКТ құрылғылары мен жүйелеріне біріктірілуі мүмкін. Бұл олардың сенімділігін, құпиялылығын және тұтастығын қамтамасыз ететін заманауи байланыс және деректерді беру жүйелерін дамытуға жаңа мүмкіндіктер ашады.

Алынған нәтижелер және ПЛИС негізіндегі деректерді шифрлау және дешифрлеудің әзірленген әдістері мен алгоритмдері ақпараттық-коммуникациялық технологияларда, бұлтты сақтауда, электрондық коммерция жүйелерінде және т.б. ақпаратты қорғауды қажет ететін тәжірибелік қолданбаларда қолданылуы мүмкін. Бұл ақпараттық қауіпсіздікті дамытуға және деректерді қорғаудың неғұрлым сенімді және тиімді жүйелерін құруға ықпал етеді.

Алынған нәтижелердің практикалық маңыздылығы халықаралық рецензияланатын басылымдардағы жарияланымдармен және тұрақты халықаралық конференцияларға қатысумен, сондай-ақ ҚР № 22917 авторлық куәлігімен расталады.

Алынған нәтижелердің дұрыстығы мен негізділігі

Диссертациялық жұмыста алынған нәтижелердің дұрыстығы ҚР БжҒМ Білім және ғылым саласында сапаны қамтамасыз ету комитеті (БҒССҚЕК) ұсынған басылымдарда, импакт-факторы нөлден жоғары алыс шетелдердің журналдарында және халықаралық конференциялардың еңбектерінде жарияланымдардың болуымен расталады.

Автордың жеке үлесі – зерттеу әдісін таңдаудан бастап нормативтік-техникалық құжаттаманы әзірлеуге дейінгі бүкіл зерттеу процесін дербес жүзеге асырғаны. Сонымен қатар, тапсырма қою нәтижелерді талқылау ғылыми жетекшілермен бірлесіп жүргізілді.

Диссертациялық жұмыстың аппробациясы

Диссертациялық жұмыс материалдары негізінде 10 баспа жұмыстары жарық көрді:

Thomson Reuters деректер базасы бойынша немесе Scopus халықаралық ғылыми деректер базасына енетін басылымдарда жоғары импакт-факторлы мақалалар:

1. Ibraimov M.K., Tynymbayev S.T., **Skabylov A.A.**, Kozhagulov Y., Zhexebay D.M. Development and design of an FPGA-based encoder for NPN //Cogent Engineering. – 2022. – Vol. 9, № 1. – 2008847 **[Q2, 67%]**
2. Aitkhozhayeva Y.Zh., Tynymbayev S., Adilbekkyzy S., **Skabylov A.,** Ibraimov, M. Design and research of the behavioral model for the modular reduction device // Eurasian Physical Technical Journal 7. – 2020. – Vol. 17, № 1. – С. 151–156. **[Q3, 25%]**

ҚР ҒЖМБ ҒЖБССҚК ұсынған басылымдарда жарияланған мақалалар:

1. Kalimoldayev M., Tynymbayev S., Almen D., **Skabylov A.** Implementation of the nonconductivity check algorithm for a given binary polynomial on the FPGA // Вестник КазНИТУ. – 2020. – Т. 141, № 5. – С. 629-635.

2. **Скабылов А.А.,** Ибраимов М.К., Жексебай Д.М., Кожагулов Е.Т. Программно-аппаратная реализация qpsk на базе zynq и matlab // Вестник КазНПУ им. Абая, серия «Физико-математические науки», №1(77), 2022 г.

3. **Скабылов А.А.,** Жексебай Д.М., Ибраимов М.К., Налибаев Е.Д. Применение хаотических генераторов для секретного ключа в приемо-передающих электронных устройствах // Вестник КазНПУ. – 2023. – Т. 82, № 2. – С. 194-201

Халықаралық конференциялар тезистері жинақтарындағы жарияланымдар:

1. Әлмен Д.Б., **Сқабылов Ә.Ә.** ПЛИС негізінде GF(2) ақырғы өрістегі келтірілмейтін полиномдар базасын құру //Международная научная конференция студентов и молодых ученых, «ФАРАБИ ӘЛЕМІ», 2020. – С. 269.

2. **Сқабылов Ә.Ә.,** Әлмен Д.Б., Жексебай Д.М., Азамат Р.М. Модуль бойынша бөлу құрылғысының әрекеттік моделін жобалау және зерттеу //Международная научная конференция студентов и молодых ученых, «ФАРАБИ ӘЛЕМІ», 2021. – С. 217.

3. **Сқабылов Ә.Ә.,** Әлмен Д.Б., Жексебай Д.М., Азамат Р.М. ПЛИС негізінде шифрлау және дешифрлау алгоритмін аппараттық жүзеге асыру //Международная научная конференция студентов и молодых ученых, «ФАРАБИ ӘЛЕМІ», 2021. – С. 218.

4. **Сқабылов Ә.Ә.,** Жексебай Д.М., Әлмен Д.Б., Ихсан Г.Б. FPGA негізінде qpsk бағдарламалық-ақпараттық комплекс //Международная научная конференция студентов и молодых ученых, «ФАРАБИ ӘЛЕМІ», 2022. – С. 215.

5. **Сқабылов Ә.Ә.,** Налибаев Е.Д., Ибраимов М.К., Данабеков Б., Азамат Р.М //«Бейсызық жүйелердегі хаос және құрылымдар. Теория және тәжірибе» XII Халықаралық ғылыми конференциясы, 2022. – С. 155.

Авторлық куәлік:

1. **Сқабылов Ә.Ә.,** Ибраимов М.К., Сахыбай Т., Жексебай Д.М., Кожагулов Е.Т. Аппаратный комплекс шифрования данных на основе ПЛИС //Авторлық куәлік, 2022. № 22917.

Аяқталған ғылыми-зерттеу жұмысын оқу процесіне енгізу туралы Акт:

1. 2023 жылғы 31 тамыздағы №1 хаттама

Диссертациялық жұмыстың құрылымы мен көлемі

Диссертациялық жұмыс кіріспеден, үш тараудан, қорытындыдан және пайдаланылған әдебиеттер тізімінен тұрады. Жұмыс 54 сурет, 20 формула, 6 кесте, 117 әдебиеттер тізімі мен 114 бетті қамтиды.