«8D06201 – Радиотехника, электроника және телекоммуникациялар» білім беру мамандығы бойынша философия докторы (PhD) дәрежесін алу үшін Сқабылов Әлішер Әлиұлының «ПЛИС негізінде шифрлеуге арналған аппараттық бағдарламалық қамтамасыздандыру» тақырыбы бойынша диссертациялық жұмысына отандық ғылыми жетекшісінің

ПІКІРІ

Сқабылов Әлішер Әлиұлының диссертациялық жұмысы программаланатын логикалық интегралдық схемалар негізінде деректерді шифрлаудың аппараттық-бағдарламалық қамтамасыз етуіне арналған.

Сқабылов Әлішер Әлиұлының диссертациялық жұмысы ақпараттық-коммуникациялық технологиялардағы (АКТ) деректердің қауіпсіздігін қамтамасыз ету әдістерін зерттеуге және әзірлеуге арналған. Бұл зерттеудің негізгі нәтижелерінің бірі- программаланатын логикалық интегралды микросхемаларға (ПЛИС) негізделген деректерді шифрлау аппараттық-бағдарламалық жасақтамасы.

Зерттеу нәтижесінде докторант параллельді-конвейерлік есептеу әдістерін қолдану және шифрлау алгоритмін аппараттық жолмен енгізу арқылы деректерді өңдеу жылдамдығын бірнеше рет арттыра алды. Үлкен көлемді деректерді нақты уақыт мезетінде өңдеп және арнаға тарату мен қабылдауда мұндай жоғары жылдамдықты қамтамасыз ету өте өзекті мәселе болып табылады. Шифрлау алгоритмін жүзеге асыру үшін ПЛИС қолдану деректерді өңдеудің жоғары жылдамдығын қамтамасыз етіп қана қоймай, сонымен қатар ақпараттың қауіпсіздік деңгейін арттырады. ПЛИС күрделі шифрлау алгоритмдерін аппараттық деңгейде тиімді орындауға және деректерді сенімді және жылдам деңгейде қорғауға мүмкіндік береді. Бұл тәсіл деректерді тарату саласында өте маңызды болады. Себебі, мұнда ақпараттың жылдамдығы ғана емес, қауіпсіздігі де маңызды болып табылады.

Докторант Сқабылов Ә.Ә. ПЛИС-те жалған кездейсоқ сандардың аппараттық генерациясын жүзеге асырды. Бұл сандарды құру үшін ол сызықты емес дифференциалды теңдеулермен сипатталатын Рёсслер және Чуа сияқты динамикалық жүйелерді қолданды. ПЛИС Чуа және Рёсслер жүйелерінің алгоритмдерін аппараттық деңгейде тиімді жүзеге асыруға мүмкіндік берді, бұл деректерді өңдеудегі маңызды болатын кездейсоқ кілттерді жасауға мүмкіндік береді. Зерттеу барысында Рёсслер жүйесіндегі кезеңділік анықталды, бұл оны Чуа жүйесінен ерекшелендіреді, ол мұндай айқын кезеңділікке ие емес. Чуа жүйесінің кездейсоқтыққа жақындылығы деректерді шифрлау үшін қажетті кілттерді жасау үшін пайдалануға болатын жалған кездейсоқ сандарды алуға мүмкіндік береді.

Сонымен қатар, ізденуші Сқабылов Ә.Ә. шифрлау алгоритмін жүзеге асыру үшін қажетті келтірілмейтін көпмүшелік мәліметтер базасын құрды. Шифрлау алгоритмі үшін ПЛИС-те келтірілмейтін көпмүшелердің дерекқорын құру - бұл деректердің қауіпсіздігін қамтамасыз етудегі маңызды қадам болып табылады. Осы дерекқордың арқасында шифрлау алгоритмі көпмүшелерді олардың келтірілмейтіндігін тез тексере алады. Бұл шифрлау процесінің тиімділігін арттырады.

Көпмүшелерді келтірілмейтін тексеру үшін Бен Ор алгоритмін қолдану мүмкін емес факторларды тез анықтауға мүмкіндік береді, бұл өз кезегінде алгоритмнің жылдамдығын жақсартады. Сонымен қатар, аппараттық функциялардың бірегей үйлесімі мәліметтер базасын жабдықтың өзінде сақтауға мүмкіндік береді. Осылайша мәліметтер үшін қосымша қауіпсіздік қабатын қамтамасыз етеді.

Докторант қойған барлық міндеттер аппараттық түрде іске асырылып, біріктірілді. Зерттеу нәтижесінде жоғары қорғаныс деңгейін қамтамасыз етіп қана қоймай, шифрлау жылдамдығын арттыратын аппараттық құрал жасалды. Зерттеу нәтижелерін қауіпсіздікке ғана емес, сонымен қатар арнайы әскери байланыс, мемлекеттік жасырын байланыс, құқық қорғау және барлау қызметтері үшін қорғалған байланыс ретінде, сондай-ақ бейнебайланысты қоса алғанда басқа салаларда да қолдануға болады.

Зерттеу жұмыстарының нәтижелері отандық және халықаралық ғылыми конференцияларда баяндалды. Диссертация материалдары бойынша 10 баспа жұмыстары, оның ішінде 2 мақала Scopus базасында, 3 мақала Қазақстан Республикасы ҒЖБМ ҒЖБССҚК ұсынған басылымдарда жарияланған.

Диссертациялық жұмысты орындау барысында Сқабылов Әлішер Әлиұлы жеке өзі және топпен бірге жұмыс жасай алатынын дәлелдеді. Берілген тапсырмаларды уақытында жауапкершілікпен орындап, өзін жақсы жағынан көрсете білді.

Жоғарыда айтылғандарды түйіндей келе: Сқабылов Әлішер Әлиұлының «ПЛИС негізінде шифрлеуге арналған аппараттық бағдарламалық қамтамасыздандыру» тақырыбы бойынша диссертациялық жұмысы барлық талаптарға сәйкес келеді және оны қорғауға жіберуді ұсынамын. Ізденуші, Сқабылов Әлішер Әлиұлын «8D06201 – Радиотехника, электроника және телекоммуникациялар» білім беру бағдарламасы бойынша философия докторы (PhD) дәрежесін алуға лайықты деп есептеймін.

PhD, әл-Фараби атындағы ҚазҰУ Налибаев Е.Д.

Қолын растайды
Подпись заверяю

БИН 990140001154