«6D070400-Есептеу техникасы және бағдарламалық қамтамасыз ету» мамандығы бойынша философия докторы (PhD) дәрежесіне іздену үшін ұсынылған Темирбекова Жанерке Ерлановнаның «Есептеу кластерін және жүйені қауіпсіздігін қамтамасыз ету үшін AtmelAVR микроконтроллерін қолдану» тақырыбындағы диссертациялық жұмысына ресми рецензенттің

СЫН-ПІКІРІ

р/н №	Критерийлер	Критерийлер сәйкестігі	Ресми рецензенттің ұстанымы
1.	Диссертация тақырыбының (бекіту күніне) ғылымның даму бағыттарына және/немесе мемлекеттік бағдарламаларға сәйкес болуы	1.1 Ғылымның даму бағыттарына және/немесе мемлекеттік бағдарламаларға сәйкестігі: 1) Диссертация мемлекет бюджетінен қаржыландырылатын жобаның немесе нысаналы бағдарламаның аясында орындалған (жобаның немесе бағдарламаның атауы мен нөмірі); 2) Диссертация басқа мемлекеттік бағдарлама аясында орындалған (бағдарламаның атауы) 3) Диссертация Қазақстан Республикасының Үкіметі жанындағы Жоғары ғылыми-техникалық комиссия бекіткен ғылым дамуының басым бағытына сәйкес (бағытын көрсету)	«Есептеу кластерін және жүйені қауіпсіздігін қамтамасыз ету үшін AtmelAVR микроконтроллерін қолдану» тақырыбындағы диссертация ғылымның даму бағытына сәйкес, себебі IoT құрылғылар кластерінің қауіпсіздігін қамтамасыз ету өзекті мәселелердің бірі болып табылады.
2.	Ғылымға маңыздылығы	Жұмыс ғылымға елеулі үлесін қосады/қоспайды, ал оның маңыздылығы ашылған/ашылмаған.	Бұл диссертациялық жұмыс ғылымға елеулі үлеісн қосады. Зерттеу кезінде алынған нәтижелер ғылыми тұрғыда өте маңызды, себебі IoT қолданушылардың саны қарқынды өсуде, саны өскен сайын оның бұл құрылғылардың қауіпсіздігі басты алаңдаушылықты тудырады, тиісті қауіпсіздік шараларын қолданбаған жағдайда, кез келген IoT қосылған құрылғының жұмыс жасау мүмкіндігін, сонымен қатар пайдаланушы деректерін ұрлауға қауіпі бар. Сондықтан да IoT құрылғылар арасында жіберілетін деректерді қорғау өте маңызды болып тұр.
3.	Өзі жазу принципі	Өзі жазу деңгейі: 1) жоғары; 2) орташа; 3) төмен; 4) өзі жазбаған	Зерттеу жұмысын орындаушының диссертациялық жұмысты жазу барысында рәсімдеуі, түсіндіруі, сипаттауы жоғарцы деңгейде жазылған. Ғылыми жұмыстың жаңалығы жазу деңгейінің жоғарылығын көрсетеді.
4.	Ішкі бірлік принципі	4.1 Диссертация өзектілігінің негіздемесі: 1) негізделген; 2) жартылай негізделген; 3) негізделмеген.	Диссертация актуалды тақырыпта орындалған және өзектілігі толығымен негізделген. Ақылды үйлер, денсаулық сақтау, өнеркәсіптік автоматтандыру және ақылды қалалар сияқты әртүрлі салаларда IoT

			құрылғыларының өсіп келе жатқанын ескере отырып, олардың қауіпсіздігін қамтамасыз ету басты мәселе болып табылады.
		4.2 Диссертация мазмұны диссертация тақырыбын айқындайды 1) айқындайды; 2) жартылай айқындайды; 3) айқындамайды	Диссертация мазмұны диссертация тақырыбын айқындайды. Диссертация тақырыбы: «Есептеу кластерін және жүйені қауіпсіздігін қамтамасыз ету үшін AtmelAVR микроконтроллерін қолдану» болғандықтан ғылыми жұмыстың сипаттамасы толық мазмұнға сай.
		4.3. Мақсаты мен міндеттері диссертация тақырыбына сәйкес келеді: 1) сәйкес келеді; 2) жартылай сәйкес келеді; 3) сәйкес келмейді	Зерттеу жұмысының мақсаты мен міндеттері диссертация тақырыбына сәйкес келеді. Диссертациялық жұмыстың мақсаты. IoT құрылғалар арасында деректердің қауіпсіз сақталуын және алмасуын қамтамасыз ету үшін әртүрлі AtmelAVR микроконтроллерде шифрланған деректерге барлық арифметикалық операцияларды орындауға мүмкіндік беретін толық гомоморфты шифрлау кітапханаларының архитектурасын құру және іске асыру. Жұмыстың міндеттер толығымен тақырыпқа сәйкес.
		4.4. Диссертацияның барлық бөлімдері мен құрылысы логикалық байланысқан: 1) толық байланысқан; 2) жартылай байланысқан; 3) байланыс жоқ	Диссертация кіріспеден, 4 бөлімнен, қорытындыдан, 2 қосымшадан тұрады. Диссертацияның барлық бөлімдері, қорғауға шығарылған негіздеме бір-бірімен логикалы түрде байланысқан. Зерттеу жұмысында жазылған барлық бөлімдер логикалық жүйеде жазылған.
		4.5 Автор ұсынған жаңа шешімдер (қағидаттар, әдістер) дәлелденіп, бұрыннан белгілі шешімдермен салыстырылып бағаланған: 1) сыни талдау бар; 2) талдау жартылай жүргізілген; 3) талдау өз пікірін емес, басқа авторлардың сілтемелеріне негізделген	Автор ұсынған жаңа шешімдер (қағидаттар, әдістер) дәлелденіп, бұрыннан белгілі шешімдермен салыстырылып бағаланған. Құрылған кітапхана мен белгілі кітапханаларымен өнімділігін бағалау бойынша эксперименттер барысында диссертациялық жұмыста ұсынылған кітапхана қосылу мен пайдаланудың қарапайымдылығын көрсетті, сонымен қатар деректерді есептеу жылдамдығы шамамен 1,52 есе жоғары кітапхана ұсынған.
5.	Ғылыми жаңашылдық принципі	5.1 Ғылыми нәтижелер мен қағидаттар жаңа болып табыла ма? 1) толығымен жаңа; 2) жартылай жаңа (25-75% жаңа болып табылады); 3) жаңа емес (25% кем жаңа болып табылады)	Зерттеу жұмысының жаңалығы мен қорғауға ұсынылатын тұжырым жаңа болып табылады. Жұмыста IoMT құрылғылар тобында деректердің қауіпсіздігін қамтамасыз ету үшін және жіберілетін ақпараттық

			құпиялылығын бұзбай, осы деректерді өңдеу мақсатында IoMT құрылғылардың бірлесіп жұмыс жасауын қамтамасыз ету үшін алғаш рет AtmelAVR (DFRobot Beetle BLUE, Atmega 328, Atmega 32u4, Atmega 2560, ESP 32) микроконтроллерінде гомоморфты шифрлау алгоритмдердің кітапхана архитектурасы құрылды және іске асырылды. Ғылыми жұмыстың нәтижелері мен тұжырымдары 13 ғылыми еңбек негізінде жарық көрді. Оның ішінде 2 мақала Scopus базасында индекстелген жоғары көрсеткішті журналдарда, бақылау комитеті салалық білім және ғылым саласында ұсынылған журналдағы 4 мақала, Web Science and Scopus мәліметтер базасына енгізілген 2 және халықаралық конференцияларының материалдарындағы 5 басылымда сыннан өтті.
		5.2 Диссертацияның қорытындылары жаңа болып табыла ма? 1) толығымен жаңа; 2) жартылай жаңа (25-75% жаңа болып табылады); 3) жаңа емес (25% кем жаңа болып табылады)	Жұмыстың қорытындылары жаңа және ол жарияланған мақалалар мен авторлық құқықпен қорғалған объектіге рәсімделген куәлікпен негізделеді. Диссертациялық жұымысты орындау кезінде келесідей қорытындылар алынған: 1. AtmelAVR микроконтроллерінде қолданылатын гомоморфты шифрлау алгоритмі жетілдірілді; 2. IoT құрылғылар кластерінің қауіпсіздігін қамтамасыз ету үшін AtmelAVR (DFRobot Beetle BLUE, Atmega 328, Atmega 32u4, Atmega 2560, ESP 32) микроконтроллерінде кітапхана архитектурасын құрылып, бағдарламалық жасақтама құрылды; 3. AtmelAVR микроконтроллеріндегі кітапхана жұмысының сапасын бағаланып және қолданыстағы белгілі кітапхана жұмысымен салыстырылды, нәтижесінде жұмыста ұсынылған кітапхана 1,52 есе жоғары екені көрсетілді.
		5.3 Техникалық, технологиялық, экономикалық немесе басқару шешімдері жаңа және негізделген бе? 1) толығымен жаңа; 2) жартылай жаңа (25-75% жаңа болып табылады); 3) жаңа емес (25% кем жаңа болып табылады)	Қойылған есепті шешуде қол жеткізу үшін қолданылған техникалық шешімдер жаңа және негізделген.

6.	Негізгі қорытындылардың негізділігі	Барлық қорытындылар ғылыми тұрғыдан қарағанда ауқымды дәлелдемелерде негізделген/негізделмеген (qualitative research және өнертану және гуманитарлық бағыттары боынша)	Барлық қорытындылар ғылыми тұрғыдан қарағанда ауқымды дәлелдемелерде негізделген. Ғылыми тұрғыда дәлелденген. Ұсынылған әдістің тиімділігі AtmelAVR микроконтроллерінде эксперименталді түрде негізделген және тексерілген. Алғаш рет AtmelAVR микроконтроллер тобында гомоморфты шифрлау алгоритмдердің кітапхана архитектурасы құрылды және іске асырылды.
7.	Қорғауға шығарылған негізгі қағидаттар	Әр қағидат бойынша келесі сұрақтарға жауап беру қажет: 7.1 Қағидат дәлелденді ме? 1) дәлелденді; 2) шамамен дәлелденді; 3) шамамен дәлелденбеді; 4) дәлелденбеді 7.2 Тривиалды ма? 1) ия; 2) жоқ 7.3 Жаңа ма? 1) ия; 2) жоқ 7.4 Қолдану деңгейі: 1) тар; 2) орташа; 3) кең 7.5 Мақалада дәлелденген бе? 1) ия; 2) жоқ	7.1 Диссертанттың жұмысы бойынша қорғауға шығарылатын негізгі келесі қағадаттары дәлелденді: Зерттеу барысында әртүрлі деректер құрылымдарымен жұмыс істеу үшін SD картамен, SD модулмен және бағдарламашпен толықтырылған AtmelAVR микроконтроллерлер тобында әзірленген, IoMT құрылғылар жүйесінде деректерді қауіпсіз жіберу үшін гомоморфты шифрлау алгоритмдерінің архитектурасы ұсынылды, жасалған тәжірибелердің нәтижелері. Нәтижесі келесі мақалада дәлелденген: Pyrkova A.Yu., Temirbekova Zh.E. “Compare encryption performance across devices to ensure the security of the IoT”, Indonesian Journal of Electrical Engineering and Computer Science, -2020. -Vol. 20. -No. 2. – P. 894-902. Жұмыста шығарылған қағидаттар толығымен дәлелденді. Қорғауға шығарылған негізгі тұжырымдар тривиалды емес (7.2), жаңа (7.3), қолданудың кең (7.4) деңгейіне ие, мақалаларда дәлелденген (7.5). 7.4 Диссертациялық жұмыста ұсынылған гомоморфты шифрлау алгоритмдерінің архитектурасы IoMT, IoT құрылғылар жүйесінде деректерді қауіпсіз жіберу және сақтау үшін қолдануға болады. 7.5 Зерттеу жұмыстарының нәтижелері 13 мақала түріндегі мақала түріндегі жарияланымдармен негізделген. Оның 4-і Web of Science және Scopus базаларында индекстелген.

8.	Дәйектілік принципі Дереккөздер мен ұсынылған ақпараттың дәйектілігі	8.1 Әдістеменің таңдауы - негізделген немесе әдіснама нақты жазылған 1) ия; 2) жоқ	Диссертациялық жұмыста қолданылған әдіснаманың таңдауы негізделген және әдіснама нақты жазылған. Зерттеу жұмысында толық гомоморфты шифрлау алгоритмі жетілдіріліп, AtmelAVR микроконтроллер тобында тестілеу жүргізілген.
		8.2 Диссертация жұмысының нәтижелері компьютерлік технологияларды қолдану арқылы ғылыми зерттеулердің қазіргі заманғы әдістері мен деректерді өңдеу және интерпретациялау әдістемелерін пайдалана отырып алынған: 1) ия; 2) жоқ	Диссертациялық жұмыстың негізгі бөлімдерінің бірі болып табылатын, құрылған гомоморфты шифрлау алгоритмдерінің архитектурасын зерттеу жұмысының нәтижелері компьютерлік технологияларды қолдану арқылы ғылыми зерттеулердің қазіргі заманғы әдістері мен деректерді өңдеу және интерпретациялау әдістемелерін пайдалана отырып алынған.
		8.2 Теориялық қорытындылар, модельдер, анықталған өзара байланыстар және заңдылықтар эксперименттік зерттеулермен дәлелденген және расталған (педагогикалық ғылымдар бойынша даярлау бағыттары үшін нәтижелер педагогикалық эксперимент негізінде дәлелденеді): 1) ия; 2) жоқ	Теориялық тұжырымдар мен қорытындылар эксперименттік зерттеулермен дәлелденген және расталған.
		8.4 Маңызды мәлімдемелер нақты және сенімді ғылыми әдебиеттерге сілтемелермен расталған / ішінара расталған / расталмаған	Маңызды мәлімдемелер ғылыми әдебиеттерге сілтемемелерімен расталған. Пайдаланылған әдебиеттер тізімі зерттеу саласына сәйкес.
		8.5 Пайдаланылған әдебиеттер тізімі әдеби шолуға жеткілікті/жеткіліксіз	Пайдаланылған әдебиеттер тізімі орындалған диссертациялық жұмыстың зерттеу саласын толық қамтиды.
9	Практикалық құндылық принципі	9.1 Диссертацияның теориялық маңызы бар: 1) ия; 2) жоқ	Диссертациялық жұмыстың теориялық маңызы бар. Бүтін сандармен жұмыс істеуге және оларға барлық арифметикалық амалдарды орындауға мүмкіндік беретін толық гомоморфты шифрлау алгоритмдерін микроконтроллерлер мен IoMT құрылғыларында деректерді өңдеу процестерін жетілдіру және бейімдеу. Зерттеу жұмысында алғаш рет IoMT құрылғылар жүйесінде деректерді қауіпсіз жіберу үшін гомоморфты шифрлау алгоритмдерінің архитектурасы ұсынылған.
		9.2 Диссертацияның практикалық маңызы бар және алынған нәтижелерді практикада қолдану мүмкіндігі жоғары: 1) ия;	Диссертациялық жұмыстың практикалық маңызы бар. Жұмысты орындау барысында жетілдірілген гомоморфты шифрлау алгоритмін IoMT құрылғылар

		2) жоқ	жүйесінде деректерді қауіпсіз сақтау үшін қолдану өте маңызды болып саналады.
		9.3 Практикалық ұсыныстар жаңа болып табылады? 1) толығымен жаңа; 2) жартылай жаңа (25-75% жаңа болып табылады); 3) жаңа емес (25% кем жаңа болып табылады)	Зерттеуде толық гомоморфты шифрлау алгоритмі жетілдірілді, жетілдірілген толық гомоморфты шифрлау кітапхана архитектурасы құрылды. Жұмыста құрылған кітапхананы IoMT құрылғылар жүйесінде тәжірибелер жүргізу арқылы практикалық қолданысы көрсетілген.
10.	Жазу және ресімдеу сапасы	Академиялық жазу сапасы: 1) жоғары; 2) орташа; 3) орташадан төмен; 4) төмен.	Диссертация жоғары деңгейде жазылған, техникалық стильге ие. «Есептеу кластерін және жүйені қауіпсіздігін қамтамасыз ету үшін AtmelAVR микроконтроллерін қолдану» тақырыбындағы диссертациялық жұмысы диссертациялық жұмысқа қойылатын талаптарға сәйкес дайындалған. Диссертациялық жұмысты жазу және рәсімдеу сапасы жоғары, рәсімдеу құрылымы мен ережелері сақталған. Диссертациялық жұмыс мәтінінде орфографиялық қателер мен стилистикалық қателер кездеседі. Аталған ескертулер дұмыстың құндылығын төмендетпейді.

Ескертулер мен ұсыныстар: Зерттеу жұмысында толық гомоморфты шифрлау кітапханасының архитектурасы мен жүзеге асырылуы жақсы сипатталған, бірақ кітапхананың ішкі бөлігін көрсетілмеген. Толық гомоморфты шифрлау кітапханасы AtmelAVR микроконтроллерлер тобында қалай жүзеге асырылатынын, яғни аппараттық бөлікті көрсету ұсынылады.

Қорытынды: Темирбекова Жанерке Ерлановнаның «Есептеу кластерін және жүйені қауіпсіздігін қамтамасыз ету үшін AtmelAVR микроконтроллерін қолдану» тақырыбындағы диссертациялық жұмысы «Ғылыми дәрежелерді беру ережесінің» талаптарына сәйкес келеді, ал оның авторы «6D070400-Есептеу техникасы және бағдарламалық қамтамасыз ету» мамандығы бойынша философия докторы (PhD) дәрежесіне лайық.

Ресми рецензенттер пікірлерінің көшірмелері докторантқа диссертация қорғауға дейін кемінде 5 (бес) жұмыс күнінен кешіктірілмей беріледі.

Ресми рецензент:
Д. Серікбаев атындағы Шығыс Қазақстан техникалық университеті,
философия докторы (PhD) **Алимханова А.Ж.**