«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)	Диссертация Қазақстан Республикасының Үкіметі жанындағы Жоғары ғылыми-техникалық комиссия бекіткен «Ақпараттық, коммуникациялық және ғарыштық технологиялар» ғылым дамуының басым бағытына сәйкес келеді.
2.	Ғылымға маңыздылығы	Жұмыс ғылымға елеулі үлесін қосады/қоспайды, ал оның маңыздылығы ашылған/ашылмаған.	Бұл диссертациялық жұмыс ғылымға елеулі үлесін қосады, ал оның маңыздылығы ашылған. Зерттеу кезінде алынған нәтижелер ғылыми тұрғыда өте маңызды, себебі IoT құрылғылары 2024 жылға қарай 83 миллиардқа жетеді деп болжанғанымен, 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. Осыған байланысты IoT құрылғалар арасында деректердің қауіпсіз сақталуын және алмасуын қамтамасыз ету өте маңызды.
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 жоғарғы деңгейде жазылған.
4.	Ішкі бірлік	4.1 Диссертация өзектілігінің негіздемесі:	Диссертацияның өзектілігі жұмыстың маңызды

	принципі	1) негізделген; 2) жартылай негізделген; 3) негізделмеген.	практикалық мәселені шешуге, атап айтқанда алғаш рет AtmelAVR микроконтроллерінде IoT құрылғылар тобында деректердің қауіпсіздігін қамтамасыз ету үшін гомоморфты шифрлау алгоритмінің кітапхана архитектурасы құрылды.
		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	Бұл жұмыстың негізгі 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 болып табылады. Жұмыста қойылған барлық 4 тапсырма мәлімделген тақырыпқа сай келеді.
		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 бір-бірімен толығымен логикалық тұрғыдан өзара байланысты.
		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. Атап айтқанда Абрамов А. алгоритміне азайту, ал Кренделев С.Ф. алгоритміне азайту, бөлу арифметикақалық операциялар 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. Сонымен қатар, Абрамов А. және Кренделев С.Ф. гомоморфты шифрлау алгоритмдерін жетілдірілген, жетілдірілген алгоритм негізінде алғаш рет AtmelAVR (DFRobot Beetle BLUE, Atmega 328,

			Atmega 32u4, Atmega 2560, ESP 32) микроконтроллерінде гомоморфты шифрлау алгоритмдердің кітапхана архитектурасы құрылып, іске асырылған.
		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)	Диссертацияның қорытындылары жаңа болып табылады. Осылайша, зерттеу жұмысының қорытындыларындағы нәтижелер мынадай жаңа нәтижені көрсетеді: AtmelAVR микроконтроллер тобында қолданылатын гомоморфты шифрлау кітапханасы жетілдірілді, IoT құрылғылар кластерінің қауіпсіздігін қамтамасыз ету үшін AtmelAVR микроконтроллерінде кітапхана архитектурасы құрылды.
		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)	Техникалық, технологиялық, экономикалық немесе басқару шешімдері жаңа және негізделген. Атап айтқанда, бұл жұмыста алғаш рет IoT құрылғылар кластерінің арасында деректердің қауіпсіз жіберілуін және сақталуын қамтамасыз ету үшін AtmelAVR микроконтроллерінде гомоморфты шифрлау кітапхана архитектурасы құрылды.
6.	Негізгі қорытындыларды ң 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 эксперименталь түрде негізделген және тексерілген.
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:	Диссертанттың жұмысы бойынша қорғауға шығарылатын негізгі келесі қағидатты атауға болады: - 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. Қағидат тривиалды емес, жаңа, қолдану деңгейі кең және келесі мақалаларда дәлелденген: 1. Pyrkova A.Yu., Temirbekova Zh.E. “Compare

		1) тар; 2) орташа; 3) кең 7.5 Мақалада дәлелденген бе? 1) ия; 2) жоқ	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. 2. Temirbekova Zh.E., Pyrkova A.Yu. "Improving teachers' skills to integrate the microcontroller technology in computer engineering education", Education and information technology, -2022 doi: 10.1007/s10639-021-10875-8
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 бірнеше әдістер (микроконтроллердегі ақпараттарды өңдеу әдісі, IoT кластерлерін қорғау үшін микроконтроллерлерді пайдалану тиімділігін талдау және бағалау әдістері, гомоморфты шифрлау әдісі) қолданылды және толық сипатталады.
		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	Диссертация жұмысының нәтижелері компьютерлік технологияларды қолдану арқылы ғылыми зерттеулердің қазіргі заманғы әдістері мен деректерді өңдеу және интерпретациялау әдістемелерін пайдалана отырып алынған. Зерттеу жұмысы AtmelAVR микроконтроллерлерін қолданып, Arduino және Atmel Studio бағдарламасының соңғы нұсқасында жазылып, зерттеу кезінде әртүрлі өлшемді символдар мен файлдарды пайдаланып зерттеу жасалынған.
		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 қорытындылар, модельдер, анықталған өзара байланыстар және заңдылықтар эксперименттік зерттеулермен дәлелденген және расталған. Диссертациялық жұмыс нәтижесінде алынған өкспериментік нәтижелері бойынша: жетілдірілген гомоморфты шифрлау алгоритмдерін IoT қосымшалары мен құрылғыларына қолдануға болатынын көрсетеді. Шифрланған деректер мен шифрланбаған деректерге қосу және көбейту операцияларының өнімділіктері салыстырылды; 10^8 итерацияның орташа жұмыс уақыты есептелінді. Салыстыру нәтижесінде С.Ф. Кренделев пен

			А.Абрамов алгоритмдерге қарағанда құрылған кітапхананың өнімділігі 1.5 есе жылдам екенін сурет 4.8 және сурет 4.9-дан көруге болады
		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. Өйткені зерттеліп отырған тақырып IoT құрылғылардың арасында деректердің қауіпсіз жіберілуін және сақталуын қамтамасыз ету саласында өзекті тақырыптардың бірі.
		9.2 Диссертацияның практикалық маңызы бар және алынған нәтижелерді практикада қолдану мүмкіндігі жоғары: 1) ия; 2) жоқ	Диссертациялық жұмыстың практикалық маңызы бар және алынған нәтижелерді практикада қолдану мүмкіндігі жоғары, өйткені практикада AtmelAVR (DFRobot Beetle BLUE, Atmega 328, Atmega 32u4, Atmega 2560, ESP 32) микроконтроллерінде құрылған гомоморфты шифрлау алгоритмдердің кітапхана архитектурасы арқылы IoMT құрылғылар тобында деректердің қауіпсіздігін қамтамасыз етуге болады.
		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. Практикалық ұсыныстар жаңа болып табылады.
10.	Жазу және ресімдеу сапасы	Академиялық жазу сапасы: 1) жоғары; 2) орташа; 3) орташадан төмен; 4) төмен.	Бұл жұмыста академиялық жазудың сапасы жоғарғы деңгейге ие. Диссертациялық жұмысты жазу және рәсімдеу сапасы жоғары, рәсімдеу құрылымы мен ережелері сақталған. Диссертациялық жұмыс мәтінінде орфографиялық қателер мен стилистикалық қателер кездеседі. Аталған ескертулер жұмыстың құндылығын төмендетпейді.

Ескертулер мен ұсыныстар: Зерттеу жұмысында толық гомоморфты шифрлау кітапханасының архитектурасы және оның жүзеге асырылуы жақсы сипатталған, бірақ соңғы жылдары әлемде IoT құрылғыларына арналған толық гомоморфты шифрлау алгоритмдерімен салыстырулар жасалмаған. Мысалы: Горан Д., Милан М., Павле В. «IoT құрылғысында гомоморфты шифрлауды енгізуді бағалау».

Айтылған ескерту жұмысты әрі қарай жетілдіруге нұсқаулық ретінде көрсетілген және ол диссертациялық жұмыстың құндылығын төмендетпейді.

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:
Сәтбаев университеті,
техника ғылымдарының кандидаты, профессор **Ожикенов К.А.**

HR Қызметі

ДҰРЫС
HR қызметінің
бас менеджері
МАМАНЫ
Күні «09» 08 2023 ж.