«6D070400-Есептеу техникасы және бағдарламалық қамтамасыз ету» мамандығы бойынша философия докторы (PhD) ғылыми дәрежесін алу үшін ұсынылған «Есептеу кластерін және жүйені қауіпсіздігін қамтамасыз ету үшін AtmelAVR микроконтроллерін қолдану» тақырыбы бойынша Темирбекова Жанерке Ерлановнаның диссертациялық жұмысына

АҢДАТПА

Зерттеу тақырыбының өзектілігі IoT (Internet of Things, Интернет заттары) құрылғылары денсаулық сақтау саласынан бастап, өндіріске дейін барлық секторларда кең қолданысқа енген. IoT технологиялардың негізгі мақсаты – интернетке қосылған құрылғылардың бір-бірімен байланысуына, деректер алмасуына, деректерді сақтауына және пайдаланушының талаптарына сәйкес есептеулер жүргізуіне мүмкіндік беру.

IoT нұсқасының бірі медициналық заттардың интернеті (IoMT) денсаулық сақтау саласының өсіп келе жатқан саласы және қашықтан бақылау, деректерді жинау және талдау үшін қосылған медициналық құрылғыларды пайдалануды қамтитын IoT мамандандырылған қолдануының бірі болып табылады. Atmel AVR микроконтроллерлері IoMT құрылғыларында энергия қуатын аз тұтынуына, жоғары өнімділікке және сенімділікке байланысты кеңінен қолданылады. Atmel AVR микроконтроллерлерін пайдаланатын IoMT құрылғыларының мысалдары:

1. Тағатын денсаулық мониторлары;
2. Ақылды инсулин қаламдары;
3. Мөлшерленген доза ингаляторы;
4. Науқастарды қашықтықтан бақылау жүйелері;
5. Таблеткалары бар ақылды бөтелкелер;
6. Телемедицина құрылғылары.

Қорыта келе, Atmel AVR микроконтроллері төмен қуат тұтынуына, шағын өлшемдерге және жоғары есептеу мүмкіндігіне байланысты IoMT пайдалану үшін жан-жақты және сенімді таңдау болып табылады.

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. Palo Alto Networks 2022 жылғы есептемесі бойынша, IoT құрылғысының барлық трафигінің 98%-ы шифрланбаған, бұл желідегі жеке және құпия деректерді құпия түрде сақталмағанын көрсетеді және шабуылдаушыларға шифрланбаған желілік трафикті тыңдауға, жеке немесе құпия ақпаратты жинауға, содан кейін бұл деректерді шабуылшы өзінің жеке мақсаттарына пайдалануына мүмкіндік береді. SAM Seamless Network мәліметтері бойынша, 2021 жылы 1,5 миллиардтан астам IoT құрылғыларына шабуыл жасалынды, соның ішінде 900 миллионға жуық фишингтік шабуылдар.

IoT құрылғылары өздігінен компьютерлердің аналогы емес, олар басынан аяғына дейін ресурстарды қажет ететін кез келген тапсырманы орындай алмайды, олар оның кейбір бөлігін ғана орындайды, ал қалған бөліктерін басқа IoT құрылғылары аяқтайды. IoT белгілі бір топта немесе кластерде жұмыс істейді, олар қандай да бір мәселені бірлесіп шешеді. IoT құрылғылар кластерінің арасында жіберілетін ақпаратты қорғау үшін, олар шифрланған болуы керек және біз жұмыстың жалпы нәтижесін бұзбауымыз үшін шифрланған деректермен шифрланбаған күйде сияқты операцияларды орындай алуымыз керек. Бұл

мүмкіндікті біз медицинадағы, тұрмыстық электроникадағы және өндірістегі IoT құрылғыларын басқаратын AtmelAVR микроконтроллерлерінде (DFRobot Beetle BLUE, Atmega 328, Atmega 32u4, Atmega 2560) іске асырылуы мүмкін гомоморфты шифрлау арқылы жасай аламыз.

Соңғы жылдары әлемде IoT құрылғыларына арналған ТГШ (толық гомоморфты шифрлау) бойынша көптеген жұмыстар пайда болды. Суджой С.Р., Гоюри П., Дипика Н. жұмыстарында толық гомоморфты шифрлау алгоритмдерін IoT қосымшалары мен құрылғыларына қолдануға болатынын көрсетеді, сонымен қатар деректердің құпиялылығын сақтай отырып, есептеу жылдамдығын жоғарлатуды қамтамасыз етуге бағытталған.

Горан Д., Милан М., Павле В. «IoT құрылғысында гомоморфты шифрлауды енгізуді бағалау» жұмыстарында BFV және BGV гомоморфты шифрлау механизмдерінің ерекшеліктерін бағалап, есептеу өнімділігін өлшеді. Raspberry Pi 4 B моделіне негізделген IoT платформасындағы шифрлау схемаларын бағалап, гомоморфты шифрлау операцияларын ендірілген құрылғыларда қолдануға болатындығын көрсетеді және ең алдымен құпиялылықты жақсартуға және қосымшаларды жылдамдату үшін жоғары өткізу қабілеті мен төмен кідіріспен қамтамасыз етуге бағытталған.

Ресейлік ғылыми қоғамдастық өкілдерінің ішінде келесі ғалымдардың еңбектерін ерекше атап өтуге болады: И.Б.Саенко, В.А. Десницкий (Москва қ.), И.В.Котенко (Сверлоск қ.), П.Д. Зегжда (Санкт-Петербург).

ҚР БҒМ ҒК Ақпараттық және есептеуіш технологиялар институтының ғалымдары: Бияшев Р.Г., Нысанбаева С.Е., Капалова Н.А., Күнболат А. ғалымдардың еңбектерінде деректерді криптографиялық қорғау құралдарын зерттеген.

Жасалған талдауларды ескере отырып, IoT қосымшалары мен құрылғыларының қауіпсіздігін тиімді қамтамасыз ететін әдістер, алгоритмдер қажеттілігі туындайды және қарастырылып отырған тақырыптың **өзекті мәселе** екендігін анықтайды.

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.

Диссертациялық жұмыстың мақсатын жүзеге асыратын **зерттеу міндеттері:**

1. IoT құрылғылар кластеріндегі деректерді қорғауға арналған әдістер мен құрылғыларға талдау жасау;
2. AtmelAVR микроконтроллерінде қолданылатын гомоморфты шифрлау алгоритмін жетілдіру;
3. IoT құрылғылар кластерінің қауіпсіздігін қамтамасыз ету үшін AtmelAVR (DFRobot Beetle BLUE, Atmega 328, Atmega 32u4, Atmega 2560, ESP 32) микроконтроллерінде кітапхана архитектурасын құру, бағдарламалық жасақтама құру;
4. AtmelAVR микроконтроллеріндегі кітапхана жұмысының сапасын бағалау және қолданыстағы белгілі кітапхана жұмысымен салыстыру мақсатында есептеу эксперименттерін жүргізу.

Зерттелу нысаны. IoT құрылғылар арасында деректерді қауіпсіз жіберу.

Зерттеу пәні. Микроконтроллердің көмегімен деректерді қорғау жолдары.

Зерттеу әдістері. Микроконтроллердегі ақпараттарды өңдеу әдісі, IoT кластерлерін қорғау үшін микроконтроллерлерді пайдалану тиімділігін талдау және бағалау әдістері, гомоморфты шифрлау әдісі.

Зерттеу жұмысының жаңалығы. 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. Құрылған кітапхана мен белгілі Кренделев С.Ф. және Абрамов А. кітапханаларының өнімділігін бағалау бойынша эксперименттер барысында диссертациялық жұмыста ұсынылған кітапхана қосылу мен пайдаланудың қарапайымдылығын көрсетті, сонымен қатар деректерді есептеу жылдамдығы шамамен 1,52 есе жоғары болды.

Жұмыстың теориялық маңыздылығы.

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.

Жұмыстың практикалық маңыздылығы.

Микроконтроллерге арналған кітапхананың архитектурасын әзірлеу және оның жұмысын оңтайландыру мақсатында кітапхананың модульдері мен әдістері арасында мәліметтер алмасу схемасын, әдістемесін және тәртібін белгілеу.

Қорғауға шығарылатын негізгі тұжырым.

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 қорғауға ұсынылады.

Сенімділік дәрежесі мен апробациялау нәтижелері. Жұмыстың ғылыми нәтижелері төмендегі халықаралық ғылыми-әдістемелік конференциялар мен ғылыми семинарларда баяндалып, талқыланды:

1) «Көліктегі инновациялық технологиялар: білім, ғылым, тәжірибе» атты XLI, XLII Халықаралық ғылыми-практикалық конференциясы;

2) Международная научно-практическая конференция «Актуальные и перспективные направления развития научно-технологического прогресса»;

4) International Research Conference on Technology, Science, Engineering and Economy held Seattle, USA;

5) «Физика – математика ғылымдарының қазіргі білім беру кеңістігіндегі рөлі» VI халықаралық ғылыми-практикалық конференциясы;

6) The 5th International Conference on Energy, Environmental and Information System (ICENIS 2020), Semarang, Indonesia //E3S Web of Conferences.

Сондай-ақ бұл тақырып бірнеше рет әл-Фараби атындағы Қазақ ұлттық университетінің Ақпараттық технологиялар факультетінің «Компьютерлік ғылымдар» кафедрасында, ҚР БҒМ ҒК Ақпараттық және есептеуіш технологиялар институтының семинарларында талқыланды.

Әрбір басылымды дайындаудағы докторанттың үлесі. Жарияланған мақалалар мен ғылыми еңбектер диссертация тақырыбы бойынша зерттеу нәтижелерін сипаттайды. Ғылыми зерттеу жұмыстарын орындау барысында 12

мақала жарияланды және 1 авторлық куәлік алынды, оның ішінде, Scopus деректер базасында индекстелетін журналдарда 2 ғылыми мақала жарыққа шықты:

1. 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. (Scopus базасы бойынша процентилі - 45). Q3

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 (Scopus базасы бойынша процентилі - 95). Q1

Қазақстан Республикасы Ғылым және жоғары білім министрлігінің Ғылым және жоғары білім саласындағы сапаны қамтамасыз ету комитеті мен ұсынылған басылымда жарияланған мақалалар (3):

1. Temirbekova Zh.E., B.K. Alymbayeva. “Using Atmel AVR microcontrollers for safety-performance computing” // Вестник КазНИТУ, -2017. №2, – С. 192 - 195

2. Pyrkova A.Yu., Temirbekova Zh.E. “Possibilities of using a BLE Nano Kit microcontroller to develop cryptographic libraries” // Вестник КазНИТУ:, - 2018. №2, – С. 477 - 481

3. Pyrkova A.Yu., Temirbekova Zh.E. “Performing symmetric encryption mbed platform” // Вестник КазНИТУ, - 2018. №2, – С. 473 – 476

Scopus деректер базасында индекстелген халықаралық ғылыми-тәжірибелік конференциялар жинақтарында 2 ғылыми мақала жарияланған:

1. Temirbekova Zh.E., Pyrkova A.Yu. “Using FHE in a binary ring Encryption and Decryption with BLE Nano kit microcontroller” //E3S Web of Conferences 202 (ICENIS 2020), -2020. 15002

2. Temirbekova Zh.E., Pyrkova A.Yu., Abdiakhmetova Zh. “Library of fully homomorphic encryption on a microcontroller” //2022 International Conference on Smart Information Systems and Technologies 28-30 April, 2022, Nur-Sultan, doi:10.1109/SIST54437.2022.9945722.

Халықаралық ғылыми конференциялар жинақтарында 5 ғылыми мақала жарияланды:

1. Temirbekova Zh.E “Programming microcontroller AVR Atmega8” // «Көліктегі инновациялық технологиялар: білім, ғылым, тәжірибе» атты XLI Халықаралық ғылыми-практикалық конференцияның материалдары, 3-4 сәуір 2017 ж., Алматы, Казахстан, (I том), 102-104 б.

2. Pyrkova A.Yu, Temirbekova Zh.E “Use homomorphic encryption for data security” // «Көліктегі инновациялық технологиялар: білі, ғылым, тәжірибе» атты XLII Халықаралық ғылыми-практикалық конференцияның материалдары, 2018 ж., Алматы, Казахстан, (I том), 83 -85 б.

3. Temirbekova Zh.E “For data security symmetric encryption algorithm” // Международная научно-практическая конференция «Актуальные и перспективные направления развития научно-технологического прогресса», 30 января, 2020 года, Россия, г. Кемерово, С. 26-30

4. Pyrkova A.Yu, Temirbekova Zh.E. “Using microcontrollers to ensure data security”, International Research Conference on Technology, Science, Engineering and Economy held Seattle, USA, February 28th, 2020, P. 52-60

5. Темирбекова Ж.Е. “Толық гомоморфты шифрлеу алгоритмінің кітапханасы” «Физика – математика ғылымдарының қазіргі білім беру кеңістігіндегі рөлі» VI

халықаралық ғылыми-практикалық конференция материалдар жинағы, 7 желтоқсан 2021 ж., Атырау, Казахстан, 326-331 б.

Жұмыс көлемі мен құрылымы. Диссертациялық жұмыс кіріспеден, төрт бөлімнен, қорытындыдан, 104 пайдалынылған әдебиеттер тізімінен және екі қосымшадан тұрады. Зерттеу жұмысының жалпы көлемі – 92 бет оның ішіне 46 сурет, 17 кесте кіреді.

Кіріспеде диссертациялық жұмыстың өзектілігін негіздейді. Жұмыстың мақсаты, зерттеу жұмысының объектісі мен пәні тұжырымдалды. Ғылыми жаңалығы мен практикалық маңыздылығы анықталды. Жүргізілген зерттеу нәтижелері сипатталған. Зерттеу және жариялау нәтижелерін апробациялау туралы ақпарат берілген.

Бірінші бөлімде әртүрлі AtmelAVR микроконтроллердің архитектурасы қарастырылып, шолу берілген. Диссертациялық жұмысқа қатысты қолданылған терминдер мен ұғымдар берілген. Әртүрлі AtmelAVR микроконтроллердің сенімділігі есептеліп, соның негізінде диссертациялық жұмыста қолданылатын микроконтроллер анықталды. AtmelAVR микроконтроллерінде әртүрлі гомоморфты шифрлау криптожүйелеріне эксперименттік есептеулер жүргізілді. Микроконтроллерде эксперименттік есептеулер негізінде тиімді гомоморфты шифрлау алгоритмдері көрсетілген. Осы тақырып бойынша ғылыми еңбектерге сілтеме жасалып, шолу жүргізілді.

Екінші бөлімде гомоморфты шифрлаудың жетілдірілген әдістері: С.Ф. Кренделев алгоритміне азайту және бөлу операциялары қосылды, А.Абрамовтың алгоритміне – азайту операциясы қосылды. Жетілдірілген толық гомоморфты шифрлау іс-әрекет диаграмма түрінде көрсетілді.

Үшінші бөлімде AtmelAVR микроконтроллері үшін жетілдірілген толық гомоморфты шифрлау кітапхана архитектурасы жүзеге асырылды. Құрылған кітапхана архитектурасы микроконтроллермен байланысу схемасы зерттелді. Atmega 328 микроконтроллерінде орнатылған кітапхана архитектурасы көрсетілді. Жетілдірілген шифрлау алгоритмі үшін құрылған бағдарламалық жасақтама модулі туралы ақпарат берілген. Жетілдірілген шифрлау алгоритмі блок-схемалар негізінде түсіндірілген (кілтті генерациялау, шифрлау, гомоморфтылық, кері шифрлау). Бағдарламалық жасақтаманың негізгі жүйелік талаптары, жұмыс істеу түсіндірмелері көрсетілді.

Төртінші бөлімде ұсынылған архитектура негізінде құрылған кітапхана AtmelAVR микроконтроллерінде есептеу жылдамдықтарына эксперименттік зерттеу жұмыстары жүргізілді. Нәтижелері диаграмма түрінде көрсетілді. Құрылған кітапханаларды басқа белгілі авторлардың жұмыстарымен салыстырулар жүргізіліп, диссертациялық жұмыста ұсынылған, яғни жетілдірілген толық гомоморфты шифрлау салыстырмалы түрде есептеу жылдамдығы 1.5 есе жылдам жұмыс жасайтыны көрсетілді.

Қорытындыда диссертацияда алынған негізгі нәтижелер тұжырымдалды.