АННОТАЦИЯ

диссертационной работы Темирбековой Жанерке Ерлановны на тему «Использование AtmelAVR микроконтроллеров для обеспечения безопасности вычислительных кластеров и систем», представленной на соискание степени доктора философии (PhD) по специальности «6D070400-Вычислительная техника и программное обеспечение»

Актуальность работы. В каждом секторе, от здравоохранения до производства, используются устройства IoT (Internet of Things, Интернет вещей). Основная цель технологии IoT заключается в том, чтобы позволить подключенным устройствам взаимодействовать друг с другом, обмениваться данными, хранить данные и выполнять вычисления в соответствии с требованиями пользователя.

Одной из разновидностей IoT является интернет медицинских вещей (IoMT) - это растущая область здравоохранения и одно из специализированных направлений использования IoT, которое включает в себя использование подключенных медицинских устройств для удаленного мониторинга, сбора и анализа данных. Микроконтроллеры Atmel AVR широко используются в устройствах IoMT из-за их низкого энергопотребления, высокой производительности и надежности. Вот несколько примеров устройств IoMT, в которых используются микроконтроллеры Atmel AVR:

1. Носимые мониторы здоровья;
2. Интеллектуальные инсулиновые ручки;
3. Подключенные ингаляторы;
4. Системы удаленного мониторинга пациентов;
5. Умные бутылочки с таблетками;
6. Устройства телемедицины.

К 2024 году прогнозируется, что общее количество IoT устройств достигнет 83 миллиарда. Очевидно, что без надлежащих мер безопасности любое подключенное устройство IoT уязвимо для взлома, потери функций или пользовательских данных. Согласно отчету Palo Alto Networks за 2022 год, 98% всего трафика устройств IoT не зашифровано, что указывает на то, что частные и конфиденциальные данные в сети не хранятся в секрете и позволяют злоумышленникам подслушивать незашифрованный сетевой трафик, собирать личную или конфиденциальную информацию и затем использовать эти данные в своих целях. По данным SAM Seamless Network, в 2021 году было совершено более 1,5 миллиарда атак на IoT-устройства, почти 900 миллионов из которых были фишинговыми атаками, связанными с IoT.

IoT устройства сами по себе не являются аналогами компьютеров, они не могут выполнять какую-либо ресурсоемкую задачу от начала до конца, они выполняют только какую-то ее часть, а остальные части дорабатывают другие IoT-устройства. Другими словами, IoT-ы работают в определенной группе или кластере, они совместно решают некоторую задачу. Передаваемая между ними информация с целью её защиты должна быть зашифрована, но с другой стороны, чтобы мы не нарушили общий результат работы и имели возможность выполнять операции над этими данными, должна быть возможность выполнять действия над зашифрованными отдельными пакетами данных так, как если бы они были в незашифрованном виде. Эту возможность нам даёт гомоморфное шифрование, которые может быть реализовано в микроконтроллерах AtmelAVR (DFRobot Beetle BLUE, Atmega 328,

Atmega 32u4, Atmega 2560), управляющих IoT-устройствами в медицине, бытовой электронике и производстве.

За последние годы в мире появляется все больше работ, связанных с ПГШ (полностью гомоморфное шифрование) для IoT-устройств. Суджой С.Р., Гоюри П., Дипика Н. показывают, что алгоритмы гомоморфного шифрования могут применяться к приложениям и устройствам IoT, а также направлены на увеличение скорости вычислений при сохранении конфиденциальности данных.

Горан Д., Милан М., Павле В. в работе «Оценка реализации гомоморфного шифрования в IoT-устройстве» оценили особенности механизмов BFV и BGV гомоморфного шифрования и измерили их производительность. В работе оценили схемы шифрования на платформе IoT на основе модели Raspberry Pi 4, которые показывают, что гомоморфные операции шифрования могут применяться на встроенных устройствах и направлены, прежде всего, на повышение конфиденциальности и обеспечение более высокой пропускной способности и меньшей задержки для ускорения большего количества приложений ПГШ.

Среди представителей российского научного сообщества можно выделить работы следующих ученых: И.Б.Саенко, В.А. Десницкий (Москва), И.В. Котенко (Екатеринбург), П.Д. Зегда (Санкт-Петербург).

Ученые Института информационных и вычислительных технологий КН МОН РК: Бияшев Р.Г., Нысанбаева С.Е., Капалова Н.А., Кунболат А.

Исходя из вышеизложенного, можно сделать вывод, что использование эффективных алгоритмов, методов и программного обеспечения для безопасности IoT устройств и приложений является весьма **актуальным**. А микроконтроллеры AtmelAVR можно весьма эффективно использовать в широком спектре приложений IoMT для сбора и передачи данных в режиме реального времени, что позволит медицинским работникам принимать обоснованные решения о здоровье своих пациентов.

Цель диссертационного исследования: Разработать и реализовать архитектуру библиотеки полностью гомоморфного шифрования, позволяющую выполнять все арифметические операции над зашифрованными данными на группе микроконтроллерах AtmelAVR для безопасного хранения и защиты передачи информации между IoT устройствами.

Задачи исследования, реализующие цель диссертационной работы:

1. Анализ методов и устройств защиты данных в кластере IoT-устройств.
2. Усовершенствование алгоритма гомоморфного шифрования, используемого в микроконтроллере AtmelAVR.
3. Разработка архитектуры библиотеки в микроконтроллере AtmelAVR (DFRobot Beetle BLUE, Atmega 328, Atmega 32u4, Atmega 2560, ESP 32) для обеспечения безопасности кластера IoT устройств.
4. Оценка качества работы библиотеки на микроконтроллере AtmelAVR, а также сравнение её производительности с производительностями других известных библиотек.

Объект исследования. Безопасная передача данных между IoT устройствами.

Предмет исследования. Способы защиты данных с помощью микроконтроллера.

Методы исследования. Методы обработки информации в микроконтроллере, методы анализа и оценки эффективности использования микроконтроллеров для защиты IoT-кластеров, метод гомоморфного шифрования.

Научная новизна:

Научная новизна работы заключается в том, что впервые была разработана и реализована архитектура библиотеки гомоморфных алгоритмов шифрования на микроконтроллерах AtmelAVR (DFRobot Beetle BLUE, Atmega 328, Atmega 32u4, Atmega 2560, ESP 32) для защиты передачи данных в группе IoMT-устройств, с тем чтобы, не нарушая конфиденциальности передаваемой информации, обеспечить совместную работу IoMT-устройств по обработке этих данных, как если бы они были в незашифрованном виде. В ходе экспериментов по оценке производительности разработанной библиотеки и известных алгоритмов гомоморфного шифрования Кренделева С.Ф. и Абрамова А., предложенная в диссертационной работе библиотека показала удобство в подключении и использовании, а также скорость вычисление данных около 1,52 раза выше.

Теоретическая значимость работы. Усовершенствование и адаптация для микроконтроллеров и процессов обработки данных на IoMT-устройствах алгоритмов полностью гомоморфного шифрования, позволяющих работать с целыми числами и выполнять над ними все арифметические операции.

Практическая значимость работы. Разработка архитектуры библиотеки для микроконтроллера и установление схемы, методики и порядка обмена данными между модулями и методами библиотеки с целью оптимизации её работы.

Основные положения, выносимые на защиту.

К защите представлена архитектура библиотеки гомоморфных алгоритмов шифрования для защиты передаваемых данных в системе IoMT-устройств, разработанная и реализованная на группе микроконтроллеров AtmelAVR, которые в процессе исследования были дополнены SD-картой, SD-модулем и программатором для расширения возможностей работы с разными структурами данных.

Уровень достоверности и результаты апробации. Научные результаты работы были представлены и обсуждены на следующих международных научных конференциях и научных семинарах:

1) XLI, XLII Международная научно-практическая конференция «Инновационные технологии на транспорте: знания, наука, опыт»;

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) VI международная научно-практическая конференция «Физика – роль математических наук в современном образовательном пространстве»;

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

Также эта тема обсуждалась неоднократно на кафедре компьютерных наук Казахского национального университета имени аль-Фараби и на научных семинарах факультета информационных технологий, а также в КН МОН РК Институте информационных и вычислительных технологий.

Вклад докторанта в подготовку каждой публикации. В опубликованных статьях и научных трудах описаны результаты исследования по теме диссертации. За время научной работы было написано 12 научных работ и получено 1 авторское свидетельство, в том числе: 2 научная статья в журнале, индексируемых в базе данных Scopus:

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

3 статьи в журналах, рекомендованных Комитетом по Контролю в Сфере Образования и Науки Министерства образования и науки Республики Казахстан:

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

В сборниках международных научно-практических конференций, индексируемых в базе данных Scopus, опубликовано 2 научных статьи:

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.

В сборниках международных научных конференций опубликовано 5 научных статей:

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.

Объем и структура работы. Общий объем работы – 92 страницы. Диссертационная работа состоит из введения, 4 разделов, заключения, списка используемых источников из 104 наименований, 2 приложения, включает 46 рисунков и 17 таблиц.

Во введении обсуждается актуальность выбранной темы диссертационный работы, цель, объект, предмет и задачи исследования. Описаны полученные результаты проведенных исследований, их научная новизна и практическая значимость.

Первый раздел посвящен анализу различных архитектур микроконтроллеров AtmelAVR. Представлены термины и понятия, используемые применительно к диссертационной работе. Рассчитана надежность различных микроконтроллеров AtmelAVR, и на основании этого определен микроконтроллер, используемый в диссертационной работе. Экспериментальные расчеты для различных криптосистем гомоморфного шифрования проводились на микроконтроллере AtmelAVR. На основе экспериментальных расчетов показаны эффективные алгоритмы гомоморфного шифрования на микроконтроллере. Были даны ссылки и рецензии на научные работы по этой теме.

Во втором разделе описан процесс модификации методов гомоморфного шифрования: в алгоритм С.Ф. Кренделева добавлены операции вычитания и деления, в алгоритм А. Абрамова добавлена операция вычитания. Усовершенствованное полностью гомоморфное шифрование представлено в виде блок-схемы.

В третьем разделе представлена архитектура библиотеки полностью гомоморфного шифрования для микроконтроллера AtmelAVR. Исследована схема связи встроенной библиотеки на микроконтроллере. Усовершенствованный алгоритм шифрования поясняется на основе блок-схем (генерация ключей, шифрование, гомоморфное преобразования, дешифрование). Показаны основные системные требования программного обеспечения, пояснения по работе.

В четвертом разделе описано тестирование производительности библиотеки, построенной на основе предложенной архитектуры, на микроконтроллере AtmelAVR. Результаты представлены в виде диаграммы. Разработанная библиотека сравнивается с работами других авторов и результаты исследований показывают, что усовершенствованное полностью гомоморфное шифрование, представленное в диссертации, работает около 1,52 раза быстрее.

В заключении представлены выводы данной диссертационной работы.