REVIEW

from foreign scientific adviser for dissertation work doctoral student (PhD) Temirbekova Zhanerka Erlanovna on the topic "Using Atmel AVR microcontrollers for safety-performance computing clusters and systems", submitted for the Doctor of Philosophy degree in the specialty "6D070400-Computer Engineering and software"

Dissertation Zh.E. Temirbekova on the topic "Using Atmel AVR microcontrollers for safety-performance computing clusters and systems" is devoted to the development of a library architecture on a microcontroller based on the proposed algorithms and its implementation for homomorphic operations on integers on a group of Atmel AVR microcontrollers (DFRobot Beetle BLUE, Atmega 328, Atmega 32u4, Atmega 2560) to ensure secure connection and data exchange of IoT(Internet of Things) devices.

Atmel AVR microcontrollers today have an unprecedented breadth of application as the main computing and control elements of household and industrial automation. On their basis, embedded systems, systems such as «smart home», «Internet of things», etc. are built. In this regard, the task of efficient and safe programming on microcontrollers is relevant.

Every sector, from healthcare to manufacturing, uses IoT devices. However, even though the total number of devices is predicted to reach 83 billion by 2024, the security of these devices remains a major concern. Without proper security measures, any connected IoT device is vulnerable to hacking, loss of functionality or user data.

According to SAM Seamless Network, there were over 1.5 billion IoT attacks in 2021, almost 900 million of which were IoT-related phishing attacks. In 2021, there were about 62 million DDoS attacks.

In this regard, one of the most relevant applications of the library developed on the microcontroller can be IoT devices, data exchange between them and their remote connection.

To achieve this goal, the dissertation student obtained the following scientific results:

1. Modified methods of homomorphic encryption: to the algorithm of S.F. Krendelev, the operations of subtraction and division were added, to A. Abramov's algorithm - subtraction.
2. The architecture of the library of fully homomorphic operations on integers has been developed.
3. The developed library architecture was implemented based on the Atmel AVR core (DFRobot Beetle BLUE, Atmega 328, Atmega 32u4, Atmega 2560) for various microcontrollers.
4. A comparative analysis of the developed methods based on computational experiments has been carried out.

The dissertation work has all the signs of relevance, scientific novelty, theoretical and practical significance, the results are scientifically substantiated.

The theoretical significance of this work lies in the modification of the existing fully homomorphic encryption, which allows you to work with integers and perform all mathematical operations on them (addition, difference, multiplication and division).

The practical significance of this work lies in the fact that the research carried out and the results obtained are of great value and can be used to store and protect confidential information, in particular, a library on a microcontroller can be used to protect data exchange between IoT devices.

The results obtained were reported and discussed at international conferences and published in the relevant collections of papers. The main results of the dissertation were also presented in foreign publications indexed in the international database «SCOPUS». Part of the research was carried out during a scientific internship at the ISEL Institute, Portugal in 2017.

Based on the foregoing, I believe that the dissertation of Zhanerke Erlanovna Temirbekova is an independent completed scientific qualification work and meets the requirements for dissertations.

Thus, she can be recommended for the defense of the PhD degree in the specialty "6D070400-Computer Engineering and Software".

Foreign Scientific Adviser:
Professor, Manuel Martins Barata, ISEL, Portugal

Assinado por: **Manuel Martins Barata**
Num. de Identificação: 04194637
Data: 2022.12.29 17:07:12+00'00'

CHAVE MÓVEL

«Әл-Фараби атындағы Қазақ ұлттық университеті» коммерциялық емес акционерлік қоғамы
Некоммерческое акционерное общество «Казахский национальный университет имени аль-Фараби»
Non-profit joint-stock company «Al-Farabi Kazakh National University»
АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР ФАКУЛЬТЕТІ

ОТЗЫВ

научного консультанта на диссертационную работу Темирбековой Жанерке Ерлановны «Использование AtmelAVR микроконтроллеров для обеспечения безопасности вычислительных кластеров и систем», представленную на соискание степени доктора философии по специальности «6D070400-Вычислительная техника и программное обеспечение»

Диссертация Ж.Е. Темирбековой на тему «Использование AtmelAVR микроконтроллеров для обеспечения безопасности вычислительных кластеров и систем» посвящена разработке на базе предложенных алгоритмов архитектуры библиотеки на микроконтроллере и её реализация для гомоморфных операций над целыми числами на группе микроконтроллеров AtmelAVR (DFRobot Beetle BLUE, Atmega 328, Atmega 32u4, Atmega 2560) для обеспечения безопасного соединения и обмена данных IoT-устройств (Internet of Things).

Микроконтроллеры AtmelAVR на сегодняшний день имеют беспрецедентную широту применения в качестве основных вычислительных и управляющих элементов бытовой и промышленной автоматики. На их основе строятся встраиваемые системы, системы типа “умный дом”, “интернет вещей” и т.д. В связи с этим актуальной является задача эффективного и безопасного программирования на микроконтроллерах.

В каждом секторе, от здравоохранения до производства, используются устройства IoT. Однако, несмотря на то, что к 2024 году прогнозируется, что общее количество устройств достигнет 83 миллиардов, безопасность этих устройств остается серьезной проблемой. Без надлежащих мер безопасности любое подключенное устройство IoT уязвимо для взлома, потери функций или пользовательских данных.

По данным SAM Seamless Network, в 2021 году было совершено более 1,5 миллиарда атак IoT, почти 900 миллионов из которых были фишинговыми атаками, связанными с IoT. В 2021 году было совершено около 62 миллионов DDoS-атак.

В связи с этим одним из наиболее актуальных применений разработанной на микроконтроллере библиотеки могут стать IoT устройства, обмен данными между ними и удаленное их подключение.

Для достижения поставленной цели, диссертантом получены следующие научные результаты:

1. Модифицированы методы гомоморфного шифрования: к алгоритму С.Ф. Кренделева были добавлены операции вычитания и деления, к алгоритму А.Абрамова - вычитания.
2. Разработана архитектура библиотеки полностью гомоморфных операций над целыми числами.
3. Разработанная архитектура библиотеки была внедрена на базе ядра AtmelAVR (DFRobot Beetle BLUE, Atmega 328, Atmega 32u4, Atmega 2560) для разных микроконтроллеров.
4. Произведен сравнительный анализ разработанных методов на основе вычислительных экспериментов.

Диссертационная работа обладает всеми признаками актуальности, научной новизны, теоретической и практической значимости, результаты научно обоснованы.

Теоретическая значимость данной работы заключается в модификации существующего полностью гомоморфного шифрования, позволяющего работать с целыми числами и выполнять над ними все математические операции (сложение, разность, умножение и деление).

Практическая значимость данной работы заключается в том, что проведенные научные исследования и полученные результаты имеют большую ценность и могут быть использованы для хранения и защиты конфиденциальной информации, в частности

библиотека на микроконтроллере может быть использована для защиты обмена данными между IoT устройствами.

Полученные результаты были доложены и обсуждены на международных конференциях и опубликованы в соответствующих сборниках трудов. Основные результаты диссертации также были представлены в зарубежных публикациях индексированных в международной базе «SCOPUS». Часть исследований была проведена во время научной стажировке в Институте ISEL, Португалии в 2017 году.

Исходя из вышеизложенного считаю, что диссертация Темирбековой Жанерке Ерлановны является самостоятельной законченной научной квалификационной работой и соответствует требованиям, предъявляемым к диссертациям. Таким образом, она может быть рекомендована к защите на соискание степени PhD доктора по специальности «6D070400-Вычислительная техника и программное обеспечение».