МРНТИ 20.01.45
УДК 004.056.55

https://doi.org/10.51889/2959-5894.2023.81.1.019

Ж.Е. Темирбекова[1], А.Ю. Пыркова[1], Г.К. Ордабаева[1], Е. Зуева[1]

[1]Әл-Фараби атындағы Қазақ Ұлттық университеті, Алматы қ., Қазақстан
[*]e-mail: temyrbekovazhanerke2@gmail.com

ATMELAVR ЯДРОСЫНА НЕГІЗДЕЛГЕН ӘРТҮРЛІ ӨНІМДІЛІКТЕГІ МИКРОКОНТРОЛЛЕРЛЕР ҮШІН ГОМОМОРФТЫ ШИФРЛАУ КІТАПХАНАСЫН ЖОБАЛАУ

Аңдатпа

Қазіргі уақытта студенттердің микроконтроллер мен микросхемаларды зерттеуі "Компьютерлік инженерия"білім беру бағдарламасы бойынша өте маңызды және сұранысқа ие болып отыр. Бұл білім мен дағдылар түлектерді өнеркәсіпте, ғылымда және білім беруде жұмысқа орналастыру үшін қажет болады. Осы жүйелердің архитектурасын және осы жүйелерді қауіпсіз және сенімді пайдалану дағдыларын түсінуді қажет ететін үлкен техникалық жүйелер пайда болуда. Бұл мақалада шифрланған мәліметтер бойынша есептеулерді алдымен шифрын ашпастан жүргізуге мүмкіндік беретін толық гомоморфты шифрлау технологиялары қарастырылады. Мұндай технологияларға деген қызығушылықтың артуы толық гомоморфты шифрлауды қолдайтын бағдарламалық құралдар мен кітапханалардың пайда болуына әкелді. Алайда, криптографияның осы саласына қатысты салыстырмалы түрде жас болғандықтан, толық гомоморфты шифрлау схемаларын қолдану бойынша стандарттар мен ұсыныстар әлі де дамуда. Мақалады гомоморфты шифрлауды қолданудың негізгі салалары көрсетілген. Гомоморфты шифрлау саласындағы қолданыстағы кітапханаларға талдау жасалды. Талдаудың нәтижесінде гомоморфты шифрлаудабөлу мен азайту операциясын жүзеге асыру қажеттілігі, сондай-ақ бүтін сандарға гомоморфты шифрлау кітапханасын іске асыруды әзірлеудің өзектілігі анықталды. Гомоморфты шифрланған мәліметтерге бөлу әрекетін орындауға мүмкіндік беретін гомоморфты бөлу әдісі ұсынылды.

Түйін сөздер: Компьютерлік инженерия саласындағы білім, Atmel AVR микроконтроллер, толық гомоморфты шифрлау, микроконтроллерлерді зерттеуді ынталандыру.

Аннотация

Ж.Е. Темирбекова[1], А.Ю. Пыркова[1], Г.К. Ордабаева[1], Е. Зуева[1]
[1]Казахский Национальный Университет имени Аль-Фараби, г.Алматы, Қазахстан

ПРОЕКТИРОВАНИЕ БИБЛИОТЕКИ ГОМОМОРФНОГО ШИФРОВАНИЯ ДЛЯ МИКРОКОНТРОЛЛЕРОВ РАЗЛИЧНОЙ ПРОИЗВОДИТЕЛЬНОСТИ НА ОСНОВЕ ЯДРА ATMELAVR

В настоящее время изучение микроконтроллеров и микросхем студентами становится очень важным и востребованным по образовательной программе "компьютерная инженерия". Эти знания и навыки будут необходимы для трудоустройства выпускников в промышленности, науке и образовании. Появляются большие технические системы, требующие понимания архитектуры и навыков безопасного и надежного использования этих систем. В статье рассматриваются технологии полного гомоморфного шифрования, позволяющие производить расчеты по зашифрованным данным без предварительного дешифрования. Повышенный интерес к таким технологиям привел к появлению программных средств и библиотек, поддерживающих полное гомоморфное шифрование. Однако, будучи относительно молодым в этой области криптографии, стандарты и рекомендации по использованию полностью гомоморфных схем шифрования все еще развиваются. В статье перечислены основные области применения гомоморфного шифрования. Проведен анализ существующих библиотек в области гомоморфного шифрования. В результате анализа выявлена необходимость осуществления операции гомоморфного шифрования и вычитания, а также актуальность разработки реализации библиотеки гомоморфного шифрования целых чисел. Предложен метод гомоморфного разделения, позволяющий выполнять операцию разделения гомоморфных зашифрованных данных.

Ключевые слова: знания в области компьютерной инженерии, микроконтроллер Atmel AVR, полное гомоморфное шифрование, стимулирование исследований микроконтроллеров.

Abstract

DESIGNING A HOMOMORPHIC ENCRYPTION LIBRARY FOR MICROCONTROLLERS OF VARIOUS PERFORMANCE BASED ON THE ATMELAVR CORE

Temirbekova Zh.E. [1]*, Pyrkova A.Yu.* [1]*, Ordabaeva G.K.* [1]*, ZuevaE.* [1]

[1] *Al-Farabi Kazakh National University, Almaty, Kazakhstan*

Currently, the study of microcontrollers and microcircuits by students is becoming very important and in demand in the educational program "computer engineering". This knowledge and skills will be necessary for the employment of graduates in industry, science and education. Large technical systems are emerging that require an understanding of the architecture of these systems and the skills to use these systems safely and reliably. This article discusses the technologies of complete homomorphic encryption, which allow calculations to be performed on encrypted data without prior decryption. Increased interest in such technologies has led to the emergence of software tools and libraries that support full homomorphic encryption. However, being relatively young in this field of cryptography, standards and guidelines for the use of fully homomorphic encryption schemes are still evolving. The article lists the main areas of application of homomorphic encryption. The analysis of existing libraries in the field of homomorphic encryption is carried out. As a result of the analysis, the necessity of carrying out the operation of homomorphic encryption and subtraction, as well as the relevance of developing the implementation of the library of homomorphic encryption of integers, is revealed. A method of homomorphic separation is proposed, which allows performing the operation of separating homomorphic encrypted data.

Keywords: computer engineering knowledge, Atmel AVR microcontroller, fully homomorphic encryption, stimulation of microcontroller research.

Кіріспе

Кәзіргі таңда "Заттар интернеті" қарқынды дамуы өте өзекті етті, ал ол өз кезегінде микроконтроллердің күрделенуіне және қорғаныс жүйесінің қажеттілігіне әкелді. Микроконтроллер MMU, MPU және RTOS сияқты кеңейтілген перифериялларды қолдану кеңінен таралды [1]. MMU (memory protect unit) рұқсатсыз кіруден қорғау осы бағдарламалардың қате немесе зиянды код салдарынан бұрмаланудан сақталуына кепілдік беруге мүмкіндік береді. Ол үшін әртүрлі әдістерді қолдануға болады. Солардың бірі біздің қарастырып отырған статикалық кітапханалар құру, байланыстыру және қолдану болып табылады.

Шифрланған мәліметтерді қауіпсіз есептеу негізгі арифметикалық операцияларды қажет ететін аудандардағы мәліметтер жиынтығын талдау үшін маңызды (геномды өңдеу, жеке деректерді біріктіру, бұлтты есептеу, электронды дауыс беру). Алайда, гомоморфты шифрлау тек шифрланған сандарды қосуға және көбейтуге мүмкіндік береді. Кейбір жағдайларда орташа мәндерді, орташа квадраттық қателерді есептеу үшін бөлу операциясы қажет [2].

Көптеген криптографиялардың ішінде гомоморфты шифрлау ерекше өнімділігі арқасында ғалымдардың назарын аударды. Кәдімгі криптография шифрланған деректермен есептеулерді тікелей орындай алмайды, алайда гомоморфты шифрлау гомоморфты шифрланған деректермен жұмыс істеуге мүмкіндік береді. Гомоморфты шифрлауды қауіпсіз көп партиялы есептеу, электронды дауыс беру, шифрланған мәтінді іздеу, шифрланған поштаны сүзу және мобильді шифрлау сияқты салаларда қолдануға болады.

Кәзіргі таңда гомоморфты шифрлау үшін бірнеше кітапханалар құрылған. Жалпыға қол жетімді және маңызды екі түрін айтсақ болады [3-4]. Олар:

- Ш. Хавели және Виктор Шоуп жасаған HElib кітапханасы,
- Лео Дуглас пен Даниэль Миккианакио жасаған FHEW кітапханасы.

Кәзіргі таңда С.Ф. Кренделевтің гомоморфты шифрлау алгоритмі үшін кітапхана құрылмаған, сонымен қатар шифрланған мәліметтерге бөлу мен азайту операциясы іске асырылмаған. Талдауға сүйене отырып, шифрланған ақпараттармен жұмыс істеуге мүмкіндік беретін толық гомоморфты шифрлау кітапханасын дамыту қажеттілігі туралы қорытынды жасалды. Сонымен қатар барлық математикалық амалдарды (қосу, айырмашылық, көбейту және бөлу) орындауға мүмкіндік беретін кітапхананы Дербес компьютерде және микроконтроллерде құру. С.Ф. Кренделевтің айнымалысы бар көпмүшелер сақинасындағы гомоморфты шифрланған мәліметтерге бөлу және азайту операциялары жүзеге асырылды.

Бұл мақалада микроконтроллерлер, олардың мүмкіндіктері мен ерекшеліктері ақпараттық қауіпсіздік тұрғысынан зерттелді. Микроконтроллерлерде енгізілген деректердің қауіпсіздігін қамтамасыз ету әдістері ұсынылды. Әзірленген кітапхана қауіпсіз қосымшаларды құруға және студенттерге микроконтроллерлерде бағдарламалау принциптері мен дағдыларын үйрету құралы

ретінде қолдануға мүмкіндік береді. Қазіргі білім адамды ақпараттық ресурстарды пайдалануға үйретуге, тиісті құзіреттіліктер мен жаңа ақпараттық кеңістікте өмір сүру қабілетін дамытуға бағытталған.

Зерттеу әдісі

Бұл бөлімде осы эксперименттік шифрлаудың әдісі мен процесі егжей-тегжейлі қарастырылады, сонымен қатар толық гомоморфты шифрлау алгоритмін құрылды. Атап айтсақ: С.Ф. Кренделевтің айнымалысы бар көпмүшелер сақинасындағы гомоморфты шифрланған мәліметтерге бөлу және азайту операциялары жүзеге асырылды.

Айнымалысы бар көпмүшелер сақинасындағы гомоморфты шифрлау

С.Ф. Кренделевтің айнымалысы бар көпмүшелер сақинасындағы гомоморфты шифрлау Гентридің алгоритміне қарағанда тиімді [5-7]. Сонымен қатар, оның бірқатар кемшіліктері бар:

1. Көпмүшелердің шексіз өсуі тиімсіз есептеулерге әкелуі мүмкін;
2. Барлық әрекеттер іс жүзінде еркін түрде орындалғанымен, жадта сақталуы керек және үлкен дәрежелі көпмүшелерде есептеулер жүргізілуі керек;
3. С.Ф. Кренделевтің алгоритмінде шифрланған ақпараттарға бөлу және көбейту орындалмайды.

Шифрлау:

1) Айталық, полином құруға арналған қандай да бір $z \in Z$ – бүтін саны берілсін. $n > 0$ – саны берілсін, бұл көпмүшенің дәрежесі,

кілт $x_0 = \frac{p}{q}, x_0 \in Q$

2) Көпмүше құрылады $f(x) = a_0 + a_1 x + ... + a_n x^n$, мұндағы коэффициенттер $a_0, a_1, ... a_n \in Z$ кездейсоқ таңдалынады.

3) $f(x_0) = f\left(\frac{p}{q}\right) = a_0 + a_1\left(\frac{p}{q}\right) + ... + a_n\left(\frac{p}{q}\right)^n$ есептелінеді, $q^n f\left(\frac{p}{q}\right) = q^n a_0 + q^{n-1} p a_1 + ... + p^n a_n$ алынады, мұндағы $q^n f\left(\frac{p}{q}\right) \in Z$.

4) z санына сәйкес көпмүше $g_z(x) = q^n f(x) - q^n f\left(\frac{p}{q}\right) + z$

Кері шифрлау: көпмүшеге бүтін санды қою

1) Шифрлаудан алынған $g_z(x)$, көпмүше берілсін

2) Онда $g_z(x_0) = q^n f(x_0) - q^n f\left(\frac{p}{q}\right) + z = z$ - бастапқы сан алынады.

Мақалада С.Ф. Кренделевтің айнымалысы бар көпмүшелер сақинасындағы гомоморфты шифрланған мәліметтерге бөлу және азайту операциялары жүзеге асырылды. Алгоритмнің диаграммасы 1-суретте көрсетілген. Айнымалысы бар көпмүшелер сақинасындағы гомоморфты шифрланған мәліметтерге бөлу және азайту операциялары келесідей іске асырылады:

$$a(x) - b(x) = a_0 - b_0 + (a_1 - b_1)x + ... + (a_n - b_n)x^n$$
$$a(x) / b(x) = a_0 / b_0 + (a_0 / b_1 + b_0 / a_1)x + ... + a_n / b_n x^{2n}$$

$$z_1 / z_2 = Dec(Enc(z_1) / Enc(z_2))$$
$$z_1 - z_2 = Dec(Enc(z_1) - Enc(z_2))$$

Құрылған жүйеге мысал:

$$z_1 - z_2 = q^n f_1(x) - q^n f_1\left(\frac{p}{q}\right) + z_1 - q^n f_2(x) - q^n f_2\left(\frac{p}{q}\right) + z_2 =$$

$$= q^n a_0 + q^n a_1 x + q^n a_2 x^2 - \left(q^n a_0 + q^{n-1} p a_1 + q^{n-2} p^2 a_2\right) + z_1 -$$

$$- q^n b_0 + q^n b_1 x + q^n b_2 x^2 - \left(q^n b_0 + q^{n-1} p b_1 + q^{n-2} p^2 b_2\right) + z_2 =$$

$$2^2 * 2 + 2^2 * (-3) + 1 + 2^2 * 4 * 1^2 - (2^2 * 2 + 2^1 * 2 * (-3) + 2^0 * 2^2 * 4) + 4 -$$

$$- 2^2 * 3 + 2^2 * 4 * 1 + 2^2 * (-2) * 1^2 - (2^2 * 3 + 2 * 2 * 4 + 2^0 * 2^2 * (-2)) + 5 = -1$$

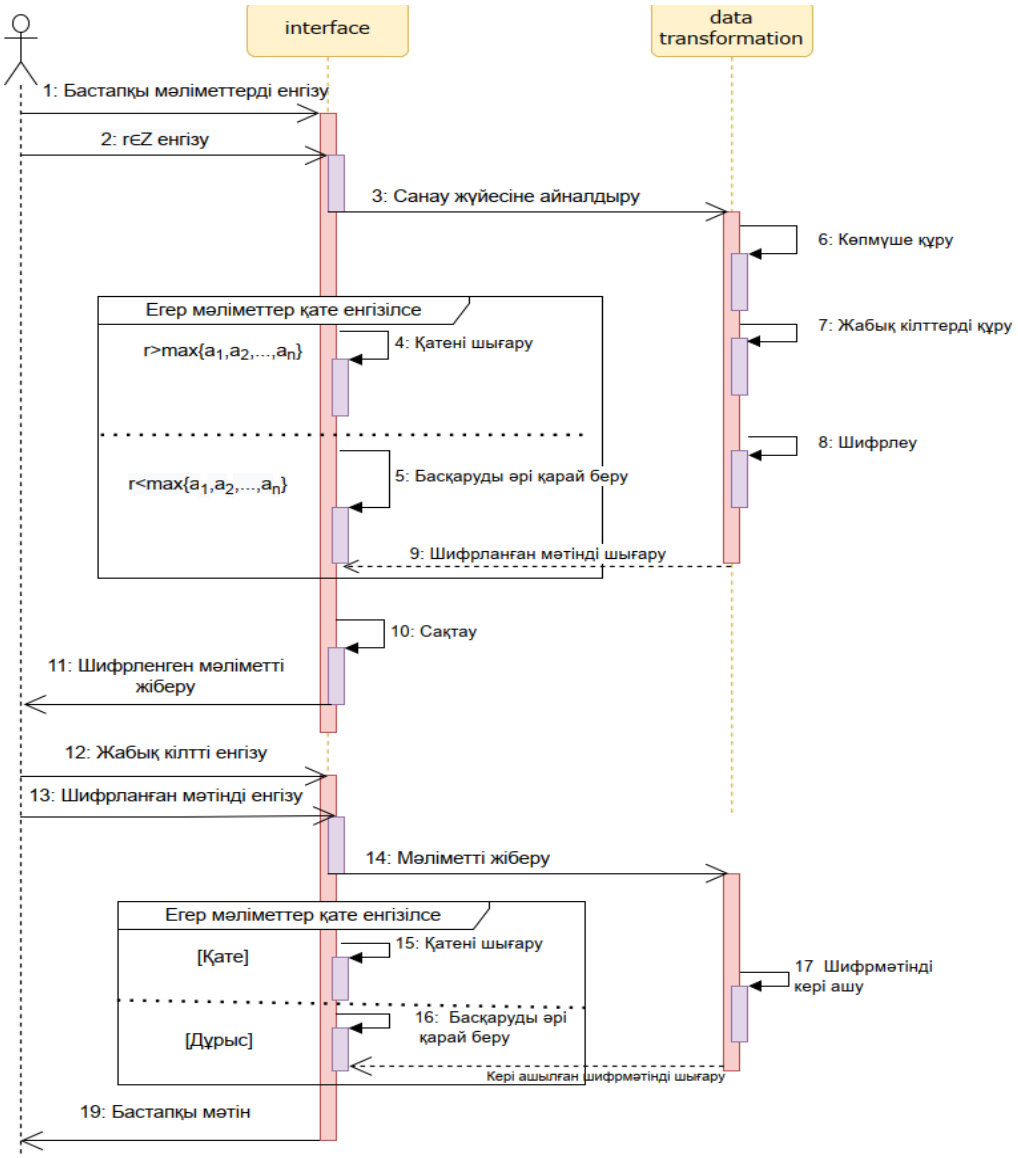
$$z_1 / z_2 = q^n f_1(x) - q^n f_1\left(\frac{p}{q}\right) + z_1 / q^n f_2(x) - q^n f_2\left(\frac{p}{q}\right) + z_2 =$$

$$= q^n a_0 + q^n a_1 x + q^n a_2 x^2 - \left(q^n a_0 + q^{n-1} p a_1 + q^{n-2} p^2 a_2\right) + z_1 /$$

$$/ q^n b_0 + q^n b_1 x + q^n b_2 x^2 - \left(q^n b_0 + q^{n-1} p b_1 + q^{n-2} p^2 b_2\right) + z_2 =$$

$$2^2 * 2 + 2^2 * (-3) + 1 + 2^2 * 4 * 1^2 - (2^2 * 2 + 2^1 * 2 * (-3) + 2^0 * 2^2 * 4) + 4 /$$

$$/ 2^2 * 3 + 2^2 * 4 * 1 + 2^2 * (-2) * 1^2 - (2^2 * 3 + 2 * 2 * 4 + 2^0 * 2^2 * (-2)) + 5 = 0.8$$

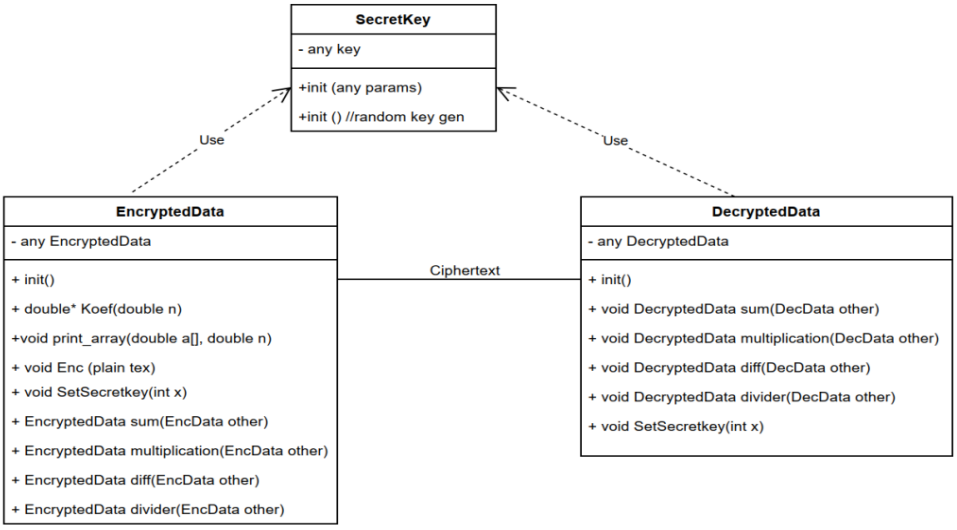


Сурет 1. Айнымалысы бар көпмүшелер сақинасындағы гомоморфты шифрлау

Кітапхананың сәулеті

Кітапхана C++тілінде өнімділігі әр-түрлі микроконтроллерде жүзеге асырылды. Құрылған кітапхананың сәулеті 2-ші суретте көрсетілген. Әзірленген кітапхананы іске асыру кезінде оның алдында келесі міндеттер тұрады:

- Бүтін сандарды өңдеу мүмкіндігі.
- Толығымен гомоморфты шифрлау.
- Барлық математикалық операцияларды, соның ішінде бөлу және азайту оперцияларын қолдау.



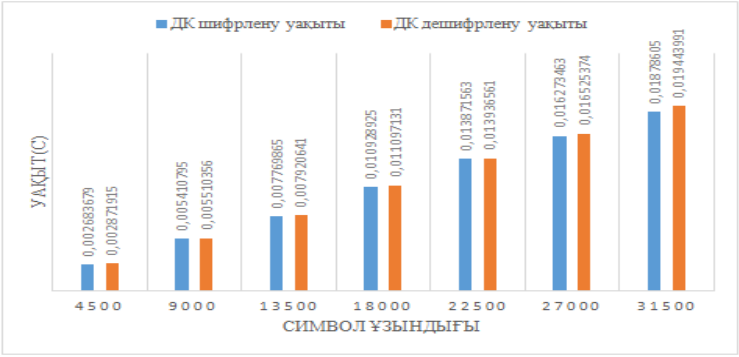
Сурет 2. Айнымалысы бар көпмүшелер сақинасындағы ТГШ құрылған кітапхана сәулеті

Secretkey класы криптографиялық алгоритмде қолданылатын құпия кілт туралы ақпаратпен жұмыс істейді. Жаңа кілтті құру, кездейсоқ құру және оны пайдалану мүмкіндіктерін ұсынады. Кітапхананың қазіргі енгізуінде кілттер мен көпмүшелерді құру үшін стандартты кітапханадан кездейсоқ сандар генераторы қолданылады, нақты уақыттаавтоматты рандомизациясы бар.

Encrypted Data. Криптографиялық деңгей деректерінің негізгі түрін анықтайтын класс болып табылады. Шифрлау және кері шифрлауды шешу алдын-ала жасалған кілтті қолдану арқылы немесе құпия параметрлерді беру арқылы мүмкін болады. Сондай – ақ, бұл класс криптографиялық деңгейдің барлық қажетті математикалық операцияларын жүзеге асырады-қосу, азайту, көбейту және бөлу.

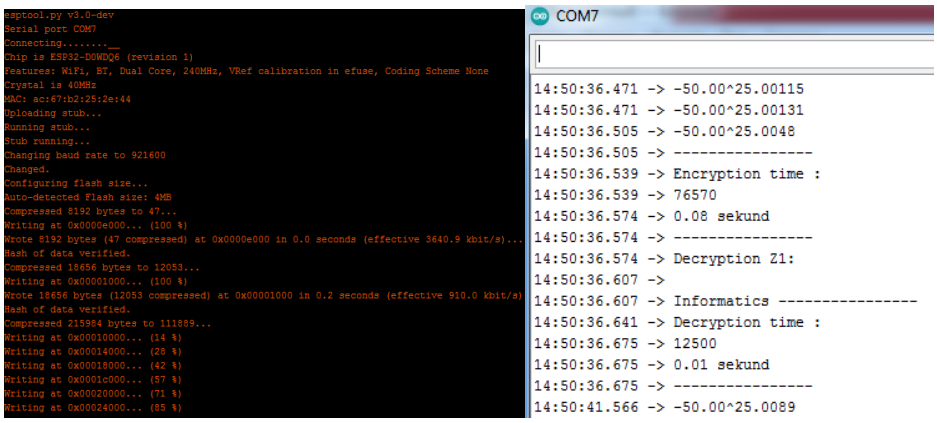
Decrypted Data. Шифрланған мәліметтермен барлық операциялармен жұмыс жасауға мүмкіндің береді. Қабылданған шифр мәтіндерін құпия кілттің көмегімен кері шифрлайды.

Осы жұмыс шеңберінде іске асырылған жүйенің өнімділігіне өлшеулер жүргізілді. Өнімділік Windows 10, Intel(R) Core(TM) процессоры i3-3220 CPU 3.30 GHz және 4 Гб жедел жады бар компьютерде бағаланды. Сонымен қатар,Мәтінді шифрлау және кері шифрлау операциясының жұмысын салыстыру тесті 10 итерация үшін орташа жұмыс уақыты есептелді. Тесттердің бірінші жиынтығында 4500, 9000, 13500, 18000, 22500, 27000, 31500 өлшем мәтіні қарастырылды. 3-суретте көрсетілген. Диаграммадан шифрлау және кері шифрлау сызықты өсетінін көруге болады.



Сурет 3. Дербес компьютерде мәтінді шифрлау және кері шифрлау уақыты

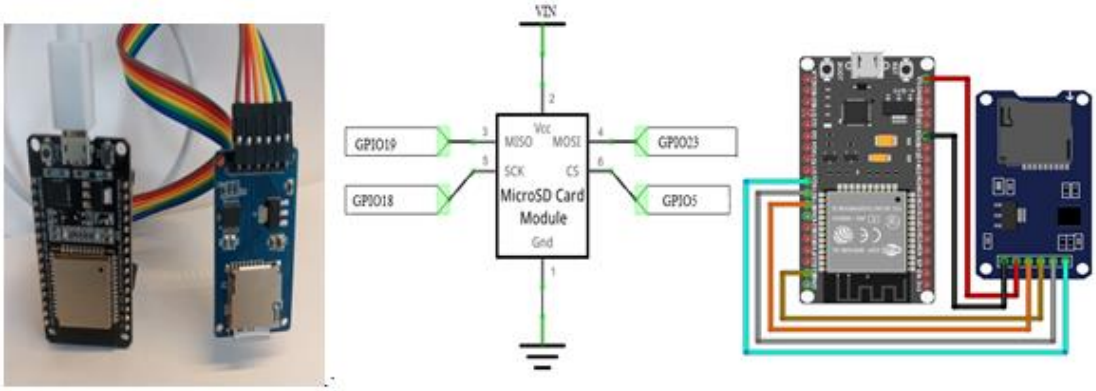
Кітапхана қолдану мысалы 4-суретте бейнелеген.



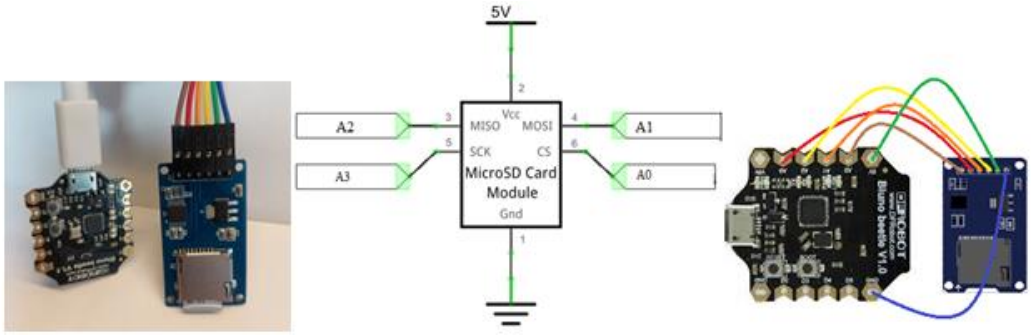
Сурет 4. Кітапхана қолдану мысалы

AtmelAVR ядросына негізделген әртүрлі өнімділіктегі микроконтроллерлер үшін Arduino ортасында гомоморфты шифрлау кітапханасы әр-түрлі өлшемдегі мәтіндердің өнімділігі тестіленді.

Микроконтроллердегі мәтіндік деректерді шифрлау үшін біз ESP 32 бар microSD картасын қолданамыз. Содан кейін біз шифрланған файлдарды microSD картасына оқып, жазамыз. MicroSD картасын ESP 32 картасымен жұптастыру үшін microSD картасының модулін (SPI байланыс протоколы) қолданамыз. ESP 32 (спецификациясы) бар microSD картасын пайдалану әсіресе деректерді тіркеу немесе файлдық жүйеге (SPIFFS) сәйкес келмейтін файлдарды сақтау үшін пайдалы [8]. Fritzing бағдарламалық жасақтамасында барлық микроконтроллерлер үшін SD карталарынан деректерді тіркеудің негізгі сызбасы жасалды. 5-7 суреттерде көрсетілген. Схемада көрсетілгендей, қосылыстар өте қарапайым, өйткені барлық компоненттер модуль ретінде қолданылады; біз оларды тікелей орналасуда жасай аламыз.



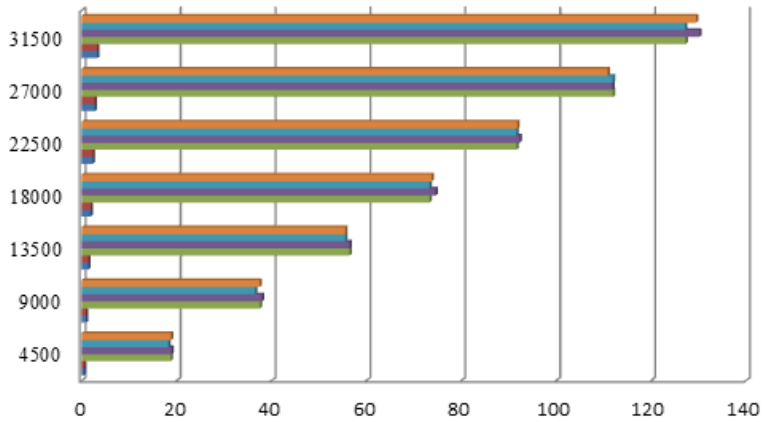
Сурет 5. ESP 32 мен microSD картасын байланыстыру сызбасы



Сурет 6. DFRobot Beetle BLE мен microSD картасын байланыстыру сызбасы

Сурет 7. ATmega2560 пен microSD картасын байланыстыру сызбасы

4500, 9000, 13500, 18000, 22500, 27000, 31500 өлшемді мәтінді AtmelAVR ядросына негізделген әртүрлі өнімділіктегі микроконтроллерлерде алгоритмнің өнімділігіне тестілеу жұмыстары жүргілді. Тестілеудің нәтижесі 8-суретте көрсетілген.



	4500	9000	13500	18000	22500	27000	31500
Arduino Uno-да дешифрлеу (с)	18,9	37,5	55,6	73,8	91,8	110,9	129,5
Arduino Uno-да шифрлеу (с)	18,33	36,6	55,6	73,32	91,63	112	127,2
DFRobot Beetle BLE -де дешифрлеу(с)	19	38	56,5	74,6	92,3	111,9	130,2
DFRobot Beetle BLE -де шифрлеу (с)	18,8	37,6	56,5	73,32	91,65	112	127,36
ESP32-де дешифрлеу (с)	0,5	0,95	1,423	1,89	2,34	2,79	3,29
ESP32-де шифрлеу (с)	0,47	0,94	1,42	1,88	2,35	2,8	3,28

Сурет 8. Айнымалысы бар көпмүшелер сақинасындағы гомоморфты шифрлауды әр-түрлі микроконтроллерде тестілеу

Тестілеу нәтижесінде алгоритмінің уақыты сызықты өсетінін көруге болады.

	ATmega2560	ATmega32u4	Atmega328	DFRobot Beetle BLE	ESP32
МК-дің істен шығу қарқындылығы $\lambda_i = \frac{1}{T_i}$	$1{,}1 * 10^{-5}\frac{1}{\text{сағ}}$	$9{,}09 * 10^{-6}\frac{1}{\text{сағ}}$	$1{,}05 * 10^{-5}\frac{1}{\text{сағ}}$	$9{,}6 * 10^{-6}\frac{1}{\text{сағ}}$	$8{,}3 * 10^{-6}\frac{1}{\text{сағ}}$
Тоқтаусыз жұмыс істеу ықтималдығы $P(t) = e^{-\lambda t}$ $t = 2000$ сағ	0,978	0,982	0,979	0,98	0,983
t уақытындағы істен шығудың орташа саны $a = \lambda_i t$	0,02222	0,01818	0,021052	0,0190476	0,016666
Бір істен шығу ықтималдығы: $P_1(2000)$	$\frac{0{,}02222^{\,1}}{1} e^{-0{,}02222} = 0{,}217$	$\frac{0{,}01818^{1}}{1} e^{-0{,}01818} = 0{,}0178$	$\frac{0{,}021052^{1}}{1} e^{-0{,}021052} = 0{,}2$	$\frac{0.0190476^{\,1}}{1} e^{-0.01904} = 0{,}0187$	$\frac{0.0.016666^{\,1}}{1} e^{-0.0166} = 0{,}0164$
Екі істен шығу ықтималдығы : $P_2(2000)$	$\frac{0{,}02222^{\,2}}{2} e^{-0{,}02222} = 0{,}0002$	$\frac{0{,}01818^{2}}{2} e^{-0{,}01818} = 0{,}00016$	$\frac{0{,}021052^{2}}{2} e^{-0{,}021052} = 0{,}0002$	$\frac{0.0190476^{\,2}}{2} e^{-0.01904} = 0{,}00018$	$\frac{0.0.016666^{\,2}}{2} e^{-0.0166} = 0{,}00014$

Сурет 9. Микроконтроллердің сенімділігін бағалауды есептеу

AtmelAVR ядросына негізделген әртүрлі өнімділіктегі микроконтроллерлердің сенімділігін бағалау нәтижесінде 2000 сағат ішінде жұмыс істемеу ықтималдығы орта есеппен 98% құрады, бұл дұрыс жұмыс істеген кезде осы құрылғының жоғары сенімділігін көрсетеді.

Қорытынды

Толық гомоморфты шифрлау алгоритмі құрылды: С.Ф. Кренделевтің айнымалысы бар көпмүшелер сақинасындағы гомоморфты шифрланған мәліметтерге бөлу және азайту операциялары жүзеге асырылды. ДК және микроконтроллерлерде толық гомоморфты шифрлау алгоритмдерінің нәтижелері талданып, бағаланды. ДК-не және микроконтроллер үшін ұсынылған әдістер мен құрылған алгоритм негізінде кітапхана құрылды. Микроконтроллердің сенімділігін бағалау есептелінді.

References:

1 Joseph Yiu "The Arduino is a microcontroller board composed of an integrated circuit that carries out the functions of a computer processing unit", 2022 Materials Science and Engineering: R: Reports

2 B. Burtyka The Techniques for Arbitrary Secure Quering to Encrypted Cloud Database Using Fully Homomorphic Encryption. IT Security. № 2(2017) http://dx.doi.org/10.26583/bit.2017.2.03

3 N.P. Smart and F. Vercauteren, "Fully homomorphic encryption with relatively small key and ciphertext sizes, public Key Cryptography," PKC Springer Berlin Heidelberg, vol. 6056, pp. 420-443, 2010

4 Gentry Craig. A fully homomorphic encryption scheme, A dissertation submitted to the department of computer science and the committee on graduate students of Standford University, 2009.

5 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.

6 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

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

8 Gourab Sen Gupta New Frontiers of Microcontroller Education: Introducing SiLabs ToolStick University Daughter Card. IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (sutc 2008) https://doi.org/10.1109/SUTC.2008.35