МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

РАХМА МОХАММЕД КАДІМ РАХМА

УДК 004.31

МОДЕЛІ ТА МЕТОДИ ПОБУДОВИ ОПЕРАЦІЙНИХ ВУЗЛІВ ДЛЯ ПОЛІВ ГАЛУА, ЯКІ ВИКОРИСТОВУЮТЬСЯ ПРИ КРИПТОГРАФІЧНОМУ ЗАХИСТІ ІНФОРМАЦІЇ НА ОСНОВІ ЕЛІПТИЧНИХ КРИВИХ

05.13.05 – Комп’ютерні системи та компоненти

Автореферат дисертації на здобуття наукового ступеня
кандидата технічних наук.

Львів-2019

Дисертацією є рукопис.

Роботу виконано в Національному університеті «Львівська політехніка» Міністерства освіти і науки України

Науковий керівник: доктор технічних наук, професор
Глухов Валерій Сергійович,
професор кафедри електронних обчислювальних машин
Національного університету «Львівська політехніка»,

Офіційні опоненти: доктор технічних наук, професор
Николайчук Ярослав Миколайович,
завідувач кафедри спеціалізованих комп'ютерних систем
Тернопільського національного економічного університету,

доктор технічних наук, професор
Потій Олександр Володимирович,
професор кафедри безпеки інформаційних систем і технологій
Харківського національного університету ім. В. Н. Каразіна.

Захист відбудеться 29 листопада 2019 р. об 15:00 годині на засіданні спеціалізованої вченої ради **Д 35.052.08** при Національному університеті «Львівська політехніка» за адресою: 79013, м. Львів, вул. С.Бандери, 28[а], ауд. 711 5-го навчального корпусу.

З дисертацією можна ознайомитися у бібліотеці Національного університету «Львівська політехніка» (79013, Львів, вул. Професорська, 1)

Автореферат розіслано 28 жовтня 2019 року.

Вчений секретар
спеціалізованої вченої ради д.т.н., проф. Луцик Я. Т.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Сучасний етап розвитку комп'ютерних технологій характеризується виникненням, розвитком і впровадженням кіберфізичних систем (КФС), а також підготовкою до появи серійних квантових комп'ютерів. Поява і розвиток КФС, однією з головних рис яких є використання бездротових технологій, гостро ставить питання захисту інформації, яку опрацьовують ці системи. Постійне зростання продуктивності комп'ютерів, поява нових технологій та алгоритмів, впровадження нової елементної бази може бути використано зловмисниками для порушення інформаційної безпеки. Це зумовлює необхідність пошуку нових, більш надійних методів криптографічного захисту інформації (КЗІ) та маскування їхньої роботи. Бажано, щоб ці методи ґрунтувалися на вже відомих технологіях і засобах і покращували їхню дієвість. Сьогодні одним з методів КЗІ є використання цифрових підписів, які базуються на алгоритмах опрацювання точок еліптичних кривих (ЕК) і елементів розширених двійкових $GF(2^m)$ та простих $GF(p)$ полів Галуа. Можливості квантових комп'ютерів роблять небезпечним використання існуючих алгоритмів, що базуються на використанні ЕК. Хоча потужні квантові комп'ютери ще не з'явилися, вже ведеться пошук алгоритмів КЗІ, які залишаться надійними і в еру квантових комп'ютерів. Одним із можливих методів є метод, що базується на використанні ізогеній суперсингулярних ЕК у полі Галуа $GF(2^m)$, для обчислення яких використовуються ті ж самі операції, що і в сучасних алгоритмах цифрового підпису, які базуються на використанні полів Галуа $GF(2^m)$. Крім двійкових полів $GF(2^m)$ можна використовувати й інші розширені поля Галуа $GF(p^n)$, такі, що $2^m \approx p^n$. При опрацювання кодів елементів згаданих полів Галуа необхідно виконувати опрацювання двійкових кодів, довжина яких приблизно дорівнює m (за сучасними стандартами m може досягати значення 1000). Саме в опрацюванні таких кодів полягає призначення операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК, та які утворюють назву цієї дисертаційної роботи. І в даній роботі розв'язується важливе науково-технічне завдання - здійснюється наукове обґрунтування доцільності застосування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК, визначення полів, які найкраще використовувати для вирішення цього завдання, а також створення методів та засобів проєктування і порівняння згаданих вузлів. Особливістю алгоритмів КЗІ є їхня багаторівнева структура, де на різних рівнях виконуються специфічні математичні операції над багаторозрядними кодами: операції над елементами простих $GF(p)$ та розширених $GF(p^m)$ полів Галуа, операції над точками еліптичних кривих. В залежності від умов використання необхідно забезпечувати конфігурацію операційних пристроїв, які реалізують вказані алгоритми: забезпечувати зміну поля Галуа, базису для представлення елементів поля, зміну еліптичної кривої**.**

В Україні використання операцій над елементами полів Галуа регулюється стандартами опрацювання цифрових підписів ДСТУ 4145-2002 та ДСТУ ISO/IEC 15946-1: 2015, в основу яких покладено операції над точками несингулярних еліптичних кривих у полі Галуа $GF(2^m)$. Популярність цього математичного апарату обумовлена можливістю застосовування відносно невеликої довжини ключа і блоку

перетворень по відношенню до інших алгоритмів. Це дає змогу при однакових апаратних витратах на реалізацію пристрою збільшити надійність цифрового підпису. Тому актуальним залишається питання мінімізації обчислювальної, апаратної, часової, структурної та програмної складностей. Хоча на сьогоднішній день стандарт дозволяє забезпечити більш ніж достатній рівень захисту, але, зважаючи на швидкий розвиток техніки і математики, перспективи появи і використання квантових комп'ютерів, актуальною також залишається необхідність його розвитку. Стандарт обмежується максимальним степенем поля 509, у той час як міжнародним стандартом рекомендуються до використання поля в оптимальному нормальному базисі з степенем розширення основного поля до 998.

На сучасному етапі, коли КЗІ впроваджуються у КФС, важливим стає забезпечення їх роботи у реальному масштабі часу. Це вимагає використання швидкодіючих апаратних рішень – спецпроцесорів, які реалізуються в програмовних логічних інтегральних схемах (ПЛІС).

Вищесказане визначає актуальність створення методів і засобів проєктування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК. І в роботі пропонуються рішення цього завдання.

Зв'язок роботи з науковими програмами, планами, темами. Дисертація відповідає науковому напряму кафедри електронних обчислювальних машин: "Питання теорії, проєктування та реалізації комп'ютерних систем та мереж, а також комп'ютерних засобів, вузлів, приладів і пристроїв вимірювальних, інформаційних, керуючих телекомунікаційних та кіберфізичних систем" та виконувалась в межах держбюджетної науково-дослідної роботи ДБ/КІБЕР «Інтеграція методів і засобів вимірювання, автоматизації, опрацювання та захисту інформації в базисі кібер-фізичних систем» (номер державної реєстрації 0115U000446).

Мета і задачі дослідження. Метою дисертаційної роботи є наукове обґрунтування доцільності застосування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК, визначення полів, які найкраще використовувати для вирішення цього завдання, а також створення методів та засобів проєктування і порівняння згаданих вузлів.

Для досягнення поставленої мети слід вирішити задачі:

провести системний аналіз сучасного стану теорії, методів та засобів проєктування спеціалізованих комп'ютерів, пристроїв КЗІ, аналіз найбільш важливих відкритих стандартів та алгоритмів для них, узагальнених структур спецпроцесорів (СП);

визначити основні архітектурні принципи побудови та розробити узагальнену модель операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК;

розробити метод оцінювання складності моделей помножувачів елементів розширених полів Галуа $GF(p^m)$ та метод оцінювання складності злому апаратних засобів КЗІ;

вдосконалити метод маскування роботи апаратних вузлів знаходження обернених елементів у двійкових полях Галуа $GF(2^m)$ у поліноміальному базисі;

вдосконалити метод вбудованого тестування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК ;

розробити технологічний засіб (генератор ядер) для проєктування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК;

розробити уточнені структуровані моделі у вигляді VHDL-описів операційних пристроїв, в тому числі інверторів, які маскують роботу засобів КЗІ;

провести експериментальне дослідження та впровадження розроблених операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК.

Об'єкт дослідження – операційні вузли для полів Галуа, які використовуються при КЗІ на основі ЕК.

Предмет дослідження – методи та засоби структурної організації операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК, методи та засоби проєктування, порівняння, синтезу та маскування роботи таких пристроїв.

Методи дослідження. Виконані дослідження використовують результати, отримані з прикладної теорії цифрових автоматів стосовно структурного синтезу й логічного проєктування цифрових пристроїв, з теоретичної моделі взаємозв'язку відкритих систем. Також використано і розвинуто: комп'ютерні методи виконання математичних операцій у простих та розширених полях Галуа у поліноміальному базисі, комп'ютерні методи виконання операцій над точками еліптичних кривих. У проведених дослідженнях широко використовується математичний апарат теорії алгоритмів, апарат теорії чисел, а також засоби моделювання цифрових схем.

Наукова новизна одержаних результатів полягає в наступному.

- 1) вперше запропоновано метод оцінювання складності моделей помножувачів елементів розширених полів Галуа $GF(p^m)$, який базується на представленні помножувача для поліноміального базису як матриці модифікованих комірок Гілда і дозволяє визначити поля Галуа $GF(p^n)$ з приблизно однаковим порядком, у яких моделі будуть мати найменше значення складності (часової, ємнісної, структурної, програмної, а також апаратної);
- 2) вперше запропоновано метод оцінювання складності злому апаратних засобів КЗІ, у якому прийнято, що засоби КЗІ реалізовано апаратно, а засоби злому – програмно, і який дозволяє визначити поля Галуа $GF(p^m)$ з приблизно однаковим порядком, у яких злом засобів КЗІ буде виконуватися найдовше;
- 3) вперше запропоновано метод маскування роботи апаратних вузлів знаходження обернених елементів у двійкових полях Галуа $GF(2^m)$ у поліноміальному базисі, який полягає у використанні незалежних від значення операндів алгоритмів знаходження обернених елементів і який дозволяє зменшити витоки інформації із засобів КЗІ сторонніми каналами;
- 4) отримав подальший розвиток метод вбудованого тестування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК, який, на відміну від відомих методів, полягає у введенні до моделі вузла детектора заборонених значень окремих розрядів кодів елементів полів Галуа, що дає можливість виявляти частину апаратних помилок.

Практичне значення одержаних результатів. Отримані у дисертаційній роботі наукові результати створюють методологічну базу для розроблення операційних

вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК, які дозволяють підвищити надійність, достовірність та захищеність сучасних апаратних засобів КЗІ.

Практична цінність дисертаційної роботи полягає у тому, що за результатами теоретичних та експериментальних досліджень для конфігуровних операційних пристроїв, які опрацьовують елементи розширених полів Галуа:

створено і апробовано технологічний засіб (генератор ядер) для проєктування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК;

створено та перевірено уточнені структуровані моделі у вигляді VHDL-описів операційних пристроїв, в тому числі інверторів, які маскують роботу засобів КЗІ;

визначено найкращі для використання розширені поля Галуа, за сукупністю показників найращим є розширене поле з характеристикою 3.

Наукові положення та висновки дисертації успішно використано під час виконання проєктних робіт на фірмі AL-NABAA Network Solution L.L.C. (Багдад, Ірак), що підтверджено відповідним Актом, та при проведенні держбюджетної науково-дослідної роботи ДБ/КІБЕР «Інтеграція методів і засобів вимірювання, автоматизації, опрацювання та захисту інформації в базисі кібер-фізичних систем» (номер державної реєстрації 0115U000446), що також підтверджено відповідним Актом).

Також результати дисертаційної роботи використано на кафедрі електронних обчислювальних машин Інституту комп'ютерних технологій, автоматики та метрології Національного університету «Львівська політехніка» при підготовці і викладанні курсів лекцій та лабораторних робіт навчальної дисципліни «Дослідження і проєктування комп'ютерних систем та мереж» (для освітньо-кваліфікаційного рівня «Магістр», спеціальність 123 «Комп'ютерна інженерія», спеціальностей «Комп'ютерні системи та мережі», «Кіберфізичні системи» та «Системне програмування»)

Особистий внесок здобувача. Усі основні положення, що становлять суть дисертації, отримано автором самостійно і повністю розкрито у публікаціях (Додаток Р). У публікаціях, що написано в співавторстві, автору дисертації належать основні теоретичні та практичні результати (методи і підходи до рішення поставлених задач). Зокрема, [21], [44], [70] – запропоновано модель помножувача елементів розширених полів Галуа для визначення його часової складності та метод її визначення, проведено дослідження та аналітичне опрацювання та узагальнення їхніх результатів; [75], [45], [71], [152]– запропоновано модель модифікованої комірки Гілда та помножувача елементів полів Галуа на її основі у поліноміальному базисі для визначення структурної складності помножувача та метод її визначення, проведено дослідження та аналітичне опрацювання й узагальнення їхніх результатів; [153]– запропоновано алгоритми знаходження обернених елементів полів Галуа у поліноміальному базисі, моделі вузлів та VHDL-описи, які реалізують дані алгоритми з різними типами помножувачів елементів полів Галуа, які характеризуються незалежним від кодів операндів часом обчислення; [156]- теоретичне обґрунтування можливості вирівнювання часу обчислення обернених елементів у поліноміальному базисі двійкових розширених полів Галуа на основі біт-паралельних помножувачів, моделі пристроїв та методи їх використання для обчислення обернених елементів; [157] – запропоновано метод оцінювання часової

складності помножувачів елементів розширених полів Галуа на універсальних комп’ютерах і графічних процесорах з врахуванням виконання ними векторних операцій; [158] - запропоновано метод оцінювання часової складності засобів КЗІ при їхній апаратній реалізації та використанні для злому універсальних комп’ютерів (програмної реалізації злому); [159] - запропоновано метод визначення ефективності апаратних реалізацій алгоритмів постквантової криптографії на основі еліптичних кривих, проведено дослідження та аналітичне опрацювання й узагальнення їхніх результатів; [43], [73] – визначено розширені поля Галуа, які є найбільш тестопридатними для організації вбудованого контролю операційних вузлів та вдосконалено метод формування ознаки збою.

Апробація результатів дисертації. Основні положення та результати роботи доповідалися і обговорювалися на таких наукових конференціях та семінарах:

V Міжнародний молодіжний науковий форум “Litteris et Artibus”. 26–28 листопада, 2015. Україна, Львів; International Youth Science Forum ”Litteris et Artibus”, November 24-26, 2016, Lviv, Ukraine; International Youth Science Forum ”Litteris et Artibus”, November 23-25, 2017, Lviv, Ukraine; 2-а Міжнародна науково-технічна конференція «Електротехнічні і комп'ютерні системи: теорія і практика (Елтекс 2016)», м. Одеса, 26–28 червня 2016 р.; Другий науковий семінар Кіберфізичні системи: досягнення та виклики, Львів, Національний університет «Львівська політехніка», 21-22 червня 2016 р.; Третій науковий семінар Кіберфізичні системи: досягнення та виклики, Львів, Національний університет «Львівська політехніка», 13-14 червня 2017 р.; Міжнародна науково-технічна конференція «Електротехнічні і комп'ютерні системи: теорія і практика (ЕЛТЕКС-2017). Одеса, Одеський національний політехнічний університет. 26 – 28 червня 2017 р.; 4th International Workshop on Theory of Reliability and Markov Modeling for Information Technologies (WS TheRMIT 2018, in frameworks of the 14th International Conference ICTERI2018). May 14, 2018, Kyiv; 9th International IEEE Conference Dependable Systems, Services and Technologies DESSERT’2018. Kyiv, May 24-27; Міжнародна науково-технічна конференція «Електротехнічні і комп'ютерні системи: теорія і практика ЕЛТЕКС – 2018, м. Одеса, Одеський національний політехнічний університет. 29 травня – 1 червня 2018 року; International Conference "Advanced Computer Information Technologies", June 1-3, 2018 in Ceske Budejovice, Czech Republic

Публікації. Основні положення дисертаційної роботи висвітлені у 16 наукових публікаціях, з яких : 1 колективна монографія: 2 статті у наукових фахових виданнях України, які включено до міжнародної науково-метричної бази РІНЦ, 4 статті у наукових фахових виданнях України, 8 матеріалів наукових конференцій та семінарів.

Структура та обсяг роботи. Дисертаційна робота складається з вступу, чотирьох розділів, висновків, списку використаних джерел і додатків. Роботу викладено на 191 сторінках, з них сторінок основного тексту - 126. Робота містить рисунків - 45, таблиць - 33, додатків - 16. Найменувань у списку використаних джерел - 209.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **Вступі** викладено сучасний стан завдання, обґрунтовано актуальність побудови операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК, сформульовано мету та задачі досліджень, описано основні наукові результати та показано їх практичне значення, представлено зв'язок роботи з науковими програмами, планами, темами. Наведено відомості про апробацію, публікації та використання результатів досліджень.

У **першому** розділі проведено системний аналіз сучасного стану теорії, методів та засобів проєктування спеціалізованих комп'ютерів, пристроїв КЗІ, аналіз найбільш важливих відкритих стандартів та алгоритмів для них, узагальнених структур спецпроцесорів (СП).

У розділі розглянуто сучасний стан розвитку комп'ютерних систем, який характеризується виникненням кіберфізичних систем (КФС). Розглянуто алгоритмічні основи проєктування комп'ютерних засобів КФС. Виділено програмно-апаратну SH-модель алгоритму. Відмічено переваги апаратних реалізацій алгоритмів.

Серед методів забезпечення захисту інформації КФС розглянуто криптографію еліптичних кривих, з її націленістю на опрацювання електронних цифрових підписів. Визначено вплив технологій квантових обчислень на використання еліптичних кривих у КЗІ. З цієї точки зору також розглянуто криптографію ізогеній суперсингулярних еліптичних кривих, яка може протистояти використанню квантових комп'ютерів.

Розглянуто використання розширених полів Галуа $GF(p^m)$ як математичної основи електронних цифрових підписів та методи оцінювання складності пристроїв опрацювання елементів полів Галуа.

Як елементну базу для побудови згаданих вузлів розглянуто ПЛІС, ядра (VHDL-описи моделей функціональних вузлів) для них та генератори ядер як основу елементної база спеціалізованих комп'ютерних систем. З цією метою проаналізовано методи генерації описів функціональних вузлів.

З метою забезпечення якості засобів КЗІ розглянуто можливості використання математичних пакетів для проведення обчислень у розширених полях Галуа. Найкращим визначено пакет Maple (Waterloo Maple Inc.). Розглянути необхідність маскування роботи засобів КЗІ як один з методів захисту від атак на них.

Другий розділ присвячено вибору та обґрунтуванню напряму досліджень та проєктування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК, у розділі наведено методи вирішення поставлених задач, визначено загальну методику проведення досліджень. Також виконується наукове обґрунтування доцільності застосування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК, визначення полів, які найкраще використовувати для вирішення цього завдання, а також створення методів та засобів проєктування і порівняння згаданих вузлів.

На сучасному етапі, коли КЗІ впроваджуються у КФС, важливим стає забезпечення їх роботи у реальному масштабі часу. Це вимагає використання швидкодіючих апаратних рішень – спецпроцесорів, які реалізуються в програмовних

логічних інтегральних схемах (ПЛІС). Як базу для проєктування засобів КЗІ взято багаторівневий спецпроцесора (СП), який при опрацюванні цифрових підписів виконує операції над точками еліптичних кривих.

Від сучасних комп'ютерних засобів вимагається дотримування принципів побудови відкритих систем, що орієнтує на використання відкритих стандартів. Вирішення завдань захисту від несанкціонованого використання і від пошкодження інформації відомі і широко використовується на практиці. Але сучасні методи, які базуються на використанні розширених полів Галуа $GF(p^m)$, де $p > 2$, та суперсингулярних еліптичних кривих і які здатні протистояти використанню квантових комп'ютерів з метою злому системи захисту, на сьогоднішній день розроблено недостатньо, особливо це стосується апаратних методів.

Першим кроком розв'язання поставленої задачі є вибір поля Галуа $GF(p^m)$, яке забезпечить створення операційних вузлів з найкращими характеристиками в порівняння з іншими полями. Для цього необхідно порівнювати вузли, створені для різних полів – порівнювати їхні складності. Щоб не порівнювати кожний вузол з аналогічними вузлами інших полів, пропонується за базу для порівняння взяти вузли для полів, які на сьогоднішній день найширше використовуються – для двійкових розширених полів $GF(2^M)$. При цьому обов'язково повинна дотримуватися умова – усі розширені поля Галуа повинні бути з приблизно однаковою кількістю елементів (з приблизно однаковим порядком), тобто, $p^m \approx 2^M$.

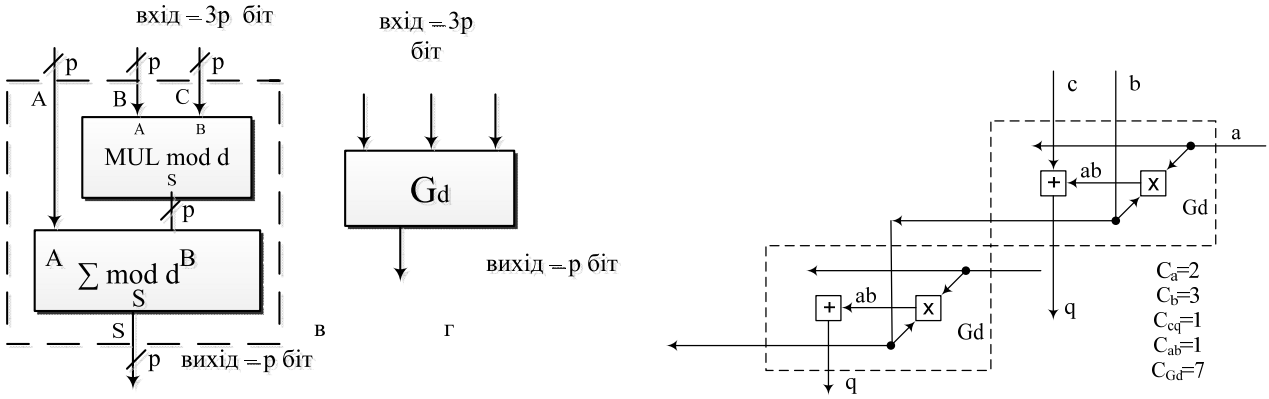
Метод оцінювання складності моделей помножувачів елементів розширених полів Галуа $GF(p^m)$ пропонується як метод знаходження розширеного поля Галуа, у якому обрані характеристики СП будуть найкращими, що забезпечить створення СП для «найкращого» поля (далі цей термін буде вживатися без лапок). Підхід базується на оцінювання складностей одного з найважливіших вузлів СП - помножувача.

Порядок застосування методу: обирається розширене поле Галуа; обирається базис представлення елементів полів Галуа; обираються базові елементи помножувача; обирається структура базових елементів; обирається структура помножувача; проводиться аналіз обраного типу складності, відносні значення параметрів складності формуються по відношенню до аналогічних параметрів розширеного двійкового поля; дослідження повторюються для всіх обраних для аналізу розширених полів Галуа; фіксуються результати дослідження; визначається найкраще поле.

Для використання в помножувачах елементів розширених полів Галуа для поліноміального базису відома модифікована комірка Гілда (рис. 1, а).

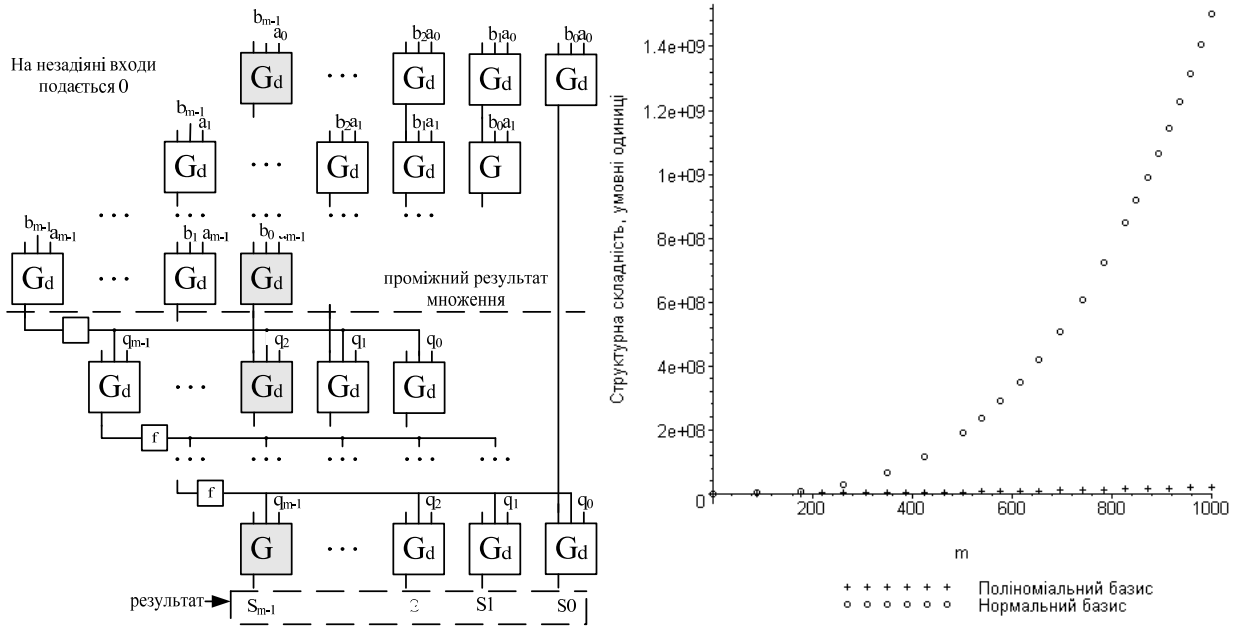
Як складові частини метод містить наступні методи, на яких проводиться аналіз обраного типу складності.

1. Метод оцінювання часової складності моделей помножувачів елементів розширених полів Галуа $GF(p^m)$. Запропонований метод передбачає оцінювання помножувачів для розширених полів Галуа $GF(d^m)$ з характеристиками $d \geq 2$, і з приблизно однаковою кількістю елементів $d^m \approx 2^n$ ($m \approx log_d 2^n = \frac{n}{log_2 d}$) для визначення поля, в якому помножувач буде мати найменшу часову складність.



а б

Рис. 1. Модифікована комірка Гілда (а) та її топологія (б)



а б

Рис. 2. Помножувач на основі модифікованих комірок Гілда для GF(p^m) (а). Структурна складність помножувачів для поліноміального та нормального базисів у полі GF(p^m) (б)

Для аналізу обрано паралельний помножувач на основі модифікованих комірок Гілда (рис. 2, а), поліноміальний базис. Тоді найбільша затримка виникає під час формування розряду Sm-1 (рис. 2, а). Вона складається із затримок послідовно з'єднаних комірок Гілда, що утворюють вертикальний стовпчик, на виході якого формується розряд S_{m-1}. Ця найбільша затримка $t_{Mul} = 2mt_G$, де t_G – затримка сигналів однією коміркою Гілда. Аналіз було проведено для двох представлень модифікованої комірки Гілда.

А) Формальний підхід до визначення часової складності модифікованої комірки Гілда. При формальному підході комірка Гілда розглядається як «чорна скринька» з відомою кількістю входів та виходів і з невідомою внутрішньою структурою. Це відповідає табличному методу обчислення (у даному випадку – множення) і реалізації помножувача у вигляді ПЗП на основі LUT. LUTv має v

входів та 1 вихід і може бути запрограмований на реалізацію довільної логічної функції v змінних.

Відносно часової складності розширеного двійкового поля Галуа GF(2^m) часова складності розширеного поля Галуа GF(d^n) (відносна часова складність $R_{d,2} = \frac{C_{t,2}}{C_{t,d}} = \frac{log_2 d}{(3\lceil log_2 d \rceil - v + 1)}$, $R_{2,2} = 1$. $R_{d,2} = \frac{C_{t,2}}{C_{t,d}} = \frac{log_2 d}{(3\lceil log_2 d \rceil - 3)}$ для v=4, $R_{d,2} = \frac{C_{t,2}}{C_{t,d}} = \frac{log_2 d}{(3\lceil log_2 d \rceil - 5)}$ для v=6. Якщо $R_{d,2} > 1$, то розширене поле з характеристикою d має меншу часову складність в порівнянні із розширеним двійковим полем. Як видно, перевагу перед двійковим полем має тільки поле з характеристикою d=3 (серед простих характеристик) при використанні LUT6 з 6 входами (рис. 3, а).

Б) Визначення часової складності модифікованої комірки Гілда з врахуванням її внутрішньої структури (помножувача і суматора за модулем d).

Тоді часова складності розширеного поля Галуа GF(d^n) (відносна часова складність) $R_{d,2} = \frac{C_{t,2}}{C_{t,d}} = \frac{log_2 d}{2(2\lceil log_2 d \rceil - v + 1)}$, $R_{2,2} = 1$. $R_{d,2} = \frac{C_{t,2}}{C_{t,d}} = \frac{log_2 d}{2(2\lceil log_2 d \rceil - 3)}$ для v=4, $R_{d,2} = \frac{C_{t,2}}{C_{t,d}} = \frac{log_2 d}{2(2\lceil log_2 d \rceil - 5)}$. для v=6. Тоді перевагу перед двійковим полем мають поля з простими характеристиками GF(5^n) та GF(7^n) при використанні LUT6 з v=6 входами та поля GF(11^n) та GF(13^n) для LUT8 з v=8 входами) (рис. 3, б).

2. Оцінювання структурної складності моделей помножувачів елементів розширених полів Галуа $GF(p^m)$ у нормальному та поліноміальному базисах.

Структурну складність моделі помножувача можна оцінити загальною довжиною L з'єднань його топології на умовній ПЛІС. Показано, що для паралельного помножувача структурна складність $C \approx (k+1)m^3, k = ½ \ldots ¾$.

Аналіз структурної складності паралельного помножувача для поліноміального базису будується на представленні топології з'єднань всередині умовної ПЛІС двох сусідніх модифікованих комірок Гілда (рис. 1). У роботі показано, що структурна складність для паралельних помножувачів для поліноміального базису для великих m (m прямує до 1000) $C_{PB} \approx 20m^2$.

Для степенів m < 12 двійкових полів Галуа $GF(2^m)$ меншу структурну складність мають помножувачі для роботи у нормальному базисі. Для $m >> 12$ використання поліноміального базису дає зменшення структурної складності в порівнянні з нормальним базисом приблизно в m разів (рис. 2, б).

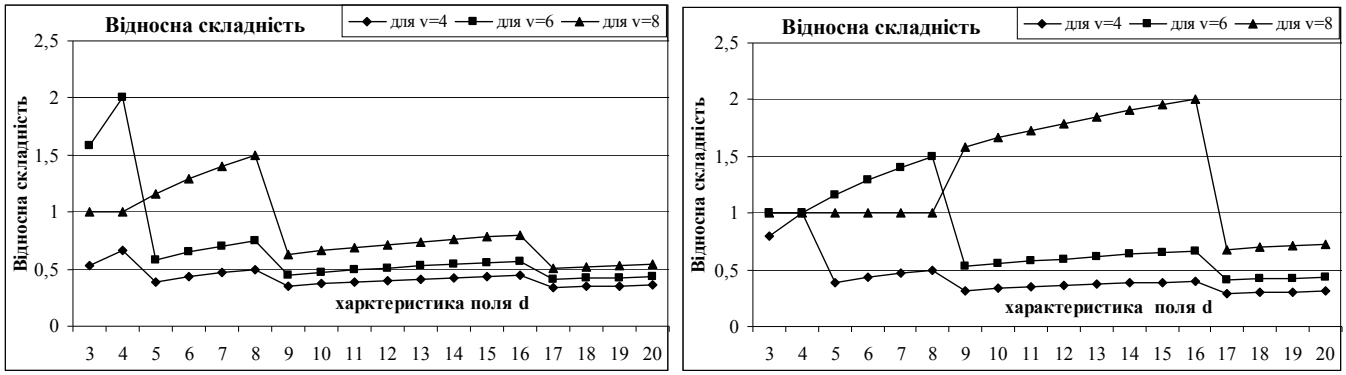
3. Оцінювання ємнісної складності моделей помножувачів елементів розширених полів Галуа $GF(p^m)$.

Довжина коду одного елемента розширеного двійкового поля GF(2^{998}) дорівнює 998 біт. Для полів GF(d^m) з порядком $d^m \approx 2^{998}$ довжина коду елемента $LC = m/\lceil \log_2 d \rceil$ (рис. 4) показана як приріст довжини відносно довжини коду елементів двійкового поля. З точки зору ємнісної складності найкраще використовувати двійкові та прості поля Галуа, але використання інших полів не приведе до збільшення довжина кодів (ємнісної складності) більше ніж на 30 %.

4. Метод оцінювання складності злому апаратних засобів КЗІ

Етапи запропонованого методу:

1) Оцінка програмно-часової складності Сп помножувачів для поліноміального базису. Для комп'ютерів загального призначення необхідно оцінити відносну програмно-часову складність через час виконання основної операції при зломі - час множення елементів полів Галуа для розширених полів з різними основами, але з приблизно однаковою кількістю елементів поля (рис. 5, а).



А Б

Рис. 3. Відносні часові складності для випадків А та Б

Рис. 4. Відносні довжини кодів елементів полів GF(d^m), в процентах

2) Оцінка апаратно-часової складності Са помножувачів у полях Галуа. Реалізовані в ПЛІС апаратні помножувачі для розширених полів Галуа *GF(dm)* з приблизно однаковою кількістю елементів $dm \approx 2n$ аналізуються з точки зору їх часової складності для визначення полів (рис. 5, б).

3) Оцінка часової складності апаратного захисту інформації і програмного злому захисту Сз = Сп/Са. (рис. 5, в).

З проведених досліджень ємнісної, структурної та часової складності помножувачів елементів розширених полів Галуа з приблизно однаковим порядком, а також з врахуванням відомих результатів оцінювання апаратної складності помножувачів, видно, що найкращими полями для побудови апаратних помножувачів є трійкове та двійкове розширені поля Галуа, а також поля з характеристиками 5 та 7. Складність криптоаналізу криптосистеми на основі ізогеній суперсингулярних кривих, що працює в полі $GF(p^m)$, з використанням квантових комп'ютерів складає $O(\sqrt[6]{p})$. Для збільшення стійкості необхідно

збільшувати *p*, що зменшує ефективність апаратної реалізації і збільшує ефективність програмних реалізацій.

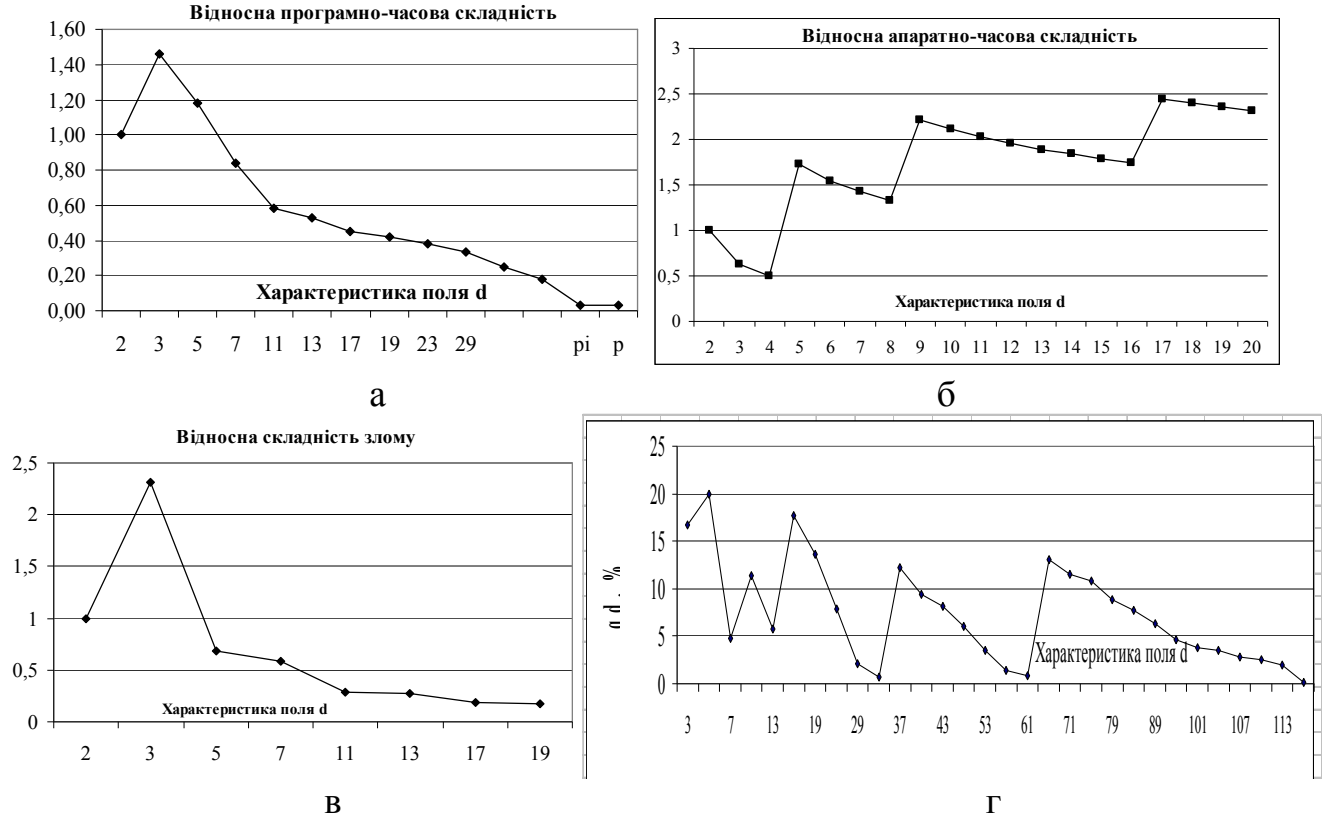


Рис. 5. Відносні складність, а - програмно-часова Сп помножувача, б – апаратно часова складність Са помножувача, в – складність злому Сз = Сп/Са.
г - Зважена тестопридатність полів $GF(d^m)$, %

Також запропоновано вдосконалений метод вбудованого тестування операційних вузлів для полів Галуа, що використовуються при КЗІ на основі еліптичних кривих. Кожний розряд коду елемента розширеного поля Галуа $GF(d^m)$ представляється $n_b = \lceil \log_2 d \rceil$ бітами, за допомогою яких можна закодувати $d_t = 2^{\lceil \log_2 d \rceil} \geq d$ різних кодових комбінацій. При цьому залишається $d_d = d_t - d$ кодових комбінацій, які ніколи не будуть зустрічатися при опрацюванні елементів полів Галуа при нормальній роботі процесорних вузлів, вузлів пам'яті та каналів передачі даних. Ці невикористані (заборонені) кодові комбінації можна задіяти для проведення контролю роботи засобів КЗІ, в ході виконання ними їхніх основних функцій (вбудованого тестування). І можна оцінити зважену тестопридатність qd = 100*dd/(dnb) для полів, які мають заборонені значення кодів (рис. 5, г). Оскільки мінімальна кодова відстань Хеммінга d_H зв'язана з кількістю *k* помилок, які можна виявити, співвідношенням $d_H \geq k + 1$, а при використанні будь-якого поля Галуа $GF(p^m)$ кодова відстань для кодів кожної цифри коду $d_{Hd} = 1$, то кількість помилок, які можна виявити в розглянутих полях, $0 \geq k$. Такий висновок говорить про те, що виявити 100 % усіх, навіть поодиноких, помилок неможливо. Результати (рис. 5, г) необхідно розглядати як оцінку частки помилок, які можна виявляти запропонованим методом.

Запропоновано табличний спосіб опису ознаки виникнення помилкових кодів. Задача синтезу ознаки помилки *Errori* є окремим випадком відомої задачі мінімізації

функції багатьох змінних. Розв'язок полегшується тим, що двійкові набори (заборонені коди), які підлягають мінімізації, розташовано послідовно і їхні коди відрізняються один від одного на +1. Приклад отримання ознаки $Error_1 = I_0 \vee I_1 \vee ... \vee I_7 = \overline{A_{16}} A_{14} A_{11} A_9 A_8 A_7 A_3 A_2 A_1 A_0 \vee \overline{A_{16}} A_{14} A_{11} A_9 A_8 A_7 A_4 \vee ... \vee \overline{A_{16}} A_{15}$ для діапазону хибних кодів від 04B8F до 0FFFF наведено в роботі.

У розділі представлено метод маскування роботи апаратних вузлів знаходження обернених елементів у двійкових полях Галуа $GF(2^m)$ у поліноміальному базисі.

Розвиток методу маскування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК полягає у вирівнюванні часу обчислення обернених елементів у поліноміальному базисі шляхом відмови від використання узагальненого алгоритму Евкліда на користь алгоритмів прямого двійкового ділення або експоненціальних алгоритмів. Використання експоненційних алгоритмів вимагає ефективного виконання операцій піднесення до квадрату або знаходження квадратного кореня. Тобто, метод передбачає введення до складу GF-процесора додаткових вузлів – квадратора і(або) вузла знаходження квадратного кореня. Маскування шляхом використання запропонованих методів призводить до збільшення часу знаходження оберненого елемента і (або) до збільшення апаратних витрат. Наприкінці розділу зроблено висновки.

У **третьому** розділі досліджено можливість апаратної реалізації операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК як багаторівневих систем.

У розділі проведено апаратну реалізацію алгоритмів роботи засобів КЗІ. Запропоновано структуру спецпроцесора для опрацювання елементів розширених полів Галуа. Протокольні процесори у цій дисертаційній роботі не розглядаються так само як і інтерфейс між ними та СпП. Запропоновано модель одного із СП для опрацювання елементів полів Галуа (GF-процесор) (рис. 7). Запропонований GF-процесор має додатковий функціональний блок для розміщення досліджуваних ядер, варіанти ядер порівнювалися за величиною апаратних витрат на реалізацію функціонального блока FU. Для проведення досліджень у ході виконання роботи було розроблено технологічний засіб (генератор ядер) для проєктування помножувачів елементів полів Галуа $GF(p^m)$ для поліноміального базису, вузлів обчислення квадратних коренів, інверторів з незалежним від операндів часом обчислення.

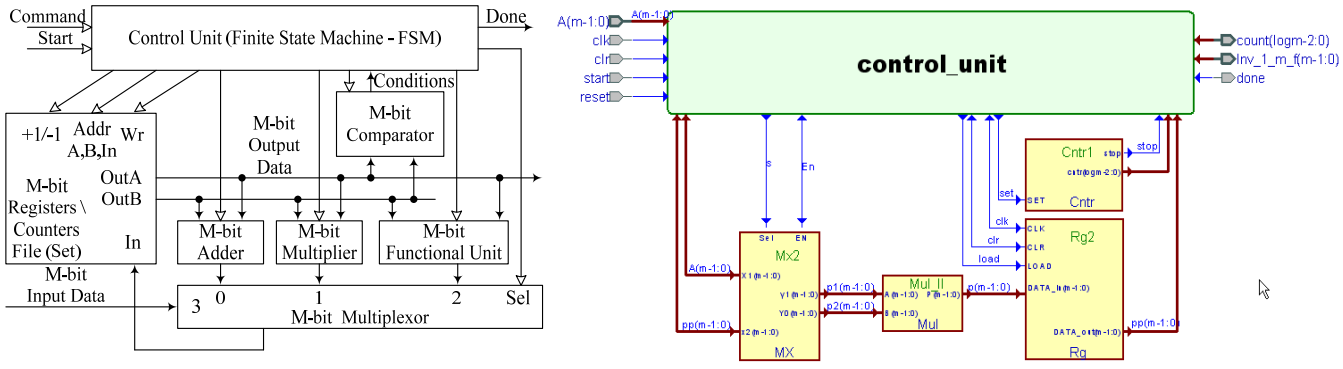


Рис. 7. GF-процесор з додатковим функціональним блоком (а)
Інвертор, який реалізує метод М (б)

Параметри основного генератора, які може встановити користувач: тип ядра; метод створення ядра (інвертора - від 1 до 5); характеристика p ($2 \le p \le 2^{1000}$) розширеного поля Галуа $GF(p^m)$; степінь m ($3 \le m \le 1000$) розширеного поля Галуа $GF(p^m)$; незвідний многочлен F, що утворює поле. При цьому порядок поля p^m не може перевищувати значення 2^{1000} ($p^m \le 2^{1000}$). Відсутні в моделі процесора ядра схемотехнічно зібрано у додатковому функціональному вузлі (FU) (рис. 7).

Реалізовані відповідно до запропонованих методів інвертування ядра інверторів з незалежним від операндів часом обчислення досліджуються в поліноміальному базисі двійкових полів Галуа $GF(2^m)$ з метою вибору найкращого за апаратною та часовою складностями. Необхідні для інвертування додаткові елементи GF-процесора займають від 119 до 919 слайсів і забезпечують час інвертування від 131 до 8629 нс ($GF(2^{64})$), що дозволяє обирати ядра в залежності від потреб замовника. Результати імплементації відповідних ядер зведено до таблиці 1. У таблиці позначено: ДД – пряме двійкове ділення; КрКв – метод на основі обчислення квадратного кореня і піднесення до квадрату; КрМ – метод на основі обчислення квадратного кореня і множення; КвМ – метод на основі піднесення до квадрату і множення; М – метод на основі множення; БП – використовується біт-паралельний помножувач, П – використовується паралельний помножувач. Варіант з меншим комплексним показником вважається найкращим за сукупністю параметрів. Детальні оцінки ресурсів для кожного з методів наведено в роботі.

Таблиця 1

Технічні ресурси інверторів в складі GF-процесора

Method (m=64)	ДД	КрКв	КрМ	КвМ	КрКв	КвМ	М
Помножувач	БП	БП	БП	БП	П	П	П
# Slices, total (S)	111	289	119	139	919	792	699
Total # FFs	278	902	556	353	277	82	78
Total # LUTs	333	981	498	447	2934	2523	2334
# FFs in FU	278	406	203	0	0	0	0
# LUTs in FU (L)	333	598	246	201	514	476	0
Min clock period (P, ns)	4,053	4,174	3,305	3,263	9,80	10,00	9,40
# clocks (C)	131	2374	8629	4535	126	126	250
Комплексний показник ($CI = S*P*C/10^6$)	0,06	2,86	3,39	2,06	1,13	1,00	1,64

Четвертий розділ присвячено впровадженню операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК.

Наукові положення та висновки дисертації успішно використано під час виконання проєктних робіт на фірмі AL-NABAA Network Solution L.L.C. (Багдад, Ірак), що підтверджено відповідним Актом.

Наукові положення та висновки дисертації було використано при проведенні держбюджетної науково-дослідної роботи ДБ/КІБЕР «Інтеграція методів і засобів вимірювання, автоматизації, опрацювання та захисту інформації в базисі кібер-фізичних систем» (номер державної реєстрації 0115U000446), що також підтверджено відповідним Актом).

Також результати дисертаційної роботи використано на кафедрі електронних обчислювальних машин Інституту комп'ютерних технологій, автоматики та метрології Національного університету «Львівська політехніка» при підготовці і

викладанні курсів лекцій та лабораторних робіт навчальної дисципліни «Дослідження і проєктування комп'ютерних систем та мереж» (для освітньо-кваліфікаційного рівня «Магістр», спеціальність 123 «Комп'ютерна інженерія», спеціальностей «Комп'ютерні системи та мережі», «Кіберфізичні системи» та «Системне програмування»).

Серед завдань, на вирішення яких було спрямовано проєкт Кібер, і до виконання яких було залучено автора цієї роботи, було, у тому числі, дослідження та розроблення принципів захищеного обміну, опрацювання та зберігання вимірювальної та службової інформації, в тому числі способів забезпечення конфіденційності, цілісності та автентичності інформації, технічного та криптографічного захисту інформаційних зв'язків між компонентами КФС та управління доступом до них, розроблення методологічних засад інформаційної та функціональної безпеки.

Модель реалізованого в ході роботи на ПЛІС процесора еліптичних кривих, відповідає багаторівневій структурі функціонального каналу. Первинно в моделі було реалізовано алгоритми виконання основних операцій у поліноміальному базисі у двійкових розширених полях Галуа та визначено апаратні та часові характеристики розроблених ядер (наведено в роботі). Потім модель було модифіковано для дослідження ядер опрацювання елементів розширених полів Галуа $GF(p^m)$ з характеристиками $p > 2$. Робота із створення вузлів, що опрацьовують елементи таких розширених полів Галуа, виявила суттєву умову, яка дозволила розв'язати задачу порівняння вузлів для різних полів – розширені поля Галуа повинні бути з приблизно однаковою кількістю елементів.

Аналіз результатів ДБ Кібер привів до необхідності теоретично їх узагальнити та обґрунтувати використання того чи іншого розширеного поля Галуа, тобто, порівнювати операційні вузли для цих полів. Внаслідок цього було розроблено метод оцінювання складності моделей помножувачів елементів розширених полів Галуа $GF(p^m)$

До основних результатів роботи, які було використано на ф. Al Nabaa Network solutions (Багдад, Ірак) і які дозволили покращити технічні рішення фірми належать: використання цифрових підписів для забезпечення безпеки, висока продуктивність запропонованих для використовування алгоритмів, ефективність та функціональність помножувачів, ефективність та функціональність знаходження мультиплікативної інверсії, рівень протидії злому даних, вбудоване тестування.

У впроваджених в навчальний процес розроблених методичних вказівках до лабораторної роботи наведено теоретичні відомості про розширені поля Галуа, про модифіковані комірки Гілда та запропоновані в роботі помножувачі на їх основі, наведено VHDL-описи модифікованої комірки Гілда та основних елементів помножувача.

У методичних вказівках, як взірець, наведено функціональну схему помножувача елементів полів Галуа $GF(3^4)$ (рис. 2) і варіанти утворюючих поле поліномів та операндів, над якими необхідно виконати множення. Студенти повинні модифікувати схему та VHDL-описи елементів, промоделювати роботи виправленої схеми і продемонструвати правильний результат.

ВИСНОВКИ

У ході виконання роботи досягнуто поставлено мету. На основі проведених досліджень здійснено наукове обґрунтування доцільності застосування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК, визначення полів, які найкраще використовувати для вирішення цього завдання, а також створення методів та засобів проєктування і порівняння згаданих вузлів, розв'язано важливе наукове завдання створення операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК, які працюють з елементами розширених полів Галуа $GF(p^m)$, розроблено структурні алгоритми їх роботи. При цьому розв'язано такі взаємозв'язані задачі і отримано такі нові наукові результати:

проведено системний аналіз сучасного стану теорії, методів та засобів проєктування спеціалізованих комп'ютерів, пристроїв КЗІ, аналіз найбільш важливих відкритих стандартів та алгоритмів для них, узагальнених структур спецпроцесорів (СП), що дозволило сформулювати мету роботи і завдання дослідження;

визначено основні архітектурні принципи побудови та розроблено узагальнену модель операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК;

розроблено метод оцінювання складності моделей помножувачів елементів розширених полів Галуа $GF(p^m)$ та метод оцінювання складності злому апаратних засобів КЗІ;

вдосконалено метод маскування роботи апаратних вузлів знаходження обернених елементів у двійкових полях Галуа $GF(2^m)$ у поліноміальному базисістворено і апробовано технологічний засіб (генератор ядер) для проєктування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК;

створено та перевірено уточнені структуровані моделі у вигляді VHDL-описів операційних пристроїв, в тому числі інверторів, які маскують роботу засобів КЗІ;

визначено найкращі для використання розширені поля Галуа, за сукупністю показників найращим є розширене поле з характеристикою 3;

проведено експериментальне дослідження та впровадження розроблених операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК.

Наукові положення та висновки дисертації успішно використано під час виконання проєктних робіт на фірмі AL-NABAA Network Solution L.L.C. (Багдад, Ірак), що підтверджено відповідним Актом, та при проведенні держбюджетної науково-дослідної роботи ДБ/КІБЕР «Інтеграція методів і засобів вимірювання, автоматизації, опрацювання та захисту інформації в базисі кібер-фізичних систем» (номер державної реєстрації 0115U000446), що також підтверджено відповідним Актом) (Додаток А, Додаток Б).

Також результати дисертаційної роботи використано на кафедрі електронних обчислювальних машин Національного університету «Львівська політехніка» при підготовці і викладанні курсів лекцій та лабораторних робіт навчальної дисципліни «Дослідження і проєктування комп'ютерних систем та мереж» (для освітньо-кваліфікаційного рівня «Магістр», спеціальність 123 «Комп'ютерна інженерія».

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Рахма, М. Часова складність помножувачів для полів Галуа / Р. Еліас, М. Рахма, В.С. Глухов / Електротехнічні та комп'ютерні системи. – Одеса: – 2016. Вид-во Наука і техніка. – № 22 (98). – С. 323-327.

2. Рахма, М. Структурна складність помножувачів елементів полів Галуа у нормальному та поліноміальному базисах / Р. Еліас, М. Рахма, В. Глухов / Електротехнічні та комп'ютерні системи. – Одеса: – 2017. Вид-во Наука і техніка. - № 25 (101). – С. 332-340.

3. Rahma, M. Galois Fields Elements Processing Units for Cryptographic Data Protection in Cyber-Physical Systems / V. Hlukhov, I. Zholubak, A. Kostyk, M. Rahma / Advances in Cyber-Physical Systems, Вид-во Національного університету Львівська політехніка. - Volume 2, Number 2, 2017. – pp. 47- 53.

4. Rahma, M. FPGA cores for fast multiplicative inverse calculation in Galois Fields / Rodrigue Elias, Valerii Hlukhov, Mohammed Rahma, Ivan Zholubak. Електротехнічні та комп`ютерні системи. – Одеса : – 2018. Вид-во Наука і техніка. 27(103), с. 227-233.

5. Рахма, М. Вбудований контроль пристроїв для опрацювання елементів розширених полів Галуа / Р. М. Еліас, В. С. Глухов, М. Рахма, І. М. Жолубак / Вісник Національного університету «Львівська політехніка» "Комп'ютерні системи та мережі", № 905. Львів, 2018. С. 64-72.

6. Рахма, М. Ємнісна складність та вбудований контроль пристроїв для опрацювання елементів розширених полів Галуа / Родріг Еліас, Валерій Глухов, Мохаммед Рахма, Іван Жолубак / Електротехнічні та комп`ютерні системи. – Одеса : – 2018. Вид-во Наука і техніка. 29(105), с. 95-102.

7. Rahma, Mohammed Kadhim. Galois Field Operational unit For Elliptic Curve Cryptography Digital Signature. V Міжнародний молодіжний науковий форум "Litteris et Artibus". 26–28 листопада, 2015. Україна, Львів. Pp. 66-71.

8. Rahma, Mohammed Kadhim. Time complexity of multipliers for Galois fields / Mohammed Kadhim Rahma, Valeriy S.Hlukhov / INTERNATIONAL YOUTH SCIENCE FORUM "LITTERIS ET ARTIBUS", 24-26 NOVEMBER 2016, LVIV, UKRAINE. Proceedings, pp. 52-53.

9. Рахма, М.К.Р. Часова складність орієнтованих на виконання криптографічних перетворень в складі кіберфізичних систем помножувачів на основі модифікованих комірок Гілда / Глухов В.С., Еліас Р.М., Рахма М.К.Р / Матеріали другого наукового семінару Кібер-фізичні системи: досягнення та виклики, Львів, Національний університет «Львівська політехніка», 21-22 червня 2016 р. С. 36-42.

10. Рахма, М. Аналіз можливості побудови багатосекційних помножувачів елементів полів Галуа для нормального та поліноміального базисів / В. С. Глухов, Р. Еліас, М. Рахма / Матеріали третього наукового семінару Кіберфізичні системи: досягнення та виклики, Львів, Національний університет «Львівська політехніка», 13-14 червня 2017 р. С. 38-47.

11. Rahma, M. Computing Square Roots and Solve Equations of ECC over Galois Fields /M. Rahma, V. Hlukhov / International Youth Science Forum "Litteris Et Artibus", November 23-25, 2017, Lviv, Ukraine, pp. 437-440.

12. Rahma, Mohammed Kadhim. Automation System for Configuration of Cryptographic Data Protection Unit Model / Ivan Zholubak, Mohammed Kadhim Rahma and Valeriy Hlukhov / Proceedings of 4th International Workshop on Theory of Reliability and Markov Modeling for Information Technologies (WS TheRMIT 2018, in frameworks of the 14th International Conference ICTERI2018). May 14, 2018, Kyiv, pp. 669-679.

13. Rahma, Mohammed Kadhim. Automation System for Configuration of Cryptographic Data Protection Unit Model / Ivan Zholubak, Mohammed Kadhim Rahma and Valeriy Hlukhov / Proceedings of 4th International Workshop on Theory of Reliability and Markov Modeling for Information Technologies (WS TheRMIT 2018, in frameworks of the 14th International Conference ICTERI2018). May 14, 2018, Kyiv, pp. 669-679.

14. Rahma, Mohammed. Devices for Multiplicative Inverse Calculation in Binary Galois Fields / Valeriy Hlukhov, Mohammed Rahma and Ivan Zholubak. / Proceedings of 9th International IEEE Conference Dependable Systems, Services and Technologies DESSERT'2018. Kyiv, May 24-27, pp. 275-278.

15. Rahma, Mohammed. Hardware components for post-quantum elliptic curves cryptography / Rodrigue Elias, Valerii Hlukhov, Mohammed Rahma, Ivan Zholubak. / Proceedings of International Conference "Advanced Computer Information Technologies", June 1-3, 2018 in Ceske Budejovice, Czech Republic, pp. 236-239.

16. Рахма, Мохаммед Кадім Рахма. Принципи побудови та проектування операційних вузлів для полів Галуа, що використовуються в задачах криптографічному захисті інформації на основі еліптичних кривих / В.С. Глухов, І.М. Жолубак, Мохаммед Кадім Рахма Рахма / Кіберфізичні системи: багаторівнева організація та проектування [Текст]: монографія – А.О. Мельник та інші. За редакцією професора А. О. Мельника. Львів: «Магнолія 2006», 2019. 238 с. С. 58-131.

АНОТАЦІЯ

Рахма Мохаммед Кадім Рахма. Моделі та методи побудови операційних вузлів для полів Галуа, які використовуються при криптографічному захисті інформації на основі еліптичних кривих. – На правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти. – Національний університет «Львівська політехніка», Міністерство освіти і науки України, Львів, 2019.

Дисертацію присвячено вирішенню науково-прикладного завдання створення операційних вузлів для полів Галуа, які використовуються при криптографічному захисті інформації на основі еліптичних кривих. Основну увагу приділено розробці методів оцінювання часової, структурної та ємнісної складності помножувачів елементів розширених полів Галуа $GF(d^m)$, методу оцінювання складності злому апаратних засобів КЗІ та методу маскування їхньої роботи, а також вдосконаленню методу вбудованого тестування операційних вузлів.

Оцінювання складності базується на представленні структури помножувачів у вигляді матриці модифікованих комірок Гілда, з первинним аналізом їхньої складності для різних полів і врахуванням отриманих результатів при оцінюванні складності помножувачів.

Застосування розроблених методів дозволило визначити найкращі в порівнянні з двійковими розширені поля Галуа (серед полів з приблизно однаковою кількістю елементів). Ними виявилися поля з характеристиками 3, 5 та 7. Також встановлено значно меншу структурну складність помножувачів для поліноміального базису в порівнянні з нормальним, що пояснює складності імплементації помножувачів для нормального базису в ПЛІС.

Запропоновано і реалізовано метод маскування роботи інверторів.

Вдосконалено метод вбудованого тестування помножувачів.

Реалізовано засіб проєктування у вигляді генератора моделей помножувачів та інверторів, з його допомогою розроблено ряд помножувачів та інверторів, виконано перевіряння адекватності запропонованих методів та засобів, здійснено їхнє впровадження.

Результати дисертаційної роботи впроваджено під час виконання проєктних робіт на ф. AL-NABAA Network Solution L.L.C. (Багдад, Ірак), при проведенні держбюджетної науково-дослідної роботи ДБ/КІБЕР «Інтеграція методів і засобів вимірювання, автоматизації, опрацювання та захисту інформації в базисі кібер-фізичних систем» та в навчальному процесі Національного університету «Львівська політехніка».

Ключові слова: кіберфізичні системи, розширені поля Галуа, еліптичні криві, модифікована комірка Гілда, вбудований контроль, маскування.

АННОТАЦИЯ

Рахма Мохаммед Кадим Рахма. «Модели и методы построения операционных узлов для полей Галуа, используемых при криптографической защите информации на основе эллиптических кривых». – На правах рукописи.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.05 - компьютерные системы и компоненты. - Национальный университет «Львивська политэхника», Львов, Министерство образования и науки Украины, 2019.

Диссертация посвящена решению научно-прикладной задачи создания операционных узлов для полей Галуа, используемых при криптографической защите информации на основе эллиптических кривых. Основное внимание уделено разработке методов оценки временной, структурной и емкостной сложности умножителей элементов расширенных полей Галуа $GF(d^m)$, метода оценки сложности взлома аппаратных средств криптографической защиты информации и метода маскировки их работы, а также совершенствованию метода встроенного тестирования операционных узлов.

Оценка сложности базируется на представлении структуры умножителей в виде матрицы модифицированных ячеек Гилда, с первичным анализом их сложности для различных полей и учетом полученных результатов при оценке сложности умножителей.

Применение разработанных методов позволило определить лучшие по сравнению с двоичными расширенные поля Галуа (среди полей с примерно одинаковым количеством элементов). Ими оказались поля с характеристиками 3, 5 и 7. Также установлено значительно меньшую структурную сложность умножителей

для полиномиального базиса по сравнению с нормальным, что объясняет сложности имплементации умножителей для нормального базиса в ПЛИС. Предложен и реализован метод маскировки работы инверторов.

Усовершенствован метод встроенного тестирования умножителей.

Реализовано средство проектирования в виде генератора моделй умножителей и инверторов, с его помощью разработан ряд умножителей и инверторов, выполнена проверка адекватности предложенных методов и средств, осуществлено их внедрение.

Результаты диссертационной работы внедрены при выполнении проектных работ на ф. AL-NABAA Network Solution L.L.C. (Багдад, Ирак), при проведении госбюджетной научно-исследовательской работы ДБ/КИБЕР «Интеграция методов и средств измерения, автоматизации, обработки и защиты информации в базисе киберфизических систем» и в учебном процессе Национального университета «Львивська политэхника».

Ключевые слова: киберфизические системы, расширенные поля Галуа, эллиптические кривые, модифицированная ячейка Гилда, встроенный контроль, маскировка.

ABSTRACT

Rahma Mohammed Kadhim Rahma. Models and methods for constructing operating units for Galois fields used in cryptographic data protection based on elliptic curves. – On the rights of manuscript.

Thesis for the degree of Candidate of Technical Sciences on a specialty 05.13.05 - computer systems and components. - Lviv Polytechnic National University, Ministry of Education and Science of Ukraine, Lviv, 2019.

The dissertation is devoted to the solution of the scientifically applied problem of creation of operating units for Galois fields used in cryptographic data protection on the basis of elliptic curves.

The main attention is paid to the development of methods for estimating the time, structural and capacitance complexity of multipliers of elements of extended Galois fields $GF(d^m)$, the method of assessing the complexity of hacking hardware cryptographic data protection tools and the method of masking their work, as well as improving the method of embedded testing of the operating units.

Complexity estimation is based on the representation of the multiplier structure in the form of a matrix of modified Guild cells, with an initial analysis of their complexity for different fields and taking into account the results obtained when evaluating the multiplier complexity.

The application of the method: an extended Galois field is selected; the basis for representing the elements of the Galois fields is selected; the basic elements of the multiplier are selected; the structure of the basic elements is selected; the structure of the multiplier is selected; the selected type of complexity is analyzed, relative values of complexity parameters are formed with respect to similar parameters of the extended binary field; studies are repeated for all selected to analyze extended Galois fields; the results of the study are recorded; the best field is determined.

The application of the developed methods allowed us to determine the best Galois extended fields in comparison with the binary ones (among fields with approximately the same number of elements). They were fields with characteristics 3, 5 and 7. A significantly lower structural complexity of multipliers for the polynomial basis than the normal one was also established, which explains the difficulty of implementing the multipliers for the normal basis in the FPGA. A method of masking the operation of inverters is proposed and implemented.

The method of built-in multiplier testing is improved. Code combinations that will never be encountered when processing elements of an extended Galois field during normal operation of processor nodes, memory nodes, and data channels exist. These unused (forbidden) code combinations can be used to monitor the performance of data protection tools while performing their essential functions (built-in controls can be implemented). But 100% of all, even single, errors can not be detected. The results obtained should be considered as an estimate of the proportion of errors that can be detected by the proposed method. A table-based method for describing the occurrence of erroneous codes is suggested.

The method of masking the operation of hardware units for finding inverted elements in extended binary Galois fields in a polynomial basis is presented. The development of a method of masking operating nodes for Galois fields used in data protection based on elliptic curves consists in equalizing the computation time of inverted elements in a polynomial basis by refusing to use the Euclid generalized algorithm in favor of direct binary algorithms or exponential algorithms. The use of exponential algorithms requires the efficient operation of squaring or finding the square root. Masking through the use of the proposed methods leads to an increase in the time of finding the inverted element and (or) to an increase in hardware costs.

The structure of the special processor for processing elements of extended Galois fields is proposed.

The design tool was implemented in the form of a generator of multiplier and inverter models, with its help a number of multipliers and inverters were developed, checks of adequacy of the proposed methods and means were carried out, their implementation was carried out.

The results of the dissertation work are implemented during the execution of design works on f. AL-NABAA Network Solution L.L.C. (Baghdad, Iraq), during the state budget research work of the DB/KIBER "Integration of methods and means of measuring, automation, processing and protection of information in the base of cyber-physical systems" and in the educational process in Lviv Polytechnic National University.

Keywords: cyberphysical systems, extended Galois fields, elliptic curves, modified Guild cell, built-in control, masking.