МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ "ЛЬВІВСЬКА ПОЛІТЕХНІКА"

Жолубак Іван Михайлович

УДК 004.315.5 : 004.382 : 512.624 : 621.3.049.771.14

МЕТОДИ ТА ЗАСОБИ СТВОРЕННЯ РЕКОНФІГУРОВАНИХ ВУЗЛІВ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ КІБЕР-ФІЗИЧНИХ СИСТЕМ

05.13.05 – комп’ютерні системи та компоненти

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Львів – 2024

Дисертацією є кваліфікаційна наукова праця на правах рукопису.

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

Науковий керівник: доктор технічних наук, професор
ГЛУХОВ Валерій Сергійович,
Національного університету «Львівська політехніка» (м. Львів),
професор кафедри електронних обчислювальних машин

Офіційні опоненти: доктор технічних наук, професор
ВОЗНА Наталія Ярославівна,
Західноукраїнський національний університет (м. Тернопіль),
професор кафедри спеціалізованих комп'ютерних систем

кандидат технічних наук, доцент
КЛЬОЦ Юрій Павлович,
Хмельницький національний університет (м. Хмельницький),
доцент кафедри системного програмування

Захист відбудеться **28 березня 2025 р. о 12$^{\underline{00}}$** годині на засіданні спеціалізованої вченої ради Д 35.052.18 у Національному університеті «Львівська політехніка» за адресою: 79013, Україна, м. Львів, вул. С. Бандери, 12, ГНК, аудиторія 226).

З дисертацією можна ознайомитись у бібліотеці Національного університету «Львівська політехніка» за адресою: 79013, Україна, м. Львів, вул. Професорська, 1.

Вчений секретар
спеціалізованої вченої ради Д 35.052.18
доктор технічних наук, доцент Леся МИЧУДА

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність роботи. У дисертації розв'язується важливе науково-технічне завдання створення реконфігурованих вузлів криптографічного захисту інформації (КЗІ), які оперують у кіберфізичних системах (КФС) елементами розширених полів Галуа $GF(p^n)$, та у порівнянні з розширеними двійковими полями $GF(2^m)$ мають більшу криптографічну стійкість. При цьому $p^n \approx 2^m$, де $p > 2$ – просте число, конфігурована характеристика поля, n, m – порядок утворюючого поле полінома, $m \leq 1024$. Основним вузлом для аналізу обрано помножувач елементів таких розширених полів Галуа $GF(p^n)$, який побудовано на основі реконфігурованого вузла - модифікованої комірки Гілда (МКГ). Запропоновано 3 варіанти структури МКГ та показано їх особливості в порівнянні із класичною коміркою Гілда (КГ). Наведено порівняння апаратних витрат різних варіантів МКГ та помножувачів.

Алгоритми КЗІ, наприклад, алгоритми опрацювання електронних цифрових підписів (ЕЦП) з використанням еліптичних кривих (ЕК), мають багаторівневу структуру, в якій різні рівні виконують специфічні математичні операції над багаторозрядними кодами. Це включає в себе операції над елементами розширених полів Галуа $GF(p^n)$, де $p \geq 2$, операції над точками ЕК та операції над результатами обробки точок ЕК. У цьому контексті для різних засобів КЗІ необхідно забезпечити можливість конфігурації операційних пристроїв, які реалізують вказані алгоритми. Важливим завданням є забезпечення зміни параметрів еліптичної кривої, характеристики p та порядку утворюючого поле полінома n для поля Галуа та структури самого пристрою.

Пристрої, які опрацьовують елементи полів Галуа також є важливими будівельними блоками багатьох інших засобів КЗІ. Традиційно, розробники апаратних засобів КЗІ намагалися скористатися простотою реалізації пристроїв, для двійкових розширених полів Галуа $GF(2^m)$, щоб зменшити апаратні витрати та підвищити продуктивність. В останні роки для збільшення криптографічної стійкості був відновлений інтерес до впровадження КЗІ на основі розширених полів Галуа $GF(p^n)$ з характеристикою p, відмінною від 2, які використовуються в таких застосунках як електронні підписи з використанням ізогеній ЕК та шифрування/розшифрування коротких повідомлень. Тому науково-технічне завдання створення реконфігурованих вузлів КЗІ, які оперують у КФС елементами розширених полів Галуа $GF(p^n)$ і забезпечують збільшення криптографічної стійкості є надзвичайно важливою та актуальною задачею.

Зв'язок дисертаційної роботи з науковими програмами, планами і темами. Дисертаційна робота відповідає науковим напрямкам кафедри електронних обчислювальних машин Національного університету "Львівська політехніка" – "Питання теорії, проектування та реалізації комп'ютерних систем та мереж, а також комп'ютерних засобів, вузлів, приладів і пристроїв вимірювальних, інформаційних, керуючих, телекомунікаційних та кіберфізичних систем". Робота була виконана в рамках держбюджетної науково-дослідної роботи ДБ/КІБЕР під назвою "Інтеграція методів і засобів вимірювання, автоматизації, опрацювання та захисту інформації в базисі кіберфізичних систем" (номер державної реєстрації 0115U000446).

Мета і завдання дослідження. Метою дисертаційної роботи є підвищення криптографічної стійкості засобів КЗІ, які використовуються в складі КФС, шляхом розвитку методів та засобів створення реконфігурованих операційних пристроїв (а саме, апаратних паралельних помножувачів на основі МКГ) для роботи з елементами розширених полів Галуа $GF(p^n)$ з характеристиками p та з порядками n утворюючого поле полінома такими, що $p^n \approx 2^m$, де $p > 2, m \leq 1024$.

Для досягнення поставленої мети слід вирішити наступні задачі:

1. Вдосконалити методи оцінювання часової складності апаратного множення елементів розширених полів Галуа $GF(p^n)$.

2. Вдосконалити методи оцінювання апаратної складності апаратного множення елементів розширених полів Галуа $GF(p^n)$, де $p > 2$.

3. Розробити метод створення для ПЛІС генераторів моделей (ядер) реконфігурованих паралельних помножувачів елементів розширених полів Галуа $GF(p^n)$ для вузлів КЗІ у КФС за трьома варіантами структури МКГ: "чорна скринька" (ЧС), на основі функціональних вузлів (ФВ), на основі логічних вузлів (ЛВ), що використовуються в вузлах КЗІ.

4. Розробити метод тестування генераторів ядер помножувачів елементів розширених полів Галуа $GF(p^n)$.

5. Розробити генератори ядер (генератори моделей) помножувачів елементів розширених полів Галуа $GF(p^n)$ такими, що порядок поля $p^n < 2^{1024}$. Генератори повинні створювати моделі помножувачів на основі МКГ з трьома варіантами структури МКГ: ЧС, ФВ, ЛВ. За допомогою генераторів ядер згенерувати ряд помножувачів елементів розширених полів Галуа $GF(p^n)$ з трьома структурами МКГ та провести їх імплементацію на ПЛІС, порівняти результати реалізації. Показати збіжність теоретичних та практичних результатів оцінювання апаратної та часової складностей помножувачів. Показати досягнення поставленої у роботі мети.

6. На основі розроблених і вдосконалених методів провести аналіз апаратних складностей створених помножувачів елементів розширених полів Галуа $GF(p^n)$, $p > 2$, та визначити поля, які найкраще підходять для реалізації помножувачів. Також провести аналіз часових складностей помножувачів елементів розширених полів Галуа $GF(p^n)$, $p > 2$, за відношенням часових витрат при програмній та апаратній реалізаціях.

Об'єкт дослідження – процеси та засоби створення реконфігурованих вузлів КЗІ у КФС.

Предмет дослідження – методи та засоби створення апаратних помножувачів для елементів розширених полів Галуа $GF(p^n)$.

Методи дослідження. При проектуванні апаратних помножувачів для елементів розширених полів Галуа $GF(p^n)$ враховувалися висновки теорії комп'ютерних систем, теорії обчислювальних систем, теорії обчислювальних машин, теорії проектування спеціалізованих комп'ютерних систем, теорії складності алгоритмів та програмно-апаратної складності комп'ютерних систем. Для реалізації елементів вузлів апаратних помножувачів елементів розширених полів Галуа $GF(p^n)$ на ПЛІС використовувалась теорія проектування НВІС. Для розробки методів обробки елементів

розширених полів Галуа $GF(p^n)$ враховувалися положення і висновки теорії інформації, теорії чисел, теорії залишків, теорії обчислень, теорії груп, для проектування спецпроцесорів, а також для вирішення задач проектування апаратних помножувачів елементів розширених полів Галуа $GF(p^n)$ застосовувалися результати теорії кодування, для створення моделей вузлів апаратних помножувачів елементів розширених полів Галуа $GF(p^n)$ та для аналізу їх роботи була використана теорія програмування, теорія моделей, обчислювальна математика, моделювання алгоритмів та апаратних засобів.

Отримані результати були перевірені шляхом моделювання згідно з теорією випробувань.

Дослідження, що були проведені, базуються на результатах теорії цифрових автоматів, на теоретичній моделі взаємодії відкритих систем та багаторівневій платформі КФС. Також були використані методи виконання математичних операцій у розширених полях Галуа $GF(p^n)$ у поліноміальному базисі. У проведених дослідженнях використовуються математичні напрацювання теорії чисел, теорії алгоритмів та засобів моделювання цифрових схем.

Наукова новизна одержаних результатів. На основі проведених досліджень розв'язано важливу науково-прикладну задачу створення реконфігурованих (на ПЛІС) паралельних помножувачів елементів розширених полів Галуа $GF(p^n)$ в складі засобів КЗІ КФС, які забезпечують засобам КЗІ більшу криптографічну стійкість. При цьому отримано такі нові наукові результати:

1. Отримав подальший розвиток метод оцінювання часової складності множення елементів розширених полів Галуа $GF(p^n)$ апаратним способом, за яким помножувач складається з МКГ, що дало можливість визначити поле $GF(3^n)$, у якому відношення часів множення програмним та апаратним способами перевищує таке відношення в інших полях щонайменше в 1,27 раза, чим забезпечує найбільшу криптографічну стійкість засобів КЗІ при інших однакових умовах.

2. Отримав подальший розвиток метод оцінювання апаратної складності помножувачів елементів розширених недвійкових полів Галуа $GF(p^n)$, де $p > 2$, який на відміну від відомих розглядає помножувачі для полів з приблизно однаковим порядком p^n і які складаються з МКГ, що дало можливість визначити поле $GF(3^n)$, де помножувачі мають щонайменше на 6 % меншу апаратну складність, у порівнянні з помножувачами для інших недвійкових полів.

3. Вперше запропоновано метод створення для ПЛІС генераторів моделей (ядер) реконфігурованих паралельних помножувачів елементів розширених полів Галуа $GF(p^n)$ для вузлів КЗІ у КФС, за яким на відміну від відомих генерується 3 варіанти помножувачів з 3 структурами МКГ, що дало можливість створити описи моделей помножувачів та визначити реальну апаратну складність кожного із помножувачів та обрати найкращу реалізацію для кожного конкретного поля.

4. Вперше запропоновано метод тестування генераторів ядер помножувачів елементів розширених полів Галуа $GF(p^n)$, який на відміну від відомих використовує 2 різні еталони (2 різні математичні пакети) для перевірки згенерованих помно-

жувачів на основі МКГ, що дало можливість підтвердити правильну роботу генераторів помножувачів та самих помножувачів для всіх варіантів їх реалізації.

Практичне значення одержаних результатів. Апаратні реалізації алгоритмів КЗІ, здебільшого на основі ПЛІС, характеризуються низьким електроспоживанням, малими габарити, високою продуктивністю, високою захищеністю, що є невід'ємними атрибутами КФС.

Отримані у дисертаційній роботі наукові та практичні результати створюють методологічну базу для розробки вузлів КЗІ, а саме, апаратних помножувачів для елементів розширених полів Галуа $GF(p^n)$, які дозволяють підвищити надійність, криптографічну стійкість та захищеність сучасних апаратних засобів КЗІ, у тому числі, засобів опрацювання ЕЦП на основі ЕК.

Практична цінність даної роботи полягає у тому, що за запропонованими методами та результатами теоретичних та практичних досліджень для реконфігурованих вузлів засобів КЗІ на основі ЕК визначено поле $GF(3^n)$, де помножувачі мають щонайменше на 6 % меншу апаратну складність, а також де відношення часів множення програмним та апаратним способами перевищує таке відношення в інших полях щонайменше в 1,27 рази, чим забезпечує найбільшу криптографічну стійкість засобів КЗІ, які працюють у полі $GF(3^n)$ при інших однакових умовах, а саме:

1. Створено і апробовано технологічні засоби (генератори ядер) для генерації ядер помножувачів елементів розширених полів Галуа $GF(p^n)$ такими, що порядок поля $p^n < 2^{1024}$ для 3 структур МКГ, що підтверджено актами впровадження.

2. Створено і перевірено низку моделей помножувачів у вигляді *VHDL*-описів помножувачів елементів розширених полів Галуа $GF(p^n)$ такими, що порядок поля $p^n < 2^{1024}$, що підтверджено актом впровадження.

3. За розробленим методом проведено оцінку апаратної складності помножувачів елементів розширених полів Галуа $GF(p^n)$ такими, що порядок поля $p^n < 2^{1024}$ та з приблизно однаковим порядком p^n, що підтверджено актом впровадження.

4. За розробленим методом проведено оцінку часової складності помножувачів елементів розширених полів Галуа $GF(p^n)$ такими, що порядок поля $p^n < 2^{1024}$ та з приблизно однаковим порядком p^n, що підтверджено актами впровадження.

5. Виконано перевірку розроблених помножувачів та генераторів помножувачів елементів розширених полів Галуа $GF(p^n)$, що підтверджено актами впровадження.

6. Розроблено методичні вказівки для використання в навчальному процесі кафедри ЕОМ (Методичні вказівки до лабораторних робіт "Проектування і моделювання елементів комп'ютерних систем та мереж" з дисципліни "Дослідження і проектування комп'ютерних систем та мереж" для студентів освітньо-кваліфікаційного рівня «Магістр», спеціальність 123 «Комп'ютерна інженерія», спеціалізації «Комп'ютерні системи та мережі», «Кіберфізичні системи» та «Системне програмування» / укл.: Глухов В.С., Жолубак І.М., Костик А.Т, Рахма М.К.Р. - Львів: видавництво Національного університету "Львівська політехніка", 2019. - 25 с.), що підтверджено актом впровадження.

Особистий внесок здобувача. Усі наукові результати, викладені у дисертаційній роботі, отримано автором особисто і повністю розкрито у публікаціях. У публікаціях, що написано в співавторстві, автору дисертації належать методи оцінювання часової та апаратної складностей помножувачів елементів розширених полів Галуа $GF(p^n)$, методи створення таких помножувачів на основі МКГ та методи їх тестування.

Апробація матеріалів дисертації. Основні положення дисертації було представлено та обговорено на:

1. 5th, 6th, 7th International youth science forum “litteris et artibus” – Львів: - 2015, 2016, 2017.
2. Міжнародній науково-практичній конференції “Інформаційні технології та комп’ютерне моделювання” – Івано-Франківськ – Яремче: - 2016.
3. 17-й міжнародній науково-практичній конференції “Современные информационные и электронные технологи” – Одесса: - 2016.
4. Кіберфізичні системи досягнення та виклики – Львів: - 2016.
5. Захист інформації і безпека інформаційних систем – Львів: - 2017.
6. 12-th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) – Dortmund, Germany: 7-9 september 2023.
7. 13-th International Conference on Dependable Systems, Services and Technologies (DESSERT’2023) - Greece, Athens: 13-15 october 2023.
8. IEEE 18-th International Conference on Computer Science and Information Technologies (CSIT), held in frames of IEEE Lviv Polytechnic Week - Lviv, UKRAINE: 19-21 October 2023.

Публікації. За темою дисертаційної роботи опубліковано 28 наукових праць, з них 1 монографія, 14 статтей у фахових наукових журналах та вісниках, 13 – у працях та тезах конференцій та семінарів, з них у Scopus – 1 стаття Q1, 2 статті Q4 та 4 тези конференцій.

Структура та обсяг дисертації. Дисертаційна робота складається із вступу, чотирьох розділів, висновків, списку використаних джерел і додатків. Чотири розділи присвячено розгляду змістовної сутності створення реконфігурованих вузлів КЗІ, які оперують у КФС елементами розширених полів Галуа $GF(p^n)$. Вони у порівнянні з вузлами, які оперують елементами двійкових полів Галуа $GF(2^m)$, мають більшу криптографічну стійкість. Найбільше уваги приділено побудові помножувачів елементів розширених полів Галуа $GF(p^n)$ та створенню генераторів ядер (*VHDL*-описів) цих вузлів. Роботу викладено на 296 сторінках, з них основний текст – 153 сторінки, рисунків – 75, таблиць – 16. Список використаних джерел – 251 найменувань.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **Вступі** виконано аналіз сучасних наукових досліджень у галузі розробки реконфігурованих компонентів для КЗІ на основі розширених полів Галуа, в тому числі засобів, що використовують еліптичні криві (ЕК). Обґрунтовано важливість використання генераторів ядер помножувачів для елементів розширених полів Галуа $GF(p^n)$, які знаходять застосування у системах КЗІ на основі ЕК. Сформульовано ціль та задачі дослідження, проаналізовано головні наукові досягнення та вказано їхню практичну цінність. Також висвітлено взаємозв'язок даної роботи з існуючими науковими програмами, планами і темами досліджень. Подається інформація про процес апробації результатів, публікації та використанні їх у практичній діяльності.

У роботі наведено структуру та архітектуру КФС, у складі якої є вузли КЗІ. ЕК широко використовуються у вузлах захисту інформації. В Україні стандарт ДСТУ 4145-2002 регулює використання ЕЦП на основі ЕК. Він обмежує використання розширених полів Галуа двійковими полями $GF(2^m)$ з порядком утворюючого поле полінома $m \leq 509$ ($GF(2^{509})$), проте міжнародні стандарти рекомендують використовувати двійкові поля з набагато більшими порядками утворюючих поліномів ($m \leq 998$). Сучасні темпи розвитку комп'ютерної техніки та загроза створення квантових комп'ютерів ведуть до створення більш стійких засобів КЗІ, до збільшення порядку (p^n) розширених полів Галуа $GF(p^n)$, які використовуються. Один з найбільш очевидних методів злому засобів КЗІ є метод перебору усіх ключів. Програмне виконання операцій над елементами розширених полів Галуа $GF(p^n)$ має більшу трудоємність, у порівнянні з $GF(2^m)$ та забезпечує більшу стійкість до злому. Апаратна реалізація реконфігурованих вузлів КЗІ забезпечує ще більшу криптографічну стійкість засобів КЗІ. За елементну базу для створення вузлів КЗІ у складі КФС у роботі було обрано програмовані логічні інтегральні схеми (ПЛІС), оскільки вони забезпечують високу продуктивність та швидкодію при виконанні вузькоспеціалізованих задач у порівнянні з програмною реалізацією. Для генерації *VHDL*-описів вузлів КЗІ, що працюють з використанням розширених полів Галуа $GF(p^n)$, для їхньої наступної реалізації у ПЛІС було розроблено мовою *C++* програми-генератори ядер помножувачів елементів розширених полів Галуа.

У **Першому** розділі розглянуто сучасний стан та перспективи розвитку засобів та методів створення реконфігурованих вузлів КЗІ. Показано місце розширених полів Галуа $GF(p^n)$ у алгоритмах КЗІ КФС, розглянуто методи створення реконфігурованих вузлів на ПЛІС. Особливу увагу приділено правилам виконання арифметичних операцій у розширених полях Галуа $GF(p^n)$. Показано, що операції множення та ділення найбільш трудомісткі, при цьому ділення найчастіше виконується програмно. Тому саме операції множення приділено найбільше часу та уваги у даній роботі.

Також розглянуто питання складності алгоритмів та апаратно-програмна модель алгоритмів, питання злому систем КЗІ, особливості тестування операційних елементів для розширених полів Галуа $GF(p^n)$, показано структуру комірки Гілда, підходи до створення генераторів ядер.

У **Другому** розділі розглянуто методи створення реконфігурованих вузлів КЗІ

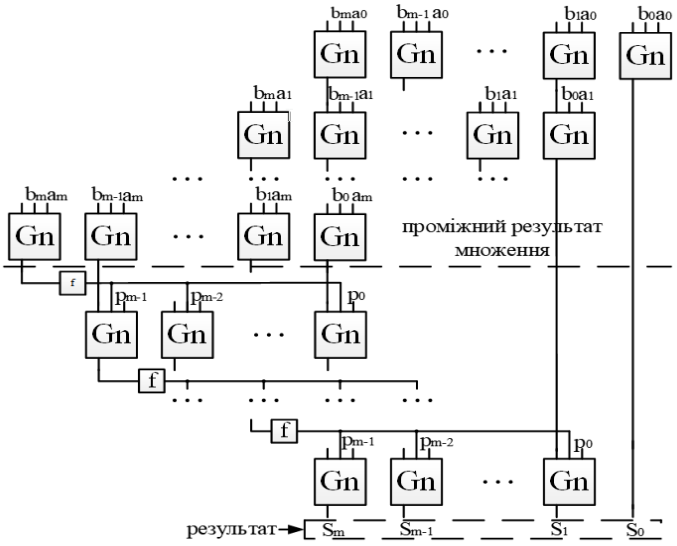

Рисунок 1 – Матричний помножувач поля $GF(p^n)$ з використанням МКГ

для КФС, загальну методику проведення дисертаційних досліджень, описано вимоги до створення реконфігурованих вузлів КЗІ, обґрунтовано доцільність створення паралельних помножувачів елементів розширених полів Галуа $GF(p^n)$ та запропоновано методи створення таких помножувачів. Вдосконалено методи оцінки часової та апаратної складностей та запропоновано метод тестування генераторів ядер таких помножувачів.

На рис. 1 наведено матричний помножувач для елементів розширених полів Галуа $GF(p^n)$ в поліноміальному базисі. Помножувач складається з модифікованих комірок Гілда (G_n) та вузлів f для знаходження коефіцієнта, на який перемножується утворюючий поле поліном, при зведенні проміжного результату за модулем такого полінома. Елемент f обчислює інверсію за модулем характеристики поля: $f = (p - G_n) \bmod p = (-G_n) \bmod p$, де p – характеристика поля, G_n – результат на виході модифікованої комірки Гілда.

Схеми МКГ та КГ для розширених полів Галуа $GF(p^n)$ з характеристиками $p > 2$ наведено на рис. 2. КГ для розширених полів Галуа з характеристикою поля $p = 2$ має входи A, B, Ci та виходи – S, Co. МКГ не має виходу переносу – Co. МКГ для розширених полів Галуа $GF(p^n)$ повинна мати $3x$ двійкових входи та x двійкових виходів, розрядністю $x = \lceil \log_2 p \rceil$ біт кожний.

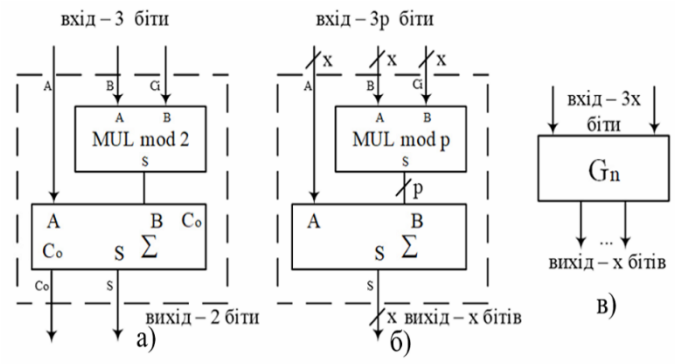

Рисунок 2 – а) КГ, б) МКГ для обробки елементів розширених полів Галуа $GF(p^n)$, в) символ МКГ МКГ $GF(p^n)$

При використанні сучасних ПЛІС, логічні комірки яких побудовано на основі програмованих 6-входових комбінаційних схем (LUT), реалізація на ПЛІС МКГ, коли не уточняється структура МКГ, а береться до уваги тільки кількість її входів та виходів, потребує $q_{LUT} = (2^{3x-5}-1) \cdot x$ LUT (LUT з 6 входами).

Оцінити кількість LUT у МКГ можна за трьома варіантами структури МКГ: ЧС, ФВ, ЛВ.

Апаратні витрати будемо оцінювати у порівнянні із витратами помножувача для розширеного поля Галуа $GF(2^m)$, при умові $p^n \approx 2^m$ При цьому враховується різниця у величинах порядків досліджуваних полів.

Для варіанту ЧС коефіцієнт апаратних витрат $k_{mul} = k_g k_k$, де $k_g = \frac{k_{gp}}{k_{g2}}$,

$k_k = \frac{k_{kp}}{k_{k2}}$ – коефіцієнти складності та кількості МКГ, k_{gp} та k_{g2}, k_{kp} та k_{k2} – кількість LUT у МКГ та кількість МКГ для полів Галуа $GF(p^n)$ та $GF(2^m)$, відповідно.

Для розширених полів Галуа $GF(2^m)$ $k_{g2} = 1$, для інших $k_{gp} = (2^{3x-5} - 1)x$, де $x = \lceil \log_2 p \rceil$. Звідси випливає що $k_{gp} = (2^{3\lceil \log_2 p \rceil - 5} - 1)\lceil \log_2 p \rceil$. Отже:

$$k_{gp} = (2^{3\lceil \log_2 p \rceil - 5} - 1)\lceil \log_2 p \rceil \quad (1)$$

В розширених полях Галуа $GF(2^m)$ для реалізації помножувача потрібно $k_{k2}=2m^2 - 2m + 1$ МКГ, а в полях Галуа $GF(p^n)$ – $k_{kx}=2n^2 - 2n + 1$ та додатково $(n-1) * (2^{3*\lceil \log_2 p \rceil - 5} - 1) * \lceil \log_2 p \rceil$ LUT для знаходження коефіцієнта, на який перемножуємо незвідний поліном. Апаратними витратами для знаходження коефіцієнта (на реалізацію елемента *f*) (рис. 1), можна, в даному випадку, знехтувати, оскільки вони малі в порівнянні з витратами на реалізацію самих МКГ. Отже:

$$k_k \approx \frac{2n^2-2n+1}{2m^2-2m+1} \quad (2); \qquad k_{mul} \approx \frac{(2^{3\lceil \log_2 p \rceil - 5}-1)\lceil \log_2 p \rceil (2n^2-2n+1)}{2m^2-2m+1}. \quad (3)$$

При цьому $p^n \approx 2^m$. Тоді $n \approx log_p 2^m = \frac{m}{log_2 p}$, $k_k \approx \frac{\frac{2m^2}{(log_2 p)^2} - \frac{2m}{log_2 p} + 1}{2m^2-2m+1} \approx log_2^{-1} p$,

$$k_{mul} \approx \frac{(2^{3*\lceil \log_2 p \rceil - 5}-1)(\log_2 p)}{log_2 p} \approx 2^{3*\lceil \log_2 p \rceil - 5} \quad (4)$$

Для малих *n* k_{mul} потрібно обчислювати за більш точними формулами (3, 4). З рис. 3 можемо бачити, що при збільшенні характеристики поля апаратні витрати стрімко зростають.

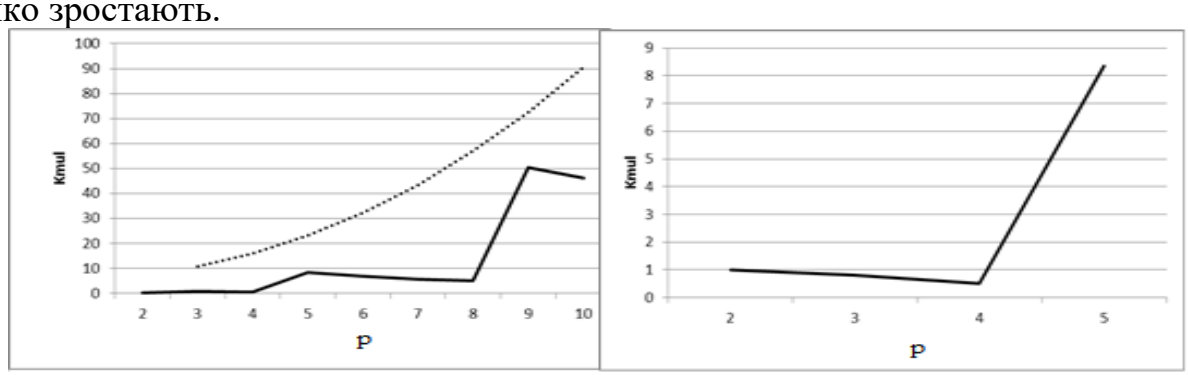

Рисунок 3 – Відношення апаратних витрат помножувачів елементів розширених полів Галуа $GF(p^n)$ та $GF(2^m)$, для структури МКГ ЧС, для різних діапазонів характеристики поля *p*

Найменші апаратні витрати, при реалізації МКГ ЧС для розширених полів Галуа $GF(p^n)$ будуть мати помножувачі для полів Галуа $GF(3^n)$, що видно із рис. 3.

Для варіанту ФВ, коли помножувач та суматор, які мають *2x* входів та *x* виходів кожний, для реалізації однієї МКГ буде потрібно $q_{ФВ} = 2(2^{2x-5} - 1)x\ LUT$.

Тоді: $\frac{q_{\text{ЧС}}}{q_{\text{ФВ}}} = \frac{(2^{3x-5}-1)\cdot x}{2(2^{2x-5}-1)\cdot x} \approx \frac{2^{3x-5}}{2(2^{2x-5})} = 2^{x-1} = 2^{\lceil \log_2 p \rceil - 1}$ – відношення витрат для реалізації однієї МКГ ЧС та МКГ ФВ. З формули видно, що внутрішня структура МКГ суттєво впливає на апаратні витрати. У порівнянні з МКГ ЧС, коли до уваги береться тільки кількість входів і виходів, додаткове врахування внутрішньої структури МКГ зменшує значення апаратної складності МКГ.

Проведемо оцінку апаратних витрат помножувача для МКГ ФВ. Для розширених полів Галуа $GF(2^m)$ $k_{g2} = 1$, для інших:

$$k_{gp} = (2^{2\lceil \log_2 p \rceil - 5} - 1)\lceil \log_2 p \rceil 2 \quad (5)$$

У розширених полях Галуа $GF(2^m)$, для реалізації помножувача потрібно $2m^2-2m+1$ МКГ, а в полях Галуа $GF(p^n)$ – $2n^2-2n+1$ МКГ. Отже: $k_k \approx \frac{2n^2-2n+1}{2m^2-2m+1}$.

При цьому $p^n \approx 2^m$. Тоді $n \approx log_p 2^m = \frac{m}{log_2 p}$,

$$k_k \approx \frac{(\frac{2m^2}{log_2^2 p}-\frac{2m}{log_2 p}+1)}{2m^2-2m+1} \approx log_2^{-1} p, \qquad k_{mul} \approx \frac{\left(2^{2*\lceil \log_2 p\rceil-5}-1\right)*\lceil \log_2 p\rceil*2}{\log_2 p} \approx 2^{2*\lceil \log_2 p\rceil-4} \quad (6)$$

Порівнюючи формули для знаходження k_{mul} для МКГ ЧС (4) та МКГ ФВ (6) видно, що для МКГ ФВ при великих значеннях p загалом зменшується значення апаратної складності помножувача в $2^{\lceil \log_2 p\rceil-1}$ рази.

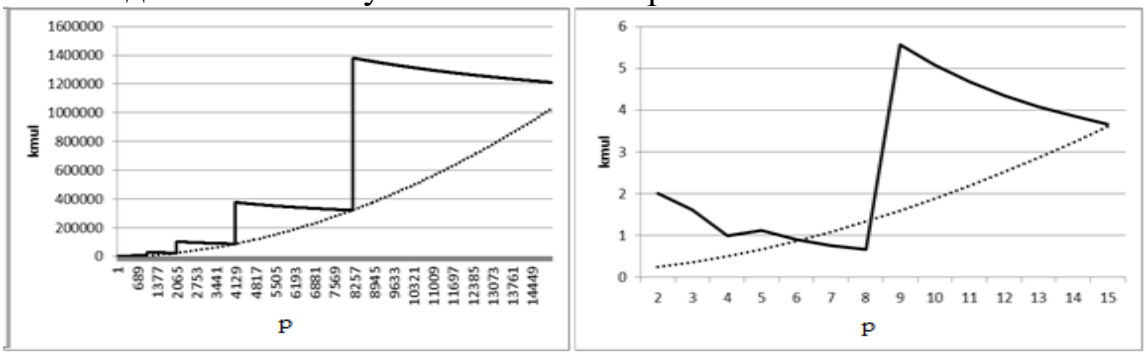

Рисунок 4 – Відношення апаратних витрат помножувачів елементів розширених полів Галуа $GF(p^n)$ та $GF(2^m)$ для структури МКГ ФВ, для різних діапазонів характеристики поля p

Як видно з рис. 4 найменші апаратні витрати для структури МКГ ФВ мають розширені поля Галуа $GF(7^m)$.

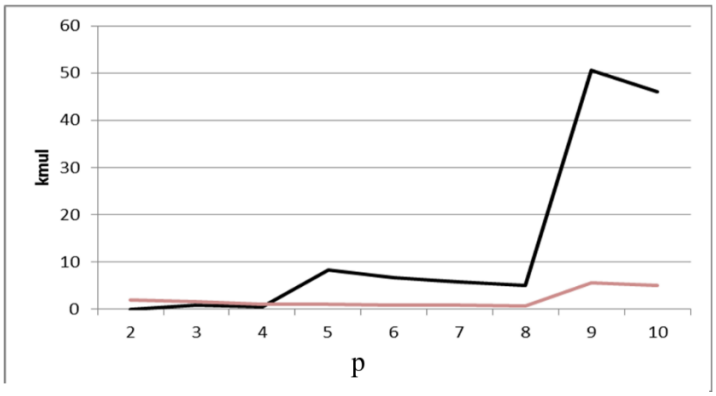

Рисунок 5 – Відношення апаратних витрат помножувачів елементів розширених полів Галуа $GF(p^n)$ та $GF(2^m)$ з структурами ЧС та ФВ

На рис. 5 наведено відношення апаратних витрат помножувачів елементів розширених полів Галуа $GF(p^n)$ до $GF(2^m)$ із структурами ЧС та ФВ.

При побудові помножувачів елементів розширених полів Галуа $GF(p^n)$ з великою характеристикою поля постає потреба у створенні МКГ з великою кількістю входів. В такому випадку булеві функції стають складними. У даному випадку помножувач та суматор, що працюють за модулем p у МКГ, можна представити такими, що складаються з базових функціональних логічних вузлів (ЛВ): мультиплексорів, однорозрядних двійкових суматорів та інших.

За варіантом ЛВ помножувач можна представити як матричний помножувач з прямим та зворотнім ходом (рис. 6). При прямому ході обчислень виконується операція множення, а при зворотному – знаходження остачі від ділення методом без відновлення залишків. При прямому ході одну комірку *SMn* можна реалізувати на *KLUT1 = 2* елементах *LUT* (4 входи та 2 виходи), при зворотному – один елемент *SMch* на *KLUT2 = 2* елементах *LUT* (5 входів, 2 виходи), а елементи *Sn* – на *KLUT3* =

1 (3 входи, 1 вихід) та *Rn* – на *KLUT4 = 1* (2 входи, 1 вихід) елементів *LUT*. Суматор *SUM_G* модифікованої комірки Гілда (рис. 7) будується за допомогою ланцюжка повних однорозрядних двійкових суматорів. Два таких суматора (5 входів, 3 виходи) можна представити за допомогою 3 *LUT*, отже *KLUT5 = 3*.

SMn – елемент помножувача, який виконує операцію модульного множення та додавання і має виходи результату та переносу, тобто, це комірка Гілда. *SMch* – елемент, який виконує операцію додавання або віднімання числа в доповняльному коді при діленні без відновлення залишків. *Sn* – це вузол, який визначає тип операції, віднімання чи додавання, при діленні без відновлення залишків. *Rn* – елемент, який визначає чи потрібно проводити ще одну операцію додавання для знаходження результату.

Коефіцієнт апаратних витрат помножувача для елементів поля $GF(p^n)$ відносно аналогічних витрат помножувача для елементів поля $GF(2^m)$ $k_{mul} = k_g k_k$, де $k_g = \frac{k_{gp}}{k_{g2}}$, $k_k = \frac{k_{kp}}{k_{k2}}$ – коефіцієнти складності та кількості МКГ, k_{gp} та k_{g2}, k_{kp} та k_{k2} – кількість *LUT* у МКГ та кількість МКГ для полів Галуа $GF(p^n)$ та $GF(2^m)$, відповідно.

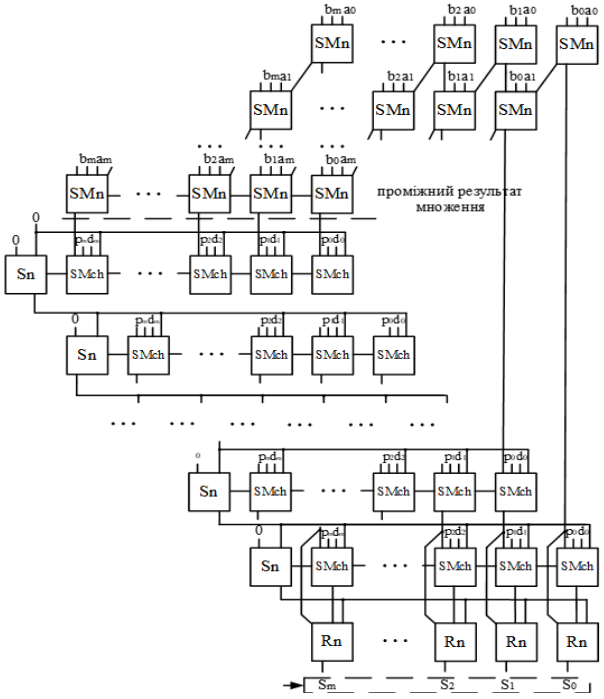

Рисунок 6 – Представлення внутрішньої структури помножувача *MUL_G* МКГ *GF(p^m)*

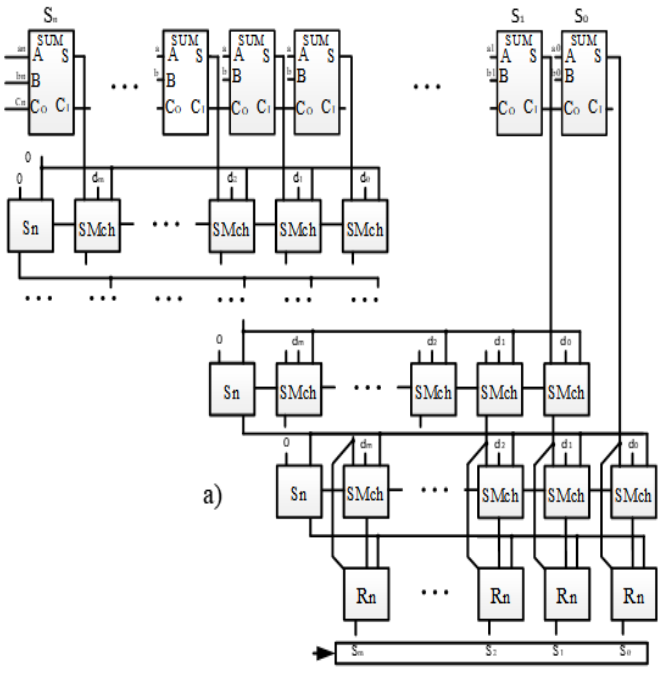

Рисунок 7 – Представлення внутрішньої структури суматора *SUM_G* МКГ *GF(p^m)*

Для розширених полів Галуа $GF(p^n)$ $k_{g2} = 7$, для інших: k_{gp}= *KSMn* × *KLUT1* + *KSMch* × *KLUT2* + *KSn* × *KLUT3* + *KRn* × *KLUT4* + *KSUMn* × *KLUT5*, *KSMn*, *KSMch*, *KSn*, *KRn* – кількість елементів, відповідно, *SMn*, *SMch*, *Sn*, *Rn* в помножувачі елементів розширених полів Галуа (рис. 6).

$$k_{gp} = (\lceil \log_2 p \rceil)^2 * 2 + (\lceil \log_2 p \rceil)^2 * 2 + \lceil \log_2 p \rceil * 1 + \lceil \log_2 p \rceil * 1 + \lceil \log_2 p \rceil * \frac{3}{2};$$

$$k_{gp} = 2(\lceil \log_2 p \rceil)^2 + 2(\lceil \log_2 p \rceil)^2 + 2\lceil \log_2 p \rceil + \frac{3}{2}\lceil \log_2 p \rceil = 4(\lceil \log_2 p \rceil)^2 + \frac{7}{2}\lceil \log_2 p \rceil.$$

$k_{gp}=(2(\lceil\log_2 p\rceil)^2+2(\lceil\log_2 p\rceil)^2+\frac{1}{2}\lceil\log_2 p\rceil+2\lceil\log_2 p\rceil=4\left(\lceil\log_2 p\rceil)^2+\frac{7}{2}\lceil\log_2 p\rceil\right)/7.$

В розширених полях Галуа $GF(2^m)$ для реалізації помножувача потрібно $k_{k2}=2m^2-2m+1$ МКГ, а в полях Галуа $GF(p^n)$ з характеристикою поля p – $k_{kp}=2n^2-2n+1$. Також додатково $(n-1)(2^{3\lceil\log_2 p\rceil-5}-1)\lceil\log_2 p\rceil$ *LUT* для знаходження коефіцієнта, на який перемножуємо незвідний поліном (цими апаратними витратами можна, в даному випадку, знехтувати, оскільки вони малі в порівнянні з витратами на реалізацію самих МКГ). Отже:

$$k_k\approx\frac{2n^2-2n+1}{2m^2-2m+1}\approx\frac{n^2}{m^2}\approx\left(\frac{n}{m}\right)^2 \text{ для великих } n \text{ (7);} \qquad k_{mul}\approx\frac{(4(\lceil\log_2 p\rceil)^2+\frac{7}{2}\lceil\log_2 p\rceil)n^2}{7m^2} \qquad (8)$$

При цьому $p^n\approx 2^m$. Тоді $n\approx log_p\,2^m=\frac{m}{log_2 p}$, $k_k\approx log_2^{-2}\,p$, $k_{mul}\approx\frac{4(\lceil\log_2 p\rceil)^2+\frac{7}{2}\lceil\log_2 p\rceil}{7(log_2 p)^2}$. $lim_{p\to\infty}\,k_{mul}=4/7$. Графік функції k_{mul} наведено на рис. 8.

Для $n < 10$ k_{mul} треба розраховувати за більш точними формулами (7, 8).

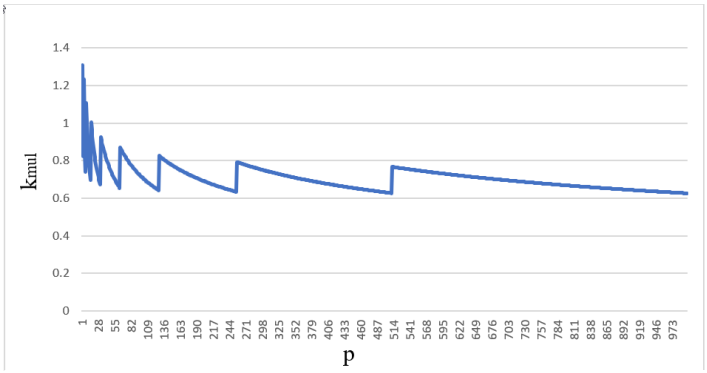

Рисунок 8 – Відношення апаратних витрат помножувачів елементів розширених полів Галуа $GF(p^n)$ та $GF(2^m)$ для структури МКГ ЛВ

Як видно з рис. 8 відношення апаратних витрат на реалізацію помножувачів у полі $GF(p^n)$ до $GF(2^m)$, при збільшенні характеристики поля будуть прямувати до асимптотичного значення $4/7$, що говорить про перевагу, з точки зору апаратних витрат, використання розширених полів Галуа з великою характеристикою p поля порівняно з двійковими розширеними полями Галуа при реалізації МКГ у варіанті ЛВ.

Метод створення паралельних помножувачів для вузлів КЗІ на основі МКГ забезпечує синтез помножувачів на основі МКГ з 3 варіантами їх структури: ЧС, ФВ, ЛВ

Створення паралельних помножувачів для вузлів КЗІ на основі МКГ із структурою ЧС

Створення паралельних помножувачів для вузлів КЗІ поділяється на створення МКГ, створення інвертора за модулем *p* – вузла *f*, створення помножувача на основі МКГ та вузла *f*. Алгоритми створення вузла *f*, МКГ, помножувача та криптопроцесора наведено нижче.

Алгоритм створення МКГ з структурою ЧС:

1.Задання характеристики *p* поля та порядку *n* утворюючого поле полінома.

2. Генерування булевих функцій, які описують МКГ як “чорну скриньку” *res = (((a × b) mod p) + c) mod p*, де *p* – характеристика поля, *a, b, c* – входи МКГ, *res* – вихід МКГ.

3. Мінімізація булевих функцій, які описують МКГ, методом Квайна–Мак-Класкі–Петрика.

4. Генерування *HDL*-опису МКГ за створеними булевими функціями.

Алгоритм створення інвертора за модулем *p* – вузла *f*:

1. Завдання характеристики *p* поля та порядку *n* утворюючого поле полінома.

2. Генерування булевих функцій для вузла *f*:

$f = (p - G_n) \bmod p = (-G_n) \bmod p$, де p – характеристика поля, G_n – результат на виході МКГ при прямому ході обчислень, *f* – результат.

3. Мінімізація булевих функцій, які описують вузол *f*, методом Квайна–Мак-Класкі–Петрика.

4. Генерування *HDL*-опису вузла *f* за створеними булевими функціями.

Алгоритм створення помножувача:

1. Створення матриці для розміщення МКГ та вузлів *f*.

2. Наповнення матриці вузлами МКГ та *f*.

3. Опис зв'язків між МКГ та вузлами *f*.

4. Створення *HDL*-опису помножувача.

Далі можливе створення криптопроцесора, який використовує синтезований помножувач.

Алгоритм створення криптопроцесора:

1. Генерування *HDL*-опису арифметико-логічного пристрою, який виконує операції над елементами розширених полів Галуа $GF(p^n)$.

2. Генерування *HDL*-опису криптопроцесора, який виконує операції над точками ЕК з використанням створеного АЛП.і

Створення паралельних помножувачів для вузлів КЗІ на основі МКГ з структурою ФВ

Алгоритми створення інвертора за модулем *p* – вузла *f*, помножувача та криптопроцесора, наведено вище. Вони є спільними для всіх структур МКГ.

Алгоритм створення МКГ з структурою ФВ складається з наступних кроків:

1. Задання характеристики *p* поля та порядку *n* утворюючого поле полінома.

2. Генерування булевих функцій, які описують помножувач МКГ:

$res_{mul} = (a \times b) \bmod p$, де p – характеристика поля, a, b – входи помножувача (*MUL*) МКГ, res_{mul} – вихід.

3. Мінімізація булевих функцій, які описують помножувач, методом Квайна–Мак-Класкі–Петрика.

4. Генерування *HDL*-опису помножувача (*MUL*).

5. Генерування булевих функцій, які описують суматор МКГ:

$res_{sum} = (res_{mul} + c) \bmod p$, де p – характеристика поля, res_{mul}, c – входи суматора (*SUM*) МКГ, *res* – вихід.

6. Мінімізація булевих функцій, які описують суматор, методом Квайна–Мак-Класкі–Петрика.

7. Генерування *HDL*-опису суматора (*SUM*).

8. Генерування *HDL*-опису МКГ із описів створеного помножувача (*MUL*) та суматора (*SUM*).

Створення паралельних помножувачів для вузлів КЗІ на основі МКГ з структурою ЛВ

Алгоритми створення інвертора за модулем *p* – вузла *f*, помножувача та крип-

топроцесора, наведено вище. Вони є спільними для всіх структур МКГ.

Алгоритм створення МКГ з структурою ЛВ складається з наступних кроків:

1. Завдання характеристики *p* поля та порядок *n* утворюючого поле полінома.

2. Створення матриці, у кожному елементі якої може бути або елемент *SMn* (КГ), який формує сигнали $C,S = ((a \times b) \bmod p) + c$, де *p* – характеристика поля, *a, b, c* – входи КГ, *S* – вихід результату, *C* – вихід переносу, або елемент *SMch*, який формує сигнали *Cout,S = A+E+(B&D or Cin&notD)*, де *A, B, Sel* – входи мультиплексора, *A, B, Ci* – входи суматора, *Cout, S* – виходи суматора.

3. Створення списку елементів *Sn*: *S = A xor B xor C, Rn: S = A & B or C & notB*, та *SUM*.

4. Визначення, де саме у матриці потрібно поставити вузли *SMn* та *SMch*.

5. Встановлення зв'язків з входами *A, B, C* та виходами *S* та *Co* вузла *SMn*, входами *A, B, C, D, E* та виходами *S* та *Co* вузла *SMch*.

6. Встановлення зв'язків з елементами *Sn* та *Rn*.

7. Встановлення зв'язків входів МКГ *A, B, C* та виходу МКГ *S*.

8. Генерування *HDL*-опису МКГ.

Метод оцінювання часової складності виконання множення елементів розширених полів Галуа $GF(p^n)$ апаратним способом

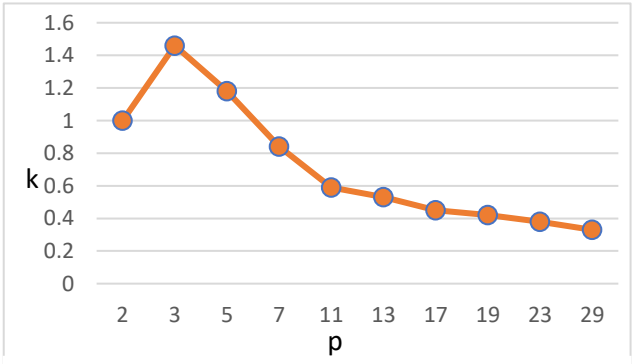

Рисунок 9 – Відносний час виконання множення елементів розширених полів Галуа $GF(p^n)$ у математичному пакеті *Maple*

Метод складається з наступних кроків:

1. Генерування помножувача.

2. Створення проекту у середовищі *Xilinx Vivado*.

3. Тестування згенерованого помножувача.

4. Проведення імплементації згенерованого помножувача.

5. Визначення максимальної часової затримки Tапар. помножувача. Інформація про максимальну часову затримку береться з середовища *Xilinx Vivado* або із звітів, які формуються після імплементації.

6. Визначення часу Tпрогр. множення у математичному пакеті *Maple*.

7. Визначення відношення часових витрат при програмній та апаратній реалізаціях множення елементів розширених полів Галуа $GF(p^n)$ $k = \frac{T\text{прогр.}}{T\text{апар.}}$.

Метод оцінювання апаратної складності помножувачів елементів розширених недвійкових полів Галуа $GF(p^n)$

Метод складається з наступних кроків:

1. Задання параметрів полів *p, n, m*, таких, що $p^n \approx 2^m$.

2. Визначення апаратних витрат у полі $GF(2^m)$.

3. Визначення апаратних витрат у полі $GF(p^n)$.

4. Визначення відносної апаратної складності як відношення апаратних витрат для полів $GF(p^n)$ та $GF(2^m)$ за формулами (1) – (8) з врахуванням коефіцієнта *Co*

(відносний порядок поля $GF(p^n)$, наведено у таблиці 4.5). Кращим вважається поле з меншим показником розрахованої відносної апаратної складності.

5. Перевірка розрахованого теоретичного показника відносної апаратної складності з результатами імплементації помножувача на ПЛІС:

1) створення помножувачів описаним вище методом;

2) створення проекту у середовищі *Xilinx Vivado*;

3) тестування створених помножувачів;

4) імплементація створених помножувачів (1 помножувач у проекті) (рис. 2.21).

6. Одним з результатів імплементації є звіт, де вказано кількість *LUT*, які було задіяно для імплементації помножувача. Кількість *LUT* є результатом оцінювання.

7. Визначення відносної апаратної складності результатів імплементації як відношення кількості *LUT* у помножувачах для полів $GF(p^n)$ та $GF(2^m)$.

Метод тестування генераторів ядер помножувачів елементів розширених полів Галуа $GF(p^n)$

Метод складається з наступних кроків:

1. Визначення поліному, який утворює розширене поле Галуа $GF(p^n)$, за допомогою математичного пакету *Maple*.

2. Генерування помножувача одним із описаних вище методів.

3. Моделювання у середовищі *Active HDL* роботи помножувача на тестових прикладах, а саме, e_{max} – максимально великий код елемента поля. Проводимо моделювання множення елементів: $e_{max} \times (e_{max} - 1)$; $e_{max} \times 0$; $e_{max} \times 1$.

4. Виконання множення цих елементів у математичному пакеті *Maple*.

5. Виконання множення цих елементів за допомогою бібліотеки *C++ GaloisCPP*.

6. Порівняння результатів. Усі три результати повинні збігатися, що є ознакою правильної роботи помножувача, а також запропонованих методів створення помножувачів та технологічного засобу (генератора ядер), який реалізує ці методи.

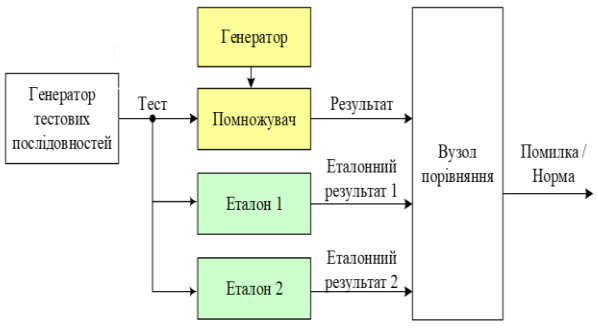

Рисунок 10 – Структурна схема процесу тестування генераторів ядер помножувачів елементів розширених полів Галуа $GF(p^n)$ з використанням 2 еталонів

На рис. 10 наведено структурну схему процесу тестування генератора помножувачів елементів розширених полів Галуа $GF(p^n)$ з використанням двох еталонів. Тестування починається із генерування тестових послідовностей, які подаються на помножувач, згенерований генератором та еталони. Далі результати подаються на вузол порівняння. При невідповідності результатів робимо висновок, що тестований об'єкт працює неправильно. Як еталони використовуються результати множення елементів розширених полів Галуа $GF(p^n)$ у математичному пакеті *Maple* та з використанням бібліотеки *GaloisCPP*.

У **третьому розділі** описано процес розробки засобів створення (генераторів ядер) помножувачів елементів розширених полів Галуа $GF(p^n)$ для вузлів КЗІ КФС. Генератори були реалізовані мовою *C++*. На рис. 11 наведено структурну схему генераторів. Генератори створюють *VHDL*-описи (ядра) помножувачі за запропонованим у роботі методом створення на ПЛІС генераторів моделей (ядер) реконфігурованих паралельних помножувачів елементів розширених полів Галуа $GF(p^n)$ для вузлів КЗІ у КФС.

Процес генерування помножувачів поділяється на такі етапи:

1) генерування булевих функцій для вузлів;
2) мінімізація цих функцій;
3) створення *VHDL*-описів вузлів помножувачів: *F*, *SUM*, *MUL*, *SMn*, *SMch*, *Sn*, *Rn* (тільки для ФВ та ЛВ);
4) створення *VHDL*-описів МКГ (*MGC*);
5) встановлення зв'язків між згенерованими вузлами (створення *VHDL*-описів помножувачів).

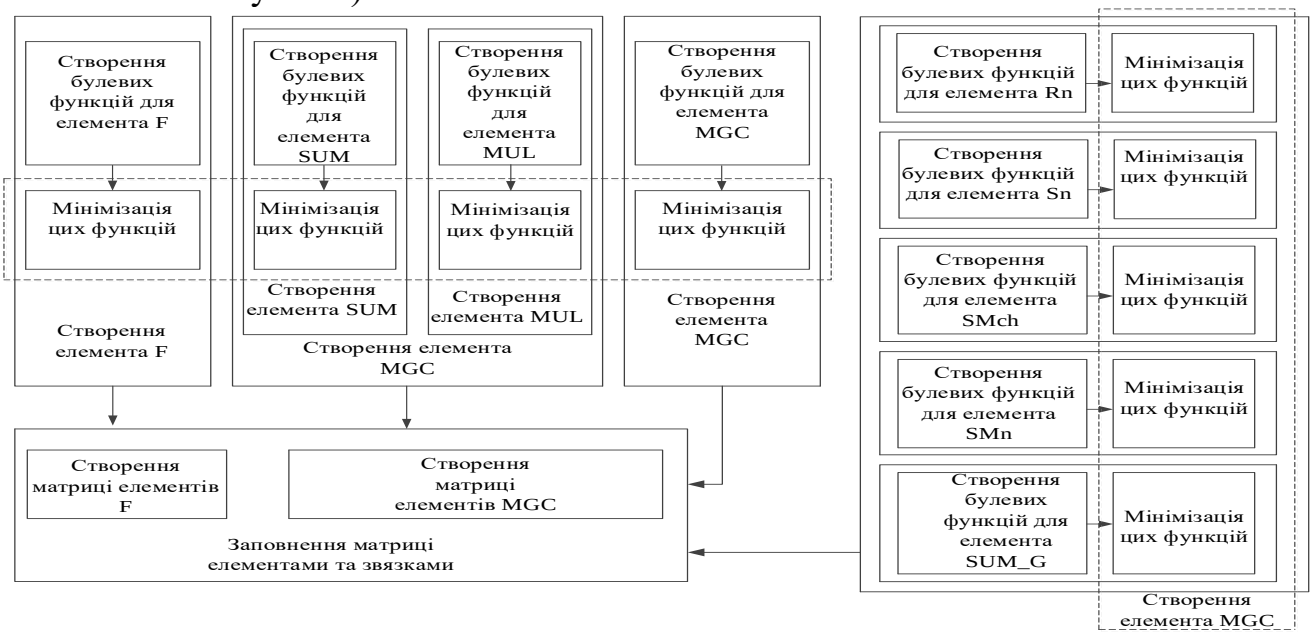

Рисунок 11 – Структурна схема генераторів ядер (*VHDL*-описів) помножувачів елементів розширених полів Галуа $GF(p^n)$

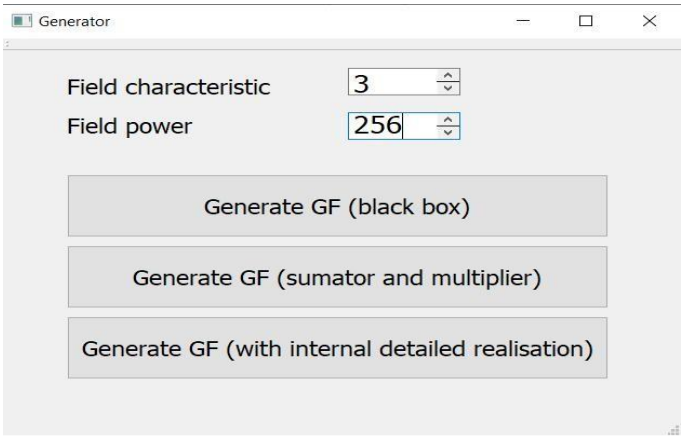

Рисунок 12 – Інтерфейс генераторів помножувачів елементів розширених полів Галуа $GF(p^n)$

Мінімізація булевих функцій відбувається методом Квайна–Мак-Класкі –Петрика. Цей процес дуже тривалий. На рис. 12 зображено інтерфейс генераторів помножувачів елементів розширених полів Галуа $GF(p^n)$. Синтезовані схеми використовуються в середовищі *Xilinx Vivado* для проектування топології кристалу ПЛІС та визначення уточнених апаратних та часових параметрів помножувачів.

Генерування помножувачів елеме-

нтів розширених полів Галуа $GF(p^n)$ з великими характеристиками поля та порядками є дуже часозатратною задачею. Найбільше часу при побудові МКГ займає процес мінімізації булевих функцій. Наприклад, генерація помножувача для поля $GF(53^{174})$ триває 1845 с.

Також у цьому розділі описано процес і наведено результати тестування згенерованих помножувачів запропонованим у роботі методом. Було протестовано роботу помножувачів для полів $GF(3^{30})$, $GF(7^{17})$, $GF(23^{10})$, $GF(53^{8})$ і показано правильність роботи генераторів ядер помножувачів елементів розширених полів Галуа $GF(p^n)$ та самих помножувачів.

В кінці розділу наведено шляхи можливого покращення характеристик помножувачів шляхом конвеєризації їх структури.

Четвертий розділ присвячено дослідженню створених в ході виконання роботи операційних вузлів (помножувачів) для полів Галуа, які застосовуються у криптографічних засобах захисту інформації на базі ЕК. Дослідження проводилися під час впровадження результатів дисертаційної роботи.

Наукові положення та висновки, сформульовані в дисертації, її результати використано під час реалізації проектних завдань у міжнародній компанії "JETSOFTPRO" (Україна, Польща, США) та в українській компанії ТзОВ “Кіберенергія” (Львів, Україна), що підтверджено відповідними актами впровадження. Також ці результати використовувалися у науково-дослідній роботі на кафедрі електронних обчислювальних машин Інституту комп'ютерних технологій, автоматики та метрології Національного університету "Львівська політехніка" ДБ/КІБЕР (номер державної реєстрації 0115U000446), що підтверджено відповідним актом впровадження. Також результати дисертації використовувались під час підготовки та викладання навчальних курсів з дисципліни "Дослідження і проектування комп'ютерних систем та мереж" на освітньо-кваліфікаційному рівні "Магістр" для спеціальності 123 "Комп'ютерна інженерія" для спеціалізацій "Комп'ютерні системи та мережі", "Кіберфізичні системи" та "Системне програмування", що підтверджено відповідним актом впровадження.

У таблиці 1 наведено реальні та теоретичні результати генерації ядер (*VHDL*-описів) помножувачів для ПЛІС *Virtex UltraScale+ XCVU9P*. При реалізації помножувачів з структурою МКГ ЧС, апаратна складність швидко зростає зі збільшенням характеристики поля. Ці витрати найменші для двійкових і трійкових полів Галуа. При реалізації помножувачів з структурою МКГ ФВ, апаратна складність також швидко зростає зі збільшенням характеристики поля. Найменшу апаратну складність за цією структурою МКГ мають помножувачі для полів з характеристиками $p = 2, 3, 5, 7$. При реалізації помножувачів на основі МКГ ЛВ, апаратна складність збільшується зі збільшенням характеристики поля. Отже, за трьома згаданими структурами МКГ можна для обраного поля з використанням створеного генератора ядер згенерувати *VHDL*-опис помножувача, який правильно сприймається засобами проектування ПЛІС, що дозволяє визначити реальні апаратні та часові характеристики помножувача. У таблицях також показано час генерації помножувача. Час збільшується зі збільшенням характеристики поля.

Таблиця 1

Апаратні витрати LUT реальні NR_p та теоретичні NT_p та час генерування помножувачів елементів розширених полів Галуа $GF(p^n)$ на ПЛІС Virtex UltraScale+ XCVU9P, які мають 2069000 LUTs

Поле	p	Порядок $GF(p^n)$, O_p	МКГ ЧС			МКГ ФВ			МКГ ЛВ		
			NR_p	T, *sec.*	NT_p	NR_p	T, *sec.*	NT_p	NR_p	T, *sec.*	NT_p
$GF(2^{50})$	2	1,12E+15	2504	1,0	4901	2190	0,5	2450	18784	0,5	29208
$GF(3^{32})$	3	1,85E+15	4034	1,4	3970	4032	0,7	1984	17950	0,5	36510
$GF(5^{22})$	5	2,38E+15	19936	1,6	41625	5615	0,8	2768	17867	0,5	35049
$GF(7^{18})$	7	1,62E+15	16851	3,0	27585	3522	1,2	1837	16689	0,5	23366
$GF(13^{14})$	3	3,93E+15	81133	8,0	185420	10211	2,0	10216	43368	0,5	58656

У таблиці 2 показано порівняння теоретичних KT_{mul} і реальних KR_{mul} апаратних витрат на реалізацію помножувачів елементів розширених полів Галуа $GF(p^n)$ відносно апаратних витрат на реалізацію помножувачів двійкових полів Галуа $GF(2^m)$ KT_2 і KR_2, МКГ реалізується за 3 структурами. $KT_{mul} = NT_d/NT_2$, $KR_{mul} = NR_d/NR_2$.

NT_p – теоретична кількість *LUT* у помножувачі для поля $GF(p^n)$;

NR_p – реальна кількість *LUT* у помножувачі для поля $GF(p^n)$;

T – час генерування помножувача.

З таблиці 2 та графіку рис. 13 видно, що для МКГ ЧС за апаратними витратами трійкові поля Галуа $GF(3^n)$ на 3 % кращі, ніж двійкові $GF(2^m)$. При реалізації помножувачів на МКГ ФВ у порівнянні з полями $GF(2^m)$ – поле з $GF(3^n)$ має на 11 % більшу апаратну складність, поле $GF(5^n)$ має на 20 % більшу апаратну складність, поле $GF(7^n)$ має на 18 % більшу апаратну складність. При реалізації помножувачів на основі МКГ ЛВ апаратна складність помножувачів є більшою ніж у помножувачів з структурами МКГ ЧС та МКГ ФВ.

Таблиця 2

Порівняння реальних та теоретичних апаратних витрати *LUT* на ПЛІС при реалізації помножувачів полів Галуа на ПЛІС *Virtex UltraScale+ XCVU9P* які мають 2069000 *LUTs*

Поле	p	Порядок $GF(p^n)$, O_p	$C_o = \frac{O_p}{O_2}$	МКГ ЧС				МКГ ФВ				МКГ ЛВ			
				KT_{mul}	$\frac{KT_{mul}}{C_o}$	KR_{mul}	$\frac{KR_{mul}}{C_o}$	KT_{mul}	$\frac{KT_{mul}}{C_o}$	KR_{mul}	$\frac{KR_{mul}}{C_o}$	KT_{mul}	$\frac{KT_{mul}}{C_o}$	KR_{mul}	$\frac{KR_{mul}}{C_o}$
$GF(2^{50})$	2	1,12E+15	1	1	1	1	1	1	1	1	1	1	1	1	1
$GF(3^{32})$	3	1,85E+15	1,65	0,81	0,43	1,61	0,97	0,81	0,49	1,84	1,11	1,25	0,75	0,95	0,57
$GF(5^{22})$	5	2,38E+15	2,12	8,49	4	7,96	3,75	1,13	0,53	2,56	1,2	1,2	0,56	0.95	0,44
$GF(7^{18})$	7	1,62E+15	1,35	5,63	4,17	6,72	4,97	0,75	0,55	1,6	1,18	0,8	0,59	0,88	0,65
$GF(13^{14})$	13	3,93E+15	3,5	37,8	10,8	32,40	9,25	4,17	1,19	4,65	1,32	2,0	0,57	2.3	0.65

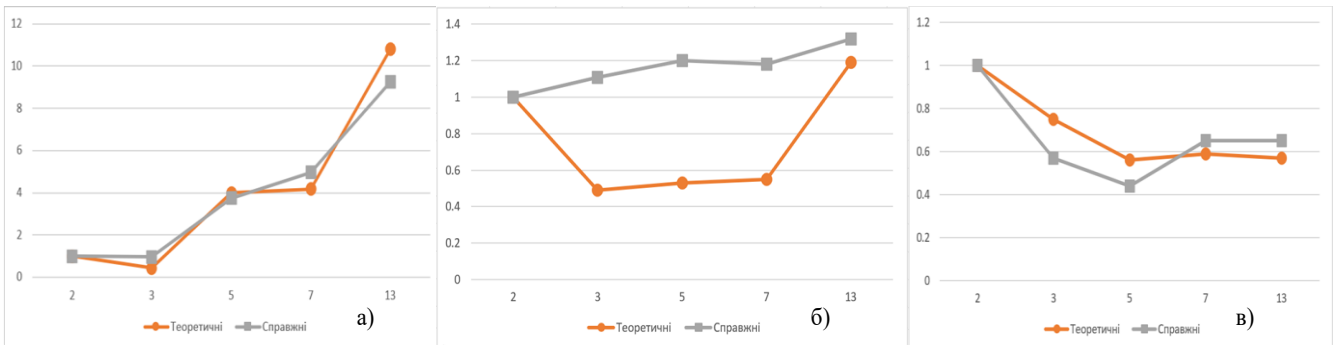

Рисунок 13 – Порівняння теоретичних $\frac{KT_{mul}}{C_o}$ та реальних $\frac{KR_{mul}}{C_o}$ коефіцієнтів апаратних витрат на реалізацію помножувачів за варіантами: а) МКГ ЧС, б) МКГ ФВ, в) МКГ ЛВ

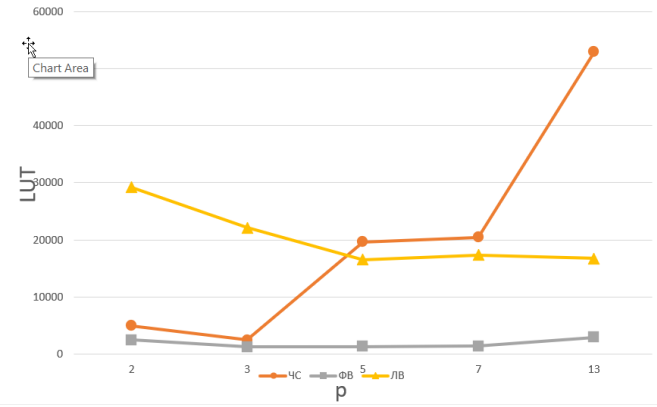

Рисунок 14 – Порівняння теоретичних апаратних витрат на реалізацію помножувачів за 3 структурами МКГ: ЧС, ФВ, ЛВ

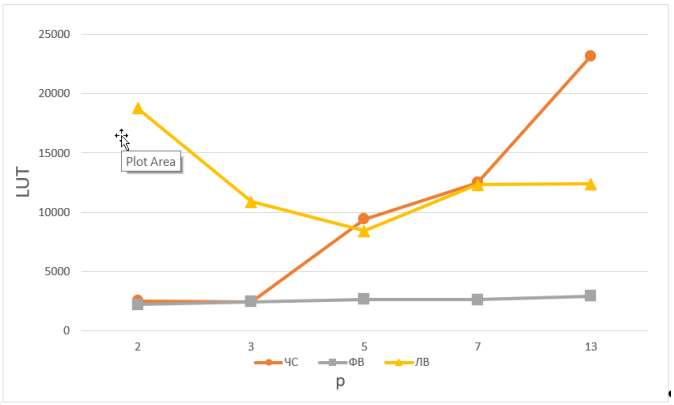

Рисунок 15 – Порівняння реальних апаратних витрат на реалізацію помножувачів за 3 структурами МКГ: ЧС, ФВ, ЛВ

На рис. 14 наведене порівняння теоретичних, а на рис. 15 реальних апаратних витрат на реалізацію помножувачів за 3 структурами МКГ: ЧС, ФВ, ЛВ. З графіків видно, що теоретичні та реальні апаратні витрати збігаються та метод оцінювання апаратної складності помножувачів забезпечує похибку прогнозування величини цих показників до 56 %. Також видно, що структура МКГ ЧС має переваги при реалізації МКГ для полів $GF(p^n)$ з характеристиками $p = 2$ та $p = 3$. Структура МКГ ФВ забезпечує найменші апаратні витрати, при реалізації помножувачів елементів полів $GF(p^n)$ з характеристиками $p = 2$, $p = 3$, $p = 5$, $p = 7$. Апаратна складність помножувачів для елементів полів $GF(p^n)$ з структурою МКГ ЧС більша ніж для помножувачів з структурою МКГ ФВ. Якщо порівнювати недвійкові розширені поля Галуа $GF(p^n)$, то з таблиці 2 видно, що найменшу апаратну складність будуть мати помножувачі для поля $GF(3^n)$, на 8 % більшу – для поля $GF(5^n)$ та на 6 % більшу – для поля $GF(7^n)$.

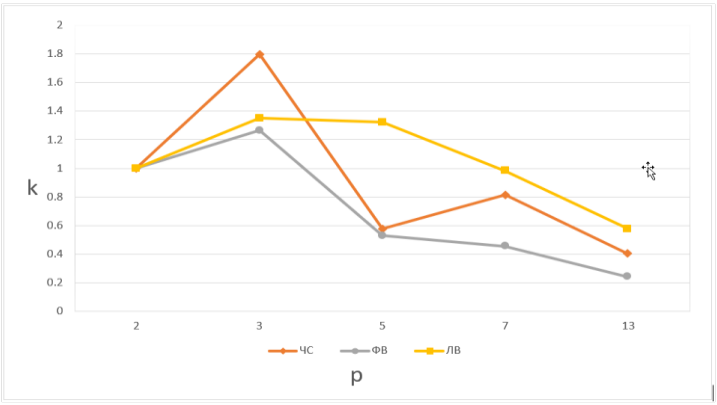

Рисунок 16 – Відношення часових витрат *k* при програмній та апаратній реалізаціях множення елементів полів $GF(p^n)$ за 3 структурами МКГ: ЧС, ФВ, ЛВ

На рис. 16 наведено відношення *k* часових витрат при програмній та апаратній реалізаціях множення елементів полів $GF(p^n)$ на ПЛІС *Virtex UltraScale+ XCVU9P*. З рис. 16 видно, що у порівнянні з двійковими полями найбільше відношення *k* часових витрат для структури МКГ ЧС мають поля з характеристикою 3 (в 1,8 разів більше), з структурою ФВ – поля з характеристикою 3 (в 1,27 разів більше), з структурою ЛВ – поля з характеристикою 3 (в 1,36 разів більше). Тобто, найкращим з огляду на криптографічну стійкість є поле $GF(3^n)$, яке в найгіршому випадку (структура МКГ ФВ, рис. 16) забезпечує в 1,27 разів більший внесок в криптографічну стійкість засобів КЗІ ніж поле $GF(2^m)$, тобто, найбільше ускладнить проведення криптоаналізу програмними методами, у порівнянні з іншими полями.

ВИСНОВКИ

У цій дисертаційній роботі було здійснено системний аналіз поточного стану теорії, методів та інструментів для проектування засобів КЗІ КФС. Також проведено дослідження ключових відкритих стандартів та алгоритмів КЗІ. Це дало змогу визначити мету та завдання дослідження. При цьому у роботі досягнуто таких результатів:

1. Отримав подальший розвиток метод оцінювання часової складності множення елементів розширених полів Галуа $GF(p^n)$ апаратним способом, за яким помножувач складається з МКГ, що дало можливість визначити поле $GF(3^n)$, у якому відношення часів множення програмним та апаратним способами перевищує таке відношення в інших полях щонайменше в 1,27 раза, чим забезпечує найбільшу криптографічну стійкість засобів КЗІ при інших однакових умовах.

2. Отримав подальший розвиток метод оцінювання апаратної складності помножувачів елементів розширених недвійкових полів Галуа $GF(p^n)$, де $p > 2$, який на відміну від відомих розглядає помножувачі для полів з приблизно однаковим порядком p^n і які складаються з МКГ, що дало можливість визначити поле $GF(3^n)$, де помножувачі мають щонайменше на 6 % меншу апаратну складність, у порівнянні з помножувачами для інших недвійкових полів.

3. Вперше запропоновано метод створення для ПЛІС генераторів моделей (ядер) реконфігурованих паралельних помножувачів елементів розширених полів Галуа $GF(p^n)$ для вузлів КЗІ у КФС, за яким на відміну від відомих генерується 3 варіанти помножувачів з 3 структурами МКГ, що дало можливість створити описи моделей помножувачів та визначити реальну апаратну складність кожного із помножувачів та обрати найкращу реалізацію для кожного конкретного поля.

4. Вперше запропоновано метод тестування генераторів ядер помножувачів елементів розширених полів Галуа $GF(p^n)$, який на відміну від відомих використовує 2 різні еталони (2 різні математичні пакети) для перевірки згенерованих помножувачів на основі МКГ, що дало можливість підтвердити правильну роботу генераторів помножувачів та самих помножувачів для всіх варіантів їх реалізації.

5. Розроблено генератори ядер (генератори моделей) помножувачів елементів розширених полів Галуа $GF(p^n)$ такими, що порядок поля $p^n < 2^{1024}$. Генератори створюють моделі помножувачів на основі МКГ з трьома варіантами структури МКГ: ЧС, ФВ, ЛВ. Це дало можливість створити ряд ядер помножувачів елементів розширених полів Галуа $GF(p^n)$ з трьома структурами МКГ та провести їх імплементацію на ПЛІС, провести порівняння результатів імплементації помножувачів для полів $GF(2^{15})$, $GF(2^{50})$, $GF(2^{998})$, $GF(3^9)$, $GF(3^{32})$, $GF(3^9)$, $GF(5^6)$, $GF(5^{22})$, $GF(7^5)$, $GF(7^{18})$, $GF(13^3)$, $GF(13^{14})$, $GF(13^{270})$. Показано збіжність теоретичних та практичних результатів оцінювання апаратної та часової складностей помножувачів.

6. На основі розроблених і вдосконалених методів проведено аналіз апаратних складностей створених помножувачів елементів розширених полів Галуа $GF(p^n)$, $p > 2$, що дало можливість визначити поля, які найкраще підходять для реалізації помножувачів. Найменшу апаратну складність мають помножувачі для полів $GF(3^n)$, на 6% більшу – для полів $GF(7^n)$ та на 8% - для полів $GF(5^n)$. Проведено аналіз ча-

сових складностей помножувачів елементів розширених полів Галуа $GF(p^n)$, $p > 2$, за відношенням часових витрат при програмній та апаратній реалізаціях, найкращим є поле $GF(3^n)$, відношення часових витрат у якому в 1,27 разів більше ніж у полі $GF(2^m)$.

Результати роботи впроваджено:

1) в міжнародній компанії “JETSOFTPRO”;

2) в українській компанії ТзОВ “Кіберенергія”;

3) в держбюджетній науково-дослідній роботі ДБ/КІБЕР (номер державної реєстрації 0115U000446);

4) у навчальному процесі кафедри ЕОМ НУ ”ЛП”.

Отримані під час виконання дисертаційної роботи наукові результати показують досягнення поставленої в роботі мети підвищення криптографічної стійкості засобів КЗІ, які використовуються в складі КФС, шляхом розвитку методів та засобів створення реконфігурованих операційних пристроїв (а саме, помножувачів) для роботи з елементами розширених полів Галуа $GF(p^n)$ з характеристиками p та з порядками n утворюючого поле полінома такими, що $p^n \approx 2^m$, де $p > 2$, $m \leq 1024$ створюють методологічну базу для розробки вузлів КЗІ, які дозволяють підвищити надійність, достовірність та захищеність сучасних апаратних засобів КЗІ, які працюють з використанням ЕК та розширених полів Галуа $GF(p^n)$.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Монографії

1. В.С. Глухов, І.М. Жолубак, Мохаммед Кадім Рахма Рахма. Принципи побудови та проектування операційних вузлів для полів Галуа, що використовуються в задачах криптографічного захисту інформації на основі еліптичних кривих. 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.

Публікації в журналах, що входять до наукометричних баз даних Scopus

1. Elias, R., Hlukhov, V., Rahma, M., Zholubak, I. Hardware Components for Post-Quantum Elliptic Curves Cryptography // Advanced Computer Information Technologies (ACIT 2018), Ceske Budejovice, Czech Republic, June 1–3, 2018. P. 236–239. (Scopus).

2. Zholubak, I., Rahma, M. K., Hlukhov, V. Automation System for Configuration of Cryptographic Data Protection Unit Model // 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 on ICT in Education, Research, and Industrial Applications (ICTERI 2018), Kyiv, Ukraine, May 14–17, 2018. С. 700–707. (Scopus).

3. Zholubak, I.M., Hlukhov, V.S. Galua Field Multipliers Core Generator. International Journal of Computer Network and Information Security, 2023. – Vol. 3. – Pp. 1–14. DOI: 10.5815/ijcnis.2023.03.01, (Scopus).

Публікації в матеріалах конференцій, що входять до наукометричних баз даних Scopus

1. Rahma, M., Zholubak, I., Hlukhov, V. Devices for multiplicative inverse calculation in binary Galois fields // The 9th IEEE International Conference on Dependable Systems, Services and Technologies (DESSERT'2018), Kyiv, Ukraine, 24–27 May 2018. P. 275–278. (Scopus).

2. Zholubak, I.M., Hlukhov, V.S. Comparison of hardware complexity of multipliers GF(p^m). In Proceedings of the 12th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2023. – Pp. 812–816. Dortmund, Germany. DOI: 10.1109/IDAACS-SWS50031.2020.9297059, (Scopus).

3. Zholubak, I.M., Hlukhov, V.S. Verification of Synthesized by the IP-core Generator Multipliers of Extended Galois Fields GF(p^n) Elements. In Proceedings of the 13th International Conference Dependable Systems, Services and Technologies (DESSERT), 2023. – Athens, Greece, (Scopus).

4. Zholubak, I.M., Hlukhov, V.S. Validation of Multipliers for Elements of Extended Galois Fields GF(p^n) and Multipliers IP-core Generator. In Proceedings of the 18th IEEE International Conference on Computer Science and Information Technologies (CSIT), 2023. – Lviv, Ukraine, (Scopus).

Статті у журналах, що включені до переліку наукових фахових видань України

1. В.С. Глухов, І.М. Жолубак, А.Т. Костик. Особливості опрацювання елементів трійкових полів Галуа на сучасній елементній базі. Вісник Національного університету "Львівська політехніка" "Комп'ютерні системи та мережі", № 830. Львів, 2015. С. 33 – 39.

2. Жолубак І. М., Глухов В.С. Визначення розширеного поля Галуа GF(d^m) з найменшою апаратною складністю помножувача. Вісник Національного університету «Львівська політехніка» "Інформаційні системи та мережі", № 854. Львів, 2016. С. 63 – 69.

3. Жолубак І. М., Глухов В. С. Апаратні витрати помножувачів полів Галуа GF(d^m) з великою основою. Вісник Національного університету «Львівська політехніка» "Комп'ютерні науки та інформаційні технології", № 864. Львів, 2017. С. 77 – 82.

4. Жолубак І. М., Глухов В. С. Реалізація у ПЛІС помножувачів елементів полів Галуа високих порядків. Вісник Національного університету «Львівська політехніка» "Комп'ютерні системи та мережі", № 881. Львів, 2017. С. 41 – 47.

5. Hlukhov, V., Kostyk, A., Zholubak, I., Rahma, M. Galois Fields Elements Processing Units for Cryptographic Data Protection in Cyber-Physical Systems // Advances in Cyber-Physical Systems. 2017. V. 2. № 2. P. 47–53.

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

7. Р.М. Еліас, В.С. Глухов, М. Рахма, І.М. Жолубак. Вбудований контроль пристроїв для опрацювання елементів розширених полів Галуа. Вісник Національного університету «Львівська політехніка» "Комп'ютерні системи та мережі", №

905. Львів, 2018. С. 64 – 72.

8. Жолубак І. М., Курман П. В. Система безконтактних платежів на основі технології NFC. Науковий журнал «Комп'ютерні системи та мережі», № 1. Львів, 2022. С. 28 – 37, DOI: https://doi.org/10.23939/csn2022.01.028

9. Жолубак І. М., Матвієць В. Ю. Трекер для сонячних електростанцій. Науковий журнал «Комп'ютерні системи та мережі», № 1. Львів, 2022. С. 37 – 46, DOI: https://doi.org/10.23939/csn2022.01.037

10. Bohdan Marii, Ivan Zholubak. Features of Development and Analysis of REST Systems. Advances in Cyber-Physical Systems. Volume 7. Number 2. Lviv Polytechnic National University. 2022. pp. 121 – 129, DOI: https://doi.org/10.23939/acps2022.02.121

11. Жолубак І. М., Аналіз алгоритмів множення в полях Галуа для криптографічного захисту інформації. Вісник Національного університету «Львівська політехніка» "Інформаційні системи та мережі", № 13. Львів, 2023. С. 338 – 349, DOI: https://doi.org/10.23939/sisn2023.13.338

Публікації у матеріалах конференцій, тезах доповідей та виданнях, що не включені до переліку наукових фахових видань України

1. Kostyk, A., Zholubak, I. Features of multiplication execution of operations in binary and ternary Galois fields // 5th International Youth Science Forum LITTERIS ET ARTIBUS 2015, Lviv, Ukraine, November 26–28, 2015.

2. В.С. Глухов, І.М. Жолубак. Порівняння апаратних витрат помножувачів елементів розширених полів Галуа. 17-а міжнародно науково-практична конференція «Сучасні інформаційні та електронні технології» Одеса, Україна, 23—27 травня 2016 р. С. 133 – 134.

3. І.М. Жолубак, В.С. Глухов. Визначення розширеного поля Галуа $GF(d^m)$ з найменшою апаратною складністю помножувача. Інформаційні технології та комп'ютерне моделювання: матеріали статей Міжнародної науково-практичної конференції, 23 – 28 травня 2016 року. - Івано-Франківськ. 2016. С. 80 - 81.

4. Глухов В.С., Жолубак І.М. Дослідження апаратної складності помножувачів елементів розширених полів Галуа $GF(d^m)$. Другий науковий семінар Кіберфізичні системи: досягнення та виклики, Львів, Національний університет «Львівська політехніка», 21-22 червня 2016 р. Матеріали Другого наукового семінару, с. 98 – 105.

5. Kostyk, A., Zholubak, I. The research of the binary codes program complication and application in cyber-physical systems // 6th International Youth Science Forum LITTERIS ET ARTIBUS 2016, Computer Science & Engineering (CSE-2016), Lviv, Ukraine, November 24–26, 2016.

6. Zholubak, I., Hlukhov, V. Research Hardware Complexity of Multipliers of Extended Galois Field GF(dm) // 6th International Youth Science Forum LITTERIS ET ARTIBUS 2016, Computer Science & Engineering (CSE-2016), Lviv, Ukraine, November 24–26, 2016.

7. Zholubak, I., Hlukhov, V. Hardware complexity of multipliers of extended Galois field in FPGA // 7th International Youth Science Forum LITTERIS ET ARTIBUS 2017, Computer Science & Engineering (CSE-2017), Lviv, Ukraine, November 23–25, 2017. P.

420–421.

8. Zholubak, I., Rahma, M., Hlukhov, V. Automation system program models configuration of cryptography cells in cyber-physical systems // 14th International Conference on ICT in Education, Research, and Industrial Applications (ICTERI 2018), Kyiv, Ukraine, May 14–17, 2018. P. 669–679.

9. Rodrigue Elias, Valerii Hlukhov, Mohammed Rahma, Ivan Zholubak. FPGA Cores for Fast Multiplicative Inverse Calculation in Galois Fields. Міжнародна науково-практична конференція «Електротехнічні та комп'ютерні системи: Теорія та практика» ЕЛТЕКС – 2018. м. Одеса, 29 травня - 1 червня 2018. Електротехнічні та комп`ютерні системи. – Одеса : – 2018. Вид-во Наука і техніка. 27(103), с. 227-233.

АНОТАЦІЯ

Жолубак І.М. Методи та засоби створення реконфігурованих вузлів криптографічного захисту інформації для кібер-фізичних систем. – 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". Львів, 2024.

У дисертації розв'язується важливе науково-технічне завдання створення реконфігурованих вузлів КЗІ на основі ЕК, які оперують у КФС елементами розширених полів Галуа $GF(p^n)$, де $p > 2$ – просте число, конфігурована характеристика поля, та n – порядок утворюючого поле полінома, степінь поля над його простим підполем. Проаналізовано апаратні витрати при реалізації таких систем у розширених полях Галуа $GF(p^n)$ з різною характеристикою p та порядком n утворюючого поле полінома. Запропоновано помножувач елементів таких полів Галуа на основі модифікованої комірки Гілда (МКГ). Запропоновано 3 структури створення МКГ. Наведено порівняння їх апаратних витрат.

В Україні стандарт ДСТУ 4145-2002 регулює використання ЕЦП на основі ЕК. Він обмежує використання розширених полів Галуа двійковими полями $GF(2^m)$ з порядком утворюючого поле полінома $m \leq 509$ ($GF(2^{509})$), проте міжнародні стандарти рекомендують використовувати двійкові поля з набагато більшими порядками утворюючих поліномів ($m \leq 998$). Сучасні темпи розвитку комп'ютерної техніки та загроза створення квантових комп'ютерів ведуть до створення більш стійких засобів КЗІ, до збільшення порядку (p^n) розширених полів Галуа $GF(p^n)$, які використовуються. Один з найбільш очевидних методів злому засобів КЗІ є метод перебору усіх ключів. Програмне виконання операцій над елементами розширених полів Галуа $GF(p^n)$ має більшу трудоємність, у порівнянні з $GF(2^m)$ та забезпечує більшу стійкість до злому. Апаратна реалізація реконфігурованих вузлів КЗІ забезпечує ще більшу криптографічну стійкість засобів КЗІ. За елементну базу для створення вузлів КЗІ у складі КФС у роботі було обрано програмовані логічні інтегральні схеми (ПЛІС), оскільки вони забезпечують високу продуктивність та швидкодію при виконанні вузькоспеціалізованих задач, у порівнянні з програмною реалізацією. Для генерації *VHDL*-описів вузлів КЗІ, що працюють з використанням розширених полів

Галуа $GF(p^n)$, для їхньої наступної реалізації у ПЛІС було розроблено мовою *C++* програми-генератори ядер помножувачів елементів розширених полів Галуа.

У **першому** розділі розглянуто сучасний стан та перспективи розвитку засобів та методів створення реконфігурованих вузлів КЗІ. Показано місце розширених полів Галуа $GF(p^n)$ у алгоритмах КЗІ КФС, розглянуто методи створення реконфігурованих вузлів на ПЛІС. Особливу увагу приділено правилам виконання арифметичних операцій у розширених полях Галуа $GF(p^n)$. Показано, що операції множення та ділення найбільш трудомісткі, при цьому ділення найчастіше виконується програмно. Тому саме операції множення приділено найбільше часу та уваги у даній роботі.

Також розглянуто питання складності алгоритмів та апаратно-програмна модель алгоритмів, питання злому систем КЗІ, особливості тестування операційних елементів для полів Галуа $GF(p^n)$, показано структуру комірки Гілда, підходи до створення генераторів ядер.

У **другому розділі** розглянуто методи створення реконфігурованих вузлів КЗІ для КФС, загальну методику проведення дисертаційних досліджень, описано вимоги до створення реконфігурованих вузлів КЗІ, обгрунтовано доцільність створення паралельних помножувачів елементів розширених полів Галуа $GF(p^n)$ та запропоновано методи створення таких помножувачів. Вдосконалено методи оцінки часової та апаратної складностей та запропоновано метод тестування генераторів ядер таких помножувачів.

У **третьому розділі** описано процес розробки засобів створення (генераторів ядер) помножувачів елементів розширених полів Галуа $GF(p^n)$ для вузлів КЗІ КФС. Генератори були реалізовані мовою *C++*. На рис. 11 наведено структурну схему генераторів. Генератори створюють *VHDL*-описи (ядра) помножувачі за запропонованим у роботі методом створення для ПЛІС генераторів моделей (ядер) реконфігурованих паралельних помножувачів елементів розширених полів Галуа $GF(p^n)$ для вузлів КЗІ у КФС.

Четвертий розділ присвячено дослідженню створених в ході виконання роботи операційних вузлів (помножувачів) для полів Галуа, які застосовуються у криптографічних засобах захисту інформації на базі ЕК. Дослідження проводилися під час впровадженню результатів дисертаційної роботи.

Наукові положення та висновки, сформульовані в дисертації, її результати використано під час реалізації проектних завдань у міжнародній компанії "JETSOFTPRO" (Україна, Польща, США) та в українській компанії ТзОВ “Кіберенергія” (Львів, Україна), що підтверджено відповідними актами впровадження. Також ці результати використовувалися у науково-дослідній роботі на кафедрі електронних обчислювальних машин Інституту комп'ютерних технологій, автоматики та метрології Національного університету "Львівська політехніка" ДБ/КІБЕР (номер державної реєстрації 0115U000446), що підтверджено відповідним актом впровадження. Також результати дисертації використовувались під час підготовки та викладання навчальних курсів з дисципліни "Дослідження і проектування комп'ютерних систем та мереж" на освітньо-кваліфікаційному рівні "Магістр" для спеціальності 123 "Комп'ютерна інженерія" для спеціалізацій "Комп'ютерні системи та мережі", "Кіберфізичні системи" та "Системне програмування", що підтверджено відпо-

відним актом впровадження.

Отримані, під час виконання дисертаційної роботи, наукові результати створюють методологічну базу для розробки вузлів КЗІ, які дозволяють підвищити надійність, достовірність та захищеність сучасних апаратних засобів КЗІ, які працюють з використанням ЕК та розширених полів Галуа.

Ключові слова: реконфігуровані вузли, кіберфізичні системи, еліптичні криві, розширені поля Гадуа $GF(p^n)$, апаратні витрати, модифікована комірка Гілда.

ABSTRACT

Zholubak I.M. Methods and means of creating reconfigurable nodes of cryptographic information protection for cyber-physical systems. – The manuscript.

Thesis for scientific degree of candidate of technical sciences, specialty 05.13.05 "Computer Systems and Components". - Lviv Polytechnic National University. Lviv, 2024.

In the dissertation, an important scientific and technical task of creating reconfigurable nodes for cryptographic information security (CIS) systems based on elliptic curves, which operate in cyber-physical systems with elements of extended Galois fields $GF(p^n)$, where $p > 2$ is a prime number, the configured characteristic of the field, and n is the order of the field-generating polynomial, the degree of the field over its prime subfield, is addressed. The hardware costs of implementing such systems in extended Galois fields $GF(p^n)$ with various characteristics p and orders n of the field-generating polynomial are analyzed. A multiplier of elements for such Galois fields based on a modified Guild cell (MGC) is proposed. Three structures for creating MGC are proposed. A comparison of their hardware costs is provided.

In Ukraine, the standard DSTU 4145-2002 regulates the use of digital signature based on elliptic curves. It limits the use of extended Galois fields to binary fields $GF(2^m)$ with the order of the field-generating polynomial $m \leq 509$ ($GF(2^{509})$), whereas international standards recommend using binary fields with much larger orders of generating polynomials ($m \leq 998$). The rapid development of computer technology and the threat of quantum computers lead to the creation of more robust CIS devices, increasing the order (p^n) of the extended Galois fields $GF(p^n)$ used. One of the most apparent methods of breaking CIS devices is the method of brute-forcing all keys. Software execution of operations over elements of extended Galois fields $GF(p^n)$ is more labor-intensive compared to $GF(2^m)$ and provides greater resistance to cracking. The hardware implementation of reconfigurable nodes provides even greater cryptographic robustness of CIS devices. FPGA were chosen as the elemental base for creating nodes in cyber-physical systems in the study because they provide high performance and speed in executing specialized tasks compared to software implementation. For generating VHDL descriptions of nodes that operate using extended Galois fields $GF(p^n)$ for their subsequent implementation in FPGA, C++ programs-generators of multiplier cores of elements of extended Galois fields were developed.

The first chapter examines the current state and prospects for the development of means and methods for creating reconfigurable nodes for CIS systems. The place of extended Galois fields $GF(p^n)$ in the algorithms of CIS systems is shown, methods for creat-

ing reconfigurable nodes on FPGAs are considered. Special attention is given to the rules for performing arithmetic operations in extended Galois fields $GF(p^n)$. It is shown that multiplication and division operations are the most labor-intensive, with division most often performed programmatically. Therefore, multiplication operations are given the most time and attention in this work.

The issues of algorithm complexity and the hardware-software model of algorithms are also considered, as well as the issues of cryptographic system hacking, the features of testing operational elements for Galois fields $GF(p^n)$, the structure of the Guild cell, and approaches to creating core generators are presented.

The second chapter considers methods for creating reconfigurable nodes for CIS systems, the general methodology for conducting dissertation research, the requirements for creating reconfigurable nodes, the rationale for creating parallel multipliers of elements of extended Galois fields $GF(p^n)$, and methods for creating such multipliers. Methods for assessing time and hardware complexities were improved, and a method for testing the generators of cores of such multipliers was proposed.

The third chapter describes the process of developing tools for creating (generators of cores) multipliers of elements of extended Galois fields $GF(p^n)$ for nodes in CIS systems. The generators were implemented in C++. Fig. 11 shows the structural diagram of the generators. The generators create *VHDL*-descriptions (cores) of multipliers using the method proposed in the work for creating FPGA model generators (cores) of reconfigurable parallel multipliers of elements of extended Galois fields $GF(p^n)$ for nodes in CIS systems.

The fourth chapter is dedicated to the research of the operational nodes (multipliers) for Galois fields, which are used in CIS devices based on elliptic curves. The research was conducted during the implementation of the dissertation work results.

The scientific principles and conclusions formulated in the dissertation, as well as its results, were used in the implementation of project tasks at the international company "JETSOFTPRO" (Ukraine, Poland, USA) and the Ukrainian company LLC "Cyberenergy" (Lviv, Ukraine), as confirmed by the relevant implementation acts. These results were also utilized in research work at the Department of Electronic Computing Machines of the Institute of Computer Technologies, Automation, and Metrology of Lviv Polytechnic National University under the DB/CYBER project (state registration number 0115U000446), as confirmed by the corresponding implementation act. Additionally, the dissertation results were used in the preparation and teaching of courses in the discipline "Research and Design of Computer Systems and Networks" at the master's level for the specialty 123 "Computer Engineering" in the specializations "Computer Systems and Networks," "Cyber-Physical Systems," and "System Programming," as confirmed by the respective implementation act.

The scientific results obtained during the dissertation work create a methodological base for developing CIS nodes, which allow enhancing the reliability, authenticity, and security of modern hardware CIS devices that operate using elliptical curves and extended Galois fields.

Keywords: reconfigurable nodes, cyber-physical systems, elliptic curves, extended Galois fields $GF(p^n)$, hardware costs, modified Guild cell.