67-72-2/1
12.03.2025

ВІДГУК
офіційного опонента
на дисертаційну роботу Жолубака Івана Михайловича
на тему «Методи та засоби створення реконфігурованих вузлів криптографічного захисту інформації для кібер-фізичних систем», подану на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 - комп'ютерні системи та компоненти

1. Актуальність теми дисертації

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 ≤ 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.

Однією з складових КЗІ є електронний цифровий підпис (ЕЦП), який використовується для забезпечення автентичності документів, повідомлень або транзакцій.

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.

2. Ступінь обгрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації

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.

Обґрунтованість одержаних результатів дисертаційної роботи забезпечено коректним використанням теорії цифрових автоматів, теоретичної моделі взаємодії відкритих систем та багаторівневої платформи КФС. Також були використані методи виконання математичних операцій у розширених полях Галуа $GF(p^n)$ у поліноміальному базисі, математичні напрацювання теорії чисел, теорії алгоритмів та засобів моделювання цифрових схем. Це свідчить про повну обґрунтованість наукових положень, висновків і рекомендацій, сформульованих у дисертації.

3. Наукова новизна отриманих результатів

Наукова новизна отриманих результатів полягає в наступному:

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.

Ознайомлення з матеріалами дисертації, ключовими публікаціями та авторефератом підтверджує успішне виконання поставлених завдань. Основні положення роботи, отримані автором особисто та містять наукову новизну.

4. Практичне значення отриманих результатів

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.

5. Структура та зміст дисертації

Структурно дисертація побудована правильно, стиль подання матеріалу забезпечує його однозначне трактування, оформлення дисертації відповідає чинним вимогам. Основна частина дисертації складається зі вступу, 4 розділів та висновків.

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 **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 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. Також наведено теоретичні підрахунки апаратної складності при реалізації помножувачів за трьома структурами МКГ:

1. МКГ є цілісним елементом (“чорна скринька”). Для кожного виходу цієї комірки формується своя булева функція та проводиться їх мінімізація методом Квайна–Мак-Класкі–Петрика (ЧС);

2. МКГ створена на основі функціональних вузлів: помножувача та суматора. Проводиться мінімізація методом Квайна–Мак-Класкі–Петрика булевих функцій, які описують роботу вказаних вузлів (ФВ);

3. МКГ створена на основі комбінаційних логічних елементів. МКГ реалізується, як комбінаційний паралельний, матричний помножувач та суматор за відповідними модулями характеристики поля (ЛВ).

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++*. 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.

Мінімізація булевих функцій відбувається методом Квайна–Мак-Класкі–Петрика. Генерування помножувачів елементів розширених полів Галуа $GF(p^n)$ з великими характеристиками поля p та порядками p^n є дуже часозатратною задачею. Наприклад, генерація помножувача для поля $GF(53^{174})$ триває 1845 с. У роботі визначено час генерування помножувачів і для інших полів.

Також 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. 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.

У роботі показано, що за відношенням k часових витрат на ПЛІС *Virtex UltraScale+ XCVU9P* при програмній та апаратній реалізаціях множення елементів полів $GF(p^n)$ у порівнянні з полями $GF(2^m)$ 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 забезпечує в 1,27 разів більший внесок в криптографічну стійкість засобів КЗІ ніж поле $GF(2^m)$.

Висновки дисертації узагальнюють отримані результати при виконанні поставлених завдань дисертаційного дослідження і містять інформацію про впровадження наукових результатів.

Список використаних джерел містить 252 найменування.

Додатки включають 4 акти впровадження та вихідні коди генераторів помножувачів елементів розширених полів Галуа $GF(p^n)$.

6. Повнота викладення положень дисертації в опублікованих працях

За темою дисертаційної роботи опубліковано 28 наукових праць, з них 1 монографія, 14 статей у фахових наукових журналах та вісниках, 13 – у працях

та тезах конференцій та семінарів, з них у Scopus – 1 стаття Q1 (квартиль 1), 2 статті Q4 (квартиль 4) та 4 тези конференцій.

7. Зауваження до змісту дисертації

1. Не розкрито процес пошуку многочленів, що утворюють поля, для виконання множень у розширених полях Галуа $GF(p^n)$.

2. У роботі для злому криптографічного шифру орієнтувались на метод грубої сили (з складністю $O(n)$) . Проте існують і інші методи злому з меншою складністю (наприклад, із складністю O(√n)). З роботи не зрозуміло, як використання інших методів може вплинути на результати досліджень.

3. У роботі досліджено та реалізовано 3 структури модифікованих комірок Гілда. Проте не виключено, що існують й інші. Відсутні пояснення щодо цього аспекту.

4. В роботі не пояснено значну розбіжність (на 56%) на рис. 4.13 теоретичних та реальних коефіцієнтів апаратних витрат на реалізацію помножувачів за варіантом МКГ з структурою на основі функціональних вузлів.

5. З роботи не зрозуміло, чому в основу досліджень покладено саме паралельний матричний помножувач елементів розширених полів Галуа $GF(p^n)$.

6. Не зрозуміло які криптографічні атаки дозволяє усунути запропонований підхід.

7. В роботі вказано, що для дослідження обрано розширені поля Галуа $GF(p^n)$ з приблизно однаковими порядками $p^n \approx 2^m$, але не визначено похибку, яка вноситься в результати дослідження за рахунок такої наближеної рівності порядків.

8. З автореферату не зрозуміло, як обирається, многочлен, що утворює розширене поле Галуа, як він враховується в запропонованих алгоритмах та методах.

8. Відповідність дисертації вимогам МОН України

Дисертаційна робота Жолубака Івана Михайловича задовольняє вимогам "Порядку присудження наукових ступенів" до робіт на здобуття наукового ступеня кандидата технічних наук, які висуває МОН України. Тема та зміст дисертації відповідають науковій спеціальності 05.13.05 – комп'ютерні системи та компоненти.

9. Рекомендації щодо використання результатів дисертаційної роботи

Результати дисертаційної роботи можуть бути застосовані в різних сферах, що потребують високого рівня безпеки та адаптивності криптографічних механізмів.

1. Використання у промислових кіберфізичних системах. Розроблені

методи можуть бути інтегровані у промислові кіберфізичні системи, для забезпечення конфіденційності, цілісності та автентифікації даних у процесах автоматизованого управління та моніторингу.

2. Впровадження в системи Інтернету речей (IoT). Результати дослідження можуть бути використані для підвищення рівня безпеки вузлів IoT, що взаємодіють у розподілених мережах. Реконфігуровані криптографічні механізми дозволяють адаптувати захист до змінних умов експлуатації.

3. Інтеграція у системи військового та спеціального призначення. Запропоновані методи можуть бути використані для розробки захищених комунікаційних систем у військовій сфері, зокрема для захисту даних під час бойових дій та у критичних ситуаціях.

4. Розробка комерційних програмних та апаратних рішень. Методи та засоби реконфігурованих криптографічних вузлів можуть бути використані в комерційних продуктах, зокрема у програмному забезпеченні для захисту даних, VPN-сервісах, а також у вбудованих апаратних рішеннях для безпечного обміну інформацією.

10. Висновки

Дисертаційна робота Жолубака Івана Михайловича «Методи та засоби створення реконфігурованих вузлів криптографічного захисту інформації для кібер-фізичних систем» є завершеною науковою працею, в якій розв'язано актуальне прикладне наукове завдання створення нового класу засобів – реконфігуровних апаратних вузлів криптографічного захисту інформації. За актуальністю розглянутих задач, обсягом проведених досліджень, науковою новизною і практичною цінністю отриманих результатів дисертаційна робота відповідає вимогам МОН України, які висуваються до кандидатських дисертацій.

Наукові положення та висновки дисертації успішно використано під час виконання проєктних робіт у міжнародній компанії "JETSOFTPRO" (Україна, Польща, США), та українській компанії ТзОВ "Кіберенергія" (Львів, Україна), 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). Також результати дисертаційної роботи використано у Національному університеті «Львівська політехніка» Інституту комп'ютерних технологій, автоматики та метрології на кафедрі електронних обчислювальних машин 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»).

Дисертація є актуальним науковим дослідженням, спрямованим на вирішення важливих питань створення та вдосконалення засобів криптографічного захисту інформації для кіберфізичних систем. Зважаючи на сучасні виклики, зокрема у воєнний час, тема дослідження має значну практичну та наукову цінність.

За актуальністю обраної теми, обсягом та рівнем виконаних дисертаційних досліджень, повнотою вирішення поставлених наукових та практичних задач, новизною і ступенем обґрунтованості отриманих результатів вважаю, що дисертаційна робота Жолубака Івана Михайловича відповідає вимогам МОН України, які вимагаються до кандидатських дисертацій, а її автор заслуговує присудження йому наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти.

Професор кафедри спеціалізованих
комп'ютерних систем
Західноукраїнського національного
університету,
д-р. техн. наук, професор Наталія ВОЗНА

«11» березня 2025 р.

Підпис Наталія Возна

Завіряю:
НАЧАЛЬНИК ЗАГАЛЬНОГО ВІДДІЛУ Алла Сенюк