67-72-2/2
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 обраної теми та мети дисертаційної роботи

Дисертація присвячена розробці реконфігурованих вузлів криптографічного захисту інформації (КЗІ) для кіберфізичних систем (КФС), що працюють з елементами розширених полів Галуа $GF(p^n)$. Такі поля, порівняно з традиційними двійковими полями $GF(2^m)$, забезпечують вищу криптографічну стійкість при $p^n \approx 2^m$, де $p > 2$ – просте число, а $m \leq 1024$.

Основний досліджуваний вузол – помножувач елементів розширених полів Галуа $GF(p^n)$, реалізований на основі модифікованої комірки Гілда (МКГ). Запропоновано три варіанти її структури, проаналізовано їхні особливості та порівняно апаратні витрати з класичною коміркою Гілда (КГ).

Такі пристрої застосовуються у реалізації електронного цифрового підпису (ЕЦП) та інших засобів КЗІ. Хоча традиційно використовувалися двійкові розширені поля, для зменшення апаратних витрат, останнім часом зростає інтерес до $GF(p^n)$, завдяки їхній підвищеній стійкості, особливо у застосуваннях, пов'язаних із використанням ізогеній ЕК. Створення таких вузлів є актуальним завданням для забезпечення безпеки сучасних КФС.

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

Вирішення поставленого наукового завдання забезпечено використанням теорії обчислювальних систем, теорії обчислювальних машин, теорії проектування спеціалізованих комп'ютерних систем, теорії складності алгоритмів та програмно-апаратної складності комп'ютерних систем.

Наукові положення, висновки та рекомендації, сформульовані в дисертації, мають високий ступінь обґрунтованості. Це підтверджується всебічним теоретичним аналізом, використанням сучасних математичних моделей, експериментальною перевіркою запропонованих методів, а також їхньою практичною реалізацією у вигляді прототипів. Дослідження пройшли апробацію через виступи на конференціях, публікації у фахових виданнях і рецензування експертами, що свідчить про їх відповідність сучасним вимогам. Отримані результати можуть бути застосовані для підвищення рівня захищеності кіберфізичних систем.

3. Наукова новизна отриманих результатів

Наукова новизна результатів, отриманих в дисертації Жолубака І. М., 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.

4. Практичне значення отриманих результатів

Результати дисертаційної роботи впроваджено у проектних завданнях міжнародної компанії "JETSOFTPRO" (Україна, Польща, США) та української компанії ТзОВ “Кіберенергія” (Львів), що підтверджено відповідними актами. Наукові результати дисертації також використовувалися в науково-дослідній роботі кафедри електронних обчислювальних машин Національного університету "Львівська політехніка" (ДБ/КІБЕР, №0115U000446) та при викладанні курсу "Дослідження і проєктування комп'ютерних систем та мереж" для магістрів спеціальності 123 "Комп’ютерна інженерія", що підтверджено відповідними актами.

5. Структура та зміст дисертації

Дисертація має правильну структуру, чіткий стиль викладу та відповідає чинним вимогам. Основна частина складається з вступу, 4 розділів і висновків.

Вступ містить аналіз сучасних досліджень у сфері реконфігурованих компонентів для КЗІ на основі розширених полів Галуа $GF(p^n)$ та еліптичних кривих. Обґрунтовано важливість генераторів ядер помножувачів для $GF(p^n)$,

сформульовано мету, завдання та практичну цінність дослідження. Висвітлено зв'язок роботи з науковими програмами, подано інформацію про апробацію результатів та їх впровадження.

Перший розділ присвячений аналізу методів створення реконфігурованих вузлів КЗІ, ролі розширених полів Галуа $GF(p^n)$ в алгоритмах КФС і реалізації таких вузлів на ПЛІС. Окремо розглянуто арифметичні операції, зокрема множення як найбільш трудомістку операцію. Також досліджено складність алгоритмів, моделі атак, тестування операційних елементів та підходи до створення генераторів ядер.

Другий розділ присвячений методам створення реконфігурованих вузлів КЗІ для КФС, загальній методиці дослідження та вимогам до таких вузлів. Обґрунтовано доцільність використання паралельних помножувачів елементів розширених полів Галуа $GF(p^n)$ та запропоновано методи їх реалізації. Вдосконалено методи оцінювання часової та апаратної складностей, розроблено метод тестування генераторів ядер. Проведено теоретичний аналіз апаратної складності для трьох структур МКГ:

1. Чорна скринька (ЧС) – мінімізація булевих функцій методом Квайна–Мак-Класкі–Петрика.
2. Функціональні вузли (ФВ) – мінімізація булевих функцій помножувача та суматора.
3. Логічні елементи (ЛВ) – реалізація паралельного матричного помножувача та суматора.

Третій розділ описує розробку генераторів ядер помножувачів елементів розширених полів Галуа $GF(p^n)$ для КЗІ у КФС. Генератори, реалізовані на C++, створюють *VHDL*-описи для ПЛІС відповідно до запропонованої методики. Мінімізація булевих функцій виконується методом Квайна–Мак-Класкі–Петрика. Визначено час генерації для різних полів, проведено тестування помножувачів полів $GF(3^{30})$, $GF(7^{17})$, $GF(23^{10})$, $GF(53^8)$, що підтвердило коректність роботи генераторів. Також запропоновано конвеєризацію для покращення характеристик помножувачів.

Четвертий розділ присвячено дослідженню створених у межах роботи операційних вузлів (помножувачів) для полів Галуа, що застосовуються в криптографічних засобах на базі ЕК. Аналіз проводився під час впровадження результатів дисертації.

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 узагальнюють отримані результати дослідження та підтверджують практичне впровадження наукових розробок.

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 дисертації 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. З роботи незрозуміло, чому в основу досліджень покладено паралельний помножувач на модифікованих комірках Гілда.
2. З роботи незрозуміло, чому для досліджень обрано поліноміальну форму представлення елементів розширених полів Галуа.
3. Наведені у роботі формули дають наближені значення результатів, але не оцінено точність, отриманих таким способом результатів.
4. У запропонованому алгоритмі створення модифікованої комірки Гілда з структурою "чорна скринька" генеруються булеві функції, які залежать від двійкових розрядів трьох чисел (a, b, c), кожне з яких менше або дорівнює характеристиці p поля Галуа. У роботі розглядаються поля з характеристиками $p \leq 1024$, тобто, числа a, b, c можуть бути 10-бітними. За запропонованим алгоритмом необхідно проводити мінімізацію згенерованих функцій, які залежать від розрядів чисел a, b, c (тобто, від 30 аргументів) методом Квайна-МакКласкі-Петрика. Аналогічно, для алгоритму створення модифікованих комірок Гілда з структурою на основі функціональних вузлів необхідно проводити мінімізацію функцій алгебри логіки, які залежать від 20 змінних. З роботи не зрозуміло, чи це можливо реалізувати.
5. Не пояснено, що необхідно робити за методом тестування генераторів ядер помножувачів елементів розширених полів Галуа, якщо з трьох отриманих різними способами результатів збігаються не всі результати, а тільки 2 або результати не збігаються зовсім.
6. На рисунках 2.6 – 2.11 на яких зображено відношення апаратних витрат помножувачів елементів розширених полів Галуа з структурами модифікованих комірок Гілда як "чорна скринька" та на основі функціональних вузлів видно що графіки мають чітко виражені локальні максимуми та спали. З чим це повязано?

8. Відповідність дисертації вимогам МОН України

Дисертаційна робота Жолубака І. М. відповідає діючим вимогам «Порядку присудження наукових ступенів», які висуваються до кваліфікаційних наукових робіт на здобуття наукового ступеня кандидата технічних наук. Дисертація за змістом та отриманими в ній науковими результатами відповідає науковій спеціальності 05.13.05 — комп'ютерні системи та компоненти.

9. Рекомендації щодо використання результатів дисертаційної роботи

Результати дослідження можуть бути впроваджені у різні сфери, що

потребують високого рівня криптографічного захисту та адаптивності в умовах змінного середовища.

1. Інтеграція в промислові кібер-фізичні системи. Використання запропонованих методів у системах автоматизованого управління для забезпечення надійного захисту даних. Впровадження реконфігурованих криптографічних вузлів у промислові контролери та сенсорні мережі для підвищення їхньої стійкості до кібератак.
2. Застосування у безпекових системах Інтернету речей (IoT). Використання реконфігурованих криптографічних механізмів для захисту даних під час взаємодії IoT-пристроїв у розподілених мережах. Оптимізація алгоритмів шифрування для енергоефективних обчислювальних платформ, що використовуються в IoT.
3. Використання у військових та спеціальних інформаційних системах. Розробка криптографічних рішень для захисту тактичних комунікаційних систем та безпечного обміну даними в польових умовах. Інтеграція методів у системи захисту критичної інфраструктури для забезпечення конфіденційності та стійкості до атак.
4. Розробка програмних та апаратних рішень для інформаційної безпеки. Впровадження методів у програмне забезпечення для криптографічного захисту даних у хмарних сервісах та VPN. Створення вбудованих апаратних засобів на основі FPGA та ASIC для реалізації високопродуктивних криптографічних модулів.
5. Наукові дослідження та освітня діяльність. Використання результатів у навчальних програмах для підготовки спеціалістів з інформаційної безпеки та криптографії. Подальший розвиток методів оптимізації криптографічних обчислень для перспективних кібер-фізичних систем.

Використання розроблених методів та засобів дозволяє суттєво підвищити безпеку кібер-фізичних систем, адаптуючи їх до сучасних викликів у сфері криптографічного захисту інформації.

10. Висновки

Дисертаційна робота Жолубака І. М. на тему «Методи та засоби створення реконфігурованих вузлів криптографічного захисту інформації для кібер-фізичних систем» є науковим досягненням, яке спрямоване на вирішення важливого завдання щодо розробки нового класу засобів для захисту інформації – реконфігурованих апаратних вузлів криптографічного захисту інформації. З огляду на актуальність розглянутих питань, обсяг проведених досліджень та їх наукову новизну, а також практичну цінність отриманих результатів, ця робота відповідає вимогам Міністерства освіти і науки України до кандидатських дисертацій.

Наукові результати дисертаційної роботи знайшли практичне застосування в міжнародних компаніях «JETSOFTPRO» (Україна, Польща, США) і ТзОВ «Кіберенергія» (Львів, Україна), а також у рамках держбюджетної науково-дослідної роботи ДБ/КІБЕР «Інтеграція методів і засобів вимірювання, автоматизації, обробки та захисту інформації в кібер-фізичних системах»

(номер державної реєстрації 0115U000446). Крім того, результати дослідження використовуються в Національному університеті «Львівська політехніка» на кафедрі електронних обчислювальних машин в процесі підготовки магістрів за спеціальностями «Комп'ютерні системи та мережі», «Кіберфізичні системи», «Системне програмування».

Дисертаційна робота присвячена актуальним проблемам розробки та вдосконалення методів криптографічного захисту для кібер-фізичних систем, що особливо важливо в умовах сучасних викликів, зокрема в воєнний час. Практична та наукова значущість теми не викликає сумнівів.

Враховуючи актуальність, обсяг та рівень виконаних досліджень, новизну результатів та їх обґрунтованість, можна зробити висновок, що дисертація Жолубака І. М. повністю відповідає вимогам МОН України до кандидатських дисертацій. Автор заслуговує присудження наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти.

завідувач кафедри кібербезпеки
Хмельницький національний університет

к.т.н., доцент Ю.П. Кльоц
12 березня 2025 р.