64-72-113/1
15.11.2019

ВІДГУК

офіційного опонента на дисертаційну роботу Рахма Мохаммед Кадім Рахма «Моделі та методи побудови операційних вузлів для полів Галуа, які використовуються при криптографічному захисті інформації на основі еліптичних кривих», подану на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 - комп'ютерні системи та компоненти

Актуальність теми дисертаційної роботи

Сучасний етап розвитку комп'ютерних технологій характеризується розвитком і впровадженням кіберфізичних систем (КФС), Інтернету речей, а також підготовкою серійних квантових комп'ютерів. При цьому зростання продуктивності серійних комп'ютерів, реалізація нових технологій та алгоритмів, впровадження нової елементної бази полегшує задачу порушення інформаційної безпеки. Це зумовлює необхідність пошуку нових, більш надійних апаратних методів криптографічного захисту інформації (КЗІ) та методів маскування їхньої роботи. Сьогодні одним з методів КЗІ є використання цифрових підписів, які базуються на алгоритмах опрацювання точок еліптичних кривих (ЕК) і елементів розширених двійкових $GF(2^m)$ та простих $GF(p)$ полів Галуа. Можливості квантових комп'ютерів роблять небезпечним використання існуючих алгоритмів, що базуються на використанні ЕК. Тому вже ведеться пошук алгоритмів КЗІ, які залишаться надійними і в еру квантових комп'ютерів. Одним із перспективних методів є метод, що базується на використанні ізогеній суперсингулярних ЕК у полі Галуа $GF(2^m)$. Крім двійкових полів $GF(2^m)$ можна використовувати й інші розширені поля Галуа. Тому дана робота, у якій розв'язується науково-технічна задача - здійснюється наукове обґрунтування доцільності застосування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК є актуальною та важливою.

Ступінь обґрунтованості наукових положень і достовірність результатів

Достовірність отриманих здобувачем науково-практичних результатів підтверджена актами впровадження, зокрема результати дисертаційної роботи використовувались при виконанні 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), фірмою AL-NABAA Network Solution L.L.C. (Багдад, Ірак), а також в навчальному процесі Національного університету «Львівська політехніка».

Отримані результати є обґрунтованими та достовірними, що підтверджується обсягом здійснених досліджень, результатами моделювання, поданим фактичним матеріалом та його науковою інтерпретацією, практичним використанням запропонованих розробок та апробацією на наукових конференціях. При проєктуванні операційних вузлів для полів Галуа, які використовуються при КЗІ на

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

Достовірність та новизна висновків та рекомендацій

У процесі розв'язання поставлених у роботі завдань, її автором отримано наступні нові, науково обґрунтовані результати:

вперше запропоновано метод оцінювання складності моделей помножувачів елементів розширених полів Галуа $GF(p^m)$, який базується на представленні помножувача для поліноміального базису як матриці модифікованих комірок Гілда і дозволяє визначити поля Галуа $GF(p^n)$ з наближено однаковим порядком, у яких моделі будуть мати найменше значення складності**;**

вперше запропоновано метод оцінювання складності злому апаратних засобів КЗІ, у якому прийнято, що засоби КЗІ реалізовано апаратно, а засоби злому – програмно, і який дозволяє визначити поля Галуа $GF(p^m)$ у яких злом засобів КЗІ буде виконуватися найдовше**;**

вперше запропоновано метод маскування роботи апаратних вузлів знаходження обернених елементів у двійкових полях Галуа $GF(2^m)$ у поліноміальному базисі, який полягає у використанні незалежних від значення операндів алгоритмів знаходження обернених елементів і який дозволяє зменшити витоки інформації із засобів КЗІ сторонніми каналами**;**

отримав подальший розвиток метод вбудованого тестування операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК, який, на відміну від відомих методів, полягає у введенні до моделі вузла детектора заборонених значень окремих розрядів кодів елементів полів Галуа, що дає можливість виявляти частину апаратних помилок**.**

Практичне значення одержаних результатів.

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

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

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

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

Повнота викладення матеріалів дисертації в публікаціях

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

Структура та зміст дисертації

Дисертаційна робота складається з вступу, чотирьох розділів, висновків, списку використаних джерел і додатків. Роботу викладено на 190 сторінках, з них сторінок основного тексту - 134. Робота містить рисунків - 42, таблиць - 32, додатків - 16. Найменувань у списку використаних джерел - 209.

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

У **першому** розділі проведено системний аналіз сучасного стану теорії, методів та засобів проєктування спеціалізованих комп’ютерів, пристроїв КЗІ, аналіз найбільш важливих відкритих стандартів та алгоритмів для них, узагальнених структур спецпроцесорів. У розділі розглянуто сучасний стан розвитку комп’ютерних систем, який характеризується реалізацією кіберфізичних систем (КФС). Розглянуто алгоритмічні основи проєктування комп’ютерних засобів КФС. Виділено програмно-апаратну SH-модель алгоритму. Відмічено переваги апаратних реалізацій алгоритмів**.**

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

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

багаторівневих систем**.**

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

Зауваження до дисертаційної роботи

1. У тексті дисертації багато разів пояснюються скорочення багатьох загальновживаних термінів, наприклад:

еліптичні криві (ЕК) ст. 17, 18, 53

спецпроцесор (СП) ст. 17, 20, 28, 53;

спеціалізована комп'ютерна система (СКС) Ст. 17, 20, 53;

ПЛІС ст. 17, 53 та інші.

2. У першому розділі дисертації (ст. 43) є посилання на рисунки третього розділу (рис. 3.1 ст. 9, рис 3.2 та рис. 33 ст. 99.), на яких представлені відомі структури протокольних та шифропроцесорів. Причому на ст. 98 дисертант стверджує, що такі протокольні процесори в дисертації не розглядаються. Доцільно було б ці рисунки та опис функцій таких процесорів подати у першому розділі.

3. На ст. 103 (рис. 3.7) представлена модель запропонованого вузла обчисення квадратного кореня у двійковому полі Галуа, але не пояснені переваги такої моделі у порівнянні з відомими.

4. У наведених на рис. 4.5 та 4.6 структурах помножувача з накопиченням та двійкового алгоритму ділення многочленів застосовуються логічні елементи «Виключаюче АБО», які можуть мати різні структурні схеми (2-5) вентилів та різну часову затримку сигналу (1-3) мікротакти, але аналіз їх впливу на апаратну та часову складність таких пристроїв в роботі не проведений.

5. Не досліджувалася можливість використання існуючих в ПЛІС готових помножувачів та суматорів на вдосконалених структурах комірок Гілда.

6. У тексті дисертації зустрічаються описки, наприклад:

ст. 44 «надійність таких **ПЛИС**»

ст. 68 «часова **складності** розширеного поля Галуа»

ст. 72 «складність **дорівнює складається** усіх квадраторів»

ст. 76 «до першої **заправа** комірки Гілда»

Висновок про відповідність дисертації вимогам МОН України

Оформлення дисертації за структурою та змістом відповідає вимогам, що ставляться МОН України до дисертаційних робіт на здобуття наукового ступеня кандидата технічних наук. Дисертаційна робота написана сучасною науково-технічною мовою, послідовно та логічно. Автореферат достатньо повно розкриває її зміст. Стиль викладу матеріалів досліджень, наукових положень та висновків забезпечує доступність їх сприйняття.

1. Дисертація Рахма Мохаммед Кадім Рахма на тему «Моделі та методи побудови операційних вузлів для полів Галуа, які використовуються при криптографічному захисті інформації на основі еліптичних кривих» є самостійною, завершеною науковою працею з чіткою структурою, в якій міститься розв'язок важливого науково-технічного завдання – здійснюється наукове обґрунтування доцільності застосування операційних вузлів для полів Галуа, які використовуються при криптографічному захисті інформації на основі еліптичних кривих, здійснюється визначення полів, які найкраще використовувати для вирішення цього завдання, а також здійснюється створення методів та засобів проєктування і порівняння згаданих вузлів.

2. Дисертаційна робота та її автореферат за змістом та оформленням відповідають встановленим вимогам. Результати дисертації достатньо повно опубліковані у фахових наукових виданнях та апробовані на науково-технічних конференціях та наукових семінарах.

3. За змістом дисертаційна робота відповідає вимогам паспорту спеціальності 05.13.05 - комп'ютерні системи та компоненти. Автореферат дисертації об'єктивно та з необхідною повнотою відображає основні положення дисертації.

4. Приведені зауваження у цілому не знижують загальної позитивної оцінки дисертаційної роботи.

5. За актуальністю, обґрунтованістю наукових положень, новизною і достовірністю отриманих результатів, їх теоретичною та практичною цінністю дисертаційна робота «Моделі та методи побудови операційних вузлів для полів Галуа, які використовуються при криптографічному захисті інформації на основі еліптичних кривих» повністю відповідає вимогам МОН України, які висуваються до робіт на здобуття наукового ступеня кандидата технічних наук, зокрема, пп. 9, 11, 12 положення про «Порядок присудження наукових ступенів», а її автор Рахма Мохаммед Кадім Рахма заслуговує присудження йому наукового ступеня кандидата технічних наук із спеціальності 05.13.05 - комп'ютерні системи та компоненти.

Офіційний опонент:
Завідувач кафедри
спеціалізованих комп'ютерних систем
Тернопільського національного
економічного університету,
д.т.н., професор Я.М. Николайчук

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

Підпис Я.М. Николайчук
Завіряю:
Зав. загальним відділом Г.В. Тарнавська