67-72-113/2
14.11.2019

ВІДГУК

офіційного опонента на дисертаційну роботу

Рахма Мохаммед Кадіма Рахма

«Моделі та методи побудови операційних вузлів для полів Галуа, які використовуються при криптографічному захисті інформації на основі еліптичних кривих», яку представлено на здобуття наукового ступеню кандидата технічних наук за спеціальністю 05.13.05 – Комп'ютерні системи та компоненти.

Актуальність теми дисертації та зв'язок її з науковими програмами, планами і темами.

Розвиток квантових обчислень обумовив появу нових загроз для методів класичної криптографії. Стійкість існуючих алгоритмів несиметричної криптографії, у разі створення квантового комп'ютера з можливістю програмування, буде суттєво знижена. Можна казати, що існуючі алгоритмі не можна буде застосовувати на практиці. Саме тому в США, ЕС, Японії починаючі з 2016 року проводяться національні конкурси на розробку та впровадження нових криптографічних алгоритмів, що будуть стійкими до квантових обчислень. Почала розвиватися постквантова криптографія. Основними напрямками постквантової криптографії є: алгоритми що базуються на використанні функцій хешування та дерева Меркле, алгоритми, що базуються на завадостійкому кодуванні, алгоритми, що базуються на використані математичного апарату мультиваріативних перетворень, та алгоритмів, що базуються на використанні математичного апарату ізогеній суперсингулярних еліптичних кривих. За результатами досліджень, найбільш перспективними вважаються методи, що базуються на функціях хешування та еліптичних кривих. Це підкреслює актуальність обраного напрямку досліджень – розробка методів та засобів проектування операційних вузлів для полів Галуа, що застосовуються при реалізації

алгоритмів КЗІ (а саме цифрового підпису). Важливість для держави даного напрямку досліджень підкреслює і те що дослідження виконувалися в рамках держбюджетної НДР «Інтеграція методів і засобів вимірювання, автоматизації, опрацювання та захисту інформації в базисі кіберфізичних систем».

З огляду на вищевказане, тематика дисертаційного дослідження є актуальною як в науковому, так і в прикладному плані.

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 приблизно 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 $GF(p^m)$ з приблизно однаковим порядком, 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.

Загальна характеристика дисертаційної роботи

Представлена дисертація складається з вступу, чотирьох розділів, загальних висновків, списку використаних джерел і додатків.

У **вступі** обґрунтовано актуальність теми роботи, визначено мету та основні задачі досліджень, сформульовано наукову новизну та практичне значення одержаних результатів, надано характеристику особистого внеску здобувача, а також надані дані про апробацію основних положень дисертації.

У **першому** розділі наведено аналіз сучасного стану теорії, методів та засобів проектування спеціалізованих вузлів, що реалізують криптографічні примітиви, проведений аналіз вимог міжнародних та національних стандартів методів несиметричного криптографічного захисту. Також проаналізований сучасні напрямку розвитку кіберфізичних систем та проблем захисту інформації в таких системах. Вказано на вплив технологій квантових обчислень на стійкість сучасних методів несиметричної криптографії, а саме на використання математичного апарату еліптичних кривих для реалізації алгоритмів електронного цифрового підпису. В якості перпективног напрямку обрано криптографію ізогеній суперсингулярних еліптичних кривих, яка може протистояти майбутнім квантовим комп'ютерам. Проаналізовано методи генерації описів функціональних вузлів та розглянути ПЛІС в якості елементної бази для побудови функціональних вузлів. У розділі також наданий опис методів досліджень.

Другий розділ присвячено вибору та обґрунтуванню напряму досліджень та проектування 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 проектування і порівняння згаданих вузлів.

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

Четвертий **розділ** присвячено впровадженню операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК. Продемонстрована можливість використання запропонованих рішень при реалізації засобу КЗІ, а саме алгоритму ЕЦП ECDSA.

Повнота викладення матеріалів дисертації в публікаціях

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

Ступінь обґрунтованості та достовірності наукових положень, висновків і рекомендацій дисертаційної роботи.

Отримані результати є обґрунтованими та достовірними, що підтверджується значним обсягом здійснених досліджень, результатами моделювання, поданим фактичним матеріалом та його науковою інтерпретацією, практичним використанням запропонованих розробок та апробацією на наукових конференціях. При проектуванні операційних вузлів для полів Галуа, які використовуються при КЗІ на основі ЕК враховувалися висновки теорії комп'ютерних систем, теорії проектування спеціалізованих комп'ютерних систем. Виконані дослідження використовують результати, отримані з прикладної теорії цифрових автоматів стосовно структурного синтезу й логічного проектування цифрових пристроїв, з теоретичної моделі

взаємозв'язку відкритих систем. Також використано і розвинуто: комп'ютерні методи виконання математичних операцій у простих та розширених полях Галуа у поліноміальному базисі, комп'ютерні методи виконання операцій над точками еліптичних кривих. У проведених дослідженнях широко використовується математичний апарат теорії алгоритмів, апарат теорії чисел, а також засоби моделювання цифрових схем.

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 кіберфізичних систем» (номер державної реєстрації 0115U000446), фірмою AL-NABAA Network Solution L.L.C. (Багдад, Ірак), а також в навчальному процесі Національного університету «Львівська політехніка».

Зауваження до дисертаційної роботи

1. У першому розділі дисертації здійснюється аналіз стійкості сучасних алгоритмів ЕЦП, а також вимог щодо побудови апаратних засобів ЕЦП. На жаль, автор не розглянув вимоги європейських стандартів щодо проектування апаратних засобів кваліфікованого цифрового підпису (стандарти серії Мандат 460). Крім того, бажано було б також розглянути вимоги до малоресурсної криптографії, оскільки автор вказує на можливість використання запропонованих рішень у кіберфізичних системах, а саме технології IoT. До таких систем висуваються досить жорсткі вимоги щодо ресурсів, що витрачаються на реалізацію криптографічних алгоритмів.

2. В роботі (другий та третій розділ) наводяться результати оцінки часової, структурної, відносної програмно-часової та апаратно-часової складності запропонованих рішень. Наведені результати оцінки не викликають сумнівів у достовірності. Але, на жаль, в роботі не наводяться комплексні оцінки рішень, що запропоновані. Такі оцінки необхідні для

аналізу ефективності програмно-апаратної реалізації алгоритму ЕЦП в цілому. Так, для оцінки ефективності апаратного рішення зараз використовуються такий показник як кількість «гейт-еквівалентів», що витрачаються на реалізацію криптографічного примітиву. При цьому відрізняють кількість «геійт-еквівалентів» на реалізацію математичних операцій та на зберігання ключів.

3. У четвертому розділі наводяться результати, які свідчать про можливість використання запропонованих рішень для реалізації засобів криптографічного захисту. В якості приклада, розглянуті моделі реалізації алгоритму ECDSA. Але в роботі не наводяться результати порівняльного аналізу реалізації, що запропоновані автором, та реалізацій, що вже існують на цей час на ринку. Особливо важливим показником для порівняльного аналізу є час накладання підпису, та час перевірки підпису. Відсутність такого порівняння ускладнює оцінку практичної значимості отриманих рішень.

Висновок про відповідність дисертації вимогам МОН України

Оформлення дисертації за структурою та змістом відповідає вимогам, що висуваются 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 – розробка методів проектування та оцінки 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.

2. Дисертаційна робота та її автореферат за змістом та оформленням відповідають встановленим вимогам. Результати дослідження 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
Заступник головного конструктора АТ «ІІТ»,
провідний науковий співробітник кафедри безпеки інформаційних систем і технологій Харківського національного університету ім. В. Каразіна (за сумісництвом)

доктор технічних наук, професор ПОТІЙ О.В.

УКРАЇНА
ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО «ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ»
№22723472
м. Харків