ВІДГУК

офіційного опонента про дисертаційну роботу Літави Гжегожа Владислава

«Моделі та засоби підвищення живучості інформаційно-управляючих систем на основі еліптичних кривих», подану на здобуття наукового ступеня кандидата технічних наук зі спеціальності 05.13.06 – інформаційні технології

Цей відгук підготовлено за матеріалами дисертації, що містить основний текст роботи на 133 стор., додатки, акти впровадження результатів дисертації, автореферат на 21 стор. і копії 14 наукових робіт: 8 із них – наукові статті, серед яких 6– статті у наукових фахових виданнях України, 2 наукові статті – у провідних закордонних журналах, які входять до міжнародних наукометричних баз, 2 розділи у закордонній монографії, а також 4 публікації в матеріалах конференцій.

.

1. Актуальність теми дисертаційної роботи

Глобалізація процесів інформатизації в житті сучасного суспільства привели до появи ряду нових проблем, найважливіша з яких - необхідність забезпечення ефективного захисту інформації і засобів її обробки.

Стрімкий розвиток комп'ютерних систем оброблення, зберігання та надання доступу до інформації в реальному масштабі часу вимагає використання надійних методів захисту інформації.

Тому забезпечення захисту інформації сьогодні є одним з найважливіших елементів національної безпеки України в умовах багатоукладної економіки і впровадження передових інформаційних технологій. Одним з найбільш розповсюджених методів захисту інформації є її шифрування.

У сучасних криптосистемах перевага віддається блоковим шифрам. При цьому вихідне повідомлення розбивається на блоки фіксованої довжини, наприклад, рівної n біт (де n-довжина секретного ключа). Потім кожен блок шифрується за допомогою секретного ключа, що полегшує розкриття шифру методом тотального перебору по всьому простору можливих ключів. В даний час реально здійснювати перебір 10^{20} варіантів за допомогою домашнього ПК , що відповідає довжині ключа n = 64. На сьогодні застосовуються ключі розміром 1024 - 4096 біт і вважаються досить надійними. З розвитком комп'ютерної техніки цей поріг збільшується і тому доводиться збільшувати простір можливих ключів.

Еліптичні криві активно вивчалися математиками протягом останніх 150 років. Однак криптографія на еліптичних кривих була винайдена тільки в 1985 році, а серйозно вивчалася лише кілька останніх років.

Розглянуто проблеми розробки та реалізації ефективного паралельного алгоритму дискретного логарифмування в групі точок

В цьому напрямку перспективним і актуальним є використання моделей та засобів підвищення живучості інформаційно-управляючих систем на основі еліптичних кривих.

Тема досліджень дисертації, що розглядається, відповідає державній науковій програмі розвитку технічного захисту інформації в Україні і виконувалась за напрямком наукових досліджень Тернопільського національного технічного університету імені Івана Пулюя (ДР № 0113U000258).

Таким чином, усе сказане обумовлює актуальність теми дисертаційної роботи Літави Гжегожа Владислава і новизну поставлених задач досліджень.

2. Наукова новизна результатів роботи

У роботі досліджено питання удосконалення моделей та засобів для підвищення живучості інформаційно-управляючих систем на основі еліптичних кривих.

Виходячи з того, що нові наукові результати - це нові знання в певній галузі фундаментальних чи прикладних наук, можна вважати основними науковими результатами дисертації таке:

- удосконалено структурну модель підвищення живучості інформаційно-управляючої системи, що базується на еліптичних кривих з врахуванням дефектів зовнішніх впливів за ознаками ймовірності та детермінованості, що дало змогу створити підґрунтя для проектування ефективних засобів цих систем.
- удосконалено технології обчислень на еліптичних кривих шляхом заміни множення за модулем в алгоритмі Крестенсона, що дало змогу звести множення до операції додавання, яка відрізняється від відомих новою архітектурою і меншою складністю у порівнянні з підходом, який ґрунтується на традиційному множенні, завдяки чому збільшено швидкість обчислень і прискорено дію алгоритму розв'язання задачі дискретного логарифмування у пристроях інформаційно-управляючої системи, що базується на еліптичних кривих.
- вперше одержано модифіковані моделі засобів обчислень на еліптичних кривих у пристроях інформаційно-управляючої системи, що базується на еліптичних кривих з врахуванням дефектів зовнішніх впливів на них, що дозволило по-новому визначити розмір кривих, які застосовуються в інтегрованих інформаційних системах, і забезпечити підвищену ефективність засобів протидії потенційним впливам.
- вперше, ґрунтуючись на алгоритмі модульного множення в теоретико-числових базисах Радемахера-Крестенсона щодо розв'язання дискретного логарифму, розроблено моделі, технології та структури засобів обчислень на еліптичних кривих в інформаційно-управляючої системи, що базується

на еліптичних кривих для виконання криптографічних операцій, завдяки чому здійснено верифікацію параметрів живучості інформаційно-управляючої системи, що базується на еліптичних кривих та доведення збільшення його рівня.

3. Достовірність наукових результатів

Достовірність основних наукових результатів роботи підтверджується наведеною в розділах 2, 3 і 4 системою формальних методик і моделей, що не містить принципових помилок, а також рядом прикладів, результатами експериментальних досліджень програмної реалізації системи виявлення та ідентифікації порушника та збіжністю теоретичних розрахунків з результатами впровадження розроблених засобів.

4. Цінність дисертаційної роботи для науки

Цінність дисертації полягає в тому, що в ній на основі запропонованих моделей та технологій обчислень створено, з імплементацією в середовищі програмованих користувачем вентильних матриць FPGA (Field Programmable Gate Array), апаратні засоби для реалізації стежок блукання ρ -алгоритму Полларда, які використано складовою частиною комплексної апаратно-програмної системи розв'язання дискретного логарифма на еліптичних кривих, що дало змогу отримати відомості про параметри живучості засобів інформаційно-управляючої системи, що базується на еліптичних кривих. Змістовний аспект запропонованого рішення, який спрямований на підвищення живучості інформаційно-управляючої системи, що базується на еліптичних кривих, з врахуванням дефектів зовнішніх впливів за ознаками ймовірності та детермінованості, дав змогу створити підґрунтя для проектування ефективних засобів функціонування систем виявлення та попередження загроз вторгнень, що не було відоме раніше.

5. Практична корисність роботи

Практична цінність роботи полягає в тому, що визначено час захисту засобів в залежності від розміру застосованих кривих, завдяки чому оцінено максимальне зростання ризику в короткостроковій перспективі, ґрунтуючись на особливостях симульованих дефектів впливу і даних щодо підвищення продуктивності нових апаратних рішень. Це забезпечило вибір оптимальних розмірів еліптичних кривих в спеціалізованих рішеннях, де важливим є компроміс між обчислювальною потужністю та рівнем захисту з врахуванням часу, протягом якого даний засіб повинен бути живучим.

Додатковим фактором практичної цінності роботи є здійснення додавання точок та реалізації ρ -алгоритму Полларда за допомогою створеної системи, побудованої на основі програмованих матриць FPGA типу Stratix III, завдяки чому забезпечено високу швидкодію і втричі зменшено час, необхідний для розв'язання дискретного логарифма на тій самій кривій, в

порівнянні з програмною системою, яка працює на процесорі типу Itanium2. Побудовано паралельну систему, в якій швидкість зростає пропорційно до кількості застосованих програмованих матриць FPGA, здійснено також перенесення і симуляцію функціонування заімплементованої моделі на кластері FPGA (120 компонентів), який базується на програмованій матриці серії Virtex-4.

6. Структура роботи

Дисертаційна робота містить вступ, 4 розділи, висновки, додатки та перелік використаних джерел.

У вступі обгрунтовано актуальність теми дисертації, відзначено зв'язок роботи з науковими темами, сформульовано мету і задачі дослідження, визначено об'єкт, предмет і методи дослідження, показано наукову новизну отриманих результатів та їх практичне значення, апробацію результатів дисертації.

У першому розділі на основі аналітичного огляду літературних джерел розкрито стан досліджуваної проблеми. Проведено аналіз математичних моделей оцінювання живучості інформаційно-управляючих систем, який дозволив сформулювати відповідні технічні і наукові дані, що лежать в основі дисертаційних завдань для розв'язання. Зроблено огляд основних типів еліптичних кривих криптографічних систем, що використовуються в засобах інформаційно-управляючих систем. Показано важливість дискретного логарифма для живучості інформаційно-управляючих систем, в яких складовими елементами виступають криптографічні засоби. Проаналізовані ефективні методи розв'язання дискретного логарифма. Обґрунтовано необхідність досліджувати нові, ефективніші моделі і технології обчислень та їх вплив на живучість інформаційно-управляючих систем.

Другий розділ представлено структурну модель підвищення живучості інформаційно-управляючих систем з врахуванням дефектів зовнішніх впливів, обчислювальні платформи та компоненти, за допомогою яких здійснюються основні обчислення на еліптичних кривих і цілих числах великої розрядності на потреби створення живучих інформаційно-управляючих систем. Розглянуто питання розпалелювання операцій, що виконуються як на числах великої розрядності, так і на кривих. Висвітлено способи побудови апаратних та апаратно-програмних систем, що реалізують паралельний ρ -метод Полларда. Подано моделі та технології обчислень для випадку сумування і множення чисел великої розрядності та реалізації основних операцій на еліптичних кривих. Доведено, що вибір відповідно швидких обчислювальних алгоритмів та ефективна імплементація в специфічних умовах можуть помножити швидкість

розв'язання дискретного логарифма, а отже призвести до порушення безпеки інформаційно-управляючих систем еліптичних кривих. Обґрунтовано, що для визначення живучості інформаційно-управляючих систем еліптичних кривих слід змодифікувати алгоритми та імплементаційні рішення в обчислювальних середовищах, а також оцінити швидкість розв'язання логарифму.

У третьому розділі представлено моделі обчислювальних платформ, за допомогою яких у пристроях інформаційно-управляючих систем на еліптичних кривих виконуються основні операції на еліптичних кривих із застосуванням розроблених автором перемножувачів, що грунтуються на теоретико-числових базисів Радемахера-Крестенсона, і суматорів, базованих на паралельному сумуванні чисел великої розрядності, наприклад, довжини 100 і більше бітів. Побудовано і проаналізовано моделі та апаратні імплементації для виконання основних операцій на еліптичних кривих. Розроблено операційні пристрої для здійснення обчислень на еліптичних кривих. Реалізовано апаратний засіб, який виконує поодиноку стежку ρ -методу Полларда, а також його паралельну версію. Проведено аналіз та виконано оцінювання особливостей функціонування та застосування побудованих засобів і удосконалених методів щодо живучості інформаційно-управляючих систем на еліптичних кривих, здійснюваної шляхом розв'язання дискретного логарифма. Показано придатність розроблених моделей та алгоритмів в шифруванні і розшифруванні.

У четвертому розділі здійснено симуляцію роботи моделей та технологій обчислень, запропонованих в попередньому розділі. Проведено аналіз симуляції роботи апаратно-програмних систем для розв'язування дискретного логарифма, який є підставою для підвищення живучості інформаційно-управляючих систем на еліптичних кривих. На основі результатів розв'язування дискретного логарифма для кривих різних розмірів здійснено оцінювання живучості інформаційно-управляючих систем на еліптичних кривих.

У додатках подано акти про впровадження результатів дисертаційного дослідження.

7. Публікації за темою дисертації

Наукові положення дисертації, що пов'язані з удосконаленням моделей та засобів для підвищення живучості інформаційно-управляючих систем на основі еліптичних кривих, достатньо повно відображені в публікаціях автора і пройшли апробацію на міжнародних науково-технічних конференціях і семінарах.

8. Автореферат дисертації

Автореферат дисертації за своїм змістом повністю відповідає дисертаційній роботі.

9. Зауваження щодо змісту дисертаційної роботи та автореферату

1. В роботі загалом і, зокрема, у назві підрозділу 2.3.2., сторінка 52, та на сторінках 57, 62, 65, 81, 97, 110 та інших, автор вальяжно пише про криві $GF(2^m)$, що є некоректним використанням термінології теорії Галуа. Правильно було б написати – криві у полі Галуа $GF(2^m)$, оскільки поле - це алгебраїчна структура.
2. Автор дисертації на сторінках 53, 54 другого розділу зазначає, що «розрахунок оберненості заснований на алгоритмі Евкліда», проте обчислюють значення обернених елементів на основі використання Розширеного алгоритму Евкліда, а сам алгоритм Евкліда використовують для знаходження найбільшого спільного дільника, таке тлумачення є порушенням правил наукової етики.
3. Дисертант у третьому розділі пропонує модель живучості інформаційно-управляючої системи яка записана виразами (3.1), (3.2), (3.3). В цій математичній моделі не згадано самої живучості, невідомо, як співвідносяться вирази моделі, чи це система, чи сукупність. Автор пише, що «Основна особливість моделі полягає в заміні операції модулярного множення цілих чисел великої розрядності додаванням за модулем, яке проводиться на основі використання теоретико-числового базису Крестенсона, а також застосуванням паралельного додавання чисел, що дає змогу прискорити виконання операції на відміну від традиційного підходу», проте в самій моделі явно не зазначено таке удосконалення нового алгоритму дисертанта.
4. У таблицях 4.5 та 4.6 автор наводить результати дослідження швидкості шифрування файлів використовуючи значення часу в секундах, що відрізняється від загальноприйнятого уявлення поняття про швидкість. На рисунку 4.6 Порівняно час, а не швидкості шифрування файлів методом Ель-Гамаля з використанням стандартних алгоритмів, реалізованих програмно та апаратно на основі системи залишків Радемахера-Крестенсона.

Однак зазначені зауваження не зменшують наукового рівня дисертації в цілому та отриманих в ній практичних результатів.

10. Загальна оцінка дисертації

Оцінюючи роботу в цілому, вважаю, що в дисертації отримано нове рішення важливої науково-технічної задачі, спрямованої на підвищення якості систем захисту інформаційних ресурсів за рахунок удосконалення моделей та засобів для підвищення живучості інформаційно-управляючих систем на основі еліптичних кривих.

Дисертація є завершеною науково-дослідною роботою. Вважаю, що за

актуальністю вибраної теми, обсягом і рівнем виконаних теоретичних і експериментальних досліджень, достовірністю і обґрунтованістю висновків, новизною досліджень, значенням отриманих результатів для науки і практики дисертаційна робота задовольняє вимогам "Порядку присудження наукових ступенів та присвоєння вченого звання старшого наукового співробітника" затвердженого постановою Кабінету Міністрів України від 24 липня 2013 р. № 567, а її автор Літава Гжегож Владислав заслуговує присудження наукового ступеня кандидата технічних наук зі спеціальності 05.13.06 – інформаційні технології.

Офіційний опонент
Професор кафедри прикладної інформатики
Краківської гірничо-металургійної академії ім. С. Сташіца
(м. Краків, Польща).
доктор технічних наук, професор О.С. Петров

Akademia Górniczo-Hutnicza
im. Stanisława Staszica
30-059 Kraków, Al. A. Mickiewicza 30
Wydział Zarządzania
(4)