ВІДГУК

офіційного опонента про дисертаційну роботу Котуха Євгена Володимировича «Методи та засоби універсального гешування за алгебричними кривими Судзукі», подану на здобуття наукового ступеня кандидата технічних наук зі спеціальності 05.13.21 – системи захисту інформації

Цей відгук підготовлено за матеріалами дисертації, що містить основний текст роботи на 169 стор., акти впровадження результатів дисертації, автореферат на 22 стор. і копії 16 наукових праць здобувача.

1. Актуальність теми дисертаційної роботи

В даний час інформаційні системи (ІС) різного масштабу стали невід'ємною частиною базової інфраструктури держави, бізнесу, громадянського суспільства. Все більше інформації, що підлягає захисту, переноситься в ІС. Сучасні інформаційні технології забезпечують не тільки нові можливості організації бізнесу, ведення державної та громадської діяльності, але і створюють значні потреби в забезпеченні та безпеки для захисту конфіденційної інформації. Відомо, що більше 25% зловживань інформацією в ІС відбувається внутрішніми користувачами, партнерами і постачальниками послуг, що мають прямий доступ до ІС. До 70% з них - випадки несанкціонованого отримання прав і привілеїв, крадіжки і передачі облікової інформації користувачів ІС, що стає можливим через недосконаліть технологій розмежування доступу і аутентифікації користувачів ІС. Удосконалення методів системи розмежування доступу і реєстрації користувачів інформаційних ресурсів є одним із пріоритетних напрямків розвитку ІС. Основними процедурами реєстрації користувачів в ІС є процедура ідентифікації і аутентифікації. Несанкціоноване заволодіння зловмисником доступом до ІС пов'язано в першу чергу з порушенням процедури аутентифікації.

Тема досліджень дисертації, що розглядається, відповідає державній науковій програмі розвитку технічного захисту інформації в Україні і виконувалась в рамках науково-дослідних робіт Харківського національного університету радіоелектроніки, а саме двох держбюджетних робіт: «Обґрунтування вимог, розроблення та впровадження інфраструктури електронного цифрового підпису в МОНУ» (№ ДР 0103U001981), «Методи, системи та засоби кріптографічного захисту інформації з гарантованим рівнем стійкості та підвищеною швидкодією» (№ ДР 0115U002431); та госпдоговірної роботи «Організація та розроблення проекту національного стандарту України та методичних рекомендацій щодо застосування міжнародних стандартів» (шифр «Гармонія» – 2007).

Таким чином, усе сказане обумовлює актуальність дисертаційної роботи Котуха Є.В. і наукову новизну поставлених в ній задач досліджень.

2. Наукова новизна результатів роботи

У роботі досліджено підвищення якості універсального гешування за рахунок побудови доказово стійкої автентифікації із забезпеченням гарантованої ймовірності колізії та зменшенням складності обчислень на основі використання кривих Судзукі.

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

- вперше запропоновано метод універсального гешування за раціональними функціями кривої Судзукі, що дозволило зменшити ймовірність колізії і збільшити довжину даних, що геруються, у порівнянні з гешуванням за максимальними плоскими кривими;
- вперше запропоновано метод обчислення геш-функцій за кривою Судзукі на основі чотирьох параметричної схеми Горнера, в якій враховується розмірність раціональних функцій кривих;
- подальший розвиток одержав метод універсального гешування за раціональними функціями алгебричних кривих, шляхом обчислення геш-функцій з обмеженням функціонального поля алгебричних кривих;
- подальший розвиток одержав метод каскадного універсального гешування на основі добутку функціональних полів, шляхом застосування гешування в каскаді за кривою Судзукі.

3. Достовірність наукових результатів

Достовірність основних наукових результатів роботи підтверджується наведеною в розділах 2, 3, 4 і 5 системою формальних методик і перетворень, що не містить принципових помилок, а також рядом прикладів, результатами комп'ютерного моделювання і впровадженням розроблених засобів.

4. Цінність дисертаційної роботи для науки

Цінність дисертації полягає в тому, що в ній запропоновано нове рішення важливої науково-технічної задачі в теорії побудови засобів автентифікації даних з підвищеною стійкістю. Змістовний аспект запропонованого рішення, який спрямований на підвищення якості універсального гешування за рахунок побудови доказово стійкої автентифікації із забезпеченням гарантованої ймовірності колізії та зменшенням складності обчислень, не був відомий раніше.

5. Практична корисність роботи

Практична корисність роботи обумовлена тим, що використання запропонованих в ній формальних методів і конкретних рішень дозволяє отримувати більш досконалі, порівняно з відомими, засоби гешування. Результати роботи впроваджено в ДП НТК «Імпульс» та навчальний процес Харківського національного університету радіоелектроніки.

6. Структура роботи

Дисертаційна робота містить вступ, 5 розділив, висновки, додатки та перелік використаних джерел.

У вступі сформульовано актуальність теми роботи, мету і задачі дослідження, наукову новизну і практичне значення отриманих результатів, показано зв'язок роботи з науковими-дослідними темами, виконуваними у Харківському національному університеті радіоелектроніки, наведено відомості про реалізацію і апробацію роботи, про публікації за її темою.

У першому розділі наведено аналіз існуючих алгоритмів вироблення MAC-кодів і виконано обгрунтування шляхів підвищення колізійної стійкості, зменшення обчислювальної складності. Визначається вплив обчислювальної потужності на вимоги до безпеки хешування. На основі запропонованих вимог проведено аналіз MAC-алгоритмів та їх реалізіцій. Визначені питання, що потребують дослідження.

Другий розділ присвячено методам універсального гешування та алгоритмам обчислення геш-кодів універсальних класів, зокрема гешуванню на основі скалярного добутку та на основі алгебричних кодів, а також поліноміальному хешуванню. Особливу увагу приділено реалізації задачі автентифікації на основі строгого універсального гешування за раціональними функціями алгебричних кривих. Визначено асимптотичні оцінки ймовірності колізії для гешування за кращими алгебричними максимальними кривими. Обгрунтовано, що найкращими кривими для реалізації гешування за раціональними алгебричними кривими є криві Судзукі, так як вони є неплоскими і відповідно мають істотно більшу кількість точок ніж інші криві, що розглядалися.

Сформульовано принцип розробки методів та побудови алгоритмів універсального хешування за раціональними алгебричними кривими, суть якого полягає у виборі алгебричних кривих, обчисленні їх алгеброгеометричних параметрів та здійсненні оцінки їх застосування.

Третій розділ присвячено розробці методу універсального гешування за кривою Делінге-Лустіга, яка відноситься до групи кривих Судзукі. Для цього наведено визначення та властивості кривих, що відносяться до групи Судзукі,

проведено оцінку їх параметрів та здійснено побудову функціонального поля даних кривих. Показано, що гешування за кривою Судзукі має перевагу по ймовірності колізії, довжині даних, складності обчислень у порівнянні з гешуванням за похідними кривих Судзукі і кривої над полем четвертого ступеня розширення.

У четвертому розділі розроблено метод швидкого універсального гешування за кривою Судзукі на основі чотирьохпараметричної схеми Горнера, що характеризується зменшеною складністю обчислення за рахунок обмеження функціонального поля.

Показано, що застосування розробленого методу дозволяє реалізувати багатопотокове універсальне гешування за рахунок розпаралелення обчислень поліноміального виразу з наступним об'єднанням результатів, що забезпечує підвищення швидкості реалізації.

П'ятий розділі присвячено розробці методу багаторазового каскадного універсального гешування за алгебричними кривими та композиційного універсального гешування з оцінкою їх параметрів. Розглянуто побудову безумовної автентифікації в композиційній конструкції Стінсона та здійснено оцінку параметрів.

У додатках подано акти про впровадження результатів дисертаційного дослідження.

7. Публікації за темою дисертації

Наукові положення дисертації, що пов'язані з розробкою методів універсального хешування, які забезпечують доказово стійку автентифікацію із забезпеченням гарантованої ймовірності колізії та зменшенням складності обчислень, 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 работе рассмотрено хеширование по кривым Судзуки по подгруппе максимального порядка и не рассмотрено хеширование по производным кривым подгрупп меньших порядков.

2. Вывод о том, хеширование по кривой Судзуки с параметрами поля $q = 2q_0^2$ и $q_0 = 2^s$ имеет преимущество по вероятности коллизии, длине данных,

сложности вычислений по сравнению с хешированием по производным кривым Судзуки и кривой над полем четвертой степени расширения является декларативным и требует конкретного обоснования.

3. Универсальное хеширование по кривой Судзуки на полем четвертой степени расширения описано в общем виде, без вывода формулы для хеш вычислений. Решение задачи оптимизации хеш вычислений при пяти параметрическом хешировании не является очевидным.

4. Отсутствует обоснование правила выбора базисных функций по полю рациональных функций кривой Судзуки при построении универсального хеширования в методе с ограничением функционального поля алгебраических кривых. Решение задачи представлено для случая двух координатного базиса. Не обосновано преимущество такого выбора.

5. В методе каскадного универсального хеширования по кривой Судзуки на основе произведения функциональных полей, как и в других каскадных методах, не рассмотрен вопрос согласования конечных полей каждого каскада. Так хеширование по кривой Эрмита выполняется в квадратичном поле в общем случае произвольной характеристики, а хеширование по кривым Судзуки определено только над полем с нечетной степенью расширения характеристикой два.

6. Разделы 2.1.4 «Универсальное хеширование по рациональным функциям алгебраических кривих» и 2.4.1 «Определение универсального хеширования по алгебраическим кривым» являются дополнениям друг друга и могли быть объединены.

7. Существуют сложности в восприятии представленных в работе отдельных результатов, например, по коллизионным оценкам в табл.2.3, из-за отсутствия пояснений по отдельным параметрам в формулах.

8. В автореферате в формуле для хеш вычислений в алгоритме быстрого хеширования по кривой Судзуки по четырех параметрической схеме Горнера пропущены слова сообщения.

9. В дисертації та авторефераті відмічено що результати роботи впроваджені НТК ДП «Імпульс», а в акті зазначено що результати впроваджені на ДП НТК «Імпульс».

10. В авторефераті 5 розділ завершено таблицею «Оцінки ймовірності колізії і складності обчислень для багаторазового гешування по алгебричним кривим над полем F_q » (ст..18) аналіз якої не проведено і висновки не зроблено.

10. Загальна оцінка дисертації

Оцінюючи роботу в цілому, вважаю, що в дисертації отримано нове рішення важливої науково-технічної задачі, спрямованої на підвищення якості універсального гешування за рахунок побудови доказово стійкої автентифікації із забезпеченням гарантованої ймовірності колізії та зменшенням складності обчислень на основі використання кривих Судзукі.

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", а її автор Котух Євген Володимирович заслуговує присудження наукового ступеня кандидата технічних наук зі спеціальності 05.13.21 – системи захисту інформації.

Офіційний опонент
завідувач кафедри інформаційної безпеки та комп'ютерної інженерії
Черкаського державного технологічного університету,
д.т.н., професор В. М. Рудницький

Підпис Рудницького В.М.
засвідчую
Відділ кадрів

Підпис д.т.н., професора Рудницького В.М. завіряю.
Т.в.о секретаря Вченої ради ЧДТУ,
к. філософ. наук, доцент В.С. Даценко