ВІДГУК

офіційного опонента к.т.н., доцента Гнатюка Сергія Олександровича на дисертацію Котуха Євгена Володимировича «Методи та засоби універсального гешування за алгебричними кривими Судзукі», представлену на здобуття наукового ступеня кандидата технічних наук за науковою спеціальністю 05.13.21 – «Системи захисту інформації»

Актуальність

Стрімкий розвиток інформаційних та комунікаційних технологій позитивно впливає на усі галузі діяльності людини, суспільства та держави, проте часто породжує множини неконтрольованих внутрішніх та зовнішніх загроз, які негативно відбиваються на характеристиках безпеки інформації. Одними з базових характеристик безпеки є цілісність та достовірність даних. Для перевірки цілісності до повідомлень засобами відправника додається MAC-підпис, як результат хеш-функції від перетворення змісту повідомлення та криптографічного ключа. Засобами отримувача виконується аналогічне перетворення такою самою хеш-функцією змісту повідомлень та криптографічного ключа. Після цього отриманий MAC-підпис та MAC-підпис, згенерований для перевірки, порівнюються. Якщо обидва MAC-підписи збігаються, це підтверджує цілісність повідомлення та ідентичність відправника.

Дисертаційна робота Котуха Євгена Володимировича присвячена **актуальним питанням** побудови доказово стійкої автентифікації повідомлень, яка задовольняє вимогам складності і швидкості обчислення, характеристикам і реалізаціям алгоритму для побудови національного стандарту. Актуальність дисертаційної роботи також підтверджується науково-дослідними та госпрозрахунковими роботами, з якими вона пов'язана:

1) «Обґрунтування вимог, розроблення та впровадження інфраструктури електронного цифрового підпису в МОНУ» (№0103U001981);

2) «Методи, системи та засоби криптографічного захисту інформації з гарантованим рівнем стійкості та підвищеною швидкодією» (№0115U002431);

3) «Організація та розроблення проекту національного стандарту України та методичних рекомендацій щодо застосування міжнародних стандартів» (шифр «Гармонія» – 2007).

Метою дисертаційної роботи є розробка методу універсального гешування за раціональними функціями кривих Судзукі для побудови доказово стійкої автентифікації із забезпеченням гарантованої ймовірності колізії зі зменшеною складністю обчислення. Для досягнення поставленої мети коректно

сформульовано основні задачі дослідження, які в роботі послідовно розв'язано. У результаті це дозволило дисертанту розробити метод універсального гешування за раціональними функціями алгебричної кривої Судзукі для побудови доказово стійкої автентифікації повідомлень з гарантованою ймовірністю колізії та мінімізацією витрат на ключовий простір і складність обчислень.

Оцінка обґрунтованості та достовірності наукових положень, висновків та рекомендацій

Ступінь обґрунтованості нових положень, висновків і рекомендацій у дисертації обумовлена коректністю застосування методів теорії груп Судзукі, теорії алгебричних кривих і кривих Судзукі; теорії лінійного простору над функціональним полем проективного різноманіття для побудови методу універсального гешування за кривими Судзукі; теореми Рімана-Роха для обчислення розмірності лінійного базисного простору і оцінювання параметрів універсального гешування; теорії композиційного гешування Стинсона для розробки методів каскадного універсального гешування; теорії ймовірності для оцінки колізійних властивостей універсального гешування. Достовірність основних положень та висновків підтверджено застосуванням програмних засобів для побудови кривих, обчислень їх точок і властивостей (кратності), моделювання лінійного базисного простору з раціональними функціями кривих і статистичного оцінювання ймовірності колізії гешування шляхом обчислення кратності перетину гіперповерхонь лінійного простору з точками кривої.

Ідентичність змісту автореферату й основних положень дисертації

У авторефераті дисертації з необхідною повнотою відображено загальну характеристику, основний зміст та висновки дисертації. Структура дисертації відповідає вимогам, які ставляться до кандидатських дисертацій. Дисертаційна робота складається зі вступу, п'яти розділів і висновків, має загальний обсяг 209 сторінок, з яких 169 сторінок основного тексту, містить 16 рисунків, 25 таблиць, список використаних джерел з 164 найменувань на 17 сторінках.

Результати дисертації викладено послідовно та структуровано, відповідно до поставлених задач дослідження.

У першому оглядовому розділі виконаний аналіз існуючих алгоритмів вироблення MAC-кодів і обґрунтування шляхів підвищення колізійної стійкості, зменшення обчислювальної складності.

У другому оглядовому розділі розглянуто методи універсального гешування на основі алгебричного кодування, за раціональними функціями алгебричних кривих, властивості універсальних геш-функцій, асимптотичні межі для

ймовірності колізії, а також безумовна автентифікація на основі строго універсального гешування.

У третьому розділі надані оцінка властивостей групи Судзукі, алгебричної кривої, асоційованої з групою Судзукі, побудова її функціонального поля кривої, універсального гешування за раціональними функціями і оцінка параметрів.

У четвертому розділі запропоновано метод універсального гешування за кривою Судзукі на основі схеми Горнера зі зменшеною складністю обчислення, метод універсального гешування з обмеженням функціонального поля за алгебричної кривої Судзукі і багатопотокове універсальне гешування.

У *п'ятому розділі* представлено метод багатокаскадного універсального гешування за раціональними функціями кривої Судзукі, виконана оцінка параметрів багатокаскадного універсального гешування за алгебричними кривими, порівняння за обчислювальними витратами, витратами ключа складності обчислення точок алгебричних кривих, надані практичні рекомендації.

Варто також зауважити, що для основних положень дисертації та змісту автореферату характерна повна ідентичність.

Наукове та практичне значення результатів дисертаційної роботи

Наукова новизна отриманих результатів дисертаційної роботи, на мою думку, перш за все, полягає у такому:

1. Вперше запропоновано метод універсального гешування за раціональними функціями кривої Судзукі, що дозволило зменшити ймовірність колізії в корінь шостого ступеня від розмірності поля обчислення і збільшити довжину даних, що гешуються, в корінь квадратний від розмірності поля обчислення у порівнянні з гешуванням за максимальними плоскими кривими.

2. Вперше запропоновано метод обчислення геш-функцій за кривою Судзукі на основі чотирьохпараметричної схеми Горнера, в якій враховується розмірність раціональних функцій кривих, що дозволило зменшити складність обчислення в два рази у порівнянні із загальним підходом.

3. Подальший розвиток одержав метод універсального гешування за раціональними функціями алгебричних кривих, який, на відміну від відомих, дозволив зменшити складність обчислень пропорційно підмножині раціональних функцій, які використовуються для гешування

4. Подальший розвиток одержав метод каскадного універсального гешування на основі добутку функціональних полів, який, на відміну від відомих, дозволив зменшити ймовірність колізії в корінь ступеня числа, що визначається

кількістю каскадів від кореня кубічного числа слів даних, і збільшити розмір даних, що гешуються.

Практичне значення результатів дисертації полягає у такому:

1. Побудовано функціональне поле кривої, асоційованої з підгрупою групи Судзукі над кінцевим полем довільного ступеня розширення. Отримано оцінки алгеброгеометричних параметрів кривих Судзукі над кінцевими полями.

2. Побудовано алгоритм гешування за кривою Судзукі за методом обчислення геш-коду на основі чотирьохпараметричної схеми Горнера, що дозволило отримати найменшу складність обчислень.

3. Розроблено практичні рекомендації щодо використання універсального гешування за кривою Судзукі в схемах багаторазового, багатокаскадного, композиційного гешування доказово стійкої і безумовної автентифікації повідомлень, що дозволило мінімізувати ймовірність колізії, складність обчислень і оптимізувати витрати на ключовий простір.

4. Отримано оцінки універсального гешування, складності обчислення геш-коду для двохкаскадного гешування і багатокаскадного гешування з гешуванням за кривою Судзукі в схемі, коли у внутрішньому каскаді використовується гешування за проективною прямою.

5. Розроблено програмні засоби для побудови кривих, обчислень їх точок і властивостей (кратності), моделювання лінійного базисного простору з раціональними функціями кривих і статистичного оцінювання ймовірності колізії гешування шляхом обчислення кратності перетину гіперповерхонь лінійного простору з точками кривої.

Результати дисертаційної роботи впроваджено в дослідницьких і конструкторських роботах в НТК ДП «Імпульс», в навчальному процесі кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки що підтверджено відповідними актами впровадження..

Повнота викладу результатів дисертаційної роботи в опублікованих працях та їх апробація

Результати виконаних досліджень опубліковано у 10 статтях у фахових виданнях, що входять до переліку МОН України, 6 матеріалів і тез наукових конференцій.

Дисертація Котуха Є.В. має достатній рівень апробації на наукових конференціях і семінарах. Опубліковані праці повністю відображають зміст та висновки дисертаційної роботи.

Зауваження

1. У п.1 наукової новизни дисертант запропонував метод універсального гешування за раціональними функціями кривої Судзукі, що дозволило зменшити ймовірність колізії в корінь шостого ступеня від розмірності поля обчислення і збільшити довжину даних, що гешуються, в корінь квадратний від розмірності поля обчислення у порівнянні з хешуванням за максимальними плоскими кривими. Проте чітко не наведено за рахунок чого вдалося досягти такого ефекту.

2. На мою думку назва першого розділу роботи «Аналіз сучасних вимог до криптографічних примітивів» не зовсім вдала, так як не досить влучно відображає його вміст, а саме проведення аналізу відомих методів побудови MAC-кодів універсального і строго універсального гешування.

3. У роботі не наведено порівняння отриманих дисертантом результатів з відомими, які належать дослідникам, що займаються універсальним і строго універсальним гешуванням (наприклад. О.Кузнецов, В.Чевардін та ін.) Можливо це пов'язано з обмеженням доступу до деяких матеріалів.

4. На с. 11 автореферату здобувач вказує, що при асимптотичній оцінці ймовірності колізії найбільш ефективними є криві Ерміта, проте відсутня чітка аргументація необхідності переходу до іншого типу кривих, у т.ч. до кривих Судзукі. Проте на с. 13 (передостанній абзац) автор стверджує, що гешування на кривій Судзукі має перевагу над кривою Ерміта. Подібно цьому, в табл.6 на с. 18 показано порівняння багатокаскадних геш-функцій на основі кривих Ерміта та Судзукі, де перевага кривих Судзукі є доволі спірною як за ймовірністю колізії, так і за складністю обчислень – до того ж розмір ключа є завідомо більшим у геш-функції на основі кривих Судзукі при подібному розмірі геш-образу.

5. Тексти дисертаційної роботи та автореферату містять велику кількість скорочень, абревіатур та формул, що значно ускладнює загальний процес оцінки при читанні. Крім того, текст дисертації не позбавлений орфографічних помилок та неточностей, наприклад, в авторефераті: с.3, абзац 4 (повідомлень і значенням) кома перед «і» не потрібна, абзац 5, там де практичне значення (п.1), правильно писати «алгебро геометричних», а не «алгеброгеометрічних»; с.6-7, там де апробація, між датами необхідно писати дефіс, а не тире; с.7, останній абзац, після «З точки зору вимог до архітектури» потрібно ставити кому; с.8, абзац 2,

некоректно «найбільш високошвидкісним», абзац 5, «універсальним», а не «універсальнім»; с.9, абзац 1, «Рімана – Роха», «Ріда – Соломона» та «Хассе – Вейля» необхідно писати через дефіс тощо. У дисертаційній роботі: присутні різні варіанти позначення лапок у всьому тексті дисертації; між прізвищами потрібно ставити дефіс, а не тире: Рида-Соломона, Вейля-Карлитца-Ушиямы, Римана-Роха, Картера-Вемана, Дэлигнэ-Лустига, Хассе-Вейля, Дэлигнэ-Лустига тощо; у списку літератури № 59-61, 66-69, 71-72, 110, 160, 161 вкінці немає номерів сторінок, що необхідно відповідно до чинних вимог оформлення списку джерел тощо.

Висновки

Зазначені недоліки не є суттєвими та критичними і не впливають на загальну позитивну оцінку роботи здобувача. У цілому дисертаційна робота Котуха Євгена Володимировича є закінченою науковою працею, яка містить нові науково обґрунтовані теоретичні та експериментальні результати, що у сукупності є суттєвими для забезпечення цілісності та достовірності даних, які передаються в інформаційно-комунікаційних системах.

Вважаю, що дисертаційна робота «Методи та засоби універсального гешування за алгебричними кривими Судзукі» повністю відповідає вимогам «Порядку присудження наукових ступенів», затвердженого Постановою КМ України від 24.07.2013 р. № 567 (із змінами, внесеними згідно з Постановами КМ України № 656 від 19.08.2015 р., № 1159 від 30.12.2015 р. № 567 від 27.07.2016 р.), а її автор Котух Євген Володимирович заслуговує присудження наукового ступеня кандидата технічних наук за науковою спеціальністю 05.13.21 – «Системи захисту інформації».

Офіційний опонент
доцент кафедри безпеки інформаційних технологій
Національного авіаційного університету
к.т.н., доцент С.О. Гнатюк

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ Національний авіаційний університет м. КИЇВ

Підпис Гнатюка С.
Засвідчую
Вчений секретар
Національного авіаційного університету
Г. Єлчева