Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0512U000248

Особливі позначки: відкрита

Дата реєстрації: 12-04-2012

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Халімов Геннадій Зайдулович
2. Khalimov Gennady Zaydulovich

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор наук

Аспірантура/Докторантура: ні

Шифр наукової спеціальності: 05.13.05

Назва наукової спеціальності: Комп'ютерні системи та компоненти

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 14-03-2012

Спеціальність за освітою: 0701

Місце роботи здобувача: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: 61166, м. Харків, пр. Науки, 14

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): Д64.052.01

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: 61166, м. Харків, пр. Науки, 14

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 81.14.11.05

Тема дисертації:

1. Теоретичні основи універсального гешування за алгебричними кривими

2. Theoretical basis of universal hashing on algebraic curves

Реферат:

1. Метою роботи є розробка теорії універсального гешування за раціональними функціями алгебричних кривих для побудови системи доказово-стійкої автентифікації. Об'єкт дослідження є процеси автентифікації повідомлень в комп'ютерних системах та мережах в умовах жорстких вимог відносно доказової стійкості і мінімізації витрат на автентифікацію. Предмет дослідження є основні положення теорії універсального гешування для побудови доказово-стійкої і безумовної автентифікації повідомлень в комп'ютерних системах та мережах (інформаційно технічніх системах) в умовах дій порушника, направлених на модифікацію і порушення цілісності повідомлень. Розроблено теоретичні положення універсального гешування за раціональними функціями алгебричних кривих, що дозволило вирішити основне протиріччя автентифікації між ймовірністю колізії, витратами ключового простору і довжиною повідомлення, що гешується. Запропоновано метод універсального гешування над функціональним полем алгебричних кривих, отримано оцінки ймовірності колізії універсального гешування, асимптотичні верхні границі ймовірності колізії. Побудовано функціональні поля максимальних кривих першого, другого та третього роду. Проведено

теоретичні дослідження алгебричних кривих, розроблено методи обчислення числа точок кривих Ферма та Гурвіця, методи побудови нетривіальних кривих та максимальних Гурвіця, визначені найкращі криві для універсального гешування. Розроблено метод обчислення геш функцій на основі обчислення за багатопараметричною схемою Горнера, побудовано алгоритми гешування за максимальними кривими найбільшого першого, другого та третього роду, за кривими Ферма та Гурвіця з великим числом точок, за кривою Сузукі зі зменшеною складністю обчислення. Розроблено методи каскадного універсального гешування, практичні рекомендації для застосування методів універсального гешування за алгебричними кривими, програми аналізу та побудови універсального гешування за раціональними функціями кривих.

2. The aim is to develop a theory of universal hash functions for rational algebraic curves to construct a system demonstrable persistent authentication. The object of study is a message authentication processes in information systems and information technology systems under tight requirements for demonstrable resilience and minimize costs for authentication. Purpose of the study is the main tenets of the theory of universal hashing to construct provably secure message authentication and unconditional in information systems and information technology systems in terms of the offender, to the modification and tampering with messages. Theoretical positions universal hashing on rational functions of algebraic curves that allowed to resolve the basic contradiction of authentication between probability of a collision, expenses of key space and length hashing messages has developed. The method of universal hashing over a functional field of algebraic curves has offered, assessment of the collision's probability of universal hashing as well as asymptotic upper boarder of collisions has obtained. Functional fields on the maximum curves of the first, second and third genus are constructed. A theoretical study of the algebraic curves is conducted, methods of point's quantity calculation of the Fermat and Hurwitz curves has designed, construction methods of the uncommon curve and maximum curves of Hurwitz are developed, and best curves for universal hashing has defined. The method of hash functions calculation based on calculation via multi-parametrical Horner's scheme is developed, the algorithms of hashing on maximum curves within highest first, second and third genus on Fermat and Hurwitz curves, on a curve of Suzuki with a great number of points and the reduced calculation complexity has constructed. Methods of cascade universal hashing, practical recommendations of application of the universal hashing methods on algebraic curves, software of the analysis and construction universal hashing on rational functions of curves are developed.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки:

Стратегічний пріоритетний напрям інноваційної діяльності:

Підсумки дослідження:

Публікації:

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації:

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Горбенко Іван Дмитрович

2. Gorbenko Ivan Dmitrievich

Кваліфікація: д.т.н., 20.01.09

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Корченко Олександр Григорович
2. Корченко Олександр Григорович

Кваліфікація: д.т.н., 05.13.21

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Олексійчук Антон Миколайович
2. Олексійчук Антон Миколайович

Кваліфікація: д.т.н., 05.13.21

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Мороз Борис Іванович
2. Мороз Борис Іванович

Кваліфікація: д.т.н., 05.25.05

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Бондаренко Михайло Федорович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Бондаренко Михайло Федорович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності Юрченко Т.А.