Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0416U004871

Особливі позначки: відкрита

Дата реєстрації: 07-12-2016

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Котух Євген Володимирович
2. Kotukh Yevgen Volodymyrovych

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 05.13.21

Назва наукової спеціальності: Системи захисту інформації

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 11-11-2016

Спеціальність за освітою: 7.05010104

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): К 64.052.05

Повне найменування юридичної особи: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

Місцезнаходження: проспект Науки, 14, м. Харків, Харківський р-н., Харківська обл., 61166, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

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: 20.51.35

Тема дисертації:

1. Методи та засоби універсального гешування за алгебричними кривими Судзукі

2. Methods and means of universal hashing by algebraic Suzuki curves

Реферат/анотація:

1. Дисертація присвячена вирішенню важливої науково-технічної задачі, яка полягає в розробці методу та засобів універсального гешування за раціональними функціями кривих Судзукі для побудови доказово стійкої автентифікації із забезпеченням гарантованої ймовірності колізії зі зменшеною складністю обчислення. Розроблено метод універсального гешування за раціональними функціями кривої Судзукі та метод обчислення геш-функцій за кривою Судзукі на основі багатопараметричної схеми Горнера. Побудовано функціональні поля кривих, що асоційовані з підгрупами групи Судзукі над кінцевим полем довільного ступеня розширення. Отримано оцінки алгеброгеометричних параметрів кривих Судзукі над кінцевими полями. Отримано оцінки універсального гешування за кривою Судзукі, складності обчислення геш-коду, ключові витрати. Набув подальшого розвитку метод універсального гешування з обмеженням функціонального поля за раціональними функціями алгебричних кривих та метод каскадного універсального гешування на основі добутку функціональних полів.

2. The thesis is devoted to solution of important scientific and technical problem, which consists in the development of the methods and means of universal hashing by the rational functions of Suzuki curves to build authentication scheme with provable security to ensure the guaranteed probability of collision with reduced computational complexity. Method of universal hashing based on rational functions of the Suzuki curve and the method of hash function computing based on Horner multiparameter scheme were developed. Functional field for curves associated with subgroups of the Suzuki group over the finite field with arbitrary power of expansion was built. The parameters of algebraic Suzuki curves over finite fields were estimated. The complexity of hash code computing and key space for universal hashing on Suzuki curve were obtained.

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. Халімов Геннадій Зайдулович
2. Khalimov Hennadii Zaidulovych

Кваліфікація: д.т.н., 05.13.05

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. Рудницький Володимир Миколайович

2. Рудницький Володимир Миколайович

Кваліфікація: д.т.н., 05.13.06

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. Гнатюк Сергій Олександрович

2. Гнатюк Сергій Олександрович

Кваліфікація: к.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

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Халімов Геннадій Зайдулович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Халімов Геннадій Зайдулович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності



Юрченко Т.А.