Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0415U001664

Особливі позначки: відкрита

Дата реєстрації: 14-04-2015

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Колованова Євгенія Павлівна
2. Kolovanova Ievgeniia Pavlivna

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: 31-03-2015

Спеціальність за освітою: 7.080403

Місце роботи здобувача: Харківський національний університет імені В.Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: Україна, 61022, м. Харків, майдан Свободи,4

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 імені В.Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: Україна, 61022, м. Харків, майдан Свободи,4

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. Математичні та обчислювальні методи прогнозування кількості слабких ключів режиму вибіркового гамування з прискореним виробленням імітовставки

2. Mathematical and computational methods of forecasting the number of GCM & GMAC weak keys

Реферат:

1. Дисертаційна робота присвячена вирішенню важливої науково-технічної задачі, яка полягає в розробці математичних та обчислювальних методів прогнозування кількості слабких ключів режиму вибіркового гамування з прискореним виробленням імітовставки, обґрунтуванні практичних рекомендації щодо його застосування в Україні. В дисертаційній роботі вперше розроблено математичні моделі та методи оцінки кількості слабких ключів режиму вибіркового гамування з прискореним виробленням імітовставки, зокрема, отримано аналітичні оцінки ймовірності виникнення слабких ключів, що призводять до виродженої роботи застосовуваної функції ґешування, доведено, що ймовірність появи слабких ключів не залежить від їхньої довжини, а визначається зворотно до потужності множини блоків повідомлення. Вперше розроблено математичну модель зменшеної (міні) версії режиму вибіркового гамування з прискореним виробленням імітовставки, яку засновано на масштабуванні застосовуваних симетричних криптоперетворень зі збереженням їх алгебраїчної структури, що дозволяє прогнозувати різні показники криптографічної стійкості

повної версії режиму при застосуванні шифрів-оригіналів. Отримав подальший розвиток обчислювальний метод прогнозування криптографічних властивостей блокових симетричних шифрів, який призначено для вивчення колізійних властивостей формованих імітовставок із прогнозуванням відповідних характеристик на випадок застосування повної версії режиму і шифрів-оригіналів. Ключові слова: режим шифрування, імітовставка, міні-версія, ґешування, прогнозування, ґеш-значення, слабкий ключ, гамування, криптоперетворення.

2. The thesis is devoted to the solution of important scientific and technical problem, which is to develop mathematical and computational methods for forecasting the number of GCM & GMAC weak keys, the justification of practical recommendations for its use in Ukraine. The thesis first developed the mathematical models and methods for estimating the number of GCM & GMAC weak keys. Analytical evaluations of the probability of weak keys, which leads to a degenerate work hashing function, were obtained. It was proved that the probability of occurrence of weak keys do not depend on their length, and is determined by back to the power of the blocks messages set. The thesis first developed the mathematical model of reduced (mini) version of GCM & GMAC based on the scaling symmetrical cryptotransformations preserving their algebraic structure. This allows to forecast the various cryptographic strength parameters of the full version mode when using originals ciphers. The computational method of forecasting the cryptographic properties of block symmetric ciphers was further developed. It designed to study collisional properties of formed message authentication codes with forecasting the corresponding characteristics when applying the full mode version and originals ciphers. Keywords: encryption mode, message authentication code, mini-version, hashing, forecasting, hash-code, weak key, counter, cryptotransformation.

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. Кузнецов Олександр Олександрович
2. Kuznetsov Oleksandr Oleksandrovych

Кваліфікація: д.т.н., 20.02.12

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. Харченко Вячеслав Сергійович
2. Харченко Вячеслав Сергійович

Кваліфікація: д.т.н., 20.02.14

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

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Горбенко Іван Дмитрович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Горбенко Іван Дмитрович
Відповідальний за підготовку облікових документів	
Реєстратор	
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Т.А.