Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0413U005674

Особливі позначки: відкрита

Дата реєстрації: 17-10-2013

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Іваненко Дмитро Вікторович
2. Ivanenko Dmytro Viktorovych

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: 24-09-2013

Спеціальність за освітою: 7.091501

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: 81.14.11.05

Тема дисертації:

1. Методи підвищення стійкості схем направленого шифрування в кільцях зрізаних поліномів до атак спеціального виду на реалізацію

2. Survivability improving methods for directional encryption schemes over truncated polynomials rings against side channel attacks on the implementation

Реферат:

1. Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 - системи захисту інформації. - Харківський національний університет радіоелектроніки МОН України, Харків, 2013. Дисертаційна робота присвячена дослідженню та обґрунтуванню вибору методу направленого шифрування на решітках, ANSI X9.98 NTRU, національним стандартом України. Запропоновано вдосконалений метод направленого шифрування на решітках, ANSI X9.98 NTRU, що на відміну від існуючих дозволяє забезпечити стійкість до атак спеціального виду на реалізацію, які використовують SPA- метод, за рахунок використання додаткових "додавань", внаслідок чого приблизно на 9% зросте час обчислення алгоритму. Запропоновано універсальний метод протидії атакам спеціального виду, яку базуються на аналізі спектру енергоспоживання, який на відміну від відомих ґрунтується на рандомізації t та рандомізації масиву b, що дозволяє підвищити стійкість алгоритму NTRU у n-разів. Ключові слова: теорія решіток, багаточлен, атака

спеціального виду, енергоспоживання, SPA, DPA, CPA, метод Хемінга, відстань Хемінга, операція згортки.

2. Thesis for a Ph.D. science degree by specialty 05.13.21 information security systems. Kharkiv National University of Radioelectronics of the MES of Ukraine, Kharkiv, 2013. The thesis is devoted to research and justification of directional encryption schemes over truncated polynomials rings, ANSI X9.98 NTRU, that in contrast to the existing approaches allows to reach resistibility against side channel attacks on the implementation using SPA method that is based on operating with additional components, it results in 9% growth of the algorithm calculations time. There is a new universal reaction method against side channel attacks is proposed in the thesis, it is based on randomization of the t parameter and the b array that allows to increase the NTRU algorithm strength by n times. Keywords: Lattice, the polynomial, side channel attacks, consumption energy, SPA, DPA, CPA, Hamming weight, Hamming distance, convolution operation.

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. Бондаренко Михайло Федорович
2. Bondarenko Mikhaylo Fedorovych

Кваліфікація: д.т.н., 05.13.01

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. Кранобаєв Віктор Анатолійович

2. Кранобаєв Віктор Анатолійович

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. Єсін Віталій Іванович

2. Єсін Віталій Іванович

Кваліфікація: к.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

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.