Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0417U003324

Особливі позначки: відкрита

Дата реєстрації: 29-06-2017

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Коркішко Леся Мирославівна
2. Korkishko Lesya

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: 15-06-2017

Спеціальність за освітою: 7.051002

Місце роботи здобувача: Тернопільський національний технічний університет імені Івана Пулюя

Код за ЄДРПОУ: 05408102

Місцезнаходження: м. Тернопіль, вул. Руська, 56

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): Д 26.062.17

Повне найменування юридичної особи: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: пр. Космонавта Комарова 1, м. Київ, Київська обл., 03058, 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: Тернопільський національний економічний університет

Код за ЄДРПОУ: 33680120

Місцезнаходження: 46020, м. Тернопіль, вул. Львівська, 11

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.37.23

Тема дисертації:

1. Методи та засоби маскованої арифметики для пристроїв систем захисту інформації

2. Methods and structures of masked arithmetic for information security systems devices

Реферат/анотація:

1. Дисертаційна робота присвячена розв'язанню актуальної наукової задачі побудови і дослідження методів та засобів виконання маскованої арифметики, що можуть використовуватися для побудови криптографічних пристроїв із підвищеною стійкістю до інженерно-криптографічних атак на основі аналізу споживаної потужності. У роботі запропоновано метод виконання операції диз'юнкції над даними у маскованому представленні, що, за рахунок обчислення функції корекції маски результату з використанням виключно маскованих даних та їх масок, дозволяє використати таку операцію для побудови структур криптографічних операційних блоків виконання операції диз'юнкції, масштабованих до кількості масок даних у їх маскованому представленні. Також запропоновано метод перетворення маскованого представлення даних, що, за рахунок використання операції додавання за модулем 2N над даними у маскованому представленні, побудованої на основі маскованих логічних операцій, дозволяє перетворювати масковане представлення даних із арифметичним маскуванням у дані із логічним маскуванням та навпаки, а також використати таке перетворення для створення структур криптографічних операційних блоків, які використовують часту зміну

типу маскування. Розвинуто метод виконання операції кон'юнкції над даними у маскованому представленні, що, за рахунок введення у функцію корекції маски результату обчислень з урахуванням усіх масок вхідних та вихідних даних, дозволяє використати таку операцію для побудови структур криптографічних операційних блоків виконання операції кон'юнкції, масштабованих до кількості масок даних у їх маскованому представленні. Розвинуто метод інвертування даних у маскованому представленні у полях виду GF(2N), що, за рахунок введення у функцію корекції маски результату обчислень з урахуванням усіх масок вхідних та вихідних даних, дозволяє обробляти дані із довільною кількістю масок, а також використати таке перетворення для побудови структур криптографічних операційних блоків інвертування даних у полях виду GF(2N), які використовують табличні методи виконання операцій у цих полях.

2. The thesis is devoted to solving actual scientific problem of development and research of methods and means of implementing the masked arithmetic, which can be used to build cryptographic devices with increased resistance to cryptographic engineering attacks based on analysis of power consumption. The methods for performing basic operations of cryptographic algorithms for masked data representation are proposed in this work. The list of considered operations are: logical operations of conjunction and disjunction, data inversion in fields GF(2N), table-based transformations, conversion of mask type for masked data. Developed methods for performing logical operations of conjunction and disjunction, data inversion in fields GF(2N) on the data in the masked representation are characterized by the ability to process data with any given number of masks. For method for conversion of mask type for masked data further developed a method of adding masked data modulo 2N. Due to this developed method allows one to convert masked presentation of data from arithmetic masking to logical masking and vice versa. For proposed method for table-based transformations of masked data, additional intermediate masking of agreed type of mask input was introduced. That allowed one to perform table-based transformations on input with either logical or arithmetic masking and get the result with the given masking type. Based on developed methods for operations on masked data, developed Verilog-models of structures for cryptographic operation units performing the above operations and cores of specialized hardware-based processor of symmetric block encryption algorithms mCrypton and GOST 28147-89, which process masked data with one logical mask and allow a creation of cryptographic processor with high resistance to attacks by analyzing the power consumption.

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. Карпінський Микола Петрович

2. Karpinskiy Mykola

Кваліфікація: д.т.н., 05.11.05

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. Терейковський Ігор Анатолійович
2. Терейковський Ігор Анатолійович

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. Хохлачова Юлія Євгеніївна
2. Хохлачова Юлія Євгеніївна

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	Корченко Олександр Григорович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Корченко Олександр Григорович
Відповідальний за підготовку облікових документів	
Реєстратор	
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Т.А.