Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0411U001775

Особливі позначки: відкрита

Дата реєстрації: 25-03-2011

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Зюзя Олександр Андрійович

2. Zyuzya Oleksandr Andrijovich

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

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: 21-03-2011

Спеціальність за освітою: 8.091501

Місце роботи здобувача: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: 03056, м.Київ, пр.Перемоги, 37

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 26.002.02

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського" Інститут енергозбереження та енергоменеджменту

Код за ЄДРПОУ: 247571500

Місцезнаходження: вул. Борщагівська 115, м. Київ, Київська обл., 03056, 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: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: 03056, м.Київ, пр.Перемоги, 37

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.09

Тема дисертації:

1. Методи захисту інформації від її реконструкції аналізом споживання потужності в термінальних компонентах комп'ютерних систем

2. Methods for data protection from reconstruction by power analysis in terminal components of computer systems

Реферат/анотація:

1. Дисертація присвячена проблемі захисту ключів криптографічних алгоритмів при їх реалізації на мікроконтролерах і смарт-картах від можливої реконструкції аналізом споживання потужності. Виконано аналіз структур та базових операцій криптографічних алгоритмів з позицій можливості поліморфної реалізації. Показано, що для симетричних алгоритмів, таких як DES, Rijndael та ГОСТ 28.147-89 існує два рівня поліморфної реалізації - рівень обробки блоків повідомлення і рівень шифрування окремого блоку. Теоретично доведено, що поліморфна реалізація алгоритму Rijndael обмежена двома послідовними ітераціями алгоритму. Розроблено і досліджено методи поліморфної реалізації алгоритмів Rijndael та ГОСТ 28.147-89. Запропонований метод поліморфної реалізації алгоритму Rijndael забезпечує варіацію моментів

виконання операції в межах 85% від часу обчислення однієї ітерації алгоритму. Показано, що ступінь операції модулярного експоненціювання, яка є закритим ключем алгоритмів RSA, El-Gamal та DSA, може бути реконструйована при застосування часового аналізу споживання потужності. В якості протидії розроблено метод поліморфної реалізації модулярного експоненціювання. Запропонований метод не використовує умовних операторів і забезпечує поліморфне виконання модулярних множень за рахунок збереження в пам'яті операндів. Застосування запропонованих методів дозволяє суттєво підвищити надійність захисту даних в термінальних пристроях комп'ютерних мереж.

2. Thesis is dedicated to a problem of protection the keys of cryptographic algorithms during its implementation on microcontrollers and smart cards from power analysis. The analysis of cryptographic algorithm's structures and basic operations with respect to the requirement of their polymorphic implementation is performed. It has been shown that for symmetric algorithms, such DES, Rijndael and GOST 28.147-89 there are two levels of polymorphic implementation: level of blocks of message computing and level of iterations several block processing. By theoretical way has been proved that Rijndael polymorphic implementation of operations is bounded only to two consecutive iterations of algorithm. The techniques for Rijndael and GOSN 28.147-89 polymorphic implementation based on random choosing of program sections sequences have been proposed and investigated. The proposed method for Rijndael stochastically polymorphic implementation provides the variation of moment operation time bounded by 85% from one iteration processing time. It has been shown that exponent of modular exponentiation which is secret key of RSA, El-Gamal and DSA can be reconstruction by timing power analysis. As countermeasure the technology for polymorphic implementation modular exponentiation has been worked out. Proposed method does not conditional operators use and proved the polymorphic implementation of modular multiplications at a sacrifice of storage in memory operands for those operations The application of the proposed method enables a significant increase in the reliability of data security in networked devices.

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. Самофалов Костянтин Григорович

2. Markovsky Oleksandr Petrovich

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. Зайцев Володимир Григорович
2. Зайцев Володимир Григорович

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. Корченко Олександр Григорович
2. Корченко Олександр Григорович

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

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Самофалов Костянтин Григорович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Самофалов Костянтин Григорович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності



Юрченко Т.А.