Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0406U003933

Особливі позначки: відкрита

Дата реєстрації: 19-10-2006

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Рамзі Анвар Саліба Сунна
2. Ramzi Anwar Saliba Sunna

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: ні

Шифр наукової спеціальності: 05.13.13

Назва наукової спеціальності: Обчислювальні машини, системи та мережі

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 16-10-2006

Спеціальність за освітою: 7.091501

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: 50.05

Тема дисертації:

1. Високопродуктивна реалізація протоколів захисту інформації на базі операцій медулярної арифметики
2. High-efficiency implementation of the data protection protocols based on modular arithmetic operations

Реферат:

1. Дисертація присвячена проблемі підвищення продуктивності реалізації протоколів захисту інформації в комп'ютерних мережах, в основі яких лежить модулярна арифметика. Підхід, що пропонується для вирішення цієї проблеми, має за основу те, що при практичному застосуванні систем захисту інформації з відкритим ключем таких як RSA та DSS, останній міняється достатньо рідко. Відповідно, рідко міняється і модуль. Це дозволяє прискорити реалізацію модулярних операцій за рахунок використання передобчислень, що залежать тільки від модуля. Представлені нові алгоритми модулярного множення, що використо¬вують передобчислення при фіксованому модулі. Один з них має за основу класичну схему модулярного множення, а другий являє собою модифікацію алгоритму Монтгомері. Показано, що продуктивність розроблених алгоритмів приблизно вдвоє вища в порівнянні з алгоритмом Монтгомері при прийнятних об'ємах потребуємої пам'яті. Запропоновано нові алгоритми для модулярного піднесення до квадрату та

множення, що мають за основу рекурсію Монтгомері.

2. The proposed approach to solving of this problem is base on of assumption that in practice the keys of the most public-keys data protection systems such as RSA and Digital Signature Standard, are changing rarely. So the modulus is changing a rather rarely too. This fact allows to speed up of modular operations implementation by using of precomputations which are depend on modulus only. The new precomputation modular multiplication algorithms are presented for modular multiplication for a fixed modulus. One of them is base on classical modular multiplication scheme and second is the modification of Montgomery algorithm. It has been shown that performance of proposed algorithms approximately twice high in compare to Montgomery algorithm and the amount of required storage is moderate. The new algorithms for modular squaring and multiplication by fixed number based on reduction of Montgomery have been proposed. By including of excess operations and using of precomputations the computational complexityof the proposed algorithm is less in compare to Montgomery modular multiplication algorithm.

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 К.Г.

2. Samofalov K. G.

Кваліфікація: д.т.н., 05.13.13

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. Печурін М. К.
2. Печурін М. К.

Кваліфікація: д.т.н., 05.13.13

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. Алішов Надір Ісмаіл-огли
2. Алішов Надір Ісмаіл-огли

Кваліфікація: к.т.н., 05.13.13

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 Луцький Г.М.

Власне Прізвище Ім'я По-батькові головуючого на засіданні Луцький Г.М.

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Т.А.