Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0420U102286

Особливі позначки: відкрита

Дата реєстрації: 18-12-2020

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Охріменко Андрій Олександрович
2. Okhrimenko Andriy

Кваліфікація:

Ідентифікатор ORCHID ID: Не застосовується

Вид дисертації: кандидат наук

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: 26-11-2020

Спеціальність за освітою: 125 Кібербезпека

Місце роботи здобувача: ТОВ САЙФЕР ПРО

Код за ЄДРПОУ: 42125815

Місцезнаходження: ВУЛИЦЯ НАГІРНА, будинок 25-27, м. Київ, 04107, Україна

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Сектор науки: Не застосовується

III. Відомості про дисертацію

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, буд. 1, м. Київ, Київська обл., 03058, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Сектор науки: Не застосовується

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: пр. Космонавта Комарова, буд. 1, м. Київ, Київська обл., 03058, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Сектор науки: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.37.23

Тема дисертації:

1. Методи арифметичних перетворень в полях і кільцях для криптографічних застосувань

2. Methods of arithmetic operations in rings of integers and prime fields for cryptographic applications

Реферат:

1. Дисертаційна робота присвячена розв'язанню актуальної науково-практичної задачі дослідження і розробки нових методів арифметичних перетворень над великими цілими числами з відкладеним переносом для підвищення швидкодії реалізації криптографічних перетворень, що мають місце в інформаційно-телекомунікаційних системах центрів сертифікації ключів національної інфраструктури відкритих ключів України. В роботі запропоновано метод представлення цілих чисел з відкладеним переносом, який за рахунок можливості відкласти операцію переносу зі старших розрядів в молодші та операцію займу з молодших розрядів у старші, дозволяє виключити взаємозалежність між машинними словами при виконанні арифметичних перетворень. Удосконалено методи арифметичних перетворень додавання, віднімання, зсуву вліво, зсуву вправо, множення, піднесення до квадрату, приведення за модулем,

ділення та порівняння, які за рахунок використання цілих чисел в представленні з відкладеним переносом дозволяють підвищити швидкодію перетворень в полях та кільцях цілих чисел. Також в роботі запропоновано методи арифметичних перетворень множення, піднесення до квадрату та приведення за модулем великих цілих чисел з відкладеним переносом та розпаралелюванням в два та декілька потоків. Використання запропонованих методів дозволяє підвищити швидкодію перетворень в криптографічних системах електронного підпису, що використовуються в національній інфраструктурі відкритих ключів.

2. Thesis is devoted to solving the scientific and practical task of research and development new methods of arithmetic transformations over large integers with delayed carry for increasing implementation of cryptographic transformations that take place in information and telecommunication systems of certification authorities in national public key infrastructure of Ukraine. The national PKI regulates the use of a qualified electronic signature according to the algorithms of DSTU 4145-2002, ECDSA, DSA and RSA. Operations of creating and verifying electronic signature are based on various mathematical methods: transformation in a ring of integers, field of integers and polynomials, in a group of points of an elliptic curve. All these transformations are impossible without arithmetic operations on integers. In this work proposed the method of integer representation with delayed carry, which due to the possibility of postponing carry operation from higher to lower words and the loan operation from lower to higher words, eliminates the interdependence between machine words when performing arithmetic operations. Performing operations with integers in the DCF representation, the processor operates with machine words in which two blocks are allocated to store the carry bits and to store the information bits. To convert a binary number to DCF it is necessary to reserve in the machine word r-bits for carry, and the remaining v-bits are filled with bits from the integer in a binary form. To convert a number from a DCF representation to a binary form, it is necessary to adjust carry (iteratively apply the carry from the lower machine word to the higher). To perform operations with integers in the DCF representation, it is necessary to modify the algorithms of arithmetic operations. Improved methods of arithmetic operations – addition, subtraction, left shift, right shift, multiplication, squaring, modular reduction, division and comparison, which by using integers in the delayed carry representation can increase the speed of operations in fields and rings of integers. The use of delayed carry allows to apply some approaches of parallelization for methods of arithmetic operations, for example, multiplication, squaring and modular reduction. In these operations, there is a multiplication operation, which consists of two multiplication cycles that can be parallelized. The first approach involves the parallel execution of the first and second multiplication cycles with subsequent adjustment of the results in two threads. The second approach involves the parallel execution of iterations of the first and the second multiplication cycles, followed by the merging of intermediate results, using multiple parallel threads. Proposed the methods of arithmetic operations of multiplication, squaring and modular reduction of large integers with delayed carry and parallelization in two or multiple threads.

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. Ковтун Владислав Юрійович

2. Kovtun Vladislav Yuriyovych

Кваліфікація: 05.13.21

Ідентифікатор ORCHID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Сектор науки: Не застосовується

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Смірнов Олексій Анатолійович

2. Smirnov Oleksii

Кваліфікація: 21.05.01

Ідентифікатор ORCHID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Сектор науки: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Кузнецов Олександр Олександрович

2. Кузнецов Олександр Олександрович

Кваліфікація: 05.13.21

Ідентифікатор ORCHID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Сектор науки: 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.