Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0410U005409

Особливі позначки: відкрита

Дата реєстрації: 30-07-2010

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Неласа Ганна Вікторівна
2. Nelasa Ganna Victorivna

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: ні

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: 05-07-2010

Спеціальність за освітою: 8.080403

Місце роботи здобувача: Запорізький національний технічний університет

Код за ЄДРПОУ: 02070849

Місцезнаходження: 69063 м. Запоріжжя, вул. Жуковського, 64

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: 50.37.23

Тема дисертації:

1. Удосконалення методів перетворень в якобіанах гіпереліптичних кривих для криптографічних додатків

2. Improvement of methods of transformation in jacobians of hyperelliptic curves for cryptographic applications

Реферат:

1. Дисертаційна робота присвячена удосконаленню методів виконання обчислень в якобіанах гіпереліптичних кривих, а також оцінці можливостей і перспектив застосування арифметики гіпереліптичних кривих в криптографічних додатках з урахуванням вимог по стійкості та складності. Набула подальшого розвитку модель асиметричних перетворень в якобіанах гіпереліптичних кривих. Удосконалено метод скалярного множення на еліптичних і гіпереліптичних кривих з передобчисленнями за критерієм продуктивності, який базується на розпаралелюванні обчислень і виключенні операції подвоєння в нульових вікнах. Удосконалено метод обчислення елементів матриці Хассе-Вітта для гіпереліптичних кривих спеціального виду довільного роду шляхом зведення обчислень до визначення біноміальних коефіцієнтів.

2. The thesis is devoted to improvement of transformation methods on hyperelliptic curves, and to estimate features and future trends of using hyperelliptic curves arithmetic in cryptographic protocols with taking into account resistance and complexity requirements. The model of asymmetric transformations in jacobians of hyperelliptic curves obtains the further development. The method of scalar multiplication on elliptic and

hyperelliptic curves with precomputation has been improved. Its efficiency is caused by simultaneous use of multisequencing of computational process and by exception of operations of doubling in zero windows. In the work the method of Hasse-Witt matrix elements for hyperelliptic curves of a special kind of any genus calculation has been improved by means reduction of calculations to computation of binomial coefficients.

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. Долгов Віктор Іванович
2. Dolgov Victor Ivanovich

Кваліфікація: д.т.н., 20.01.09

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. Бессалов Анатолій Володимирович
2. Бессалов Анатолій Володимирович

Кваліфікація: д.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

Власне Прізвище Ім'я По-батькові:

1. Борисенко Олексій Андрійович
2. Борисенко Олексій Андрійович

Кваліфікація: д.т.н., 05.13.05, 05.25.05

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 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.