Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0421U101606

Особливі позначки: відкрита

Дата реєстрації: 14-05-2021

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Циганкова Оксана Валентинівна

2. Tsygankova Oksana V.

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: 28-04-2021

Спеціальність за освітою: системи захисту інформації

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

Код за ЄДРПОУ: 247571500

Місцезнаходження: Борщагівська, 115, к. 306, м. Київ, 03056, Україна

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 26.002.29

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

Код за ЄДРПОУ: 02070921

Місцезнаходження: проспект Перемоги, буд. 37, м. Київ, 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 "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 247571500

Місцезнаходження: Борщагівська, 115, к. 306, м. Київ, 03056, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 28.29, 50.41.25

Тема дисертації:

1. Методи підвищення швидкодії асиметричних криптосистем з використанням еліптичних кривих у формі Едвардса

2. Methods for increasing the speed of asymmetric cryptosystems using elliptic curves in Edwards form

Реферат/анотація:

1. Роботу присвячено дослідженню криптографічних властивостей еліптичних кривих у формі Едвардса (ЕКФЕ) з метою використання їх в алгоритмах асиметричних криптосистем для підвищення їх швидкодії. Основну увагу зосереджено на ЕКФЕ над полями з модулем p, де p ⊓P. У роботі представлена удосконалена класифікація кривих в узагальненій формі Едвардса, яка поділяє множину цих кривих на три класи, що не перетинаються. Отримано результати аналізу властивостей ЕКФЕ різних, класів. Дано оцінку кількості та визначено умови існування ЕКФЕ з мінімальним кофактором порядку кривої. Отримано аналітичні оцінки швидкості експоненціювання точки на ЕКФЕ та на кривих у формі Вейєрштрасса та отримано результати порівняльного аналізу кількості операцій експоненціювання точок на цих кривих. Доведено, що експоненціювання точки класів повних і скручених ЕКФЕ швидше в 1,6 разів ніж експоненціювання точки на

кривих Вейєрштрасса. Розроблено новий метод знаходження точки простого порядку на повних та скручених, за новою класифікацією ЕКФЕ, на основі якого створено нові алгоритми пошуку генератора криптосистеми на ЕКФЕ. За допомогою розроблених алгоритмів пошуку генератора криптосистеми та з застосуванням запропонованого методу зниження складності операцій розраховано загальносистемні параметри 25 криптостійких скручених кривих Едвардса над простими полями з довжиною модулів, які рекомендовані стандартами FIPS-186-2-2000, FIPS-186-4-2013 та ISO/IECCD 15946.

2. This work is dedicated to studying the cryptographic properties of elliptic curves in Edwards form (ECEF) and to the subsequent use of those in the asymmetric cryptosystems in order to increase their speed. The main focus is on the elliptic curves in the Edwards form over fields modulo p, where p is prime. An improved classification of elliptic curves in generalized Edwards form is presented, which splits the set of these curves into three non-intersecting classes. New analytical results about properties of newly introduced ECEF classes are obtained. The existence conditions are determined and a cardinality are evaluated for elliptic curves in Edwards form with the minimum cofactor that can be used in the cryptographic algorithms. Analytical estimates of the point exponentiation efficiency on the elliptic curves in Edwards form and on curves in Weierstrass form are obtained. Comparative performance analysis are provided in terms of the number of scalar products. It is proved that the point exponentiation in complete and twisted ECEF classes is many times faster than the exponentiation of a point on the Weierstrass curves. Analysis of published works has shown that some inaccuracies arise in the ECEF properties describing because of the incorrect classification of curves proposed by D. Bernstein and co-authors. However, known results about the properties of the Edwards curves have not been sufficiently mathematically researched for the purpose to find the fastest and easiest-to-implement curves for use in cryptosystems. Based on the new proposed classification, conditions were obtained for the existence of ECEF with a minimum order coefficient of the curve, which allowed to calculate the number of curves that can be used to find crypto-resistant ECEF for use in the asymmetric cryptosystems. As a result of the calculations, it was obtained that over a prime finite field there are about 3/8 of the total number of elliptic curves in the generalized Edwards form which have order 4n, where n is prime, which can be used to find cryptographically strong curves for use in the asymmetric cryptosystems. A comparative analysis of the point exponentiation on the Edwards curves and the Weierstrass curves was performed, using the method of calculating the number of operations for the scalar product of the curve points, which allowed to estimate analytically the efficiency of point exponentiation on different curves. The results of the analysis show that the point exponentiation of classes of complete and twisted ECEF (by new classification) is 1.6 times faster than the point exponentiation on the Weierstrass curves used in the modern digital signature algorithms. In particular, the Edwards curves win with the ternary representation of k. A new method for determining the order of random points of the ECEF has been developed on the base of three theorems about properties of points and curve parameters, which makes it possible to simplify the finding of a prime order point by testing the coordinate of a random point. A new algorithm for finding a cryptosystem generator using the proposed method of determining the order of the random points is formulated, which allows to find the cryptosystem generator on the Edwards curves in O(logn) times faster than on the Weierstrass curves (here n is the order of the group of points of the elliptic curve). Using the new algorithms of cryptosystem generator search and the method of minimization of complexity of operations, parameters of 25 twisted and 39 complete cryptographically strong elliptic curves in Edwards form over the prime fields with a modulo length p = 192, 224, 256, 384 i 521 bit (recommended by standards FIPS-186-2-2000, FIPS-186-4-2013 and ISO/IECCD 15946) are found, that allows to use them in asymmetric cryptoalgorithms. A new, simpler and faster than known, method of finding the ECEF order and reconstructions of all points of the complete Edwards curve is proposed. It can be used for teaching disciplines related to elliptic mathematics. The dissertation consists of an introduction, four sections, conclusions, a list of sources used, five appendices. The introduction substantiates the relevance of the topic of the dissertation, formulates the purpose and objectives of the research, scientific novelty and practical significance of the obtained results. The information about implementation of work results, their validation, publications and personal contribution of the applicant are given.

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. Бессалов Анатолій Володимирович
2. Bessalov Anatoliy V

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

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Яремчук Юрій Євгенович
2. Yaremchuk Yuriy Ye

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. Корнейко Олександр Васильович

2. Korneyko Olexander V

Кваліфікація: к.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

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради — Теленик Сергій Федорович

Власне Прізвище Ім'я По-батькові головуючого на засіданні — Новіков Олексій Миколайович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності — Юрченко Т.А.