Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0418U002123

Особливі позначки: відкрита

Дата реєстрації: 16-02-2018

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Ганзя Роман Сергійович

2. Hanzia Roman Serhiiovych

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: 18-01-2018

Спеціальність за освітою: Безпека державних інформаційних ресурсів

Місце роботи здобувача: Харківський національний університет імені В.Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: майдан Свободи, 4, м. Харків, Харківський р-н., Харківська обл., 61022, 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 64.051.29

Повне найменування юридичної особи: Харківський національний університет імені В.Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: майдан Свободи, 4, м. Харків, Харківський р-н., Харківська обл., 61022, 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: 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

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.37.23

Тема дисертації:

1. Моделі, методи та засоби генерування загальносистемних параметрів еліптичних кривих для криптографічних застосувань

2. Models, methods and means for generating elliptic curves general system parameters for cryptographic applications

Реферат:

1. Дисертаційна робота присвячена вирішенню важливої наукової задачі, яка полягає у розробці моделей та методів побудови криптостійких загальносистемних параметрів (ЗСП) для криптографічних перетворень в групах точок еліптичних кривих (ЕК), обґрунтування можливостей використання таких параметрів у постквантовий період, реалізація засобу генерування криптостійких параметрів для криптографічних перетворень в групах точок ЕК високого та надвисокого рівнів стійкості для національних стандартів асиметричних криптоперетворень. У дисертаційній роботі вперше запропоновано метод обчислення значення норми елемента з кільця р адичних чисел через детермінант матриці Сильвестра для знаходження сліду ендоморфізму Фробеніуса при об-числені порядку ЕК для застосування в криптографічних перетвореннях, що дозволило значно зменшити складність обчислення порядку ЕК за рахунок відсутності необхідності переходити між базисами у певних системних рішеннях. Вперше обґрунтовано властивості ЗСП

криптографічних перетворень в групі точок ЕК та умови застосування ЕК в постквантовий період, що дозволило змінити математичну модель генерування криптостійких ЗСП в напрямку підвищення рівня стійкості криптографічних пере-творень на базі ЕК у випадку появи квантового комп'ютера із значенням регістра, що буде достатнім для криптоналізу асимет-ричних криптоперетворень сучасних розмірів. Удосконалено метод обчислення норми через детермінант матриці Сильвестра при побудові ЗСП ЕК великого порядку базової точки для криптографічних застосувань, що відрізняється від існуючих використан-ням особливостей внутрішньої будови матриці при обчисленні детермінанта та дозволяє прискорити знаходження порядку кривої та формування кортежу ЗСП ЕК. Удосконалено та адаптовано під національні стандарти електронного цифрового підпису (ЦП) та направленого шифрування (НШ) математичну модель побудови криптостійких параметрів для ЕК, що визначені над двійковим полем, в умовах протидії квантовому криптоаналізу, що відрізняється від існуючих використанням оптимальних (за часовим показником) методів обчислення порядку ЕК та подальшої побудови ЗСП і дозволяє продовжити використання таких криптоперетворень без суттєвої зміни існуючої математичної бази та програмного забезпечення навіть після появи квантового комп'ютера, що здатен виконувати квантові алгоритми криптоаналізу. Удосконалено моделі порушника та загроз для сучасних та перспективних криптографічних перетворень, що дозволило обґрунтувати вимоги до розмірів ЗСП в умовах появи квантово-го комп'ютера та застосування його для криптоаналізу. Отримані практичні результати полягають у наступному. Розроблено програмний засіб, що здатен генерувати параметри високого та надвисокого рівнів стійкості за поліноміальний час, та ґрунтуєть-ся на використані моделей та методів, що були розроблені та удосконалені. Зроблено пропозиції, щодо модифікації бази ЗСП криптоперетворень в діючому стандарті ЕЦП України ДСТУ 4145–2002 у напрямку доповнення існуючих параметрів розмірами від 431 біта до 1031 біта, для підвищення рівня стійкості криптографічних перетворень, що на даний момент широко використовуються для криптографічного захисту інформації в Україні, у випадку появи квантових комп'ютерів з можливістю здійснення криптоаналізу за поліноміальний час. На основі проведеного аналізу та дослідження моделей та методів обчислення кількості точок на ЕК, запропоновано методи та засоби побудови криптографічних стійких параметрів для криптоперетворень, визначених в національних стандартах ЕЦП та НШ, за умови, що кінцевий користувач може власноруч генерувати собі загальні параметри відповідно до потреб використання у криптографічних додатках. Отримано аналітичні співвідношення, що визначають умови забезпечення стійкості сучасних криптосистем проти квантового криптоаналізу, а також запропоновано напрямки розвитку пост-квантових криптоалгоритмів для забезпечення захисту інформації після появи квантових комп'ютерів. Отримано оцінки (наприклад, використання модифікованого методу нормування дає виграш у часі приблизно на 15% у порівнянні зі стандартним методом) та аналітичні співвідношення для реалізації методу обчислення норми через детермінант матриці Сильвестра, які можуть бути застосовані в програмних засобах при побудові ЗСП, а сам метод відповідно до цього може бути розпаралелений з подальшим підняттям його швидкодії для великих значень розмірів базових параметрів ЕК.

2. The thesis is devoted to solving an important scientific problem, which consists in the development of models and methods for cryptographic transformations in groups of points of elliptic curves (EC) strong general system parameters (GSP) generating, justification the possibilities of using such parameters in the post-quantum period, generating strong GSP for high and ultrahigh security levels cryptographic transformations in EC groups of points mean implementation for national asymmetric cryptographic transformation standards. The object of the research is generating strong GSP for cryptographic transformations in EC groups of points over a finite binary field process-es. Subject of research is generating strong GSP for using in modern cryptographic applications methods, includes using in the post-quantum period. In the thesis norm of element value from p-adic elements ring with the help of Sylvester matrix determinant which can be used to find the trace of the Frobenius endomorphism when computing the EC order for using in cryptographic transformations calculation technique was developed for the first time. This allows significantly reduce the EC order computation complexity because of the lack of necessity to switch between bases in certain system solutions. Cryptographic transformations in the group of EC points GSP features and conditions of their use in the post-quantum period were grounded for the first time. Such decision

allowed changing generating strong GSP mathematical model along the lines of cryptographic transformation based on EC security level increasing in case of quantum computer with sufficient value register for modern sizes asymmetric cryptographic transformations cryptanalysis appearance. Norm computation method with the help of Sylvester matrix determinant for the large order base point EC GSP generating was improved. Proposed method differs from existing by using the features of the internal structure of the matrix for determinant computing. This allows curve order finding and GSP cortege generating forcing. Strong GSP for EC which determined over binary field mathematical model generating in the conditions of quantum cryptanalysis counteraction was improved and adapted to the national standards of electronic signature and asymmetric encryption. Proposed method differs from existing by using optimal (by time indices) computing EC order and further GSP generating methods. This permits to keep on using such cryptographic transformations without changing of existing mathematical base and software even after quantum computer which will be capable of quantum cryptanalysis algorithms performing appearance. The intruder and threat models for modern and prospective cryptographic transformations were improved which allowed to substantiate the require-ments for GSP size in the conditions of the quantum computer, which can be used for cryptanalysis appearance. The obtained practical results are follows. A software tool that is capable of generating parameters of high and ultra-high security levels for polynomial time was developed. It's based on using models and methods that have been developed and improved. Proposals for GSP cryptographic transformations based on the modifications for the national digital signature standard DSTU 4145-2002 currently in force were made. Modifications touch on the issue of additions the existing parameters with the sizes from 431 bits to 1031 bits. This is necessary for cryptographic transformations security level increasing. Because such type of cryptographic transformations are currently used for cryptographic security in Ukraine. Then quantum computer will have to have more than 7,000 qubits for cryptanalysis. Based on conducted analysis as well as computing the number of EC points models and methods research on conditions that user according to the cryptographic applications needs can independently generate GSP in the dissertation methods and means for generating elliptic curves general system parameters for the nationals standards of electronic signatures and asymmetric encryption are proposed The analytical relations which determine the conditions for ensuring the modern cryptosystems security against quantum cryptanalysis were obtained. Also areas of development of post-quantum cryptographic algorithms for information protection after the quantum computers appearance were proposed. Estimates (for example, the use of the modified norm computation method gives a gain of about 15% in the time complexity in comparison with the standard method) and analytical relations for implementing the norm computation method with the help of the Sylvester matrix determinants were obtained. Derived result can be applied in the GSP generating software. The obtained scientific and practical results are implemented at the performance of researches which are related with strong EC GSP generation. The developed proposals were used for creating software and in the education.

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. Горбенко Іван Дмитрович

2. Gorbenko Ivan Dmytrovych

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. Харченко В'ячеслав Сергійович

2. Harchenko Vjacheslav Sergijovych

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

Власне Прізвище Ім'я По-батькові:

1. Толюпа Сергій Васильович

2. Toliupa Serhii Vasylovych

Кваліфікація: д. т. н., 05.12.02

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	Краснобаєв Віктор Анатолійович
Відповідальний за підготовку облікових документів	
Реєстратор	
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Т.А.