Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0518U000308

Особливі позначки: відкрита

Дата реєстрації: 12-01-2018

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Чевардін Владислав Євгенійович

2. Chevardin Vladyslav Evgenievich

Кваліфікація: к. т. н., 05.13.21

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор 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: 14-12-2017

Спеціальність за освітою: Комплекси, системи та засоби автоматизації управління військами та озброєнням

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 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

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.37.23

Тема дисертації:

1. Методи побудови генераторів псевдовипадкових послідовностей на основі ізоморфних перетворень еліптичних кривих

2. Methods of deterministic random bit generators building based on isomorphic transformations of elliptic curves

Реферат:

1. Проведено аналіз відомих підходів до побудови генераторів псевдовипадкових послідовностей, отримані результати оцінки їх криптографічної стійкості, статистичної безпеки та швидкодії. Розкриті недоліки та переваги відомих генераторів ПВП. Отримані практичні та аналітичні оцінки числа кроків до першого зациклення окремого класу генераторів на еліптичних кривих, який є меншими у порівнянні зі спрощеною моделлю, майже у $\sqrt{N}$ разів. Вдосконалені методи генерації ПВП на основі скалярного множення точок еліптичної кривої за рахунок використання перетворень в групі точок кривих Едвардса, ізомофрних перетворень канонічної форми еліптичної кривої, що дозволило використовувати всю множину ізоморфних перетворень еліптичної кривої та збільшити період генератора ПВП пропорційно квадрату характеристики поля p, у порівнянні з існуючим стандартом. Розроблено методи генерації ПВП на основі використання ізоморфних трансформацій еліптичної кривої, який відрізняється від існуючих методів використанням ізоморфної трансформації на основі секретного ключа. Отримані в роботі результати дозволили вирішити

проблему побудови криптографічно стійких генераторів ПВП підвищеної швидкодії за рахунок використання ізоморфних перетворень еліптичних кривих.

2. The analysis of modern situation of the cryptographic security of information in a world and in the country is received. The impossibility of future developing of cryptographic security of information systems without safe deterministic random bit generators (DRBG) with increasing a security and a rapid is defined. It becomes more actuality in conditions of future increasing power and number of quantum computers. In the work much results of researches in the cryptographic security field were analyzed. Using the results of analysis there was defined the conditions for search of new solutions in cryptography field and methods of building safe and resistance of DRBG based on theoretical problems. The research results showed much more possibilities for improvement of modern DRBG based on elliptic curves with measures: security resistance, prediction resistance, backtracking resistance and computational complexity (performance). However except of known shortcomings of DRBG on elliptic curves in research process the pseudorandom sequences with anomaly small periods were detected. The results were received with famous approach to building DRBG based on elliptic curves arithmetic. The results of the analysis of different approaches to building RBG, the results of estimate cryptographically resistance, statistical properties of sequences and performances of famous DRBGs with considering requires ISO/IEC 18031, ANSI X.9.82, AIS 20 were showed in the work. In the chapter the limitations and advantages of RGB based on different cryptographic primitives: block ciphers, hash functions, theoretical problems are detected. The pseudorandom sequences with anomaly small periods and preperiods from DRBG on elliptic curve are showed. There was received practical estimates of anomaly small numbers before first cycling DRBG on elliptic curves that justify the necessity of their theoretical estimation. The theoretical estimates give more justify values of numbers before first DRBG cycle. The received theoretical estimates of number of generator iterations before first DRBG cycle are smaller than idealized simplified model nearly in $\sqrt{N}$. There were enhanced DRBGs based on the scalar multiplication of elliptic curve points by using transformation in group of Edwards curve points over Galois field like a generator of DRBG internal states. It allowed to reduce of the DRBG calculate complexity in 2 – 3 times in the pseudorandom sequences generation in comparison with the standard Dual_EC_DRBG as a result the elliptic curve DRBG speed was increased. The number of elliptic curve transforms from canonical form to canonical form under Galois field shows linear dependence of isomorphic transformation highest bound from characteristic field p. For transformation from canonical to elliptic curve normal form that boundary increases proportionally p4. The method of generation of pseudorandom sequences based on double scalar elliptic curve point multiplication over Galois field with characteristic $p \neq 2,3$ was developed, which defers from existing by using full elliptic curve isomorphic transformation set. It allowed to increase number of internal states of DRBG proportionally field characteristic p and it increases the period of pseudorandom sequence and increase the DRBG resistance proportionally p2 in comparison with existing standard.

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. Ковальчук Людмила Василівна
2. Kovalchuk Liudmyla Vasulivna

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. Ковальчук Людмила Василівна
2. Kovalchuk Liudmyla Vasulivna

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

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Максимович Володимир Миколайович
2. Maxymovych Volodymyr Mykolayovych

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. Василіу Євген Вікторович
2. Vasiliu Evhen Viktorovych

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. 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	Горбенко Іван Дмитрович
Відповідальний за підготовку облікових документів	
Реєстратор	
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Т.А.