Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0520U100483

Особливі позначки: відкрита

Дата реєстрації: 22-09-2020

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Бабенко Віра Григорівна
2. Babenko Vira

Кваліфікація: 05.13.21

Ідентифікатор ORCHID ID: Не застосовується

Вид дисертації: доктор наук

Шифр наукової спеціальності: 05.13.05

Назва наукової спеціальності: Комп'ютерні системи та компоненти

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 18-09-2020

Спеціальність за освітою: Спеціалізовані комп'ютерні системи

Місце роботи здобувача: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження: бульвар Шевченка, 460, м. Черкаси, Черкаський р-н., Черкаська обл., 18006, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Сектор науки: Не застосовується

III. Відомості про дисертацію

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): Д 73.052.04

Повне найменування юридичної особи: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження: бульвар Шевченка, 460, м. Черкаси, Черкаський р-н., Черкаська обл., 18006, 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: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження: бульвар Шевченка, 460, м. Черкаси, Черкаський р-н., Черкаська обл., 18006, 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: 20.51.35, 50.37.23

Тема дисертації:

1. Методологія синтезу операцій перетворення інформації для комп'ютерної криптографії

2. The methodology for the synthesis of information transformation operations for computer cryptography

Реферат:

1. Дисертаційна робота присвячена вирішенню проблеми підвищення ефективності функціонування криптосистем на основі використання створеної методології синтезу операцій криптографічного перетворення інформації. Застосування технології побудови та використання криптопримітивів на основі синтезованих операцій криптоперетворення, що мають властивості афінності та нелінійності, забезпечило можливість збільшення стійкості за рахунок варіативності операцій та швидкості перетворення внаслідок паралельної реалізації. Розроблено технологію синтезу операцій для мультиопераційних матричних криптографічних примітивів підвищеної стійкості. Удосконалено методи синтезу та аналізу криптографічних алгоритмів на основі узагальненої моделі криптографічного алгоритму. Отримано можливість забезпечення гнучкого керування параметрами криптографічних алгоритмів у процесі їх синтезу, виходячи з задач

проектування. Ключові слова: комп'ютерна криптографія, операції криптографічного перетворення, нелінійність, варіативність, паралельна реалізація, узагальнена модель, криптостійкість, швидкість перетворення.

2. The dissertation is devoted to solving the problem of increasing the efficiency of the use of cryptosystems based on created methodology for the synthesis of operations of cryptographic transformation of information and the construction of cryptographic primitives based on them. The object of the research is the processes of synthesis of information transformation operations. The subject of research is methods and means of synthesizing information transformation operations for computer cryptography. A methodology for the synthesis of operations of cryptographic transformation of information is proposed on the basis of existing and developed methods of the synthesis of operations of direct, reverse and mutual cryptographic transformation by their classification and generalization, which has made it possible to expand the base of operations, the use of which allows to improve existing cryptoalgorithms and crypto primitives and synthesize new ones. The use of the technology for the construction and use of crypto primitives based on synthesized cryptographic transformation operations with affinity and nonlinearity properties has provided the possibility to increase the security due to the variability of operations and the conversion speed due to parallel implementation. A technology for synthesizing operations for multioperational matrix cryptographic primitives of increased security has been developed. This technology has been developed for the synthesis of operations for multioperational matrix cryptographic primitives based on the construction of new groups of operations accurate to permutation by using the proposed tabular model of the cryptographic transformation operation, which has made it possible, due to the variability of operations, to increase the cryptographic security of existing cryptographic primitives. Methods for constructing cryptographic primitives have been improved on the example of sliding encryption primitives based on matrix operations of cryptographic transformation and the obtained generalized recurrent sequences for building models by their parallel implementation, which has provided an increase in encryption speed up to 2 times and security to linear cryptanalysis. The methods of synthesis and analysis of cryptographic algorithms based on a generalized model of the cryptographic algorithm by sequentially-parallel implementation of operations of cryptographic transformation of information at macro and micro levels have been improved, which has made it possible to resolve contradictions between cryptographic security, complexity and speed in order to achieve a given efficiency, based on design tasks. Mathematical models and methods of the synthesis of elementary functions and operations of cryptographic transformations have been further developed on the basis of the group of elementary functions of the extended matrix cryptographic transformation selected from the classification, by improving the mathematical apparatus for synthesizing direct and inverse matrix models of non-affine discrete transformations. Together they have provided the possibility of synthesizing operations of nonlinear cryptographic transformations and confirmed the correctness of the main provisions of the proposed methodology. Variants of implementation at the software and hardware levels of new groups of cryptographic operations of a given bit width with the properties of affinity and nonlinearity, in particular, matrix and extended matrix transformations are proposed. The use of synthesized operations of cryptographic transformation based on the proposed options for combining the use of matrix and extended matrix transformations in the design of algorithms allows to increase the cryptographic security from 2166 to 28157 times in proportion to stream encryption while reducing the encryption time from 1.3 to 8 times. The ability to provide flexible control of the parameters of cryptographic algorithms in the process of their synthesis, based on design problems, has been obtained. Keywords: computer cryptography, cryptographic transformation operations, nonlinearity, variability, parallel implementation, generalized model, cryptographic resistance, transformation speed.

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. Рудницький Володимир Миколайович
2. Rudnytskyi Volodymyr M.

Кваліфікація: 05.13.06

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. Рудницький Володимир Миколайович
2. Rudnytskyi Volodymyr M.

Кваліфікація: 05.13.06

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. Корченко Олександр Григорович

2. Korchenko Oleksandr H.

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

Власне Прізвище Ім'я По-батькові:

1. Можаєв Олександр Олександрович

2. Mozhaiev Oleksandr O.

Кваліфікація: 05.13.05

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. Семенов Сергій Геннадійович

2. Semenov Serhii H.

Кваліфікація: 05.13.05

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

Власне Прізвище Ім'я По-батькові:

1. Єременко Володимир Станіславович
2. Yeremenko Volodymyr S.

Кваліфікація: 05.13.05

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. Семенов Сергій Геннадійович
2. Semenov Serhii H.

Кваліфікація: 05.13.05

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. Федоров Євген Євгенович

2. Fedorov Yevhen Yevhenovych

Кваліфікація: 05.13.05

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. Фауре Еміль Віталійович

2. Faure Emil V.

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

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Рудницький Володимир Миколайович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Федоров Євген Євгенович
Відповідальний за підготовку облікових документів	
Реєстратор	
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Т.А.