Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0421U100320

Особливі позначки: відкрита

Дата реєстрації: 19-02-2021

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Бреус Роксолана Василівна

2. Breus Roksolana Vasylivna

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

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: 09-02-2021

Спеціальність за освітою: Комп’ютерна інженерія

Місце роботи здобувача: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження: бульвар Шевченка, буд. 460, м. Черкаси, Черкаський р-н., Черкаська обл., 18006, 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 73.052.04

Повне найменування юридичної особи: Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

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

Код за ЄДРПОУ: 05390336

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

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.41.27, 50.05.19

Тема дисертації:

1. Генерація псевдовипадкових послідовностей операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда

2. Generation of pseudo-random sequences of operations of strict stable cryptographic coding based on the transformation of the second operand

Реферат:

1. Дисертаційна робота присвячена підвищенню швидкості потокового шифрування за рахунок генерації псевдовипадкових послідовностей групи двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда. Для досягнення даного результату в другому розділі було розроблено метод синтезу обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда шляхом реалізації моделі автомата побудови другого операнда оберненої операції. В третьому розділі розроблено метод синтезу групи двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда відомої операції шляхом виконання над ним двохрозрядної

одноопераднної операції. В четвертому розділі розроблено метод генерації псевдовипадкових послідовностей двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда, що дозволяє значно спростити процес синтезу групи операцій та робить можливим використання даних операцій у вдосконаленому методі підвищення стійкості і надійності потокового шифрування. Результати впроваджені в Черкаському державному технологічному університеті, Черкаській міській консультативно-діагностичній поліклініці (філія №2), ТОВ «Нова Пошта», ПАТ «Черкасиобленерго». Ключові слова: комп'ютерна криптографія, операції криптографічного перетворення, потокові шифри, синтез операцій.

2. The dissertation is devoted to increasing of the speed of streaming encryption at the expense of generating of pseudo - random sequences of a group of two-bit two-operand operations of a strict stable cryptographic coding (further TBTOO of SSCC) based on the transformation of the second operand. The first section provides an overview of publications on the synthesis of operations of cryptographic coding of information. The directions of improvement of cryptographic coding are defined, the purpose and on its basis, the tasks of dissertation research are formulated. The second section is devoted to the synthesis of inverted TBTOO of SSCC based on the transformation of the second operand, the technology of studying the relationship between direct and inverse operations of cryptic transformation is proposed. The third section is devoted to the development of a method for the synthesis of the TBTOO of SSCC group based on the transformation of the second operand of a known operation. The relationship between direct and inverse operations allows the synthesis of inverse operations, and each inverse operation, in its turn, is a direct operation for another inverse operation, i.e. it is possible to synthesize another operation by converting the second operand with a single operand operation. The fourth section is devoted to the development of a method for generating pseudo-random sequences of TBTOO SSCC based on the transformation of the second operand, for this purpose, the results of synthesis of groups of TBTOO of SSCC based on the first operation are generalized. For the first time the method of synthesis of inverse two-bit two-operand operations of strict stable cryptographic coding based on a set of two-bit two-operand operations of strict stable cryptographic coding is developed; the relationships between direct and inverse operations, by transforming the second operand are established; all previously mentioned measures provided the possibility of practical application of these operations. For the first time a method of synthesis of a group of two-bit two-operand operations of strict stable cryptographic coding on the basis of using the known twobit two-operand operation of strict stable cryptographic coding and transformations of the second operand was developed. It was achieved by sequentially performing on this operation a group of two-bit single-operand operations, which provided the opportunity to increase the variability of crypto-primitives in the practical application of these operations. For the first time the method of generation of pseudo-random sequences of two-bit two-operand operations of strict stable cryptographic coding on the basis of use of groups of two-bit two-operand operations of strict stable cryptographic coding and two-bit one-operand operations of strict stable cryptographic coding was developed. It was done by transforming the second operands of direct and inverse two-operand operations, which allowed to increase the speed of streaming encryption by generating pseudo-random sequences of direct and inverse two-bit two-operand operations of strict stable cryptographic coding. The practical value of the work lies in bringing the developed methods to discrete models of operations and algorithms for automatic generation of pseudo-random sequences of operations of strict stable cryptographic coding for streaming computer encryption systems. The variability of cryptographic transformations is expanded by increasing the number of operations from 12 to 24. The developed pseudo-random sequence generator of two-bit two-operand operations of strict stable cryptographic coding provides synthesis of operations 15-20% faster than the tabular method of synthesis when providing a sequence period (24 !)2 . The obtained result provided the speed of implementation of the method of increasing the stability and the reliability of streaming encryption with maximum uncertainty of the conversion results.

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 Mykolaiovych

Кваліфікація: д. т. н., 05.13.06

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. Грищук Руслан Валентинович
2. Hryshchuk Ruslan Valentynovych

Кваліфікація: д. т. н., 21.05.01

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. Можаєв Олександр Олександрович
2. Mozhaiev Oleksandr Oleksandrovych

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

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Єременко Володимир Станіславович
2. Yeremenko Volodymyr Stanislavovych

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. Федоров Євген Євгенович
2. Fedorov Yevhen Yevhenovych

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. Семенов Сергій Геннадійович
2. Semenov Serhii Hennadiiovych

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

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.