Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0418U001260

Особливі позначки: відкрита

Дата реєстрації: 23-03-2018

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Полуяненко Микола Олександрович
2. Poluianenko Mykola Oleksandrovych

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: 22-02-2018

Спеціальність за освітою: Радіофізика та електроніка

Місце роботи здобувача: Управління Державної служби спеціального зв'язку та захисту інформації України в Харківській області

Код за ЄДРПОУ: 34755762

Місцезнаходження: вул. Чернишевська, 21., м. Харків, Харківський р-н., Харківська обл., 61002, Україна

Форма власності:

Сфера управління:

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. Моделі та методи синтезу регістрів зсуву з нелінійними зворотними зв'язками для схем потокового симетричного шифрування

2. Models and methods of synthesis of nonlinear feedback shift registers for the scheme of the symmetric key algorithm

Реферат:

1. Дисертаційна робота присвячена вирішенню важливої науково-технічної задачі, яка полягає в розробці та теоретичному обґрунтуванні методу синтезу регістрів зсуву з нелінійними зворотними зв'язками заданої довжини та встановленими конструктивними характеристиками для їхнього застосування в схемах потокового симетричного шифрування. Метою роботи є зменшення обчислювальної складності синтезу регістрів зсуву заданої довжини з нелінійними зворотними зв'язками, які відповідають встановленим вимогам стійкості для їхнього застосування в схемах потокового симетричного шифрування. У дисертаційній роботі удосконалено метод синтезу регістрів зсуву з нелінійними зворотними зв'язками другого порядку, який полягає в обґрунтуванні необхідних умов формування псевдовипадкових послідовностей максимального періоду, відрізняється застосуванням розробленої математичної моделі зі спрощеним формалізованим описом нелінійних зворотних зв'язків другого порядку, що дозволяє суттєво

зменшити обчислювальну складність процесу синтезу. В роботі також вперше розроблено метод синтезу регістрів зсуву з нелінійними зворотними зв'язками, що формують послідовність максимального періоду, який відрізняється від наявних методів переборного пошуку зменшеною обчислювальною складністю та дозволяє провести пошук нелінійних регістрів зсуву великих розмірів із встановленими конструктивними характеристиками. За допомогою розробленого апаратно-програмного засобу реалізовано алгоритм пошуку регістрів зсуву з нелінійними зворотними зв'язками, що формують послідовність максимального періоду, розміром до 32-х комірок включно. Набула подальшого розвитку модель оцінки криптографічної стійкості схем потокового симетричного шифрування, яка полягає в розробці системи критеріїв і показників стійкості псевдовипадкової послідовності, що сформовано регістрами зсуву з нелінійними зворотними зв'язками. Проведені дослідження дозволили проаналізувати захищеність регістрів зсуву з нелінійними зворотними зв'язками порівняно з лінійними регістрами від деяких розповсюджених криптографічних атак та обґрунтувати переваги застосування в системах потокового шифрування конструкції з використанням регістрів зсуву з нелінійними зворотними зв'язками. Отримані практичні результати полягають у наступному. Отримано метод синтезу регістрів зсуву з нелінійними зворотними зв'язками другого порядку з максимальним періодом послідовності, що сформовано та встановленими конструктивними характеристиками, що дозволяє скоротити обчислювальну складність переборних методів та процедур синтезу нелінійних регістрів зсуву. Розроблено апаратно-програмний комплекс синтезу регістрів зсуву з нелінійними зворотними зв'язками заданої довжини та встановленими конструктивними характеристиками із застосуванням апаратної частини на базі програмованих логічних інтегральних схем та обчислювальної потужності CPU та GPU. Розроблені рекомендації щодо його застосування. Отримано, експериментально перевірено та впроваджено при розробці схем потокового симетричного шифрування система аналітичних та емпіричних оцінок стійкості регістрів зсуву з нелінійними зворотними зв'язками другого порядку. Розроблено спеціальне математичне та апаратно-програмне забезпечення для експериментального дослідження властивостей псевдовипадкових послідовностей, що згенеровано регістрами зсуву з нелінійними зворотними зв'язками.

2. The dissertation solves scientific task - developing and theoretical substantiation of method for synthesis nonlinear feedback shift registers with given length and given constructive characteristics for their use in the scheme of the symmetric-key algorithm. The main goal of the work is decreasing computation complexity of synthesis nonlinear feedback shift registers with given length that satisfies given requirements of encryption protection for their use in the scheme of the symmetric-key algorithm. In this paper, the method for synthesis nonlinear feedback shift registers of the order two was improved. This method substantiates necessary conditions for forming of maximum length pseudorandom sequences. This method differs from other methods in that it uses developed mathematical model with simplified formalized description of nonlinear feedback of the second order, it allows to significantly reduce computation complexity of the synthesis process. The new method for synthesis nonlinear feedback shift registers with maximum length sequences was created in the work; the method differs from existing methods for selection search in that it has lower computation complexity and allows to find big nonlinear shift registers with given constructive characteristics. It has been created algorithm for search for nonlinear feedback shift registers with the help of the developed software and hardware means that form of maximum length sequences for up to 32 cells. The model of evaluation of cryptographic stability of scheme of the symmetric-key algorithm is further developed. According this model systems of criteria and indicators of stability of the pseudorandom sequence formed by nonlinear feedback shift registers were created. Those studies allow to analyze of rate of protection of nonlinear feedback shift registers in compare with linear feedback shift registers against of widespread cryptographic attacks. Advantages of using constructions of nonlinear feedback shift registers in stream cipher systems are substantiate. The obtained practical results are as follows. The new method for synthesis of nonlinear feedback shift registers of the second order with maximal forming sequence length and given constructive characteristics is obtained. Those practical results allow to decrease computation complexity of search methods and procedures of synthesis nonlinear feedback shift registers. Software and hardware complex for synthesis nonlinear feedback shift registers with given constructive characteristics and length has been

developed. The hardware part use programmable logic device with help of computing power of CPU and GPU. The recommendations for it use are given. A system of evaluation of analytical and empirical stability of the nonlinear feedback shift registers of the second order in the process of developing the scheme of the symmetric-key algorithm was obtained, experimentally verified and implemented. Special mathematical, hardware and software means have been developed. Those means are used for experimental study of the properties of pseudorandom sequences that generated by nonlinear shift registers.

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. Потій Олександр Володимирович
2. Potii Oleksandr

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. Чевардін Владислав Євгенійович

2. Chevardin Vladyslav Evgenievich

Кваліфікація: к. 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. Кудін Антон Михайлович

2. Kudin Anton Mykhailovych

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

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.