Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0414U004165

Особливі позначки: відкрита

Дата реєстрації: 07-10-2014

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Соколов Артем Вікторович
2. Sokolov Artem Viktorovich

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: 11-09-2014

Спеціальність за освітою: 8.17010201

Місце роботи здобувача: Одеський національний політехнічний університет

Код за ЄДРПОУ: 02071045

Місцезнаходження: пр. Шевченка, 1, м. Одеса-44, 65044 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): К 41.052.11

Повне найменування юридичної особи: Одеський національний політехнічний університет

Код за ЄДРПОУ: 02071045

Місцезнаходження: пр. Шевченка, 1, м. Одеса, Одеська обл., 65044, 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: Одеський національний політехнічний університет

Код за ЄДРПОУ: 02071045

Місцезнаходження: пр. Шевченка, 1, м. Одеса-44, 65044 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 синтезу багатобайтових нелінійних підстановок для підвищення ефективності сучасних шифрів

2. Synthesis methods of nonlinear multi-byte substitutions for modern ciphers efficiency improvement

Реферат:

1. Дисертація присвячена розробці методів синтезу нелінійних підстановок, що володіють високим рівнем криптографічної якості з метою підвищення ефективності сучасних криптографічних алгоритмів. Так, для створення S-блоків підстановки високої якості на основі досконалих алгебраїчних конструкцій побудовані методи синтезу повних класів бент-послідовностей та послідовностей де Брейна, а також лінійних рекурентних послідовностей великої довжини на основі всіх ізоморфних уявлень полів Галуа. На основі синтезованих досконалих алгебраїчних конструкцій побудовані криптографічні S-блоки підстановки, що володіють високою степеню криптографічної якості: є високо нелінійними, володіють мінімальною кореляцією векторів виходу та входу, відповідністю критерію розповсюдження, великими періодами повернення, та іншими привабливими криптографічними властивостями. Розроблені методи дозволяють синтез S-блоків підстановки будь-якої довжини, що може бути реалізована обчислювальною технікою. На основі послідовностей де Брейна синтезовано економічні S-блоки підстановки, що дозволяють значно зменшену за ресурсомісткістю апаратну та програмну реалізацію і при цьому зберігають відповідність

основним критеріям криптографічної якості. Показано, що на основі досконалих алгебраїчних конструкцій також можуть бути синтезовані генератори псевдовипадкових ключових послідовностей, які володіють не тільки більшою криптографічною та стохастичною якістю, але і дозволяють більш швидкодіючу реалізацію, що встановлено в процесі їх математичного моделювання.

2. Thesis is devoted to the development of methods of synthesis of the non-linear permutations according to the highest standards of cryptographic quality in order to improve the efficiency of modern cryptographic algorithms. In order to create the S-boxes with high quality based on perfect algebraic structures we developed methods of synthesis of complete classes of bent sequences, de Bruijn sequences, and linear recurring sequences of great length on the basis of all isomorphic representations of Galois fields. On the basis of synthesized advanced algebraic structures we built cryptographic S-boxes having a high degree of cryptographic quality: high nonlinearity, the minimum correlation between output and input vectors, respondent to the criteria of distribution, with long periods of return to initial state, and other attractive cryptographic properties. The developed methods allow the synthesis of any length of S-box that can be realized by modern computing devices. Based on de Bruijn sequences we synthesized economical S-boxes that significantly reduced hardware and software implementation and compliance to the basic criteria of the cryptographic quality. It is shown that on the basis of perfect algebraic structures pseudo-random key sequences generators can also be synthesized have not only higher cryptographic and stochastic quality but also allow a faster implementation, which was demonstrated in the process of mathematical modeling.

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. Мазурков Михайло Іванович
2. Mazurkov Michael Ivanovich

Кваліфікація: д.т.н., 05.12.13

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. Скопа Олександр Олександрович
2. Скопа Олександр Олександрович

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. Яремчук Юрій Євгенович
2. Яремчук Юрій Євгенович

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

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Кобозєва Алла Анатоліївна

Власне Прізвище Ім'я По-батькові головуючого на засіданні Кобозєва Алла Анатоліївна

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Т.А.