Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0499U000361

Особливі позначки: відкрита

Дата реєстрації: 01-12-2000

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Бардіс Ніколас

2. Bardis Nikolas

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 05.13.13

Назва наукової спеціальності: Обчислювальні машини, системи та мережі

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 25-01-1999

Спеціальність за освітою: 7.0915001

Місце роботи здобувача: Національний технічний університет України "Київський політехнічний інститут", фізико-математичний факультет

Код за ЄДРПОУ: 02070921

Місцезнаходження: 03056, Київ-56, пр-т. Перемоги, 37

Форма власності:

Сфера управління: Міністерство освіти України

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): Д 26.002.02

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського" Інститут енергозбереження та енергоменеджменту

Код за ЄДРПОУ: 247571500

Місцезнаходження: вул. Борщагівська 115, м. Київ, Київська обл., 03056, 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: Національний технічний університет України "Київський політехнічний інститут", фізико-математичний факультет

Код за ЄДРПОУ: 02070921

Місцезнаходження: 03056, Київ-56, пр-т. Перемоги, 37

Форма власності:

Сфера управління: Міністерство освіти України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 28.21.19

Тема дисертації:

1. Розробка підходу і застосування апарату булевих функцій для аналізу і синтезу ефективних криптографічних алгоритмів систем захисту інформаціє

2. Development of an approach and application of Boolean Functions tools to analysis and synthesis of effective Cryptographic algorithms of Information Security Systems.

Реферат/анотація:

1. Дисертація присвячена розробці підходу до аналізу рівня захищеності та синтезу алгоритмів криптографічного захисту інформаціє на основі використання апарату булевих функцій. Показана тотожність проблеми розкриття криптографічних алгоритмів та розв'язання системи булевих рівнянь, які визначаються булевими функціями бітових перетворень що реалізуються алгоритмом. Встановлено критеріє оцінки складності розв'язання систем булевих рівнянь та засоби єх практичного визначення. Запропоновані методи синтезу булевих функцій, які забезпечують високий рівень криптостійкості алгоритмів, побудованих на єх основі. З використанням запропонованого підходу проведено дослідження криптостійкості найпоширеніших алгоритмів захисту інформаціє.

2. The aim of the thesis is to develop an approach for analysis the level and to synthesis of cryptographic information security algorithms on the basis of Boolean function tool application. The identity of the problem of cryptograhic algorithm break^ with solution of a system of Boolean equations< which are determined by the algorithm has been shown. Criteria for evaluation of equivalent Boolean function system solution difficalty are wored out as well as means of their practical identification are presented. Method of Boolean function synthesis, which ensure a high level of cryptoresistance for the algorithms constructed on this basis are suggested. Verification of cryptoresistance of the most wodespead algorithms for information security have been carried out with application of above approach.

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. Самофалов Костянтин Григорович

2. Самофалов Костянтин Григорович

Кваліфікація: д.т.н., 01.05.03

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. Брюхович Євген Іванович

2. Брюхович Євген Іванович

Кваліфікація: д.т.н., 05.13.13

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. Селігей Олександр Минович

2. Селігей Олександр Минович

Кваліфікація: к.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

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Луцький Г.М.

Власне Прізвище Ім'я По-батькові головуючого на засіданні Луцький Г.М.

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності



Юрченко Т.А.