

Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0404U002451

Особливі позначки: відкрита

Дата реєстрації: 17-06-2004

Статус: Захищена

Реквізити наказу МОН / наказу закладу:



II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Абу Усбах Олексій Нідалійович

2. Abu Usbakh Oleksiy Nidaliovych

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: 10-06-2004

Спеціальність за освітою: 8.091501

Місце роботи здобувача: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: 03056, м.Київ, пр.Перемоги, 37

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 26.185.01

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

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 імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: 03056, м.Київ, пр.Перемоги, 37

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 20.53.17

Тема дисертації:

1. Методи синтезу та спосіб обчислення булевих функцій спеціального класу для засобів захисту інформації
2. Synthesis and calculation methods of special class Boolean functions for data security means

Реферат:

1. Дисертація присвячена дослідженню шляхів підвищення ефективності засобів захисту даних за рахунок використання булевих функціональних перетворень, основаних на функціях спеціального класу. Запропоновано новий клас булевих функцій, який характеризується інваріантністю до лінійних перетворень та має властивості важливі для його використання в булевих функціональних перетвореннях засобів захисту даних. Запропоновано новий метод синтезу нелінійних балансних булевих функцій, що задовольняють критерію чіткого лавинного ефекту, а також каскадний метод побудови булевих функціональних перетворень на основі таких функцій. Запропоновано новий таблично-паралельний спосіб обчислення булевих функціональних перетворень для блокових засобів захисту інформації. Спосіб має лінійну обчислювальну складність і дозволяє підвищити ефективність засобів захисту даних шляхом використання в них перетворень великої розрядності.

2. Thesis is dedicated to a problem of research the ways to increase the data security means efficiency by using Boolean function transformations based on special class functions. New class of Boolean functions is suggested. Being balanced and nonlinear the class functions satisfy strict avalanche criterion. The class properties are invariant for any class functions linear combination. Class functions can be effectively calculated by means of bit operation unification with concurrent execution. New synthesis method of balanced nonlinear SAC-functions is given. Cascade construction method of the Boolean function transformations is proposed as well. Unlike other methods this one allows varying transformations' nonlinearity with its computation complexity. Also the Cascade method can be used for large block transformations construction. New calculation method for Boolean function of suggested class is proposed. The method has linear computational complexity that allows increasing efficiency of data security means by large block transformation utilization.

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 ОПВ:

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. Samofalov Konstantin Grigorievich

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

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Мохор Володимир Володимирович
2. Мохор Володимир Володимирович

Кваліфікація: д.т.н., 01.05.02

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. Гузій Микола Миколайович
2. Гузій Микола Миколайович

Кваліфікація: к.т.н., 01.02.05

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**

Євдокимов Віктор Федорович

**Власне Прізвище Ім'я По-батькові
головуючого на засіданні**

Євдокимов Віктор Федорович

**Відповідальний за підготовку
облікових документів**

Реєстратор

**Керівник відділу УкрІНТЕІ, що є
відповідальним за реєстрацію наукової
діяльності**



Юрченко Т.А.