

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0219U101714

Державний реєстраційний номер: 0118U005441

Особливі позначки: відкрита

Дата реєстрації: 21-10-2019

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Дослідження математичних методів аналізу властивостей булевих функцій та їх використання для аналізу криптографічних систем

Початок етапу: 10.2018

Закінчення етапу: 09.2019

Вид звітнього документа: Остаточний звіт

III. Відомості про виконавця ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського "

Код за ЄДРПОУ: 34979237

Місцезнаходження: вул. Верхньоключова, 4, 27 корпус, м. Київ, Київська обл., 03056, Україна

Форма власності:

Сфера управління: Адміністрація державної служби спеціального зв'язку та захисту інформації

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 380442049151

IV. Відомості про співвиконавців ДіР

V. Відомості про замовника ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського "

Код за ЄДРПОУ: 34979237

Місцезнаходження: вул. Верхньоключова, 4, 27 корпус, м. Київ, Київська обл., 03056, Україна

Форма власності:

Сфера управління: Адміністрація державної служби спеціального зв'язку та захисту інформації

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 380442049151

VI. Джерела, напрями та обсяги фінансування ДіР

Підстава для проведення ДіР: 43 - власна ініціатива (якщо робота виконується з власної ініціативи за кошти виконавця НДР або безкоштовно)

Напрямок фінансування: 2.2 - прикладні дослідження і розробки

Джерела фінансування

7706 - безплатно (договір про науково-технічне співробітництво, тощо)

VII. Відомості про ДіР

Назва роботи українською:

Дослідження математичних методів аналізу властивостей булевих функцій та їх використання для аналізу криптографічних систем

Назва роботи англійською:

The study of mathematical methods for the analysis of singularities of Boolean functions and their use for the analysis of cryptographic systems

Реферат українською:

Об'єкт дослідження – оцінювання та обґрунтування стійкості криптографічних алгоритмів та протоколів відносно методів криптоаналізу. Мета роботи – дослідження існуючих та створення нових математичних методів аналізу властивостей булевих функцій з точки зору їх використання для оцінки стійкості криптографічних алгоритмів та протоколів, застосування отриманих результатів при вивченні навчальних дисциплін спеціальної кафедри № 1. Методи дослідження – методи теорії булевих функцій, лінійної алгебри, теорії ймовірностей та математичної статистики. Робота спрямована на вирішення наукового завдання, суть якого полягає в розробці математичних методів аналізу властивостей булевих функцій з точки зору їх використання для оцінки стійкості криптографічних алгоритмів та протоколів, що включає в себе: розробку методу розпізнавання -вимірності булевих функцій (БФ), заданих за допомогою оракулів; розробку поліноміальних алгоритмів оцінювання відстані між булевою функцією та множиною -вимірних БФ; розробку методу побудови -вимірних наближень БФ, заданих за допомогою оракулів. У результаті виконання науково-дослідної роботи розроблено метод розпізнавання -вимірності БФ, заданих за допомогою оракулів, поліноміальні алгоритми оцінювання відстані між БФ та множиною -вимірних БФ, метод побудови високіймовірних -вимірних наближень булевих функцій та метод обґрунтування відсутності високіймовірних -вимірних наближень булевих функцій. Отримані в науково-дослідній роботі результати можуть бути використані в освітньому процесі спеціальної кафедри № 1 під час проведення лекцій та практичних занять з навчальних дисциплін "Основи криптографії", "Математичні методи побудови та аналізу симетричних криптосистем", "Криптографічні протоколи".

Реферат англійською:

The object of the study is to evaluate and justify the stability of cryptographic algorithms and protocols against cryptanalysis methods. The purpose of the work is research of existing and creation of new mathematical methods of analysis of properties of Boolean functions from the point of view of their use for estimation of stability of cryptographic algorithms and protocols, application of the obtained results in studying of disciplines of special department № 1. Research Methods are methods of Boolean function theory, linear algebra, probability theory, and mathematical statistics. The work is aimed at solving a scientific problem, the essence of which is to develop mathematical methods for analyzing the properties of Boolean functions in terms of their use to evaluate the stability of cryptographic algorithms and protocols, which includes: development of a method of recognition - dimension of Boolean functions (BF), given by oracles; development of polynomial algorithms for estimating the distance between the Boolean function and the multiple-dimensional BF; development of a method for constructing -dimensional BF approximations, given by oracles. As a result of the research work, a method of recognition of the BF dimensions measured by oracles was developed, polynomial algorithms for estimating the distance between the BF and the multidimensional BF, the method for constructing high-dimensional Boolean functions and the method for substantiating the absence of high-probability features. The results obtained in the research work can be used in the educational process of the special department № 1 during lectures and practical training in the disciplines "Fundamentals of cryptography", "Mathematical methods for constructing and analyzing symmetric cryptosystems", "Cryptographic Protocols".

Індекс УДК:002:651.928(083.73), 512.624.95

Коди тематичних рубрик: 20.51.35

Керівники роботи

Власне Прізвище Ім'я По-батькові: Конюшок Сергій Миколайович

Науковий ступінь: к. т. н.

Вчене звання: доц.

Ідентифікатор ORCID ID:

Додаткова інформація:

VIII. Наукова (науково-технічна) продукція (НТП)

Назва НТП українською: Звіт про науково-дослідну роботу

Назва НТП англійською: Report on research work

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати: Методи, теорії

Галузь застосування: Криптографія

Реєстраційний номер картки технології:

Опис НТП: Отримані в науково-дослідній роботі результати можуть бути використані в освітньому процесі спеціальної кафедри № 1 під час проведення лекцій та практичних занять з навчальних дисциплін "Основи криптографії", "Математичні методи побудови та аналізу асиметричних криптосистем", "Криптографічні протоколи".

Соціально-економічна спрямованість НТП: Забезпечення промисловості чи населення новим видом інформаційно-комунікаційних послуг

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу:

Закінчення етапу:

Споживачі продукції:

Перспективні ринки:

Характер співробітництва з інвестором

Потрібний обсяг інвестицій, тис. грн.:

Права, що надаються інвестору після завершення роботи: Права не надаються

Наявність бізнес-плану: Ні

Техніко-економічне обґрунтування: Ні

Потенціальний обсяг продажу, тис. грн.:

Очікуваний термін окупності (років):

Додаткова інформація:

IX. Бібліографічний опис

Х. Заключні відомості

Керівник юридичної особи

Пучков Олександр Олександрович

к. філос. н.

Перелік осіб-виконавців

Іщенко Анатолій Олександрович

Бондаренко Юлія Леонідівна

Василенко Сергій Вікторович

(к. т. н.)

Гиренко Ігор Миколайович

(к. т. н.)

Кондакова Анастасія Михайлівна

Конюшок Сергій Миколайович

(к. т. н.)

Марченко Андрій Олександрович

Мостюк Дмитро Леонідович

Олексійчук Антон Миколайович

(д.т.н., 05.13.21)

Пучков Олександр Олександрович

(к. філос. н.)

Синицина Наталія Георгіївна

Степанюк Петро Петрович

Тарапата Олег Петрович

Уваркіна Олена Василівна

(д.філос.н., 09.00.10)

Відповідальний за підготовку облікових документів

Василенко С.В.

Телефон

+38 (044) 204-91-51

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

