

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0214U001792

Державний реєстраційний номер: 0113U005813

Особливі позначки: відкрита

Дата реєстрації: 27-06-2014

II. Етап виконання ДіР

Номер етапу: 2

Назва етапу: Аналіз сучасних криптографічних систем, математичних моделей та методів криптоаналізу. Модифікація та розробка нових алгебраїчно-ймовірнісних методів криптоаналізу симетричних та асиметричних криптосистем (Етап 1). Дослідження сучасних алгеброїчно-ймовірнісних методів криптоаналізу симетричних та асиметричних криптосистем, застосування цих методів до окремих систем криптографічного захисту інформації (Етап 2) .

Початок етапу: 12.2013

Закінчення етапу: 06.2014

Вид звітнього документа: Остаточний звіт

III. Відомості про виконавця ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження:

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 236-70-98, 406-81-76

IV. Відомості про співвиконавців ДіР

V. Відомості про замовника ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Служба зовнішньої розвідки України; військова частина К1410

Код за ЄДРПОУ: 33240845

Місцезнаходження: вул. Володимирська, 33, м. Київ, Київ, 01034, Україна

Форма власності:

Сфера управління: Служба безпеки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 0442262124

VI. Джерела, напрями та обсяги фінансування ДіР

Підстава для проведення ДіР: 52 - договір з вітчизняною організацією (органами місцевої ради, фондом, асоціацією, концерном тощо)

Напрямок фінансування: 2.2 - прикладні дослідження і розробки

Джерела фінансування

7713 - кошти держбюджету

Код програмної класифікації видатків і кредитування (КПКВК): 6621010

Фактичний обсяг фінансування (тис. грн.): 98.476

VII. Відомості про ДіР

Назва роботи українською:

Дослідження сучасних алгебраїчно-ймовірнісних методів криптоаналізу симетричних та асиметричних криптосистем і застосування цих методів до окремих систем криптографічного захисту інформації

Назва роботи англійською:

Researt of modern probabilistic cryptanalytic methods of symmetric and asymmetric cryptosystems, implementations of these methods to selected information security problems.

Реферат українською:

Застосовуються та розробляються нові алгебраїчно-ймовірнісні методи криптоаналізу симетричних та асиметричних криптосистем. Побудовано алгоритми перевірки стійкості шифрів до диференціального крипто аналізу. Досліджено апроксимації булевих функцій функціями меншої розмірності. Запропоновани статистичні атаки, досліджено імовірнісні характеристики розподілів в криптографічних перетвореннях. Проведено аналіз використання нейронних мереж для побудови криптографічних систем. Розроблено алгоритми для кривих Едвардса.

Реферат англійською:

New algebraically-probabilistic methods of cryptanalysis of symmetric and asymmetric cryptosystems are used. We construct estimates of probabilities of differentials and integer differentials of block ciphers, algorithms to check the security of the ciphers against the differential cryptanalysis. The approximation of Boolean functions by the functions of lower dimension are investigated. The statistical attack on the software implementation of the stream generator with reinitialization initial state is proposed. The analysis of the characteristics of probability distributions in some cryptographic transformations is provided. An analysis of the use of neural networks to build cryptographic systems in classical and postquantom computing models is proposed. The terms of the effectiveness of the proposed methods of cryptanalysis are defined.

Індекс УДК: 004.7, 681.3.06:519.248.681

Коди тематичних рубрик: 50.37.23

Керівники роботи

Власне Прізвище Ім'я По-батькові: Савчук Михайло Миколайович

Науковий ступінь:

Вчене звання:

Ідентифікатор ORCID ID:

Додаткова інформація:

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

Назва НТП українською: Науково-технічний звіт, в якому описано розроблені нові алгебраїчно-ймовірнісні методи криптоаналізу, що застосовані разом з модифікованими відомими методами до криптоаналізу симетричних та асиметричних криптосистем.

Назва НТП англійською: The scientific report in which the developed new algebraichno-probabilistic methods of the cryptoanalysis used together with modified known methods for cryptoanalysis of symmetric and asymmetric cryptosystems are described.

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати:

Галузь застосування: 73.10.1- Дослідження і розробки в галузі природничих та технічних наук

Реєстраційний номер картки технології:

Опис НТП: Застосовано та розроблено нові алгебраїчно-ймовірнісні методи криптоаналізу симетричних та асиметричних криптосистем. Побудовано оцінки ймовірностей диференціалів та цілочисельних диференціалів блокових шифрів, алгоритми перевірки стійкості шифрів до диференціального криптоаналізу. Досліджено апроксимації булевих функцій функціями меншої розмірності. Запропонована статистична атака з програмною реалізацією на генератор гами з лінійним законом реініціалізації початкового стану. Досліджено оцінки ймовірнісних характеристик розподілів в деяких криптографічних перетвореннях. Проведено аналіз використання нейронних мереж для побудови криптографічних систем в класичній та постквантовій моделях обчислень. Розроблено алгоритми для знаходження точок кривих Едвардса. Визначено умови ефективності запропонованих методів криптоаналізу.

Соціально-економічна спрямованість НТП:

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:

Наявність бізнес-плану:

Техніко-економічне обґрунтування:

Потенціальний обсяг продажу, тис. грн.:

Очікуваний термін окупності (років):

Додаткова інформація:

ІХ. Бібліографічний опис

1. Ковальчук Л., Кучинская Н. Построение верхних оценок средних вероятностей целочисленных дифференциалов раундовых функций блочных шифров определенной структуры. // "Кибернетика и системный анализ" - 2012, - №5, С. 71 - 81. 2. Алексейчук А.Н., Конюшок С.Н. О статистических свойствах нелинейности сужений булевых функций на случайно выбранное подпространство // Прикладная дискретная математика - 2012. - Вып. 1(15). - С. 5 - 10. 3. Бессалов А.В., Діхтенко А.А. Криптостойкие кривые Эдвардса над простыми полями. Прикладная радиоэлектроника, 2013, Том 12, №2. С. 285-291.

Х. Заклучні відомості

Керівник юридичної особи

Ільченко Михайло Юхимович

Перелік осіб-виконавців

Єндовицький П.О.

А.Олексійчук

А.Фесенко

Бессалов А.В.

Діхтенко А.

Завадська Л.О.

Конюшок С.В.

Л.Ковальчук

О.Фаль

С.Яковлев

Савчук М.М.

Семібаламут М.

Сторожук А.

Відповідальний за підготовку облікових документів

Телефон

Реєстратор

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

