

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0214U002102

Державний реєстраційний номер: 0113U005813

Особливі позначки: відкрита

Дата реєстрації: 17-01-2014

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Аналіз сучасних криптографічних систем, математичних моделей та методів криптоаналізу. Модифікація та розробка нових алгебраїчно-ймовірнісних методів криптоаналізу симетричних та асиметричних криптосистем. Теоретичні та експериментальні дослідження запропонованих методів криптоаналізу, умов їх ефективності, оцінка складності.

Початок етапу: 09.2013

Закінчення етапу: 12.2013

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", Фізико-технічний інститут

Код за ЄДРПОУ: 02070921

Місцезнаходження:

Форма власності:

Сфера управління: Міністерство освіти і науки, молоді та спорту 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.): 50.524

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:

Об'єкт дослідження - системи та процеси криптографічного захисту інформації та криптоаналізу, криптографічні атаки на системи захисту інформації. Запропонована сукупність методів побудови аналітичних оцінок верхньої межі імовірності існування диференціалів через відповідні параметри раундових функцій, яка застосована для оцінювання стійкості немарковських шифрів. Побудовано верхні оцінки середніх імовірностей цілочисельних диференціалів відображень, які є композиціями суматора, блока підстановки та оператора перестановки.

Реферат англійською:

Objects of research are systems and processes of cryptographic security, cryptanalysis, and cryptographic attacks in information security. A set of techniques is proposed for upper bounding of differential probabilities via corresponding round function parameters. Security of some non-Markov ciphers are estimated with these techniques.

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: Сучасні алгебраїчно-ймовірнісні методи криптоаналізу симетричних та асиметричних криптосистем і застосування цих методів до окремих систем криптографічного захисту інформації

Назва НТП англійською: Researct of modern probabilistic cryptanalytic methods of symmetric and asymmetric cryptosystems, implementations of these methods to selected information security problems.

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: Запропонована сукупність методів побудови аналітичних оцінок верхньої межі імовірності існування диференціалів через відповідні параметри раундових функцій, яка застосована для оцінювання стійкості немарковських шифрів. Побудовано верхні оцінки середніх імовірностей цілочисельних диференціалів відображень, які є композиціями суматора, блока підстановки та оператора перестановки. Розроблено методи побудови апроксимацій булевих функцій булевими функціями меншої розмірності та досліджено властивості таких апроксимацій. Досліджено способи перетворення алгебраїчних нормальних форм у кон'юнктивні нормальні форми з метою подальшого використання SAT-розв'язувачів. Представлено новий імовірнісний ефективний алгоритм розв'язку часткового випадку задачі про приховану дію абелевої групи в квантовій моделі обчислень, який може використовуватися для перевірки стійкості односторонніх функцій.

Соціально-економічна спрямованість НТП:

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: 2013-2015

Закінчення етапу:

Споживачі продукції: СЗР України

Перспективні ринки: Україна

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. Построение верхних оценок средних вероятностей целочисленных дифференциалов композиции ключевого сумматора, блока подстановки и оператора сдвига. // "Кибернетика и системный анализ" - 2010, - №6, С. 89 - 96. 2. 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. 3. Алексейчук А.Н. Усовершенствованный тест k-мерности для булевых функций / А. Н. Алексейчук, С. Н. Конюшок // Кибернетика и системный анализ. 2013. Т. 49. № 2. С. 27-35. 4. Alekseychuk A.N. Fast algorithm for reconstruction of high-probable low-dimensional approximations for Boolean functions / A. N. Alekseychuk, S. N. Konyushok // Modern Stochastics: Theory and Applications III, Proceedings. Kyiv. Taras Shevchenko National University. 2012. P. 32.

Х. Заклучні відомості

Керівник юридичної особи

Ільченко Михайло Юхимович

Перелік осіб-виконавців

А.Олексійчук

А.Фесенко

Л.Ковальчук

О.Фаль

С.Яковлев

**Відповідальний за підготовку
облікових документів**

Телефон

Реєстратор

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

