

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0215U009238

Державний реєстраційний номер: 0115U004118

Особливі позначки: відкрита

Дата реєстрації: 10-12-2015

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Вибір та аналіз напрямів дослідження. Дослідження та застосування методів криптоаналізу симетричних криптосистем (проміжний)

Початок етапу: 05.2015

Закінчення етапу: 11.2015

Вид звітнього документа: Проміжний 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 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.): 120
--

VII. Відомості про ДіР

Назва роботи українською:

Дослідження та застосування сучасних математичних методів аналізу окремих перетворень у системах криптографічного захисту інформації. Етап 1 (проміжний).

Назва роботи англійською:

Research and application of modern mathematical methods of single element analysis in cryptographic systems of information security

Реферат українською:

Досліджено імовірнісні та статистичні властивості операцій, що реалізуються у ключових суматорах блокових шифрів, отримано оцінки стійкості блокових шифрів з різними ключовими суматорами до узагальненого різницевого криптоаналізу. Проведено криптоаналіз на основі зсуву стандарту шифрування ДСТУ ГОСТ 28147:2009, апроксимація S-блоків за допомогою ARX функцій з побудови атаки часткового відновлення ключа. Досліджено ефективність кубічних атак з певними степенями макстермів та характеристики ймовірнісних розподілів в криптографічних перетвореннях.

Реферат англійською:

Probabilistic and statistical properties of operations in the key summators of block ciphers are researched, the security against generalized differential cryptanalysis of block ciphers with different key summators. Rotational cryptanalysis of GOST cipher was, approximation of S-blocks by ARX functions were used to partial recognition of the key. Efficiency of cube attacks with the certain degrees of maxterms was studied and probability distributions of certain cryptographic transformations was described

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: Звіт про науково-дослідну роботу "Дослідження та застосування сучасних методів аналізу окремих перетворень у системах криптографічного захисту інформації", шифр "Мокрель".
Етап 1. Вибір та аналіз напрямів дослідження. Дослідження та застосування методів криптоаналізу симетричних криптосистем (проміжний).

Назва НТП англійською: Report about research work " Research and application of modern mathematical methods of single element analysis in cryptographic systems of information security", code "MOKREL". stage 1. (intermediate).

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати: науково-технічний звіт

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

Реєстраційний номер картки технології:

Опис НТП: Науково-технічний звіт, в якому описано, що: досліджено імовірнісні та статистичні властивості операцій, що реалізуються у ключових суматорах блокових шифрів; отримано оцінки стійкості блокових шифрів з різними ключовими суматорами до узагальненого різницевого криптоаналізу; розроблено практичний метод побудови верхніх оцінок ймовірностей диференціалів немарковських блокових шифрів із урахуванням точного розподілу ймовірностей диференціалів S-блоків та особливостей лінійних перетворень; розроблено, теоретично обґрунтовано та експериментально досліджено ефективність статистичних атак на основі алгебраїчно вироджених наближень булевих функцій, що реалізуються алгоритмами потокового шифрування; проведено криптоаналіз на основі зсуву стандарту шифрування ДСТУ ГОСТ 28147:2009, апроксимація S-блоків за допомогою ARX функцій з побудови атаки часткового відновлення ключа; досліджено ефективність кубічних атак з певними степенями макстермів та характеристики ймовірнісних розподілів в криптографічних перетворен

Соціально-економічна спрямованість НТП:

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: 2015 рік

Закінчення етапу:

Споживачі продукції: СЗР України

Перспективні ринки: не досліджується

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. Завадська Л.О., Семибаламут М.А. Профиль линейной сложности как средство оценки качества случайных последовательностей // Проблемы управления и информатики, 2015. -2. -с.144-156. 2. Serhiy Yakovliev Provable Security of SAFER-like Substitution-Permutation Network against Differential Cryptanalysis// International Conference "Probability, Reliability and Stochastic Optimization", April 7-10, 2015, Kyiv, Ukraine, Confrence Materials 3. Доброногов Є.В. Обчислення верхніх меж диференціальних імовірностей для деяких класів блочних шифрів // Тринадцята наукова конференція "Теоретичні та прикладні проблеми фізики, математики та інформатики", 21- 23 травня 2015 р. - Київ 2015 - с.117-118. 4. Яковлев С.В. Доказова стійкість алгоритму шифрування "Кузнечик" до диференціального та лінійного криптоаналізу // Тринадцята наукова конференція "Теоретичні та прикладні проблеми фізики, математики та інформатики", 21- 23 травня 2015 р. - Київ 2015 - с.151-152.

Х. Заключні відомості

Керівник юридичної особи

Ільченко Михайло Юхимович

Перелік осіб-виконавців

Є.Доброногов

А.Олексійчук

А.Сторожук

А.Фесенко

В.Сергієнко

Л.Завадська

Л.Ковальчук

Н.Кучинська

О.Беспалов

О.Деркач

П.Єндовицький

С.Конюшок

С.Яковлєв

Відповідальний за підготовку

облікових документів

Телефон

Реєстратор

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

