

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0216U006601

Державний реєстраційний номер: 0115U004118

Особливі позначки: відкрита

Дата реєстрації: 11-04-2016

II. Етап виконання ДіР

Номер етапу: 2

Назва етапу: Теоретичні та експериментальні дослідження. Узагальнення і оцінювання результатів досліджень (Етап 2) (заключний)

Початок етапу: 12.2015

Закінчення етапу: 03.2016

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 України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 236-70-98, 204-81-76

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: 2.3 - виконання робіт за державними цільовими програмами

Джерела фінансування

7713 - кошти держбюджету

Код програмної класифікації видатків і кредитування (КПКВК): 6621010

Фактичний обсяг фінансування (тис. грн.): 60

VII. Відомості про ДіР

Назва роботи українською:

Дослідження та застосування сучасних методів аналізу окремих перетворень у системах криптографічного захисту інформації

Назва роботи англійською:

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

Реферат українською:

Проведено криптоаналіз на основі зсуву стандартів ДСТУ ГОСТ 28147:2009 та ГОСТ Р 34.11-2012, диференціальний криптоаналіз немарковських блокових шифрів із урахуванням особливостей операцій.. Розроблено статистичні атаки на криптографічні системи на основі алгебраїчно вироджених наближень булевих функцій. Досліджено ефективність кубічних атак за макстермами, атак збоїв на стандарт СТБ 34.101.31-2011, ефективність атак з перекриттям повідомлень в потокових шифрах. Проведено порівняльний аналіз ефективності алгоритмів обчислення на точках кривої Едвардса.

Реферат англійською:

Rotational criptoanalysis is provided to DSTU GOST 28147: 2009 cipher and GOST R 34.11-2012 hash function. Differential criptoanalysis of non-Markov block cipher are reviewed taking into account parameters used operations. Statistical attacks on the cryptographic systems, based on algebraically degenerate approximations of boolean functions, are developed. Efficiency of cube attacks with certain maxterms are reconsidered and fault attacks on STB 34.101.31-2011 cipher are reconsidered, also as efficiency of attacks based on keystream interception in stream ciphers. The comparative analysis of efficiency of algorithms of points evaluation in Edward's curves is provided.

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". Вибір та аналіз напрямів дослідження. Дослідження та застосування методів криптоаналізу симетричних криптосистем. (Етап 1). Теоретичні та експериментальні дослідження. Узагальнення і оцінювання результатів досліджень (Етап 2) (заключний)

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" . Choice and analysis of directions of researches. Research and use of methods of kryptoanalise of symmetric kriptosistem (stage 1) Theoretical and experimental researches. Generalizations and estimation of results of researches (stage 2) (final)

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: проведено криптоаналіз на основі зсуву стандартів ДСТУ ГОСТ 28147:2009 та ГОСТ Р 34.11-2012, диференціальний криптоаналіз немарковських блокових шифрів із урахуванням особливостей лінійних перетворень та операцій у ключових суматорах. Розроблено та досліджено статистичні атаки на криптографічні системи на основі алгебраїчно вироджених наближень булевих функцій. Досліджено ефективність кубічних атак з певними степенями макстермів, атак збоїв на стандарт СТБ 34.101.31-2011, ефективність атак з перекриттям повідомлень в потокових шифрах, можливість побудови trade-off модифікацій для відомих алгоритмів факторизації. Проведено порівняльний аналіз ефективності алгоритмів обчислення на точках кривої Едвардса в залежності від способу подання кривої.

Соціально-економічна спрямованість НТП:

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: 2016 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:

IX. Бібліографічний опис

1 Бессалов А.В., Цыганкова О.В. Классификация кривых в форме Эдвардса над простым полем. Прикладная радиоэлектроника: научно-техн. журнал. – 2015. – Том 14. – №4. – С.197 – 203. 2 Bessalov A.V., Kovalchuk L.V. Exact Number of Elliptic Curves in the Canonical Form, Which are Isomorphic to Edwards Curves Over Prime Field. Cybernetics and Systems Analysis: Volume 51, Issue 2 (2015), Page 165-172.
<http://www.springerlink.com/openurl.asp?genre=article&id=doi:10.1007/s10559-015-9709-x>.

X. Заключні відомості

Керівник юридичної особи

Ільченко Михайло Юхимович

Перелік осіб-виконавців

Є.Доброногов

А.Бессалов

А.Олексійчук

А.Сторожук

А.Фесенко

В.Сергієнко

Л.Завадська

Л.Ковальчук

Н.Кучинська

О.Беспалов

О.Деркач

О.Циганкова

П.Єндовицький

С.Конюшок

С.Яковлев

**Відповідальний за підготовку
облікових документів**

Телефон

Реєстратор

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

