Облікова картка ДіР

I. Загальні відомості

Державний обліковий номер: 0213U005558

Державний реєстраційний номер: 0112U008392

Особливі позначки: відкрита

Дата реєстрації: 15-07-2013

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Вибір напрямку дослідження, теоретичні та експериментальні дослідження. Узагальнення й оцінювання результатів дослідження.

Початок етапу: 12.2012

Закінчення етапу: 06.2013

Вид звітного 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: 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)

Напрям 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.): 124

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 cryptoanalytic 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. Узагальнено існуючі та створено нові математичні методи аналізу криптографічних алгоритмів, виконано узагальнення сучасних методів криптоаналізу, вдосконалено методологічну базу криптоаналізу.

Реферат англійською:

The objects of research are cryptographic security systems and processes. Existing mathematical techniques of cryptographic algorithm analysis are generalized, and some new ones are created. Methodological grounds of cryptanalysis are improved

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: Спеціальні технології, теоретичні та практичні розробки в науковому звіті про НДР "Дослідження сучасних алгебраїчно-ймовірнісних методів криптоаналізу симетричних та асиметричних криптосистем і застосування цих методів до окремих систем криптографічного захисту інформації"

Назва НТП англійською: Special technologies, theoretical and practical development in report on the results of scientific research work "Researt of modern probabilistic cryptoanalysis methods of symmetric and asimmetryc cryptosystems, implementation of these methods to selected information security"

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: За результатами НДР отримано: аналітичні оцінки верхніх меж імовірностей існування нетривіальних диференціалів та лінійних апроксимацій для незбалансованої альтерованої R-схеми; наведено конкретні нетривіальні диференціали та лінійні апроксимації, що мають імовірність 1 для довільної кількості раундів схеми шифрування; одержано аналітичну оцінку верхньої межі середніх диференціальних імовірностей SAFER-подібної SP-мережі з метою визначення стійкості до диференціального аналізу; запропоновано новий субекспоненційний алгоритм розв'язку задачі відновлення систематичних лінійних кодів за наборами спотворених кодових слів, що є менш трудомістким у порівнянні з існуючими; розглянуті різні узагальнення кубічної атаки; реалізовано алгоритм пошуку таких супермногочленів, в результаті якого знайдено 62 супермногочлени для шифру PRESENT з 80-тибітовим ключем; розглянуто один з новітніх методів криптоаналізу - аналіз на основі обертань; досліджено розподіл спільного секретного ключа у схемі Діффі-Хелмана; виведено

Соціально-економічна спрямованість НТП:

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: без обмежень

Закінчення етапу:

Споживачі продукції: Служба зовнішньо розвідки 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 обгрунтування:

Потенціальний обсяг продажу, тис. грн.:

Очікуваний термін окупності (років):

Додаткова інформація:

IX. Бібліографічний опис

1. Ковальчук Л.В., Шерстюк А.О. Дослідження різницевих характеристик раундової функції блочних шифрів MISTY1 та MISTY2 // Прикладная радиоэлектроника. - №3. - 2009. - С. 15-27. 2. Яковлев С.В. Оценки стойкости несбалансированных MISTY-подобных схем к дифференциальному и линейному криптоанализу // Проблемы управления и информатики. - №5. - 2012. - С. 142-155. 3. Ковальчук Л.В., Шерстюк А.О., Дослідження різницевих характеристик раундової функції блочних шифрів MISTY1 та MISTY2 // Прикладная радиоэлектроника. - №3. - 2009. - С. 15-27. 4. Ковальчук Л.В., Пальченко С.В., Скрипник Л.В., Застосування теорії узагальнених марковських шифрів для оцінювання стійкості сучасних блокових алгоритмів шифрування до методів різницевого криптоаналізу // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні - К.: НДЦ "Тезіс", 2009 - №2 (19) - стор. 45-56. 5. Л.В. Ковальчук, О.А. Сиренко Анализ перемешивающих свойств операций модульного и побитового сложения, определенных на одном носителе. // Кибернетика и системный анализ. - 2011. - № 5. - С. 83 - 97. 6. Л.В. Ковальчук, О.А. Сиренко Анализ перемешивающих свойств операций в конечном кольце. // Сборник тезисов XIV Международной научно-практической конференции "Безопасность информации в информационно-телекоммуникационных системах", 17-20 мая 2011, Киев, с.45-46. 7. Machulenko O. M., Savchuk M. M., Zavadska L. O. On a shared secret key distribution in Diffie-Hellman key exchange scheme // International Conference "Modern Stochastics: Theory and Applications III", September 10-14, 2012, Kyiv, Ukraine, Conftrence Materials. - P.34.

X. Заключні відомості

Керівник юридичної особи Ільченко Михайло Юхимович

Перелік осіб-виконавців

А.Олексійчук

А.Фесенко

Л.Завадська

Л.Ковальчук

О.Грязнухін

О.Фаль

П.Єндовицький

С.Яковлев

Відповідальний за підготовку облікових документів

Телефон

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності