

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0212U009088

Державний реєстраційний номер: 0111U000342

Особливі позначки: відкрита

Дата реєстрації: 28-12-2012

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Дослідження стійкості і ефективності криптографічних алгоритмів захисту інформації та їх реалізацій з використанням додаткових даних

Початок етапу: 01.2011

Закінчення етапу: 12.2012

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: 4068176, 2367098

IV. Відомості про співвиконавців ДіР

V. Відомості про замовника ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Інститут енергозбереження та енергоменеджменту Національного технічного університету України "Київський Політехнічний Інститут"

Код за ЄДРПОУ: 00027677

Місцезнаходження: пр. Перемоги 37, м. Київ, Київ, 03056, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 0442048428

VI. Джерела, напрями та обсяги фінансування ДіР

Підстава для проведення ДіР: 34 - договір (замовлення) з центральним органом виконавчої влади, академією наук (головними розпорядниками бюджетних коштів на проведення НДДКР)

Напрямок фінансування: 2.2 - прикладні дослідження і розробки

Джерела фінансування

7713 - кошти держбюджету

Код програмної класифікації видатків і кредитування (КПКВК): 2201040

Фактичний обсяг фінансування (тис. грн.): 180.077
--

VII. Відомості про ДіР

Назва роботи українською:

Дослідження стійкості і ефективності криптографічних алгоритмів захисту інформації та їх реалізацій з використанням додаткових даних.

Назва роботи англійською:

The research of the resistance and effectiveness of information security cryptographic algorithms and their implementations using additional data

Реферат українською:

Удосконалено, розвинуто та створено нові ефективні методи, процедур побудови та оцінювання ефективності криптографічних атак на системи захисту інформації з використанням додаткових даних, отримано оцінки стійкості систем криптографічного захисту інформації відносно таких атак, а також використано нові методи для визначення напрямків та способів удосконалення апаратних та програмних реалізацій алгоритмів криптографічного захисту, що враховують новітні атаки з використанням інформації з побічного каналу, даних про збої, час виконання окремих операцій працюючою апаратурою, енерговитрати тощо.

Реферат англійською:

The purpose of the work is to improve, develop and create new effective methods and procedures of constructing and evaluating the effectiveness of cryptographic attacks with additional data on information security systems, obtaining estimates of information security systems resistance against such attacks, as well as new methods for determining directions and ways to improve hardware and software implementations of IT-security algorithms that take into account the latest attacks that use side channel information, failures data, the performing time of some operations, energy consumption and so on.

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 стійкості і ефективності криптографічних алгоритмів захисту інформації та їх реалізацій з використанням додаткових даних"

Назва НТП англійською: Report on SCW "The research of the resistance and effectiveness of information security cryptographic algorithms and their implementations using additional data"

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати:

Галузь застосування: За бажанням Замовника

Реєстраційний номер картки технології:

Опис НТП: Мета роботи полягає в удосконаленні, розвитку та створенні нових ефективних методів, процедур побудови та оцінювання ефективності криптографічних атак на системи захисту інформації з використанням додаткових даних, отриманні оцінок стійкості систем криптографічного захисту інформації відносно таких атак, а також у використанні нових методів для визначення напрямків та способів удосконалення апаратних та програмних реалізацій алгоритмів криптографічного захисту, що враховують новітні атаки з використанням інформації з побічного каналу, даних про збої, час виконання окремих операцій працюючою апаратурою, енерговитрати тощо.

Соціально-економічна спрямованість НТП:

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: без обмежень

Закінчення етапу:

Споживачі продукції: МОНМС України, НАН України, Міністерство оборони України, комерційні структури тощо.

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:

IX. Бібліографічний опис

1.Ковальчук Л.В., Кучинська Н.В..Построение верхних оценок средних вероятностей целочисленных дифференциалов раундовых функций блочных шифров определенной структуры.// "Кибернетика и системный анализ". - №5, 2012, С. 71-81. 2.Ковальчук Л.В., Сиренко О.А. Анализ перемешивающих свойств операций модульного и побитового сложения, определенных на одном носителе // Кибернетика и системный анализ. - 2011, №5(сентябрь-октябрь). - С.83-97. 3.Кочубинский А.И., Фаль А.М. // Алгоритмы вычисления слепой цифровой подписи на основе национального стандарта Украины цифровой подписи ДСТУ 4145-2002 и российского стандарта цифровой подписи ГОСТ Р34.10-2001 // "Кибернетика и системный анализ" Інституту кібернетики ім. В.М. Глушкова НАН України. - 2012 (в печати). 4.Фаль О.М, А.И.Кочубинский ДСТУ 4145-2002 и российского стандарта цифровой підписи ГОСТ Р 34.10-2001 // Кибернетика и системный анализ - 2012, №4.- 6стр. 5.Фесенко А. В. Оценка стойкости коммутативного криптопримитива, построенного на некоммутативной группе обратимых многомерных векторов // Кибернетика и вычислительная техника. - 2012 (в редакции) 6.Яковлев С.В., "Оценки стойкости несбалансированных MISTY-подобных схем к дифференциальному и линейному криптоанализу" // Проблемы управления и информатики - К.: НАНУ ИКИ, 2012 - №5 - стр. 142-155. 7.Ендовицький П.А. "Решение обобщенной обратной задачи о днях рождения" // Доповіді Академії наук України (серія математика). -2012. 8.Кочубинский А. Молдовян Н.А., Фаль А.М. Слепые мультиподписи на основе стандартов ДСТУ 4145-2002 и ГОСТ Р 34.10-2001// Доповіді Національної академії наук України.- 2012.-№3.- С. 38-47. 9.Кочубинский А.И., Молдован Н.А., А.М. Фаль. // Слепые мультиподписи на основе стандартов ДСТУ 4145-2002 и ГОСТ Р34.10-2001 (в печати). 10.Ковальчук Л.В., Скрипник Л.В.,Сиренко О.А. Нарушение структуры факторгрупп при использовании различных групповых операций на одном носителе // Сборник материалов IX общероссийской научной конференции "Математики и безопасность информационных технологий (МаБИТ-2010).

Х. Заклучні відомості

Керівник юридичної особи

Ільченко Михайло Юхимович

Перелік осіб-виконавців

Ендовицький Павло Олександрович

Завадська Людмила Олексіївна

Ковальчук Людмила Васильівна

Фаль Олексій Михайлович

Фесенко Андрій В'ячеславович

Яковлев Сергій Володимирович

**Відповідальний за підготовку
облікових документів**

Телефон

Реєстратор

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

