

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0215U001276

Державний реєстраційний номер: 0113U000944

Особливі позначки: відкрита

Дата реєстрації: 06-02-2015

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Сучасні методи аналізу і синтезу криптографічних алгоритмів та протоколів

Початок етапу: 01.2013

Закінчення етапу: 12.2014

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

IV. Відомості про співвиконавців ДіР

V. Відомості про замовника ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського" Інститут енергозбереження та енергоменеджменту

Код за ЄДРПОУ: 247571500

Місцезнаходження: вул. Борщагівська 115, м. Київ, Київська обл., 03056, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 0442049690

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.): 117.27

VII. Відомості про ДіР

Назва роботи українською:

Сучасні методи аналізу і синтезу криптографічних алгоритмів та протоколів.

Назва роботи англійською:

Modern methods of analysis and synthesis of cryptographic algorithms and protocols

Реферат українською:

Удосконалено, розвинено та створено нові ефективні методи, процедури 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 у 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:

New methods, procedures of construction and evaluation of the effectiveness of attacks have been improved, developed and created. Cryptographic security solutions with additional data have been obtained assess the stability of cryptographic protection against such attacks, as well as new methods used to identify areas and ways of improvement and hardware software implementations of encryption algorithms that take into account the latest attacks using information from a side channel data failures, the performance of individual operations a working equipment, energy 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: Сучасні методи аналізу і синтезу криптографічних алгоритмів та протоколів.

Назва НТП англійською: Modern methods of analysis and synthesis of cryptographic algorithms and protocols

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати:

Галузь застосування: інформаційна безпека, захист безпеки інформації

Реєстраційний номер картки технології:

Опис НТП: Розроблено удосконалені, розвинені та нові ефективні методи 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: 1-2 роки

Закінчення етапу:

Споживачі продукції: МОН України, НАНУ, СБУ, СВР, Нацбанк, комерційні структури

Перспективні ринки: галузь інформаційної безпеки

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.Завадская Л.А., Семибаламут М.А. Профиль линейной сложности как средство оценки качества случайных последовательностей // Проблемы управления и информатики. - 2014 (в редакції). 2.Ковальчук Л., Беспалов

О., Огнев П. Рекурентні алгоритми обчислення кореня довільного степеню у кільці лишків // "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - 2013, №1(25). - С. 58-67.

3.Ковальчук Л.В., Бездетний В.Т. "Верхние оценки средних вероятностей разностных характеристик блочного шифра с чередованием марковских и обобщённо-марковских преобразований", "Кибернетика и системный анализ", том 50, №3, 2014, стр. 71-79.

4.Фаль А.М. Стандартизация в сфере защиты персональных данных // Кибернетика и системный анализ. - 2014. №2. - С.181-184

5.Фаль А.М., Козак В.Ф. Проблемы защиты персональных данных при использовании облачных вычислений // Кибернетика и системный анализ. - 2014. - №5. - С.132 -138.

6.Фесенко А. В. Складність задачі про приховану дію абелевої групи в квантовій моделі обчислень // Східно-Європейський журнал передових технологій. - 2013. - №5(65). - с. 45-49.

7.Фесенко А. В. Сведение атаки на основе открытого текста на локально коммутативный шифр к алгебраическим задачам в классической и квантовой моделях вычислений // Проблемы управления и информатики. - 2014. - № 3. - с. 148-156.

8.Фесенко А. В. Уязвимости криптопримитивов на основе задачи поиска сопрягающего элемента и степени в квантовой модели вычислений // Кибернетика и системный анализ. - 2014. - Т. 50. - №5. - с. 184-186.

9.Яковлев С.В. Методика обґрунтування стійкості немарковських симетричних блочних шифрів до диференціального криптоаналізу // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - 2013, ,№1(25). - С.74-80.

10.Ковальчук Л.В., Алексейчук А.М. Результати досліджень криптографічних властивостей алгоритму шифрування "Калина" // Збірник наукових праць "Спеціальні телекомунікаційні системи та захист інформації", вип. 1(25), 2014, с. 5-24.

11.Ковальчук Л.В., Лисенко Н.В., Скрипник Л.В. Порушення структури факторгрупи групи при заміні операцій модульного додавання на по компонентне додавання // Збірник наукових праць "Спеціальні телекомунікаційні системи та захист інформації", вип. 1(25), 2014, с. 24-34.

12.Savchuk M. Cryptography: Classical and Modern // INFORMATION SECURITY. International Training Workshop. - Kyiv-2014.-International Training Conference and Workshop on. Information Security and Responsible Science as Integral Components of a Safe and Secure Global Knowledge Society - p. 54-68.

13.Фесенко А. В. Зведення задачі обернення кусково-лінійного відображення до задачі про приховану дію на торсор над абелевою групою // Наукові записки НаУКМА. Серія Комп'ютерні науки. - 2014, №163.

14.Яковлев С.В. Доказова та практична стійкість R-схеми блочного шифрування до диференціального криптоаналізу // Вісник Національного університету "Львівська політехніка" (секція "Комп'ютерні науки та інформаційні технології"). - 2013 р. - с.107-113.

Х. Заключні відомості

Керівник юридичної особи

Новіков Олексій Миколайович

Перелік осіб-виконавців

Єндовицький 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**

