

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0214U007545

Державний реєстраційний номер: 0114U004643

Особливі позначки: відкрита

Дата реєстрації: 27-11-2014

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Аналіз важкозворотних перетворень у сучасних криптографічних системах, математичних моделей та методів криптоаналізу (проміжний)

Початок етапу: 08.2014

Закінчення етапу: 11.2014

Вид звітного 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, молоді та спорту 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.): 62

VII. Відомості про ДіР

Назва роботи українською:

Дослідження та застосування методів криптографічного аналізу важкозворотних перетворень у сучасних криптографічних системах захисту інформації з урахуванням додаткових даних

Назва роботи англійською:

Research and application of cryptographic analysis methods of one-sided transformations to the modern cryptographic systems of information security into account additional information

Реферат українською:

Результати аналізу важкозворотних перетворень у сучасних криптографічних системах, диференціальних методів криптоаналізу, неможливих диференціалів з урахуванням додаткової інформації. Результати дослідження рандомізованих потокових шифросистем Міхалевича-Імаї, оцінки їх обчислювальної стійкості відносно атак на основі відомих шифротекстів, відкритих текстів та підібраних відкритих текстів і векторів ініціалізації. Оцінки методу криптоаналізу на основі обертань та можливості застосування цього методу до криптоаналізу ДСТУ ГОСТ 28147:2009.

Реферат англійською:

The results of analyzing one-way transformations in current cryptographic systems, differential methods of cryptoanalysis, impossible differentials with account on additive information. The results of the research of randomizable stream Mihalievych-Imai ciphers, assessment of its computable security against attacks with known ciphertexts, known plaintexts, chosen plaintexts and initializing vectors. The assessment of cryptoanalytic method based on rotations and possibility of application of this method to DSTU GOST 28147:2009 cryptoanalysis.

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 методів криптографічного аналізу важкозворотних перетворень у сучасних криптографічних системах захисту інформації з урахуванням додаткових даних", шифр "Кета". Етап 1. Аналіз важкозворотних перетворень у сучасних криптографічних стемах, математичних моделей та методів криптоаналізу (проміжний).

Назва НТП англійською: Report about research work " Research and application of cryptographic analysis methods of one-sided transformations to the modern cryptographic systems of informaiton security into account additional information", code "KETA". stage 1. An analysis of one-way transformations is to the modern cryptosystems, mathematical models and methods of cryptoanalysis (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 результати аналізу важкозворотних перетворень у сучасних криптографічних системах, диференціальних методів криптоаналізу, неможливих диференціалів з урахуванням додаткової інформації. Результати дослідження рандомізованих потокових шифросистем Міхалевича-Імаї, оцінки їх обчислювальної стійкості відносно атак на основі відомих шифротекстів, відкритих текстів та підібраних відкритих текстів і векторів ініціалізації. Оцінки методу криптоаналізу на основі обертань та можливості застосування цього методу до криптоаналізу ДСТУ ГОСТ 28147:2009.

Соціально-економічна спрямованість НТП:

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: 2014 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. Ковальчук Л., Кучинська Н., Бездітний В. Побудова верхніх оцінок середніх імовірностей цілочисельних диференціалів композиції модульного ключового суматора, блоку підстановки та лінійного оператора, що має блокову структуру. // "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні" - 2014, здано до друку. 2. Ковальчук Л., Кучинская Н. Построение верхних оценок средних вероятностей целочисленных дифференциалов раундовых функций блочных шифров определенной структуры. // "Кибернетика и системный анализ" - 2012, - №5, С. 71 - 81. 3. Ковальчук Л. Построение верхних оценок средних вероятностей целочисленных дифференциалов композиции ключевого сумматора, блока подстановки и оператора сдвига. // "Кибернетика и системный анализ" - 2010, - №6, С. 89 - 96. 4. А. Алексейчук, Л. Ковальчук, Е. Скрынник, А. Шевцов. Оценки практической стойкости блочного шифра "Калина" относительно методов разностного, линейного криптоанализа и алгебраических атак, основанных на гомоморфизмах. // Прикладная радиоэлектроника. - №1. - 2008. - С. 203-210.

Х. Заклучні відомості

Керівник юридичної особи

Ільченко Михайло Юхимович

Перелік осіб-виконавців

А.Олексійчук

А.Фесенко

Л.Ковальчук

С. Гришаков

С.Яковлев

Відповідальний за підготовку

облікових документів

Телефон

Реєстратор

Керівник відділу УкрІНТЕІ, що є

відповідальним за реєстрацію наукової

діяльності

