

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0215U002352

Державний реєстраційний номер: 0114U004643

Особливі позначки: відкрита

Дата реєстрації: 23-06-2015

II. Етап виконання ДіР

Номер етапу: 2

Назва етапу: Розробка аналітичних та експериментальних методів криптографічного аналізу, що використовують алгебраїчні, комбінаторні, статистичні властивості та кореляційні залежності, та методів отримання оцінок стійкості криптосистем з урахуванням додаткових даних (заклучний)

Початок етапу: 12.2014

Закінчення етапу: 06.2015

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, 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.): 123
--

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:

Отримано результати застосування UID-методу аналізу ; доведено узагальнення теореми Ніберг для Skipjack ; створено метод побудови рандомізатору для шифросистем Міхалевича-Імаї ; доведено, що імовірність співпадіння результатів модульного та покомпонентного додавання (віднімання) дуже мала; показано, що задача визначення місця додавання відкритого тексту до псевдовипадкової послідовності у симетричних поточкових криптосистемах є еквівалентною до задачі пасивного стегааналізу; проведено оцінку потужності множини сильних простих чисел; побудовано метод визначення характеристик нерівномірних двійкових послідовностей.

Реферат англійською:

UID-method of impossible differential cryptoanalysis was implemented to some block cipher schemes. Generalization of Nyberg-Knudsen's theorem for Skipjack cipher was proven, Method of randomization for Mikhalevic-Imai's ciphers was proposed. It was proven that results of bitwise and modular addition coincide with negligible probability. The equivalence of search of meaningful text position in pseudorandom flow and of passive stegoanalysis problems was shown. The number of strong primes was estimated. Method of determination of stochastic properties of non-uniform binary sequences was developed.

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: Науково-технічний звіт щодо НДР "Дослідження та застосування методів криптографічного аналізу важкозворотних перетворень у сучасних криптографічних системах захисту інформації з урахуванням додаткових даних", шифр "Кета"

Назва НТП англійською: The scientific report of "Research and application of cryptographic analysis methods of one-sided transformations to the modern cryptographic systems of information security into account additional information", shifr "Keta"

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: Науково-технічний звіт про НДР містить описи сучасних математичних методів криптографічного аналізу важкозворотних перетворень у сучасних системах захисту інформації з урахуванням додаткових даних, напрямки подальших досліджень, узагальнення результатів досліджень.

Соціально-економічна спрямованість НТП:

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: 2015 рік

Закінчення етапу:

Споживачі продукції: СЗР 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 обґрунтування:

Потенціальний обсяг продажу, тис. грн.:

Очікуваний термін окупності (років):

Додаткова інформація:

IX. Бібліографічний опис

1. Яковлев С. Псевдофрейстелівські перетворення та їх диференціальні характеристики / С. Яковлев, Є. Коробов. // Збірник матеріалів Сьомої міжнародної конференції "Інтернет - Освіта - Наука - 2010", Вінниця. - Том 2. - Вінниця: ВНТУ, 2010. - С. 395-397. 2. Яковлев С.В. Методика обґрунтування стійкості немарковських

симетричних блочних шифрів до диференціального криптоаналізу / С.В.Яковлев // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - 2013. - №1(25). - С. 73-80. 3. Ковальчук Л.В., Лысенко Н.В., Скрыпник Л.В. Перемешивающие свойства операций, определенных на множестве N-мерных векторов над простым конечным полем // Кибернетика и системный анализ. - 2014. - № 4. - С.135 - 145. 4. Байденко П.В., Кудін А.М. Ефективність застосування алгоритмів факторизації до модулів криптосистеми RSA // X Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених "Теоретичні і прикладні проблеми фізики, математики та інформатики", Збірка тез доповідей учасників. - К. - 2012. - С.253-254.

Х. Заключні відомості

Керівник юридичної особи

Ільченко Михайло Юхимович

Перелік осіб-виконавців

Єндовицький П.О.

А.Олексійчук

А.Фесенко

Красніков С.В.

Л.Ковальчук

Прогонов Д.

С. Гришаков

С.Яковлев

Селюх П.В.

Фаль О.М.

**Відповідальний за підготовку
облікових документів**

Телефон

Реєстратор

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

