

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0210U005171

Державний реєстраційний номер: 0109U007755

Особливі позначки: відкрита

Дата реєстрації: 02-07-2010

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Аналіз сучасного стану проблеми. Розробка нових ефективних методів. Аналіз існуючих та створення нових математичних методів аналізу криптографічних алгоритмів, опис криптографічних атак з оцінками складності. Створення нових ефективних методів.

Початок етапу: 11.2009

Закінчення етапу: 03.2010

Вид звітного документа: Без звіту

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: 236-70-98

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.): 100
--

VII. Відомості про ДіР

Назва роботи українською:

Застосування сучасних математичних методів у криптографічному аналізі

Назва роботи англійською:

The application of modern mathematical methods in cryptografic analysis

Реферат українською:

Проаналізовани нові методики дослідження криптографічних алгоритмів, що виникають в задачах синтезу і аналізу криптосистем. Використовани алгебраїчні , ймовірнісні, комбінаторно-інформаційні і теоретико-складні методи. Створені нові ефективні методи, процедури та алгоритми статистичного аналізу псевдовипадкових послідовностей та генераторів випадкових послідовностей.

Реферат англійською:

The new metodologies of investigation of cryptoalgorithmes appearing in cryptosystems analysis problems are considered. Algebraic, probabilistic, combinatoric-information and comlexity theoretic methods are used. The new efficient techniques, procedures and algorithms of statistical analysis of pseudorandom sequences and random sequences generators are created.

Індекс УДК: 519.7, 681.3.06:519.248.681

Коди тематичних рубрик: 27.47

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: Алгебраїчні, статистичні, комбінаторно-інформаційні і теоретико-складнісні методи криптоаналізу, критерії та алгоритми статистичного аналізу псевдовипадкових послідовностей та генераторів випадкових послідовностей

Назва НТП англійською: Algebraic, statistic, combinatoric informational and complexity theoretic, methods of cryptanalysis, criteria and algorithms of statistical analysis algorithms of statistical analysis of pseudorandom

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: Розроблено нові методики дослідження криптографічних алгоритмів, що виникають в задачах синтезу і аналізу криптосистем, алгебраїчних, ймовірнісних, комбінаторно-інформаційних і теоретико-складнісних методів. Створено нові ефективні методи, процедури та алгоритми статистичного аналізу псевдовипадкових послідовностей та генераторів випадкових послідовностей.

Соціально-економічна спрямованість НТП:

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: без обмежень

Закінчення етапу:

Споживачі продукції: СЗРУ

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. Pometun S. Generalized Correlation and Higher Order Nonlinearity for Probabilistic Algebraic Attacks Description, <http://eprint.iacr.org/2007/448> 2. Алексейчук А.Н., Шевцов А.С. Показатели и оценки стойкости блочных шифров относительно статистических атак первого порядка // Реєстрація, зберігання і обробка

даних. - 2006. - Т. 8 - Вип. 4. - С. 53 - 63. 3. А. Алексейчук, Л. Ковальчук, Е. Скрыпник, 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. 4. Алексейчук А., Ковальчук Л., Шевцов А., Скрыпник Л. Оценки практической стойкости блочного шифра "Калина" относительно разностного, линейного и билинейного методов криптоанализа. // Труды Седьмой Общероссийской научной Конференции "Математика и безопасность информационных технологий" - (МаБИТ-08), 30 октября - 2 ноября 2008. - С. 331-335. 5. Олексійчук А.Н., Ковальчук Л.В., Пальченко С.В. Криптографічні параметри вузлів заміни, що характеризують стійкість ГОСТ-подібних блокових шифрів відносно методів лінійного та різницевого криптоаналізу // Захист інформації. - 2007. - № 2. - С. 12 - 23. 6.. Ковальчук Л. Обобщённые марковские шифры: оценка практической стойкости к методу дифференциального криптоанализа // Труды Пятой Общероссийской научной Конференции "Математика и безопасность информационных технологий" - (МаБИТ-06), 25-27 октября 2006. - С. 595-599. 7. Kovalchuk L., Alekseyshuk A., Upper Bounds of Maximum Value of Average Differential and Linear Characteristic Probabilities of Feistel Cipher with Adder Modulo 2п, // Theory of Stochastic Processes. - 2006. - Vol. 12(28). - № 1, 2. - P. 20 - 32. 8. Ковальчук Л. Верхние оценки средних вероятностей дифференциальных аппроксимаций булевых отображений // Труды Четвёртой Общероссийской научной Конференции "Математика и безопасность информационных технологий" (МаБИТ-05), 2-3 ноября 2005. - С.163-167. 9. Ковальчук Л.В., Шерстюк А.О., "Дослідження різницевих характеристик раундової функції блочних шифрів MISTY1 та MISTY2" // Прикладная радиоэлектроника. - №3. - 2009. - С. 15-27. 10. Ковальчук Л. В., Бездітний В. Т., Перевірка незалежності статистичних тестів, призначених для оцінки криптографічних якостей ГВП. "Захист інформації", №2(29) 2006. 11. Ковальчук Л.В. О периодах выходных последовательностей некоторых псевдослучайных генераторов, построенных на основе односторонних функций. // "Безопасность информации в информационно-телекоммуникационных системах", III Международная научно-практическая конференция, Киев, апрель, 2000 г., с. 56-59. 12. Гулак Г.Н., Ковальчук Л.В. Різні підходи до визначення випадкових послідовностей. // НТЗ Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - вип. 3, Київ, 2001, с. 127-133. 13. Ковальчук Л., Бездітний В. Перевірка незалежності статистичних тестів, призначених для оцінки криптографічних якостей ГВП // Захист інформації. - 2006. - №2. - Вип.29. - С. 18-23. 14. Дослідження методів статистичного аналізу псевдовипадкових послідовностей: перевірка якості на малих вибірках і перевірка статистичних гіпотез при близьких альтернативах // Звіт про НДР шифр "Кашалот-2", том 2. - К., 2009. 15. Ковальчук Л.В. Скрыпник Л.В., Бездетный В.Т. Методика проверки независимости статистических тестов при неизвестных статистических свойствах генератора последовательностей // XII Международная научно-практическая конференция "Безопасность информации в информационно-телекоммуникационных системах", 19-22 мая 2009г., Киев, Тезисы докладов. - К.: ЧП "ЕКМО", НИЦ "ТЕЗИС" НТУУ "КПИ", 2009. - С.27-28.

Х. Заключні відомості

Керівник юридичної особи

Новіков Олексій Миколайович

Перелік осіб-виконавців

Єндовицький П.

Завадська Л.О.

Ковальчук Л.В.

Олексійчук А.А.

Пометун С.О.

Савчук М.М.

Фаль О.М.

Фесенко А.

Шарапов В.

Шевцов А.

Яковлев С.

**Відповідальний за підготовку
облікових документів**

Телефон

Реєстратор

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

