

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0212U007282

Державний реєстраційний номер: 0111U008680

Особливі позначки: відкрита

Дата реєстрації: 01-11-2012

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Вибір напрямку дослідження, теоретичні та експериментальні дослідження. Складання звітної документації.

Початок етапу: 09.2011

Закінчення етапу: 12.2011

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: 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.): 50

VII. Відомості про ДіР

Назва роботи українською:

Застосування сучасних математичних методів у криптоаналізі.

Назва роботи англійською:

Application of modern mathematical methods is in kryptoanalizi.

Реферат українською:

Об'єктом дослідження НДР є системи та процеси криптографічного захисту інформації, випадкові послідовності та функції, важкооборотні перетворення в класичній та постквантовій моделі обчислень, криптоаналітичні атаки. В роботі розвинуто та узагальнено існуючі методи криптоаналізу та розроблено нові математичні моделі стійкості криптографічних систем захисту інформації і методи аналізу криптографічних алгоритмів, зокрема, симетричних блочних та поточних шифрів; оцінені їх можливості, визначено стійкі та нестійкі класи шифрів відносно криптоаналітичних атак, що розглядаються; зроблено прогнозування тенденцій розвитку сучасних методів криптоаналізу та їх впливу на методологічну базу криптології

Реферат англійською:

The object of research of work are the systems and processes of cryptographic protection of information, random sequences and functions, trapdoor functions that are considered in the classic and post-quantum model of calculations, cryptanalytic attacks. The current methods of cryptanalysis are developed and generalized, the new mathematical models of security of the cryptosystems of protection of information and methods of analysis of cryptographic algorithms are worked out, in particular, of symmetric block and stream ciphers; their possibilities are evaluated, the secure and unsecure classes of ciphers are defound in relation to considered cryptanalitic attacks; prognostication of progress of modern methods of cryptanalysis and their influence trends on the methodological base of cryptology is done.

Індекс УДК: 681.3.06:004.92, 681.3.06:519.248.681

Коди тематичних рубрик: 81.14.11.05

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: Спеціальні технології за результатами НДР "Застосування сучасних математичних методів у криптоаналізі"

Назва НТП англійською: Scientific and technical report on the results of scientific research work "Application of modern mathematical methods in kryptoanalizi"

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: Одержано аналітичні оцінки стійкості немарковських SP-мереж загального вигляду та AES-подібних шифрів у випадку використання операцій із блоковою структурою. Зокрема, встановлені верхні межі імовірності існування нетривіальних диференціалів для двораундової SP-мережі загального вигляду та для чотирираундової AES-подібної SP-мережі. Розглянуто перемішуючі властивості різних алгебраїчних операцій, визначених на одному носії. Встановлено, що операції множення та додавання у скінченному полі мають гарні перемішуючі властивості, в той час як перемішуючі властивості побітового та модульного додавання, додавання та множення у деяких кільцях, додавання та обернення у деяких кільцях є доволі поганими. Проведено аналіз алгоритмів розв'язання систем лінійних булевих рівнянь із спотвореними правими частинами. Запропоновано загальну схему будови субекспоненційних алгоритмів розв'язання на основі різних зведень. Розглянуті модифікації тестів статистичного Мебіус-аналізу та нові статистичні критерії, які застосовуються

Соціально-економічна спрямованість НТП:

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: без обмежень

Закінчення етапу:

Споживачі продукції: Служба зовнішньої розвідки 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:

ІХ. Бібліографічний опис

Х. Заключні відомості

Керівник юридичної особи

Новіков Олексій Миколайович

Перелік осіб-виконавців

Єндовицький П.

Завадська Л.О.

Ковальчук Л.В.

Олексійчук А.

Фаль О.М.

Фесенко А.

Шевцов А.

Яковлев С.

**Відповідальний за підготовку
облікових документів**

Телефон

Реєстратор

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

