

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0217U006657

Державний реєстраційний номер: 0117U001817

Особливі позначки: відкрита

Дата реєстрації: 08-12-2017

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Вибір та аналіз напрямків дослідження. Теоретичні та експериментальні дослідження. Узагальнення і оцінювання результатів досліджень.

Початок етапу: 08.2017

Закінчення етапу: 12.2017

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 України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 236-70-98, 204-81-76

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.): 776
--

VII. Відомості про ДіР

Назва роботи українською:

Дослідження, розроблення і застосування методів криптоаналізу симетричних та асиметричних криптографічних систем

Назва роботи англійською:

Research, Development and Implementation of Cryptanalytic Techniques for Symmetric and Asymmetric Cryptosystems

Реферат українською:

отримано нові ефективні методи, процедури та алгоритми криптографічного аналізу сучасних симетричних та асиметричних криптосистем, визначено стійкі та нестійкі класи шифрів відносно деяких криптоаналітичних атак в класичній та квантовій моделях обчислень, одержано аналітичні оцінки для верхніх меж імовірностей диференціалів слово-орієнтованих SP-мереж, де диференціали обчислюються за певною алгебраїчною операцією над множиною слів; проаналізовано поведінку певних підпросторів вхідних текстів під час шифрування у AES-подібних блокових шифрах; узагальнено раніше відомі оцінки кількості рівнянь, необхідних та достатніх для розв'язання спеціальних систем рівнянь із заданою ймовірністю помилки, які можуть бути використані для оцінювання стійкості сучасних словоорієнтованих потокових шифрів до кореляційних атак; побудована нова загальна алгебраїчна модель симетричного шифру та доведено, що масові задачі, які описують атаку з відомим відкритим текстом, для класів симетричних та ендоморфних шифрів є поліноміально еквівалентними; досліджено клептографічні методи вбудовування у криптоалгоритми певних "лазівок" та доведення відсутності таких лазівок; запропонована концепція криптосистем на базі довіреного зовнішнього генератора випадкових послідовностей; запропонована схема узгодження ключа за протоколом Діффі-Хеллмана з доведеною відсутністю клептографічної лазівки SETUP.

Реферат англійською:

New efficient methods, techniques, and algorithms were provided for cryptographic analysis of contemporary symmetric and asymmetric cryptosystems; classes of secure and insecure ciphers were described in classical and quantum computational models with respect to dedicated cryptanalytical attacks; analytic upper bounds estimations were founded for differential probabilities of word-oriented SP-networks with respect to some algebraic operation over words; message subspaces propagation in AES-like block ciphers was researched; estimations for size of linear system in special form were generalized from point of view of solving algorithms with fixed error probability; such estimations can be used for proving security of word-oriented stream ciphers against correlation attacks; new generalized algebraic model of symmetric cipher was developed; it was proven, that known plaintext security problem for symmetric and endomorph ciphers are polynomial equivalent; so-called "kleptographic" techniques for trapdoor embedding into cryptoalgorithms were researched, as well as methods for provable security providing; new concept was proposed for cryptosystem based on trusted outer pseudo-random generator; new Diffie-Hellmann-based protocol with guaranteed kleptographic SETUP trapdoor absence was proposed⁵⁴⁸¹

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, розроблення і застосування методів криптоаналізу симетричних та асиметричних криптографічних систем

Назва НТП англійською: Report about research work "Research, Development and Implementation of Cryptanalytic Techniques for Symmetric and Asymmetric Cryptosystems"

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати: криптографія

Галузь застосування: 73.10.1- Дослідження і розробки в галузі природничих та технічних наук

Реєстраційний номер картки технології:

Опис НТП: В науково-технічному звіті описано нові ефективні методи, процедури та алгоритми криптографічного аналізу сучасних симетричних та асиметричних криптосистем, визначено стійкі та нестійкі класи шифрів відносно деяких криптоаналітичних атак в класичній та квантовій моделях обчислень, одержано аналітичні оцінки для верхніх меж імовірностей диференціалів слово-орієнтованих SP-мереж, де диференціали обчислюються за певною алгебраїчною операцією над множиною слів; проаналізовано поведінку певних підпросторів вхідних текстів під час шифрування у AES-подібних блокових шифрах; узагальнено раніше відомі оцінки кількості рівнянь, необхідних та достатніх для розв'язання спеціальних систем рівнянь із заданою ймовірністю помилки, які можуть бути використані для оцінювання стійкості сучасних словоорієнтованих потокових шифрів до кореляційних атак; побудована нова загальна алгебраїчна модель симетричного шифру та доведено, що масові задачі, які описують атаку з відомим відкритим текстом, для класів симетричних та ендомо

Соціально-економічна спрямованість НТП:

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: 2017

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

Х. Заключні відомості

Керівник юридичної особи

Ільченко Михайло Юхимович

Перелік осіб-виконавців

Беспалов А.Ю.

Деркач О.Г.

Коваленко Б.

Ковальчук Л.В.

Кудін А.М.

Олексійчук А.

Поремський М.

Фаль О.М.

Фесенко А.В.

Циганкова О.В.

Яковлев С.В.

**Відповідальний за підготовку
облікових документів**

Телефон

Реєстратор

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

