

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0217U003488

Державний реєстраційний номер: 0112U008074

Особливі позначки: відкрита

Дата реєстрації: 25-04-2017

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Розробка методів, алгоритмів і програмного забезпечення стеганографічного аналізу та ефективних за швидкодією базових асиметричних криптографічних перетворень

Початок етапу: 07.2012

Закінчення етапу: 06.2016

Вид звітнього документа: Остаточний звіт

III. Відомості про виконавця ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Інститут кібернетики ім. В.М.Глушкова НАН України

Код за ЄДРПОУ: 05417176

Місцезнаходження:

Форма власності:

Сфера управління: Національна академія наук України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 526-02-88

IV. Відомості про співвиконавців ДіР

V. Відомості про замовника ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Український науково-дослідний інститут спеціальної техніки та судових експертиз СБ України

Код за ЄДРПОУ: 20001993

Місцезнаходження:

Форма власності:

Сфера управління: Служба безпеки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 422-75-58

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): 6521010

Фактичний обсяг фінансування (тис. грн.): 666
--

VII. Відомості про ДіР

Назва роботи українською:

Розробка методів, алгоритмів та програмного забезпечення стеганографічного аналізу та ефективних за швидкодією базових асиметричних криптографічних перетворень

Назва роботи англійською:

Development of methods, algorithms and software of stegananalysis and basic asymmetric cryptographic transformations which are effective on operation speed

Реферат українською:

Виконано аналіз існуючих стеганоаналітичних методів для аудіоконтейнерів та графічних контейнерів для поширених стеганографічних систем. Деякі методи стеганоаналізу удосконалено. Проаналізовано стеганографічні перетворення, що реалізовані в програмах Hide4PGP, S-Tools 4.0, Steghide 0.5.1, Steganos Privacy Suite 2012, SilentEye, MP3Stego, JSteg, JPHide 0.5, Steganos for Windows 95/98/NT, F5, Outguess 0.2. Проаналізована складність алгоритму додавання з передбаченням знаку переносу. Запропоновано алгоритм додавання чисел в паралельній моделі та проаналізована його складність. Розглянуто нові алгоритми багаторозрядного множення. Проаналізована складність алгоритмів багаторозрядного множення для паралельної моделі обчислень. Запропоновано алгоритми ділення для послідовної моделі обчислень та наведена порівняльна таблиця їх складності. Розглянуто новий алгоритм модулярного множення для паралельного обчислення. Для паралельної та послідовної моделей обчислення введені покрокові алгоритми та проаналізована складність елементарних багаторозрядних операцій та методів, на яких ці операції ґрунтуються.

Реферат англійською:

The analysis of existing methods for steganoanalychny audiodkonteyneriv and image containers for common steganographic systems. Some methods steganoanalizu improved. Steganographic analysis of transformation programs implemented Hide4PGP, S-Tools 4.0, Steghide 0.5.1, Steganos Privacy Suite 2012, SilentEye, MP3Stego, JSteg, JPHide 0.5, Steganos for Windows 95/98 / NT, F5, Outguess 0.2. Analyzed the complexity of adding predictive algorithm hyphen. The algorithm for adding numbers in a parallel model and analyzed its complexity. Considered New Algorithms multibit multiplication. Analyzed multibit multiplication complexity algorithms for parallel computing model. Algorithms for dividing the sequential model calculations and comparative table shows the complexity. Considered modular multiplication new algorithm for parallel computing. For parallel and serial models of computation algorithms introduced step by step and analyzed the complexity of multi-elementary operations and methods on which these operations are based.

Індекс УДК: 654.1; 654.14; 654.15; 654.16; 654.17; 654.19; 656.8, 621.394/.396.019.3

Коди тематичних рубрик: 49.33.35

Керівники роботи

Власне Прізвище Ім'я По-батькові: Задірака Валерій Костянтинович

Науковий ступінь:

Вчене звання:

Ідентифікатор ORCID ID:

Додаткова інформація:

VIII. Наукова (науково-технічна) продукція (НТП)

Назва НТП українською: Методи стеганографічного аналізу та ефективних за швидкістю базових асиметричних криптографічних перетворень

Назва НТП англійською: Methods of steganalysis and basic asymmetric cryptographic transformations which are effective on operation speed

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати:

Галузь застосування: Захист інформації

Реєстраційний номер картки технології:

Опис НТП: Математичні методи стеганографічного аналізу, ефективні за швидкістю та пам'яттю алгоритми реалізації базових асиметричних криптографічних перетворень для різних моделей обчислень

Соціально-економічна спрямованість НТП:

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: 2017

Закінчення етапу:

Споживачі продукції: Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки 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. Кошкіна Н.В. Стеганоаналіз МІК-стеганографії на базі матриці суміжності та методу опорних векторів / Н.В. Кошкіна // Искусственный интеллект. – 2012. – № 4. – С. 567-577. 2. Кошкина Н.В. Выявление Hide4PGP вложений в аудиосигналах / Н.В. Кошкина // Проблемы управления и информатики. – 2013. – №3. – С. 151-156. (включено до SCOPUS) 3. Кошкина Н.В. Выявление в аудиосигналах скрытых сообщений, внедренных с помощью программы S-Tools / Н.В. Кошкина // Захист інформації. – 2013. – №4. – С. 316-326. (індексується

Google Scholar та ін.) 4. Кошкина Н.В. Исследование применимости матрицы смежности для выявления стеганоаудиоконтейнеров / Н.В. Кошкина // Проблемы управления и информатики. – 2014. – №1 – С. 148-156. (включено до SCOPUS) 5. Кошкина Н.В. Стеганоанализ изображений в формате jpeg на базе атаки контрольным внедрением / Н.В. Кошкина // Управляющие системы и машины. – 2014. – № 4. – С. 3-17. (индексується Google Scholar) 6. Кошкина Н.В. Стеганоанализ бесключевых стеганосистем на основе атаки контрольным внедрением / Н.В. Кошкина // Проблемы управления и информатики. – 2014. – № 6. – С. 137-144. (включено до SCOPUS) 7. Кошкина Н.В. Обзор и классификация методов стеганоанализа / Н.В. Кошкина // Управляющие системы и машины. – 2015. – № 3. – С. 3-12. (индексується Google Scholar) 8. Кошкина Н.В. Виявлення НЗБ-стеганографії на базі рядків матриці суміжності аудіосигналів / Н.В. Кошкина // Праці міжнар. конф. "Питання оптимізації обчислень-XL". – Київ: Інститут кібернетики ім. В.М. Глушкова НАН України. – 2013. – С. 134-135. 9. Кошкина Н.В. Стеганоаналіз цифрових зображень із застосуванням контрольного вкраплення / Н.В. Кошкина // Матеріали 3 Міжнар. наук.-техн. конф. «Захист інформації і безпека інформаційних систем». – 2014. – С.98-100. 10. Кошкина Н.В. Методи стеганоаналізу з навчанням та класифікацією за характеристичними векторами / Н.В. Кошкина // Праці міжнар. конф. "Питання оптимізації обчислень-XL". – Київ: Інститут кібернетики ім. В.М. Глушкова НАН України. – 2015 – С. 153-154. 11. Терещенко А.Н., Задирака В.К. Оптимизация умножения больших N-разрядных чисел на основе N-разрядных ДПФ // Проблемы програмування. – 2012. – № 4. – С. 116-130. 12. Терещенко А.М. Оптимізація багаторозрядного множення на основі ШПФ у паралельній моделі обчислень // Захист інформації. – 2014. – № 3. – С.178-184. 13. Терещенко А.Н., Задирака В.К. Оценка сложности операции умножения многоразрядных чисел в параллельной модели вычислений // Компьютерная математика. – 2016. – № 1.

Х. Заключні відомості

Керівник юридичної особи

Сергієнко Іван Васильович
д. ф.-м. н., 01.05.03

Перелік осіб-виконавців

Задірака В.К.

Кошкина Н.В.

Нікітіна О.Ю.

Швідченко І.В.

Відповідальний за підготовку облікових документів

Телефон

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

