Облікова картка ДіР

I. Загальні відомості

Державний обліковий номер: 0218U005174

Державний реєстраційний номер: 0116U008714

Особливі позначки: відкрита

Дата реєстрації: 07-06-2018

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Синтез операцій криптографічного перетворення з заданими характеристиками

Початок етапу: 11.2016

Закінчення етапу: 11.2017

Вид звітного документа: Остаточний звіт

III. Відомості про виконавця ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження:

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: +38(0472)710092 , 710094

IV. Відомості про співвиконавців ДіР

V. Відомості про замовника ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Черкаський державний технологічний університет

Код за ЄДРПОУ: 05390336

Місцезнаходження: бульвар Шевченка, 460, м. Черкаси, Черкаський р-н., Черкаська обл., 18006, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 0472710092

VI. Джерела, напрями та обсяги фінансування ДіР

Підстава для проведення ДіР: 43 - власна ініціатива (якщо робота виконується з власної ініціативи за кошти виконавця НДР або безкоштовно)

Напрям фінансування: 2.7 - інше

Джерела фінансування

7706 - безплатно (договір про науково-технічне співробітництво, тощо)

VII. Відомості про ДіР

Назва роботи українською:

Синтез операцій криптографічного перетворення з заданими характеристиками

Назва роботи англійською:

Synthesis of cryptographic transformation operations with specified characteristics

Реферат українською:

В процесі виконання проекту розроблено новий метод синтезу операцій криптографічного перетворення з заданими характеристиками, який дозволяє забезпечити підвищення якості систем захисту інформації та оперативності обробки інформації і, перш за все, криптостійкості та оперативності функціонування систем криптографічного захисту інформації. Запропоновано: метод побудови операцій розширеного матричного перетворення з довільною кількістю змінних на основі встановлення нових взаємних зв'язків між елементарними функціями в операціях, а також між операціями прямого та оберненого перетворення, що забезпечило розширення групи операцій криптоперетворення та побудову алгоритму для практичної реалізації нових і вдосконалення існуючих криптопримітивів; удосконалено метод підвищення якості псевдовипадкової послідовності на основі використання операцій криптографічного перетворення, що забезпечило підвищення швидкості систем потокового шифрування за рахунок паралельної обробки заданої кількості бітів послідовності; синтезовано та досліджено групу операцій криптографічного додавання за модулем два з точністю до перестановки результатів виконання операцій, що забезпечило теоретичне обґрунтування підходу до підвищення стійкості та надійності систем потокового шифрування.

Реферат англійською:

In the process of project implementation a new method for synthesizing cryptographic transformation with specified characteristics has been developed. This method allows to improve the quality of information security systems and speed of information processing and, first of all, cryptographic stability and operational efficiency of cryptographic information security systems. It is suggested: method for constructing operations of an extended matrix transformation with an arbitrary number of variables based on the establishment of new interconnections between elementary functions in operations, as well as between direct and inverse transformation, it provided expansion of operations' group of cryptographic transformation and constructing algorithm for practical implementation of new cryptographic primitives and improving existing cryptographic primitives; method for improving quality of pseudo-random sequence based on the use of cryptographic transformation operations was improved, which provided speed increase of streaming encryption systems due to parallel processing of a given number of sequence bits; a group of cryptographic addition operations by the module two within the accuracy of operations' results permutation was synthesized and explored, which provided theoretical justification of approach to improving the stability and reliability of streaming encryption systems.

Індекс УДК: 004.7, 004.056.55

Коди тематичних рубрик: 50.37.23

Керівники роботи

Власне Прізвище Ім'я По-батькові: Рудницький Володимир Миколайович

Науковий ступінь:

Вчене звання:

Ідентифікатор ORCID ID:

Додаткова інформація:

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

Назва НТП українською: Синтез операцій криптографічного перетворення з заданими характеристиками

Назва НТП англійською: Synthesis of cryptographic transformation operations with specified characteristics

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати:

Галузь застосування: D DL 30.02.1 - виробництво електронно-обчислювальних машин та іншого устаткування для оброблення інформації

Реєстраційний номер картки технології:

Опис НТП: В процесі виконання проекту розроблено новий метод синтезу операцій криптографічного перетворення з заданими характеристиками, який дозволяє забезпечити підвищення якості систем захисту інформації та оперативності обробки інформації і, перш за все, криптостійкості та оперативності функціонування систем криптографічного захисту інформації. Запропоновано: метод побудови операцій розширеного матричного перетворення з довільною кількістю змінних на основі встановлення нових взаємних зв'язків між елементарними функціями в операціях, а також між операціями прямого та оберненого перетворення, що забезпечило розширення групи операцій криптоперетворення та побудову алгоритму для практичної реалізації нових і вдосконалення існуючих криптопримітивів; удосконалено метод підвищення якості псевдовипадкової послідовності на основі використання операцій криптографічного перетворення, що забезпечило підвищення швидкості систем потокового шифрування за рахунок паралельної обробки заданої кількості бітів послідовності; син

Соціально-економічна спрямованість НТП:

Вплив НТП на довкілля:

Впровадження НТП: Не впроваджено

Практична реалізація НТП

Початок етапу: 2017

Закінчення етапу:

Споживачі продукції: Державні та комерційні структури

Перспективні ринки: Україна

Характер співробітництва з інвестором

Потрібний обсяг інвестицій, тис. грн.:

Права, що надаються інвестору після завершення роботи:

Наявність бізнес-плану:

Техніко-економічне обгрунтування:

Потенціальний обсяг продажу, тис. грн.:

Очікуваний термін окупності (років):

Додаткова інформація:

IX. Бібліографічний опис

X. Заключні відомості

Керівник юридичної особи Григор Олег Олександрович

Перелік осіб-виконавців

Бабенко Віра Григорівна

Козловська Світлана Григорівна

Лада Наталія Володимирівна

Мельник Ольга Григорівна

Миронець Ірина Валеріївна

Пустовіт Михайло Олександрович

Рудницький Володимир Миколайович

Сисоєнко Світлана Володимирівна

Стабецька Тетяна Анатоліївна

Фауре Еміль Віталійович

Федотова-Півень Ірина Миколаївна

Відповідальний за підготовку облікових документів

Телефон

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

