

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0220U104088

Державний реєстраційний номер: 0120U101801

Особливі позначки: відкрита

Дата реєстрації: 07-12-2020

II. Етап виконання ДіР

Номер етапу: 1

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

Початок етапу: 03.2020

Закінчення етапу: 11.2020

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 імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: проспект Перемоги, буд. 37, м. Київ, Київська обл., 03056, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 380442367989, 380442044862

IV. Відомості про співвиконавців ДіР

V. Відомості про замовника ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Служба зовнішньої розвідки України

Код за ЄДРПОУ: 332408451

Місцезнаходження: вулиця Нагірна, будинок 24/1, м. Київ, Київська обл., 04107, Україна

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 380444816995

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: 2.3 - виконання робіт за державними цільовими програмами

Джерела фінансування

7722 - кошти підприємств, установ, організацій України

Фактичний обсяг фінансування (тис. грн.): 795

VII. Відомості про ДіР

Назва роботи українською:

"ДОСЛІДЖЕННЯ МЕТОДІВ АНАЛІЗУ КРИПТОГРАФІЧНОГО ЗАХИСТУ СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМ", ШИФР "САРГАН"

Назва роботи англійською:

"RESEARCH OF ANALYSIS METHODS FOR CRYPTOGRAPHIC SECURITY OF MODERN INFORMATION SYSTEMS" CODE "SARGAN"

Реферат українською:

У НДР увійшли результати: розробка і застосування сучасних методів крипто аналізу; дослідження криптографічних властивостей S-блоків та шифруючих перетворень з фіксованими ключами; аналіз стійкості ітеративних шифрів; аналіз стійкості блокових шифрів; дослідження диференціально-лінійних властивостей булевих відображень; дослідження властивостей NTRU-подібних криптосистем; розглянуто особливості побудови SNOW-подібних потокових шифрів та проведено криптоаналіз потокового шифру СТРУМОК; удосконалено протокол SPECTRE; дослідження стійкості криптографічних протоколів; дослідження стійкості, ефективності та масштабованості блокчейн-систем; досліджено властивості та характеристики ізогеній еліптичних кривих; оцінювано теоретичні та експериментальні результати досліджень.

Реферат англійською:

In scientific work performed: development and application of modern methods of crypto analysis; study of cryptographic properties of S-blocks and encryption transformations with fixed keys; analysis of the stability of iterative ciphers; analysis of the stability of block ciphers; study of differential-linear properties of Boolean mappings; study of the properties of NTRU-like cryptosystems; features of construction of SNOW-like stream ciphers are considered and cryptanalysis of stream stream CURRENCIES is carried out; SPECTER protocol improved; study of the stability of cryptographic protocols; study of the stability, efficiency and scalability of blockchain systems; properties and characteristics of isogenies of elliptic curves are investigated.

Індекс УДК: 002

Коди тематичних рубрик: 20

Керівники роботи

Власне Прізвище Ім'я По-батькові: Савчук Михайло Миколайович

Науковий ступінь: д. ф.-м. н.

Вчене звання: доц., член-кор.

Ідентифікатор ORCID ID:

Додаткова інформація:

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

Назва НТП українською: Звіт про НДР «ДОСЛІДЖЕННЯ МЕТОДІВ АНАЛІЗУ КРИПТОГРАФІЧНОГО ЗАХИСТУ СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМ» шифр «САРГАН» (остаточний)

Назва НТП англійською: Report of "RESEARCH OF ANALYSIS METHODS FOR CRYPTOGRAPHIC SECURITY OF MODERN INFORMATION SYSTEMS" CODE "SARGAN" (finished)

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати: Методи, теорії

Галузь застосування: Державні та комерційні структури, які використовують в своїй діяльності криптографічний захист інформаційних систем

Реєстраційний номер картки технології:

Опис НТП: Звіт про НДР остаточний складається із двох частин, які роздруковані в двох книгах . Звіт містить описи результатів наукових досліджень, описи алгоритмів досліджень, пропозиції щодо застосування результатів досліджень, пропозиції щодо напрямів подальших досліджень.

Соціально-економічна спрямованість НТП: використання методів криптографічного захисту інформаційних систем

Вплив НТП на довкілля:

Впровадження НТП: впровадження у замовника

Практична реалізація НТП

Початок етапу: 03.2020

Закінчення етапу: 11.2020

Споживачі продукції: державні та комерційні структури, що використовують криптографічний захист інформаційних систем

Перспективні ринки:

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

Х. Заключні відомості

Керівник юридичної особи

Пасічник Віталій Анатолійович

д. т. н., 05.12.13

Перелік осіб-виконавців

Грубіян Євген Олександрович

Ковальчук Людмила Василівна

(д. т. н.)

Кудін Антон Михайлович

(к.т.н., 20.02.12, 20.02.14)

Курінний Олег Вікторович

Матійко Александра Андріївна

Олексійчук Антон Михайлович

Пясецький Богдан Юрійович

Фесенко Андрій В'ячеславович

Ядуха Дарія Вікторівна

Яковлев Сергій Володимирович

(к. т. н.)

Відповідальний за підготовку облікових документів

Розумей Ольга Іллівна

Телефон

+38 (096) 678-90-91

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

