

Облікова картка НДДКР

Державний обліковий номер: 0220U104088

Державний реєстраційний номер: 0120U101801

Відкрита

Дата реєстрації: 07-12-2020



1. Етапи виконання

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

2. Виконавець

Назва організації: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код ЄДРПОУ/ІПН: 02070921

Підпорядкованість: Міністерство освіти і науки України

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

Телефон: 380442367989

Телефон: 380442044862

E-mail: mail@kpi.ua

WWW: <https://kpi.ua/>

3. Власник результатів НДДКР (продукції)

Назва організації: Служба зовнішньої розвідки України

Код ЄДРПОУ/ІПН: 332408451

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

Підпорядкованість:

Телефон: 380444816995

Телефон: 380444519708

E-mail: inform@szru.gov.ua

WWW: <http://szru.gov.ua/>

4. Джерела та напрями фінансування

Підстава для проведення робіт: 52 - договір з вітчизняною організацією (органами місцевої ради, фондом, асоціацією, концерном тощо)

КПКВК:

Напрямок фінансування: 2.3 - виконання робіт за державними цільовими програмами

Джерела фінансування

Джерело фінансування: 7722 - кошти підприємств, установ, організацій України

Фактичний обсяг фінансування за звітний етап: 795 тис. грн.

5. Науково-технічна робота

Назва роботи (укр)

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

Назва роботи (англ)

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

Реферат (укр)

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 (англ)

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 НТІ: 20

6. Науково-технічна продукція (НТП)

НТП 1

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

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

Очікувані результати: Методи, теорії

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

Опис продукції (укр): 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

Стадія завершеності НТП: Звіт по НДДКР

Впровадження НТП: впровадження у замовника

Строки впровадження: 03.2020-11.2020

Виробник продукції: Виробником продукції є співробітники Фізико-технічного інституту КПІ ім. Ігоря СІКОРСЬКОГО,

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

Перспективні ринки:

Права інтелектуальної власності: За договорами

Форми та умови передачі продукції: Спільні НДДКР

7. Бібліографічний опис

8. Звітна документація

Кількість сторінок в звіті: 412

Мова звіту: Українська

Кількість файлів у звіті: 18

9. Заключні відомості

Перелік осіб-виконавців

Грубіян Євген Олександрович

Ковальчук Людмила Василівна (д. т. н., професор)

Кудін Антон Михайлович (к.т.н., с.н.с.)

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.)

Керівник організації:

Пасічник Віталій Анатолійович (д. т. н., професор)

Керівники роботи:

Савчук Михайло Миколайович (д. ф.-м. н., доц., член-кор.)

**Керівник відділу реєстрації наукової діяльності
УкрІНТЕІ**



Юрченко Т.А.