

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0221U106668

Державний реєстраційний номер: 0121U111192

Особливі позначки: відкрита

Дата реєстрації: 17-12-2021

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Розробка, застосування та адаптація математичних моделей і методів криптоаналізу для систем криптографічного захисту інформаційних технологій у сучасному кіберпросторі

Початок етапу: 05.2021

Закінчення етапу: 12.2021

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, 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: 33240845

Місцезнаходження: вул. Нагірна, 24/1, м. Київ, 01034, Україна

Форма власності:

Сфера управління:

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: 2.3 - виконання робіт за державними цільовими програмами

Джерела фінансування

7722 - кошти підприємств, установ, організацій України

Фактичний обсяг фінансування (тис. грн.): 985.000
--

VII. Відомості про ДіР

Назва роботи українською:

Розробка, застосування та адаптація математичних моделей і методів криптоаналізу для систем криптографічного захисту інформаційних технологій у сучасному кіберпросторі, шифр "Паргус"

Назва роботи англійською:

Development, implementation and adaptation of mathematical models and methods of cryptanalysis for cryptographic security systems and technologies in modern cyberspace (code "Pargus")

Реферат українською:

Результат НДР – науково-технічний звіт про НДР "Розробка, застосування та адаптація математичних моделей і методів криптоаналізу для систем криптографічного захисту інформаційних технологій у сучасному кіберпросторі", який містить наступне: – розробку і застосування сучасних методів криптоаналізу, що використовують алгебраїчні, комбінаторні, статистичні властивості криптографічних перетворень та кореляційні залежності в інформаційних процесах систем криптографічного захисту; – уточнення розрахункових методів оцінки стійкості SP-мереж спеціального виду до диференціального та лінійного криптоаналізу; – дослідження властивостей криптографічних параметрів, які характеризують стійкість Фейстель-подібних схем до атак бумерангів; – дослідження стійкості симетричних рандомізованих кодових шифросистем (типу Мак-Еліса, Рао-Нама тощо); – дослідження алгебраїчних та комбінаторних властивостей систем лінійних заборон над скінченним полем; – застосування квантового диференціального та лінійного аналізу до сучасних симетричних криптопримітивів; – дослідження модифікацій криптографічних примітивів сімейства AJPB; – дослідження асимптотичних властивостей графу ізогеній суперсингулярних еліптичних кривих; – аналіз алгоритмів сучасних кільцевих підписів та їх застосування для анонімного зв'язку з постачальниками інформації; – використання особливостей протоколів консенсусу PoS у блокчейні, які дають можливість виконати "атаку 50%" з суттєво меншою долею стейку; – дослідження демотиваційних атак на поширені блокчейн-систем; – дослідження стійкості та ефективності асиметричних протоколів з блокчейн-ядром із узгодженням різного типу; – дослідження методів криптоаналізу безпечної реалізації децентралізованих криптографічних модулів, побудованих за блокчейн-технологіями.

Реферат англійською:

The result of the research is a scientific and technical report on research "Development, application and adaptation of mathematical models and methods of cryptanalysis for information security systems in modern cyberspace", which contains the following: – development and application of modern cryptanalysis methods, using algebraic, combinatorial, statistical properties of cryptographic transformations and correlations in the information processes of information security systems; – rectification of calculation methods for assessing the security of a special kind SP-networks to differential and linear cryptanalysis; – research on the properties of cryptographic parameters that characterize the resistance of Feistel-like schemes to boomerang attacks; – research on the security of symmetric randomized code-based cryptosystems (such as McEliece, Rao-Nama scheme, etc.); – research on algebraic and combinatorial properties of linear prohibitions systems over a finite field; – application of quantum differential and linear analysis to modern symmetric cryptoprimitives; – research on modifications of the AJPB family cryptographic primitives; – research of the asymptotic properties for the isogeny graph of supersingular elliptic curves; – algorithms analysis of modern ring signatures and their application for anonymous communication with information providers; – use of PoS consensus protocols features in the blockchain, which allow to perform a "50% attack" with a significantly lower stake share; – research on demotivation attacks on common blockchain systems; – research on the security and efficiency of asymmetric protocols with a blockchain core and different types of consensus; – research on cryptanalysis methods through secure implementation of decentralized cryptographic modules built on blockchain technologies.

Індекс УДК:

Коди тематичних рубрик: 28.31, 28.31.01

Керівники роботи

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

Науковий ступінь: д. ф.-м. н.

Вчене звання: доц.

Ідентифікатор ORCID ID:

Додаткова інформація:

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

Назва НТП українською: Звіт про НДР «Розробка, застосування та адаптація математичних моделей і методів криптоаналізу для систем криптографічного захисту інформаційних технологій у сучасному кіберпросторі» шифр «Паргус»

Назва НТП англійською: Report of Development, implementation and adaptation of mathematical models and methods of cryptanalysis for cryptographic security systems and technologies in modern cyberspace (code "Pargus")

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати: Методи, теорії, Аналітичні матеріали

Галузь застосування: використання в системах КЗІ та підготовки спеціалісті КЗІ

Реєстраційний номер картки технології:

Опис НТП: Науково-дослідна робота «Розробка, застосування та адаптація математичних моделей і методів криптоаналізу для систем криптографічного захисту інформаційних технологій у сучасному кіберпросторі» (шифр «Паргус») виконувалась з травня по грудень 2021 р. У звіт увійшли результати за такими пунктами: розробка і застосування сучасних методів криптоаналізу, що використовують алгебраїчні, комбінаторні, статистичні властивості криптографічних перетворень та кореляційні залежності в інформаційних процесах систем криптографічного захисту; вдосконалення розрахункових методів оцінки стійкості SP-мереж спеціального виду до диференціального та лінійного криптоаналізу; дослідження властивостей криптографічних параметрів, які характеризують стійкість фейстель-подібних схем до атак бумерангів; аналіз стійкості симетричних кодових шифросистем (рандомізованих типу Мак-Еліса та Рао-Нама); аналіз алгебраїчних та комбінаторних властивостей систем лінійних заборон над скінченним полем; застосування квантового диференціального та лінійного аналізу до сучасних симетричних криптопримітивів; аналіз модифікацій криптографічних примітивів сімейства AJPB; дослідження асимптотичних властивостей графу ізогеній суперсингулярних еліптичних кривих; аналіз алгоритмів сучасних кільцевих підписів та їх застосування для анонімного зв'язку з постачальниками інформації; дослідження особливостей протоколів консенсусу PoS у блокчейні; аналіз демотиваційних атак на поширені блокчейн-систем; дослідження методів криптоаналізу безпечної реалізації децентралізованих криптографічних модулів побудованих за блокчейн-технологіями; аналіз стійкості та ефективності асиметричних протоколів з блокчейн-ядром і з узгодженням різного типу; оцінювання теоретичних та експериментальних результатів досліджень; пропозиції щодо застосувань результатів досліджень; визначення можливих напрямків подальших досліджень.

Соціально-економічна спрямованість НТП: соціально-економічна спрямованість не досліджувалась

Вплив НТП на довкілля:

Впровадження НТП: використано для підготовки спеціалістів з КЗІ

Практична реалізація НТП

Початок етапу: 05.2021

Закінчення етапу: 12.2021

Споживачі продукції:

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:

ІХ. Бібліографічний опис

Kovalchuk L.V. Davydoff O.A. New efficient ring signature algorithm for provision of information by authorized people. Збірник тез VII Міжнародного науково-практичного семінару «Актуальні питання забезпечення кіберзахисту та захисту інформації», 24-27 лютого 2021 року, с. Верхне Студене.

Кудін А.М., Селюх П.В. Асиметричні криптографічні протоколи з блокчейн-ядром: проблеми побудови та їх рішення / Фізико-математичне моделювання та інформаційні технології. – Львів: 2021, – Вип. 32. – С.175-180.
<https://doi.org/10.15407/fmmit2021.32.175>

Х. Заключні відомості

Керівник юридичної особи

Згуровський Михайло Захарович

к. т. н.

Перелік осіб-виконавців

Грубіян Євген Олександрович

Коваленко Богдан Віталійович

(к. т. н.)

Ковальчук Людмила Василівна

(д. т. н.)

Кудін Антон Михайлович

(д.т.н., 05.13.21)

Курінний Олег Вікторович

Олексійчук Антон Миколайович

(д.т.н., 05.13.21)

Савчук Михайло Миколайович

(д. ф.-м. н., 01.05.01, 05.13.21)

Селюх Поліна Валентинівна

Фесенко Андрій Вячеславович

(к. ф.-м. н.)

Чіхладзе Вахтанг Зурабович

Ядуха Дарія Вікторівна

Яковлев Сергій Володимирович

(к. т. н.)

Відповідальний за підготовку

Розумей Ольга Іллівна

облікових документів

Телефон

+38 (096) 678-90-91

Реєстратор

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

