

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0226U003040

Державний реєстраційний номер: 0124U001741

Особливі позначки: відкрита

Дата реєстрації: 13-03-2026

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Теоретичне дослідження наявних методів криптоаналізу у квантовій моделі обчислень.
Розробка нових методів криптоаналізу у квантовій моделі обчислень та результати їхнього застосування.

Початок етапу: 01.2024

Закінчення етапу: 12.2025

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 Берестейський, буд. 37, м. Київ, 03056, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 380442367989, 380442044862, 380442049494

IV. Відомості про співвиконавців ДіР

V. Відомості про замовника 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 Берестейський, буд. 37, м. Київ, 03056, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 380442367989

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)

Напрямок фінансування: 2.2 - прикладні дослідження і розробки

Джерела фінансування

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

VII. Відомості про ДіР

Назва роботи українською:

Дослідження методів криптоаналізу в застосуванні до сучасних систем криптографічного захисту інформації у квантовій моделі обчислень

Назва роботи англійською:

Research on cryptanalysis methods applied to modern cryptographic information protection systems in the quantum computing model

Реферат українською:

Виконано криптографічний аналіз постквантових криптографічних примітивів і схем, включно з тими, що входять до національних стандартів. Побудовано атаки на поточковий шифр «Струмок» та уточнено оцінки стійкості схем цифрових підписів «Вершина» і «Сокіл», а також запропоновано модифікацію алгоритму обчислення теоретико-числового перетворення для схеми цифрового підпису «Вершина» з метою уникнення атак за побічними каналами. Окремо досліджено сімейство схем AJPS – варіанти побітового та блокового шифрування, а також механізм інкапсуляції ключів AJPS-KEM, що дозволило запропонувати модифікацію схеми шифрування AJPS-1, а також запропонувати модифікації задач, на складності яких ґрунтується стійкість криптографічних примітивів сімейства AJPS. Використовуючи отримані задачі, побудовані нові протоколи автентифікації та схему коду автентифікації повідомлень. Вдосконалено методи диференціального криптоаналізу для аналізу конкретних S-блоків і ARX-систем. Удосконалено підхід до зведення задачі SVP до пошуку гамільтоніана основного стану та виконано оцінку складності відповідної реалізації алгоритму QAOA. Побудовано реалізацію протоколу шести станів, квантового протоколу встановлення ключа, та квантового протоколу захищеного прямого зв'язку LM05 на основі аніонних систем в моделі топологічних квантових обчислень. Крім того, досліджені особливості різних квантових моделей обчислень та наявні методи криптоаналізу в квантовій моделі обчислень та використані їхні модифікації для уточнення рівня стійкості узагальнених фейстель-подібних шифрів та шифрів на основі схеми Лай-Мессі

Реферат англійською:

A cryptographic analysis of post-quantum cryptographic primitives and schemes has been performed, including those incorporated into national standards. Attacks have been constructed against the stream cipher «Strumok», and the security estimates of the digital signature schemes «Vershyna» and «Sokil» have been refined. Additionally, a modification of the number-theoretic transform computation algorithm for the «Vershyna» digital signature scheme has been proposed to prevent side-channel attacks. A separate study was conducted on the AJPS family of schemes – variants of bit-wise and block encryption, as well as the AJPS-KEM key encapsulation mechanism. This enabled the proposal of a modification to the AJPS-1 encryption scheme and the proposal of modified computational problems on whose hardness the security of the AJPS family primitives is based. Using these new problems, novel authentication protocols and a message authentication code scheme have been constructed. Methods of differential cryptanalysis have been improved for analyzing specific S-boxes and ARX systems. The approach to reducing the SVP (Shortest Vector Problem) to finding the ground-state Hamiltonian has been refined, and the complexity of the corresponding QAOA algorithm implementation has been evaluated. An implementation has been developed for the six-state protocol, quantum key distribution protocol, and the LM05 quantum secure direct communication protocol, based on anyonic systems within the topological quantum computing model. Furthermore, the features of various quantum computing models and existing cryptanalysis methods in the quantum computing model have been investigated. Modified versions of these methods were applied to refine the security level of generalized Feistel-like ciphers and ciphers based on the Lai-Massey scheme

Індекс УДК: 002:651.928(083.73), 002:651.928(083.73)

Коди тематичних рубрик:20.51.35

Керівники роботи

Власне Прізвище Ім'я По-батькові: Фесенко Андрій Вячеславович

Науковий ступінь: к. ф.-м. н.

Вчене звання:

Ідентифікатор ORCID ID:

Додаткова інформація:

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

Назва НТП українською: Дослідження методів криптоаналізу в застосуванні до сучасних систем криптографічного захисту інформації у квантовій моделі обчислень

Назва НТП англійською: Research on cryptanalysis methods applied to modern cryptographic information protection systems in the quantum computing model

НТП, яку передбачалося створити: Створено

Причини, через які НТП не було створено:

Отримані результати: Аналітичні матеріали

Галузь застосування: Дослідження й експериментальні розробки у сфері природничих і технічних наук

Реєстраційний номер картки технології:

Опис НТП: Стрімке зростання можливостей сучасних обчислювальних систем та розвиток методів криптографічного аналізу призводять до необхідності постійного оновлення підходів до оцінювання стійкості криптографічних схем. Поява нових моделей обчислень вимагає ретельної перевірки обґрунтованості припущень, які забезпечують відповідний рівень стійкості наявних криптосистем та схем, а також перегляду складності криптографічних алгоритмів у різних обчислювальних моделях. Особливої актуальності цей процес набуває з огляду на швидкий розвиток у квантових технологіях, які здатні суттєво вплинути на ефективність деяких наявних методів криптоаналізу, а також запропонувати абсолютно нові підходи. НДР спрямована на уточнення, вдосконалення та розробку нових методів криптоаналізу, адаптованих до використання у квантовій моделі обчислень. Очікується, що отримані результати дозволять більш точно та обґрунтовано визначати рівень захищеності криптографічних схем та систем в умовах можливого застосування квантових атак.

Соціально-економічна спрямованість НТП: Забезпечення промисловості чи населення новим видом інформаційно-комунікаційних послуг

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу:

Закінчення етапу:

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:

IX. Бібліографічний опис

X. Заключні відомості

Керівник юридичної особи

Пасічник Віталій Анатолійович

д. т. н.

Перелік осіб-виконавців

Завадська Людмила Олексіївна

(к.ф.-м.н., с.н.с., 01.01.05)

Литвиненко Юлія Семенівна

Ядуха Дарія Вікторівна

**Відповідальний за підготовку
облікових документів**

Собецька Анна Василівна

Телефон

Реєстратор

Юрченко Тетяна Анатоліївна

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



Юрченко Тетяна Анатоліївна