Облікова картка ДіР

I. Загальні відомості

Державний обліковий номер: 0217U003094

Державний реєстраційний номер: 0115U000254

Особливі позначки: відкрита

Дата реєстрації: 18-01-2017

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Дослідження та застосування методів криптоаналізу важкооборотних криптографічних перетворень в класичній та квантовій моделі обчислень

Початок етапу: 01.2015

Закінчення етапу: 12.2016

Вид звітного документа: Остаточний звіт

III. Відомості про виконавця ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Національний технічний університет України "Київський політехнічний інститут", Фізико-технічний інститут

Код за ЄДРПОУ: 02070921

Місцезнаходження:

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 044-2366913, 044-236-70-98

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" Інститут енергозбереження та енергоменеджменту

Код за ЄДРПОУ: 247571500

Місцезнаходження: вул. Борщагівська 115, м. Київ, Київська обл., 03056, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 0442049690

VI. Джерела, напрями та обсяги фінансування ДіР

Підстава для проведення ДіР: 34 - договір (замовлення) з центральним органом виконавчої влади, академією наук (головними розпорядниками бюджетних коштів на проведення НДДКР)

Напрям фінансування: 2.2 - прикладні дослідження і розробки

Джерела фінансування

7713 - кошти держбюджету

Код програмної класифікації видатків і кредитування (КПКВК): 2201040

Фактичний обсяг фінансування (тис. грн.): 180

VII. Відомості про ДіР

Назва роботи українською:

Дослідження та застосування методів криптоаналізу важкооборотних криптографічних перетворень в класичній та квантовій моделі обчислень.

Назва роботи англійською:

Research and application methods of cryptanalysis of unilateral cryptographic transformations in classical and quantum computing model.

Реферат українською:

Об'єкт дослідження - інформаційні технології, системи та процеси криптографічного захисту інформації, способи створення криптоатак на системи захисту інформації. Предмет дослідження - математичні моделі важкооборотних перетворень, процесів криптографічного захисту інформації; методи, способи та математичні моделі криптоаналізу в класичній та квантовій моделі обчислень. Мета роботиполягає ваналізі існуючих, створенні нових ефективних методів аналізу важкооборотних перетворень, криптоалгоритмів, криптографічних протоколів, процедур та алгоритмів захисту від криптоатак з урахуванням умов, в яких криптосистеми експлуатуються і функціонують,та моделей обчислень; у застосуванні розроблених методів при побудові нових криптоалгоритмів і протоколів. Результати даної НДР отримані з використанням сучасних методів дослідження стійкості криптографічних систем, методів обчислення оцінок їх стійкості в класичній та квантовій моделях відносно криптографічних атак в залежності від умов, в яких вони функціонують і відповідної моделі обчислень, та знаходяться на рівні світових аналогів. Запропоновані в роботі модифіковані та нові методи дають можливість отримувати оцінки стійкості для існуючих систем криптографічного захисту інформації з урахуванням різних моделей обчислень, а також використовувати одержані результати для удосконалення систем криптографічного захисту інформації, враховуючи перспективи розвитку сучасних напрямків криптоаналізу та засобів обчислювальної техніки. СТІЙКІСТЬ СИСТЕМ КРИПТОГРАФІНОГО ЗАХИСТУ, КРИПТОАНАЛІЗ, СКЛАДНІСТЬ АЛГОРИТМІВ, ХМАРНІ ОБЧИСЛЕННЯ, ЛЕГКА КРИПТОГРАФІЯ, ДИФЕРЕНЦІАЛЬНИЙ АНАЛІЗ, КВАНТОВА МОДЕЛЬ ОБЧИСЛЕНЬ, ПСЕВДОВИПАДКОВІ ПОСЛІДОВНОСТІ, ПОСТКВАНТОВА СТІЙКІСТЬ

Реферат англійською:

Cryptanalytical methods of one-way mappings are modified and developed in classical and quantum computational model. New statistical criteria are proposed for evaluation of random and pseudorandom generators' quality. Security evaluation methods against differential and linear cryptanalysis are developed for non-Markov symmetric block ciphers with their structural specific taken into consideration. Upper bounds of average probabilities of integral differentials are estimated for some classes of mappings. Probabilistic properties of events are investigated in cryptanalysis of keystream overlapping with intensive usage. New estimates, conditions and features are proposed for lightweight cryptography with time/memory/security tradeoffs. Modified cubic attack for Halka cipher are proposed and implemented. New parameters and features are described for cryptographic methods of cloud security computations. Applicability of algebraic methods are evaluated in quantum model, also as their implementation to security estimation of specific cryptosystems in different computational models. Proposed methods and algorithms are implemented in software.

Індекс УДК: 004.7, 681.3.06:519.248.681

Коди тематичних рубрик: 50.37.23

Керівники роботи

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

Науковий ступінь:

Вчене звання:

Ідентифікатор ORCID ID:

Додаткова інформація:

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

Назва НТП українською: Звіт про НДР "Дослідження та застосування методів криптоаналізу важкооборотних криптографічних перетворень в класичній та квантовій моделі обчислень"

Назва НТП англійською: Report of "Research and application methods of cryptanalysis of unilateral cryptographic transformations in classical and quantum computing model"

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати:

Галузь застосування: інформаційна безпека, захист безпеки інформації

Реєстраційний номер картки технології:

Опис НТП: Модифіковано та розвинуто методи криптоаналізу важкооборотних криптографічних перетворень в класичній та квантовій моделі обчислень. Побудовано нові статистичні критерії визначення властивостей та характеристик випадкових, псевдовипадкових послідовностей та генераторів таких послідовностей. Розроблено методи обчислення аналітичних оцінок стійкості немарковських симетричних блочних шифрів до диференціального та лінійного криптоаналізу із урахуванням особливостей внутрішньої структури шифру. Побудовано верхні оцінки середніх ймовірностей цілочисельних диференціалів з урахуванням особливостей внутрішньої структури ітерацій блокового шифру. Досліджено ймовірнісні характеристики подій, пов'язаних з криптоаналізом шифротекстів з перекриттям гамми при інтенсивному їх використанні. Отримано характеристики, оцінки, умови застосування важкооборотних перетворень в легкій криптографії з урахуванням компромісу швидкодії, пам'яті та стійкості. Запропоновано та реалізовано програмно модифікований алгоритм кубічної атак

Соціально-економічна спрямованість НТП:

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

- **Початок етапу:** 2016-2017
- **Закінчення етапу:**

Споживачі продукції: підрозділи, що використовують оцінки стійкості для існуючих систем криптографічного захисту інформації з урахуванням різних моделей обчислень, а також використовувати одержані результати для удосконалення систем криптографічного захисту інформації, враховуючи перспективи розвитку сучасних напрямків криптоаналізу та засобів обчислювальної техніки. також використання у навчальному процесі.

Перспективні ринки: не вивчалися

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

1.L Kovalchuk, A. Bessalov. Exact Number of Elliptic Curves in the Canonical Form, Which are Isomorphic to Edvards Curves Over Prime Field// Cybernetics and Systems Analysis, volume 51, issue 2, 2015, p. 165-172. 2. Завадська Л.О., Семибаламут М.А. Профиль линейной сложности как средство оценки качества случайных последовательностей // Проблемы управления и информатики, 2015, №2(18). -с.124-136. 3. В. К. Задирака, А. М. Кудин, П. В. Селюх, И. В. Швидченко // Облачные технологии: новые возможности вычислительного криптоанализа // Проблемы управления и информатики : международный научно-технический журнал. - 2016. - N 1. - С. 148-155. 4.Алексейчук А.М., Ковальчук Л.В. Шевцов А.С., Яковлев С.В. О криптографических свойствах нового национального стандарта шифрования Украины// Кибернетика и системный анализ.- 2016.-Том 52,№3.-С.16-31. 5. Ковальчук Л.В., Бессалов А.В., Беспалов А.Ю. Алгоритмы генерации базовой точки кривой Эдвардса с использованием критериев делимости точки // Кибернетика и системный анализ.- 2016.-Том 52,№5.-С.14-24. 6. Ковальчук Л.В. Побудова верхніх оцінок середніх імовірностей цілочисельних диференціалів композицій ключового суматора, блоку підстановки та лінійного (над деяким кільцем) оператора./ Ковальчук Л.В., Кучинська Н.В. Скрипник Л.В.// Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - вип. 1(29). - 2015р. 7. Яковлев С. В. Атаки збоїв на шифр ДСТУ ГОСТ 28147:2009 // Інформаційна безпека. - 2015. - № 2(18). - С. 124-136.

X. Заключні відомості

Керівник юридичної особи Ільченко Михайло Юхимович

Перелік осіб-виконавців

Завадська Л.

Ковальчук Л.

Селюх П.

Фаль О.

Фесенко А.

Шевченко А.

Яковлєв С.

Відповідальний за підготовку облікових документів

Телефон

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності