

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0219U101998

Державний реєстраційний номер: 0119U102099

Особливі позначки: відкрита

Дата реєстрації: 12-12-2019

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Вибір та аналіз напрямів дослідження. Теоретичні та експериментальні дослідження. Узагальнення і оцінювання результатів досліджень. Складання звітної документації.

Початок етапу: 06.2019

Закінчення етапу: 11.2019

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, 37, м. Київ, Київська обл., 03056, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 0442369673, 380442367989, 0442049858, 0442044862

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: 2.2 - прикладні дослідження і розробки

Джерела фінансування

7722 - кошти підприємств, установ, організацій України

Фактичний обсяг фінансування (тис. грн.): 789
--

VII. Відомості про ДіР

Назва роботи українською:

Дослідження, розроблення та застосування новітніх методів криптографічного аналізу систем захисту інформації в різних моделях обчислень з урахуванням умов їх функціонування", шифр "Дорадо"

Назва роботи англійською:

Research, development and application of the newest methods of cryptographic analysis of information security systems in various computing models with respect to the conditions of their functioning", cipher "Dorado"

Реферат українською:

Метою виконання НДР є отримання нових та адаптація існуючих математичних моделей, методів та алгоритмів аналізу сучасних систем криптографічного захисту інформації у різних моделях обчислень з урахуванням їх функціонування. Основні результати НДР. Побудовано аналітичні оцінки стійкості до узагальненого лінійного криптоаналізу для певних класів SP мереж та модифікованих схем Фейстеля; оцінки параметрів стійкості до диференціального та лінійного криптоаналізу для окремих класів безключових перетворень, а також запропоновано нові методи для виявлення аномалій та прихованих алгебраїчних структур певного типу у безключових перетвореннях. Наведено оцінки ймовірності помилкового розшифрування повідомлень у системах типу NTRU. Також побудовано атаку на систему на основі лінійних кодів і запропоновано метод розв'язання задачі відновлення довільного лінійного коду за набором спотворених кодових слів. Здійснено аналіз криптографічних протоколів, направлених на захист ідентифікаційних даних та іншої інформації, що стосується поведінки та діяльності фізичних осіб. Досліджено класи перестановок спеціального виду, наведено аналітичні та експериментальні оцінки потужності таких класів, а також запропоновано статистичний критерій перевірки якості генератора випадкових перестановок. Досліджено необхідні властивості арифметики за модулем числа Мерсенна та сформульовано нові алгебраїчні задачі для побудови модифікацій постквантової криптосистеми AJPS. Розглядено алгебраїчну модель, яка дозволяє узагальнити ряд новітніх алгебраїчних задач на решітках, а також проаналізовано процедуру побудови квантових станів Дікке, які використовуються при атаках на криптопримітиви на основі зазначених задач. Сформульовано метод факторизації чисел, який є аналогом методу Ленстра на кривих Едвардса, обґрунтовано його коректність, знайдено верхні оцінки для швидкодії та нижні для ймовірності успіху. Розглянуто та проаналізовано три варіанта побудови алгоритмів пошуку генератора криптосистеми (базової т

Реферат англійською:

Goals of this work are synthesis of new mathematical models, methods and algorithms of analysis for modern cryptographic security systems, as well as adaptation of existing ones under different computation models and consideration of functioning conditions. Main results of this work includes the following. Analytic security bounds against generalized linear cryptanalysis were constructed for SP-networks of special kinds and modified Feistel schemes. Security against differential and linear cryptanalysis for selected classes of keyless mappings was estimated. New techniques were proposed for anomaly detections and hidden algebraic structure recovering in keyless mappings. Estimations of error decryption probability were given for NTRU-type cryptosystems. An attack was proposed for cryptosystems based on linear error correction codes; besides, we described solution method for linear code recovering problem based on a set of corrupted codewords. Cryptographic security protocols for identification data and individual's behavior information were analysed. Special classes of permutations were analyzed, their cardinality was estimated analytically and experimentally, and also statistical criterion was proposed for testing a quality of random permutation generators. Properties of arithmetic modulo Mersenne number were studied, and new algebraic problems were formulated for modifications of post-quantum AJPS cryptosystem. We considered an algebraic model which allows to generalize a set of modern algebraic problems

based on lattices, and also we studied a procedure of Dicke's quantum states creation, which are used in attacks on cryptosystems based on mentioned problems. We proposed a factorization technique which is analogous for Lenstra's algorithm, but uses Edward's elliptic curves; for this method we gave proof of correctness, upper bounds for efficiency, and lower bounds for success probability. We proposed and gave a comparative analysis of three variants for Edwa

Індекс УДК: 002, 681.3.06:519.248.681

Коди тематичних рубрик: 20

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 заключний

Назва НТП англійською: Final raport cipher “Dorado”

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати: Науково-технічний звіт про НДР , Дані теоретичних та експериментальних досліджень, висновки щодо перспектив подальших досліджень.

Галузь застосування: 73.10.1-Дослідження і розробки в галузі природних та технічних наук

Реєстраційний номер картки технології:

Опис НТП: Основні результати НДР. У першому розділі побудовано аналітичні оцінки стійкості до узагальненого лінійного криптоаналізу для певних класів SP мереж та модифікованих схем Фейстеля. У другому розділі побудовано оцінки параметрів стійкості до диференціального та лінійного криптоаналізу для окремих класів безключових перетворень, а також запропоновано нові методи для виявлення аномалій та прихованих алгебраїчних структур певного типу у безключових перетвореннях. У третьому розділі наводяться оцінки ймовірності помилкового розшифрування повідомлень у системах типу NTRU. Також побудовано атаку на систему на основі лінійних кодів і запропоновано метод розв'язання задачі відновлення довільного лінійного коду за набором спотворених кодових слів. У четвертому розділі здійснено аналіз криптографічних протоколів, направлених на захист ідентифікаційних даних та іншої інформації, що стосується поведінки та діяльності фізичних осіб. У п'ятому розділі досліджуються класи перестановок спеціального виду, наводяться аналітичні та експериментальні оцінки потужності таких класів, а також запропоновано статистичний критерій перевірки якості генератора випадкових перестановок. У шостому розділі досліджуються необхідні властивості арифметики за модулем числа Мерсенна та формулюються нові алгебраїчні задачі для побудови модифікацій постквантової криптосистеми AJPS. У сьомому розділі розглядається алгебраїчна модель, яка дозволяє узагальнити ряд новітніх алгебраїчних задач на решітках, а також проаналізована процедура побудови квантових станів Дікке, які використовуються при атаках на криптопримітиви на основі зазначених задач. У восьмому розділі сформульовано метод факторизації чисел, який є аналогом методу Ленстра на кривих Едвардса, обґрунтовано його коректність знайдено верхні оцінки для швидкодії та нижні для імовірності успіху. У дев'ятому розділі розглянуто та проаналізовано три варіанта побудови алгоритмів пошуку генератора криптосистеми (базової точки) на кривій Едвардса над

Соціально-економічна спрямованість НТП: теоретичні дослідження в галузі криптографічного захисту інформації

Вплив НТП на довкілля:

Впровадження НТП: Звіт по НДДКР, впровадження в дослідницькій та практичній діяльності Замовника

Практична реалізація НТП

Початок етапу: 05.2019

Закінчення етапу: 11.2019

Споживачі продукції:

Перспективні ринки:

Характер співробітництва з інвестором

Потрібний обсяг інвестицій, тис. грн.:

Права, що надаються інвестору після завершення роботи: Права не надаються

Наявність бізнес-плану: Ні

Техніко-економічне обґрунтування: Ні

Потенціальний обсяг продажу, тис. грн.:

Очікуваний термін окупності (років):

Додаткова інформація:

IX. Бібліографічний опис

Яковлев С.В. Про неіснування матриць максимального індексу розгалуження над кільцем лишків за модулем / С.В. Яковлев, В.В. Дідан. // Міжнародна науково-практична конференція «Інформаційні технології та комп'ютерне моделювання 2016» (Івано-Франківськ – Яремче). – Івано-Франківськ: ПНУ ім. В. Стефаника, 2016.

Олексійчук А.М. Субекспоненційні алгоритми розв'язання систем лінійних булевих рівнянь зі спотвореними правими частинами // Прикладная радиоэлектроника. – 2012. – Т. 11. – № 2. – С. 3 – 11.

Алексейчук А.Н. Неасимптотические нижние границы информационной сложности статистических атак на симметричные криптосистемы // Кибернетика и системный анализ. – 2018 – Т. 54. – № 1. – С. 1 – 13

Алексейчук А.Н., Конюшок С.Н. О статистических свойствах нелинейности сужений булевых функций на случайно выбранное подпространство // Прикладная дискретная математика. – 2012. – Вып. 1(15). – С. 5 – 10.

Алексейчук А.Н., Грязнухин А.Ю. Метод восстановления систематических линейных кодов по наборам искаженных кодовых слов // Прикладная радиоэлектроника. – 2013. – Т. 12. – № 2. – С. 313 – 318

Kovalchuk L., Bessalov A. Exact Number of Elliptic Curves in the Canonical Form, Which are Isomorphic to Edwards Curves Over Prime Field. //Cybernetics and Systems Analysis. V. 51. I.2. 2015. P. 165–172.

Бессалов А.В., Цыганкова О.В. Производительность групповых операций на скрученной кривой Эдвардса над простым полем. // Радиотехника №181, 2015. С.58-63.

Кудін А.М., Ковальчук Л.В., Коваленко Б.А. Теоретичні засади та застосування блокчейн-технологій: імплементація нових протоколів консенсусу та краудсорсінг обчислень // Математичне та комп'ютерне моделювання. Серія: Технічні науки. Випуск 19. – 2019. – С. 56-62.

Х. Заключні відомості

Керівник юридичної особи

Ільченко Михайло Юхимович

д. т. н., 05.12.13

Перелік осіб-виконавців

Грубіян Євген Олександрович

Ковальчук Людмила Василівна

(д. т. н.)

Кудін Антон Михайлович

(д. т. н., 05.13.21)

Матійко Александра Андріївна

Оксьоненко Максим Петрович

Олексійчук Антон Миколайович

(д.т.н., 05.13.21)

Савчук Михайло Миколайович

(д. ф.-м. н.)

Фаль Олексій Михайлович

(к. ф.-м. н., 01.01.05)

Фесенко Андрій Миколайович

(к.і.н.)

Циганкова Оксана Валентинівна

Ядуха Дарія Вікторівна

Яковлев Сергій Володимирович

Відповідальний за підготовку облікових документів

Розумей Ольга Іллівна

Телефон

+38 (044) 204-81-76

Реєстратор

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

