Облікова картка ДіР

I. Загальні відомості

Державний обліковий номер: 0220U101019

Державний реєстраційний номер: 0117U000500

Особливі позначки: відкрита

Дата реєстрації: 30-01-2020

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Дослідження методів криптографічного аналізу систем захисту інформації в класичній та квантовій моделях обчислень з урахуванням додаткових даних та умов функціонування.

Початок етапу: 01.2017

Закінчення етапу: 12.2019

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 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: 380442367989, 380442044862

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): 2201020

Фактичний обсяг фінансування (тис. грн.): 693

VII. Відомості про ДіР

Назва роботи українською:

Дослідження методів криптографічного аналізу систем захисту інформації в класичній та квантовій моделях обчислень з урахуванням додаткових даних та умов функціонування .

Назва роботи англійською:

Research methods of analysis of cryptographic information security systems in classical and quantum computing models with the additional data and operating conditions.

Реферат українською:

Побудовано моделі для немарковських SP-мереж, які використовують декілька різних S-блоків на одному раунді шифрування, уточнено алгоритми обчислення верхніх меж ймовірностей диференціалів. Розроблені критерії практичного відбору ARX-криптопримітивів з певними властивостями на основі автоматичного оцінювання стійкості. Проведено криптоаналіз нового стандарту блокового шифрування України "Калина" та окремих вузлів стандарту блокового шифрування республіки Білорусь СТБ 34.101.31-2011 «BeLT». Виконано модифікацію кубічної атаки на шифр SIMECK з використанням інформації з побічного каналу. Отримано оцінки складності групових операцій для скручених еліптичних кривих Едвардса та доцільности розробки нового національного стандарту України, що базується на кривих Едвардса. Побудовано чотири моделі зловмисника в залежності від його обчислювальних можливостей з урахуванням квантових обчислень та доступу до оракулу, який обчислює досліджуване криптографічне перетворення. В постквантовій моделі обчислень розроблено критерій ефективного часткового розв'язку узагальненої задачі симетричної декомпозиції. Розроблено формальні моделі системи зв'язку та зловмисника в клептографічному сенсі, способи виявлення потенційних клептографічних механізмів, методів усунення або зменшення прихованих каналів.

Реферат англійською:

Models for non-Markov SP networks that use several different S-blocks in one encryption round are built, and algorithms for calculating upper bounds for differential probabilities are specified. The criteria for the practical selection of ARX cryptographic primitives with certain properties based on the automatic evaluation of stability are developed. The cryptanalysis of the new blockchain encryption standard of Ukraine "Kalina" and separate units of the blockchain encryption standard of the Republic of Belarus STB 34.101.31-2011 "BeLT" has been carried out. A modification of the cubic attack on the SIMECK cipher using information from the side channel was made. The complexity of group operations for twisted Edwards curves and the expediency of developing a new national standard of Ukraine based on the Edwards curves were obtained. Four models of the attacker, depending on its computing capabilities, quantum computing and access to the oracle, which calculates the studied cryptographic transformation, are constructed. The criterion for the effective partial solution of the generalized symmetric decomposition problem in the post-quantum model of calculations is developed. Formal models of the communication system and the attacker in terms of kleptography, ways to identify potential kleptographic mechanisms and methods of eliminating or reducing hidden channels have been developed.

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 методів криптографічного аналізу систем захисту інформації в класичній та квантовій моделях обчислень з урахуванням додаткових даних та умов функціювання"

Назва НТП англійською: Repot of Scientific research work "Research methods of analysis of cryptographic information security systems in classical and quantum computing models with the additional data and operating conditions"

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати: Методи, теорії

Галузь застосування: інформаційна безпека, захист безпеки інформації, кібербезпека

Реєстраційний номер картки технології:

Опис НТП: Побудовано моделі для немарковських SP-мереж, які використовують декілька різних S -блоків на одному раунді шифрування, уточнено алгоритми обчислення верхніх меж ймовірностей диференціалів. Розроблено критерії практичного відбору ARX- криптопримітивів з певними властивостями на основі автоматичного оцінювання стійкості. Проведено криптоаналіз нового стандарту блокового шифрування України "Калина" та окремих вузлів стандарту блокового шифрування республіки Білорусь СТБ 34.101.31-2011 «BeLT». Виконано модифікацію кубічної атаки на шифр SIMECK з використанням інформації з побічного каналу. Отримано оцінки складності групових операцій для скручених еліптичних кривих Едвардса та доцільності розробки нового національного стандарту України, що базується на кривих Едвардса. Побудовано чотири моделі зловмисника в залежності від його обчислювальних можливостей з урахуванням квантових обчислень та доступу до оракулу, який обчислює досліджуване криптографічне перетворення. В постквантовій моделі обчислень розроблено критерій ефективного часткового розв'язку узагальненої задачі симетричної декомпозиції. Розроблено формальні моделі системи зв'язку та зловмисника в клептографічному сенсі, способи виявлення потенційних клептографічних механізмів, методів усунення або зменшення прихованих каналів.

Соціально-економічна спрямованість НТП: Результати роботи можуть бути використані при побудові надійних систем криптографічного захисту інформації.

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу:

Закінчення етапу:

Споживачі продукції: Академія наук НАНУ, Національний банк України, комерційні структури, вищі навчальні заклади

Перспективні ринки:

Характер співробітництва з інвестором

Потрібний обсяг інвестицій, тис. грн.: 1000

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

Наявність бізнес-плану:Ні

Техніко-економічне обгрунтування: Ні

Потенціальний обсяг продажу, тис. грн.: 1000

Очікуваний термін окупності (років): 2

Додаткова інформація: немає

IX. Бібліографічний опис

Бессалов А.В., Цыганкова О.В. Суперсингулярные полные кривые Эдвардса над простым полем. // Радиотехника, №191, 2017. – С.88-98.

Циганкова О.В. Нові алгоритми пошуку генератора криптосистеми на еліптичних кривих у формі Едвардса. // НДЦ «Тезис», 2019 (подано до друку)

Беспалов О.Ю. Алгоритми факторизації та перевірки незвідності поліномів з використанням апарату еліптичних кривих. // «Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні» - 2017, - вип. 1(33), стор. 85-96.

Беспалов О.Ю. Узагальнення леми Гаусса про характери пар елементів простого скінченного поля. // Зб.наук.праць Інституту Кібернетики ім. В.М. Глушкова НАН України та Кам'янець-Подольського національного університету ім. І. Огієнка, випуск 15, 2017р., стор. 26-31.

Ільїн М.І. Модифікація методу обчислювальної реалізації крайових задач на основі Д4 декомпозиції для гібридних систем на базі графічних процесорів // Вісник НТУУ КПІ: Інформатика, управління та обчислювальна техніка. – 2017, №5. – С. 63-67. (РІНЦ).

А.М. Кудін, Л.В. Ковальчук, Б.А. Коваленко. Теоретичні засади та застосування блокчейн технологій: імплементація нових протоколів консенсусу та краудсорсінг обчислень. // Математичне та комп'ютерне моделювання. – 2019, вип. 19 - С. 62-68.

Ильин Н.И. Информационная технология мониторинга загрязнения атмосфери химически взаимодействующими примесями с учетом их аномальних свойств // Управляющие системи и машины. – 2017. – 4. – С. 59-67.

X. Заключні відомості

Керівник юридичної особи — Пасічник Віталій Анатолійович
к. т. н., 05.12.13

Перелік осіб-виконавців

Єндовицький Павло Олександрович

Беспалов Олексій Юрійович

Грубіян Євген Олександрович

Деркач Олександр Григорович

Киреєнко Олександр Володимирович

Ковальчук Людмила Василівна
(д. т. н., 05.13.21)

Козленко Олександр Володимирович

Пекарчук Ніна Андріївна

Фаль Олексій Михайлович
(к. ф.-м. н., 01.01.05)

Фесенко Андрій В'ячеславович

Циганкова Оксана Валентинівна

Яковлєв Сергій Володимирович

Відповідальний за підготовку облікових документів — Циганкова О.В.

Телефон — +38 (066) 404-60-54

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності