

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0217U003631

Державний реєстраційний номер: 0116U006384

Особливі позначки: відкрита

Дата реєстрації: 08-06-2017

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Вибір та аналіз напрямків дослідження. Теоретичні та експериментальні дослідження. Узагальнення і оцінювання результатів досліджень.

Початок етапу: 08.2016

Закінчення етапу: 05.2017

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:

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 236-70-98, 204-81-76

IV. Відомості про співвиконавців ДіР

V. Відомості про замовника ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Служба зовнішньої розвідки України; військова частина К1410

Код за ЄДРПОУ: 33240845

Місцезнаходження: вул. Володимирська, 33, м. Київ, Київ, 01034, Україна

Форма власності:

Сфера управління: Служба безпеки України

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: 2.2 - прикладні дослідження і розробки

Джерела фінансування

7713 - кошти держбюджету

Код програмної класифікації видатків і кредитування (КПКВК): 6621010

Фактичний обсяг фінансування (тис. грн.): 645
--

VII. Відомості про ДіР

Назва роботи українською:

Дослідження методів криптоаналізу в застосуванні до сучасних систем криптографічного захисту інформації з урахуванням перспектив розвитку квантових обчислень

Назва роботи англійською:

Research of cryptanalytic methods used in modern systems of cryptographic security from the perspective of quantum computing development

Реферат українською:

Проведено теоретичне дослідження сучасних методів розробки та криптоаналізу симетричних та асиметричних криптосистем; узагальнено мат. моделі методів у класичній та квантовій моделях обчислень; запропоновано нові мат. методи аналізу окремих перетворень у системах КЗІ; показано застосування методів до деяких криптосистем. Для побудованих методів обчислено оцінку складності, одержано експериментальне підтвердження. Оновлено результати та твердження щодо стійкості систем КЗІ, перевірок конкретних оцінок стійкості, адекватності модельних припущень, оцінок складності певних алгоритмів у різних обч. системах. Уточнено та узагальнено існуючі мат. методи криптоаналізу, оновлено методи, процедури та алгоритми аналізу окремих криптографічних перетворень.

Реферат англійською:

This work provides theoretical research of modern methods of symmetric and asymmetric system analysis and synthesis. Some generalizations of mathematical models in mentioned methods are developed for classical and quantum computational models, as well as new techniques for analysis of distinct mappings in cryptosystems. Proposed methods were shown to be applicable to analyze for particular cryptosystems with experimental proofs and complexity estimation. Existing methods of cryptosystem analysis and synthesis are using wide spectrum of known techniques, e.g. algebraic, probabilistic, statistical and so on. Instant development of mathematical apparatus and growth of computational possibilities drive us to reconsider cryptographic security claims continuously, including verification of specific security estimations, verification of how model assumptions are adequate and how hard specific algorithms are in different computational architectures. So refinement and generalization of existing mathematical cryptographic methods are actual and of purpose with other cryptographic problems.5481

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 науково-дослідну роботу "Дослідження методів криптоаналізу в застосуванні до сучасних систем криптографічного захисту інформації з урахуванням перспектив розвитку квантових обчислень", шифр "Кобія", (частина 1, частина 2)

Назва НТП англійською: Report about research work " Research of cryptanalytic methods used in modern systems of cryptographic security from the perspective quantum computing development", code "KOBIA", (part 1, part 2)

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати: технічні науки

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

Реєстраційний номер картки технології:

Опис НТП: В науково-технічному звіті описано, що проведено теоретичне дослідження сучасних методів розробки та криптоаналізу симетричних та асиметричних криптосистем; узагальнено мат. моделі методів у класичній та квантовій моделях обчислень; запропоновано нові мат. методи аналізу окремих перетворень у системах КЗІ; показано застосування методів до деяких криптосистем. Для побудованих методів обчислено оцінку складності, одержано експериментальне підтвердження. Оновлено результати та твердження щодо стійкості систем КЗІ, перевірок конкретних оцінок стійкості, адекватності модельних припущень, оцінок складності певних алгоритмів у різних обч. системах. Уточнено та узагальнено існуючі мат. методи криптоаналізу, оновлено методи, процедури та алгоритми аналізу окремих криптографічних перетворень.

Соціально-економічна спрямованість НТП:

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: 2017

Закінчення етапу:

Споживачі продукції: СЗР України

Перспективні ринки: не досліджується

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

Х. Заключні відомості

Керівник юридичної особи

Ільченко Михайло Юхимович

Перелік осіб-виконавців

Єндовицький П.О.

Беспалов А.Ю.

Бессалов А.В.

Деркач О.Г.

Ковальчук Л.В.

Ломаченко І.

Олексійчук А.

Фаль О.М.

Фесенко А.В.

Циганкова О.В.

Яковлев С.В.

**Відповідальний за підготовку
облікових документів**

Телефон

Реєстратор

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

