

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0211U002130

Державний реєстраційний номер: 0109U001549

Особливі позначки: відкрита

Дата реєстрації: 20-01-2011

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Розробка та удосконалення алгебраїчно-ймовірнісних методів дослідження криптографічних перетворень, аналізу симетричних та асиметричних алгоритмів шифрування.

Початок етапу: 01.2009

Закінчення етапу: 12.2010

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", Фізико-технічний інститут

Код за ЄДРПОУ: 02070921

Місцезнаходження:

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 4068176, 2367098

IV. Відомості про співвиконавців ДіР

V. Відомості про замовника ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Інститут енергозбереження та енергоменеджменту Національного технічного університету України "Київський Політехнічний Інститут"

Код за ЄДРПОУ: 00027677

Місцезнаходження: пр. Перемоги 37, м. Київ, Київ, 03056, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 0442048428

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)

Напрямок 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.): 250
--

VII. Відомості про ДіР

Назва роботи українською:

Алгеброїчно-ймовірнісні методи дослідження стійкості та ефективності криптографічних алгоритмів і протоколів

Назва роботи англійською:

Algebraic-probabilistic methods of investigation of cryptographic algorithms and protocols resistance and effectiveness

Реферат українською:

Звіт про НДР: сторінок 213, рисунків 5, таблиць 11, алгоритмів 8, теорем 19, лем 6, тверджень 0, формул 104, означень 16, джерел 114. Об'єкт дослідження - системи та процеси криптографічного захисту інформації, способи побудови криптоатак на системи захисту інформації; випадкові послідовності, генератори випадкових та псевдовипадкових послідовностей. Предмет дослідження - математичні моделі криптоатак на системи захисту інформації та методи їх дослідження, методи оцінки стійкості криптографічних систем захисту інформації, принципи створення надійних і ефективних способів криптографічного захисту; методи оцінки якості випадкових послідовностей, генераторів випадкових та псевдовипадкових послідовностей, незалежності або залежності тестів. Мета роботи полягає в удосконаленні, розвитку та розробці інноваційних алгебраїчно-ймовірнісних методів криптоаналізу, засобів криптографічного захисту інформаційних технологій симетричними та асиметричними криптосистемами з урахуванням останніх досягнень криптології. Розроблено також нові статистичні критерії для перевірки криптографічної якості випадкових і псевдовипадкових послідовностей та генераторів таких послідовностей. Результати даної НДР знаходяться на рівні світових аналогів та їх застосування дає можливість отримання оцінок стійкості існуючих та нових алгоритмів криптографічного захисту інформації, визначення умов безпечного функціонування систем зберігання та передачі інформації. КРИПТОАНАЛІЗ, КОРЕЛЯЦІЙНІ ТА АЛГЕБРАЇЧНІ КРИПТОАТАКИ, СКЛАДНІСТЬ АЛГОРИТМІВ, ТЕСТУВАННЯ ВИПАДКОВИХ ТА ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ, НЕЗАЛЕЖНІСТЬ СТАТИСТИЧНИХ ТЕСТІВ.

Реферат англійською:

Report on SRW: pages 213, drawings 5, tables 11, algorithms 8, theorems 19, lems 6, statements 0, formulas 104, determinations 16, references 114. A research object are the systems and processes of IT security, methods of construction of cryptographic attacks on the IT security systems; random sequences, generators of random and pseudorandom sequences. The subject of research is mathematical models of cryptographic attacks on IT security systems and methods of their investigation, methods of estimation of the security level of the cryptographic systems, principles of creation of reliable and effective methods of cryptographic protection; methods of estimation of quality of random sequences, generators of random and pseudorandom sequences, independence or dependence of tests. The aim of the work consists in an improvement and development of innovative algebraic probabilistic methods of cryptanalysis, facilities of cryptographic protection of information technologies by symmetric and asymmetric cryptosystems taking into account the last achievements of cryptology. New statistical criteria are worked out also for testing cryptographic quality of random and pseudo random sequences and generators of such sequences. Results of this SRW are at the level of world analogues and their application enables to achieve the estimation of security level of the existing and new algorithms of cryptographic protection, determination of safe operating conditions on the systems of information storage and transfer. CRYPTANALYSIS, CORRELATION AND ALGEBRAIC CRYPTOGRAPHIC ATTACKS, COMPLEXITY of ALGORITHMS, TESTING of RANDOM AND PSEUDORANDOM SEQUENCES, INDEPENDENCE of STATISTICAL TESTS.

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 "Алгебраїчно-ймовірнісні методи дослідження стійкості та ефективності криптографічних алгоритмів і протоколів"

Назва НТП англійською: Report on SCW "Algebraic-probabilistic methods of investigation of cryptographic algorithms and protocols resistance and effectiveness"

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати:

Галузь застосування:

Реєстраційний номер картки технології:

Опис НТП: Досліджено системи та процеси криптографічного захисту інформації, способи побудови криптоатак на системи захисту інформації. Розроблено та вдосконалено інноваційні алгебраїчно-ймовірнісні методи криптоаналізу, засоби криптографічного захисту інформаційних технологій симетричними та асиметричними криптосистемами з урахуванням останніх досягнень криптології. Також розроблено нові статистичні критерії для перевірки криптографічної якості випадкових і псевдовипадкових послідовностей та генераторів таких послідовностей .

Соціально-економічна спрямованість НТП:

Вплив НТП на довкілля:

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: без обмежень

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

1. Савчук М.Н., Шарапов В.Г. Многомерный статистический тест для двоичных последовательностей // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - 2009. - Вип. 1(18).

- С. 65-72. 2. Ковальчук Л., Пальченко С. Застосування теорії узагальнених марківських шифрів до оцінювання стійкості сучасних блокових алгоритмів шифрування до методів різницевого криптоаналізу // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. - 2009. - Вип. 1(18). 3. Фаль А.М. Атаки на потокові шифри, що поєднують статистичні та алгебраїчні методи // Захист інформації.- 2009, №2, -С.59-70 4. Яковлев С.В. Каскадная схема Фейстеля та її стійкість до лінійного та диференціального аналізу // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні- 2009. - Вип. 1(18). -С. 103-108. 5. Яковлев С.В. Сбалансовані критерії якості довгострокових ключових елементів алгоритму шифрування ГОСТ28147-89 // Інформаційні технології та комп'ютерна інженерія. - 2009.- №1(14). 6. Ковальчук Л. В., Шерстюк А. О. Дослідження стійкості блочних шифрів MISTY1, MISTY2 та KASUMI до різницевого криптоаналізу // Прикладная радиоэлектроника -2009.- т.8, №3 - С. 258-267. 7. Єндовицький П.О. Уточнение асимптотической аппроксимации раз мера группі в парадоксе дней рождений.- Кибернетика и системный анализ.-2010.-№3. -С.185-188. 8. Єндовицький П.О. Точна асимптотична оцінка розміру групи в узагальненні парадоксу днів народжень // -Наукові вісті НТУУ "КПІ".-2010. -№4(72). -с.55-59. 9. Савчук М.Н. О работах киевской школы теоретической криптографии // Кибернетика и системный анализ. -Том 46, №3, май-июнь 2010. -С.52-68 10. Савчук М.М. Векторні випадкові процеси і статистичні тести для бінарних послідовностей // Наукові вісті КПІ. - №4(72). - С.100-104. 11. Стан та перспективи розвитку інформатики в Україні: монографія / Кол. авторів, гол. ред. І.В. Сергієнко. - Київ: Наукова думка, 2010. - 1008 с.

Х. Заключні відомості

Керівник юридичної особи

Новіков Олексій Миколайович

Перелік осіб-виконавців

Єндовицький П.О.

Завадська Л.В.

Ковальчук Л.В.

Пометун С.О.

Фаль О.М.

Фесенко А.В.

Яковлев С.В.

Відповідальний за підготовку

облікових документів

Телефон

Реєстратор

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

