

Облікова картка ДіР



I. Загальні відомості

Державний обліковий номер: 0211U008952

Державний реєстраційний номер: 0107U003608

Особливі позначки: відкрита

Дата реєстрації: 02-12-2011

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Розробити математичні основи розв'язання задач інформаційної безпеки методами комп'ютерної криптографії та стеганографії

Початок етапу: 01.2007

Закінчення етапу: 12.2011

Вид звітнього документа: Остаточний звіт

III. Відомості про виконавця ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Інститут кібернетики ім. В.М.Глушкова НАН України

Код за ЄДРПОУ: 05417176

Місцезнаходження:

Форма власності:

Сфера управління: Національна академія наук України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 526-41-78, 526-74-18

IV. Відомості про співвиконавців ДіР

V. Відомості про замовника ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Національна академія наук України

Код за ЄДРПОУ: 00019270

Місцезнаходження: вул. Володимирська, 54, м. Київ, Київська обл., 01030, Україна

Форма власності:

Сфера управління: Національна академія наук України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 380442396594

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: 2.1 - фундаментальні дослідження

Джерела фінансування

7713 - кошти держбюджету

Код програмної класифікації видатків і кредитування (КПКВК): 6541030

Фактичний обсяг фінансування (тис. грн.): 3337.8

VII. Відомості про ДіР

Назва роботи українською:

Розробити математичні основи розв'язання задач інформаційної безпеки методами комп'ютерної криптографії та стеганографії

Назва роботи англійською:

To develop mathematical bases of the decision of tasks of information safety by methods computer cryptography and steganography

Реферат українською:

Мета дослідження: вирішити низку криптографічних задач аналізу та синтезу сучасних криптосистем
Методи дослідження: теорія груп, теорія скінченних полів, теорія еліптичних кривих, теорія ймовірностей та математична статистика, обчислювальні методи алгебри та теорії чисел, асимптотичний аналіз, комбінаторика, теорія алгоритмів, теорія інформації та кодування. Результати виконання роботи: Розроблено формати сертифікатів атрибутів, що відповідають вимогам криптографічних стандартів України; Розроблено протоколи обчислення та перевіряння стану сертифікатів атрибутів; Розроблено програмні засоби обчислення та перевіряння стану сертифікатів атрибутів; Вирішена проблема інваріантності для систем випадкових рівнянь над алгебраїчними структурами; Розв'язані спеціальні комбінаторні задачі великої розмірності; Вивчені криптографічні властивості булевих функцій та криптографічних перетворень.

Реферат англійською:

Aim: to solve a number of cryptographic tasks of analysis and synthesis of modern cryptosystems. Methods: group theory, the theory of finite fields, the theory of elliptic curves, probability theory and mathematical statistics, computational methods of algebra and number theory, asymptotic analysis, combinatorics, theory of algorithms, information theory and coding. The results of the work: A format attribute certificates that meet the requirements of cryptographic standards of Ukraine; Developed protocols calculation and verification of certificates of attributes; A software calculation and verification of certificates of attributes; We solve the problem of invariance for systems of random equations over algebraic structures; Solve special combinatorial problems of large dimension; Studied cryptographic properties of Boolean functions and cryptographic transformations.

Індекс УДК: 519.248:681.51, 519.21, 681.3.06

Коди тематичних рубрик: 28.29.51

Керівники роботи

Власне Прізвище Ім'я По-батькові: Коваленко Ігор Миколайович, Задірака Валерій Константинович

Науковий ступінь:

Вчене звання:

Ідентифікатор ORCID ID:

Додаткова інформація:

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

Назва НТП українською: Методи комп'ютерної криптографії та стеганографії

Назва НТП англійською: Methods computer cryptography and steganography

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати:

Галузь застосування:

Реєстраційний номер картки технології:

Опис НТП: Розроблено формати сертифікатів атрибутів, що відповідають вимогам криптографічних стандартів України; Розроблено протоколи обчислення та перевіряння стану сертифікатів атрибутів; Розроблено програмні засоби обчислення та перевіряння стану сертифікатів атрибутів; Вирішена проблема інваріантності для систем випадкових рівнянь над алгебраїчними структурами; Розв'язані спеціальні комбінаторні задачі великої розмірності; Вивчені криптографічні властивості булевих функцій та криптографічних перетворень.

Соціально-економічна спрямованість НТП:

Вплив НТП на довкілля:

Впровадження НТП: Не впроваджено

Практична реалізація НТП

Початок етапу: 2014–2015 р.р.

Закінчення етапу:

Споживачі продукції: Державні установи, виробники систем захисту інформації

Перспективні ринки: Україна. Росія

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

3. Левитская А.А. Системы случайных уравнений над конечными алгебраическими структурами // Кибернетика и системный анализ. – 2005. – №1. – С.82 -116. 4. Левитская А.А. Описание некоторых классов равновероятных булевых функций, не имеющих нулевых коэффициентов Фурье // Кибернетика и системный анализ. – 2006. – №6. – С.95 -111. 5. Левитская А.А. Теоремы инвариантности для одного класса

систем случайных нелинейных уравнений над произвольным конечным кольцом с левой единицей // Кибернетика и системный анализ. - 2008. - №6. - С.106 -115. 6. Левитская А.А. Решение проблемы инвариантности вероятностных характеристик заведомо совместных систем случайных нелинейных уравнений над конечным коммутативным кольцом с единицей // Кибернетика и системный анализ. - 2010. - №3. 7. Савчук М.М., Фесенко А.В. Симетричні комутативні та локально комутативні шифри для побудови класичних та постквантових криптографічних протоколів // Інформаційні технології та комп'ютерна інженерія. - 2008. - №2(12). - С.43-51. 8. Савчук М.Н., Шарапов В.Г. Анализ одного метода тестирования случайных последовательностей основанного на контекстном моделировании // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.-2008, випуск 1(16) - С.82-89. 9. Савчук М.Н., Фесенко А.В. Использование коммутативных шифров для построения асимметричных схем шифрования // XII Международная научно-практическая конференция "Безопасность информации в информационно-телекоммуникационных системах", 19-22 мая 2009г., Киев, Тезисы докладов. - К.: ЧП "ЕКМО", НИЦ "ТЕЗИС" НТУУ "КПИ", 2009. 10. Савчук М.М., Фесенко А.В. Аналіз стійкості використання комутативних симетричних шифрів в постквантовій криптографії // Международная научная конференция "Интеллектуальные системы принятия решений и проблемы вычислительного интеллекта"(ISDMCI'2009). -18-22 мая 2009, Евпатория. - Херсон: ХНТУ, 2009. - Т.1. - С.269-271. 11. Савчук М.Н. О работах киевской школы теоретической криптографии //Кибернетика и системный анализ. - 2010.- №3. - С. 52-68. 12. Кочубинский А.И. (Украина), Мирин А.Ю. (Россия), Молдовян Н.А. (Россия). Схема слепой подписи на основе стандарта ЭЦП Беларуси СТБ 1176.2-99 // Инновационная деятельность в Вооруженных силах Российской Федерации: Труды всероссийской научно-практической конференции. 20-21 ноября 2008, г. Санкт-Петербург. СПб.: ВАС, 2008. С.212-217. 13. Кочубинский А.И. (Украина), Мирин А.Ю. (Россия). Передача сообщений по незащищенному каналу связи с гарантированным подтверждением получения // Материалы VI Санкт-Петербургской межрегиональной конференции "Информационная безопасность регионов России (ИБРР-2009)". Санкт-Петербург, 28-30 октября. СПб.: СПОИСУ, 2009. С.131 14. Костин А.А. (Россия), Молдовян Н.А. (Россия), Фаль А.М. (Украина). О реализации протоколов слепой и коллективной подписи на основе стандартов цифровой подписи // Материалы VI Санкт-Петербургской межрегиональной конференции "Информационная безопасность регионов России (ИБРР-2009)". Санкт-Петербург, 28-30 октября. СПб.: СПОИСУ, 2009. С.111. 15. Костина А.А. (Россия), Молдовян Д.Н. (Россия), Савчук М.Н. (Украина). О построении схем открытого распределения ключей и коммутативных шифров на основе некоммутативных конечных групп // Информационная безопасность регионов России (ИБРР-2009): Материалы конференции. 28-30 октября 2009 г, Санкт-Петербург. СПб., 2009. С.111-112. 16. Савчук М. Н. (Украина), Фесенко А. В. (Украина), Заболотный А.П. (Россия). Анализ использования коммутативных шифров в квантовой модели вычислений // Информационная безопасность регионов России (ИБРР-2009): Материалы конференции. 28-30 октября 2009 г, Санкт-Петербург. СПб., 2009. С.77-78. 17. Задірака В.К., Мельнікова С.С., Бородавка Н.В. Спектральні алгоритми комп'ютерної стеганографії //Искусственный интеллект.- 2002. - № 3. - С.532 - 541. 18. Бородавка Н.В. О качестве алгоритмов решения задач конструирующей стеганографии //Компьютерная математика. - 2003. - №1. - С.109-119. 19. Бородавка Н.В., Задірака В.К. Стеганоалгоритмы на базе теоремы о свертке // Кибернетика и системный анализ. - 2004. - №1. - С.139-144. 20. Задірака В.К., Кошкіна Н.В., Олексюк О.С. Аналіз стійкості стеганографічних систем в моделі пасивного противника // Искусственный интеллект.- 2004.- № 3.- С. 801 -805. 21. Кошкина Н.В., Шевчук Е.С. Применение преобразования высокой корреляции для решения задач компьютерной стеганографии //Компьютерная математика. - 2005. - №1. - С.87-94. 22. Кошкина Н.В. О методе сокрытия информации, использующем аппроксимацию тождественной свертки сигналов //Компьютерная математика. - 2006. - №2. - С.106-113 23. Кошкина Н.В. О стеганографических методах защиты информации на бумажных носителях //Компьютерная математика. - 2007. - №1. - С. 68-76 24. Кошкина Н.В., Никитина О.Ю. К вопросу о защите интеллектуальной собственности на бумажных носителях // Искусственный интеллект.- 2006.- № 3.-С. 757-763 25. Кошкина Н.В. Выделение инварианта для процесса печати и сканирования в задачах компьютерной стеганографии // УСИМ. - 2007. - №1.- С. 30-38 26. Кошкина Н.В. О методе защиты интеллектуальной собственности на основе выделения точечных

особенностей изображения //Захист інформації. - 2007. - №4. - С. 52-63 27. Кошкина Н.В. Методы синхронизации цифровых водяных знаков //Кибернетика и системный анализ. - 2008. - №1. - С. 180-188 28. Задирака В.К., Кошкина Н.В., Никитенко Л.Л. Статистический анализ систем с цифровыми водяными знаками // Искусственный интеллект.- 2008.- № 3.-С. 315-324 29. Задирака В.К., Никитина О.Ю. "Спектральные методы встраивания цифровых водяных знаков (ЦВЗ) в изображения" // Компьютерная математика. - № 2. - 2006. - С. 100-105. 30. Никитина О.Ю. "Оптимизация по точности методов цифровых водяных знаков, основанных на преобразовании Фурье-Меллина" // Искусственный интеллект. - 2007. - № 4. - С. 335-341. 31. Нікітенко Л.Л., Нікітіна О.Ю. "Вкраплення додаткової інформації в частотну область цифрового сигналу" // Искусственный интеллект. - № 4. - 2010. - С. 271-277. 32. Швидченко И.В. Анализ криптостеганографических алгоритмов // Проблемы управления и информатики. - 2007. - № 4. - С. 149-155. 33. Швидченко И.В. Стойкие криптостеганографические алгоритмы // Искусственный интеллект. - 2009. - № 1. - С. 218-226. 34. Швидченко И.В. Криптостеганографический алгоритм с использованием методов сегментации // Проблемы управления и информатики. - 2010. - № 5. - С. 145-153.

Х. Заклучні відомості

Керівник юридичної особи

Сергієнко Іван Васильович

д. ф.-м. н., 01.05.03

Перелік осіб-виконавців

Задірака В.К.

Коваленко І.М.

Кочубінський А.І.

Кошкіна Н.В.

Кузнецов І.М.

Кузнецов М.Ю.

Левитська А.О.

Нікітенко Л.Л.

Нікітіна О.Ю.

Савчук М.М.

Синявский В.Ф.

Супроткін Р.Г.

Фаль О.М.

Шаталов О.С.

Швидченко І.В.

Шевчук Б.М.

Відповідальний за підготовку облікових документів

Телефон

Реєстратор

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

