Облікова картка НДДКР

Державний обліковий номер: 0215U000618

Державний реєстраційний номер: 0113U000363

Відкрита

Дата реєстрації: 11-03-2015

1. Етапи виконання

Номер етапу: 1

Назва етапу: Аналіз стану, визначення основних напрямів розвитку, уніфікація , стандартизація, удосконалення, розробка та впровадження криптографічних систем, включаючи систему ЕЦП на національному рівні та інфраструктури відкритих ключів на міжнародному рівні

Початок етапу: 01-2013

Закінчення етапу: 12-2014

Вид звітного документа: Остаточний звіт

2. Виконавець

Назва організації: Харківський національний університет радіоелектроніки

Код ЄДРПОУ/ІПН: 02071197

Підпорядкованість: Міністерство освіти і науки України

Адреса: 61166, м. Харків, пр. Науки, 14

Телефон: 7021397

E-mail: innov@kture.khalimov.ua

3. Власник результатів НДДКР (продукції)

Назва організації: Харківський національний університет радіоелектроніки

Код ЄДРПОУ/ІПН: 02071197

Адреса: проспект Науки, 14, м. Харків, Харківський р-н., Харківська обл., 61166, Україна

Підпорядкованість: Міністерство освіти і науки України

Телефон: 380577021013

Телефон: 380577021807

E-mail: info@nure.ua

WWW: https://nure.ua

4. Джерела та напрями фінансування

Підстава для проведення робіт: 34 - договір (замовлення) з центральним органом виконавчої влади, академією наук (головними розпорядниками бюджетних коштів на проведення НДДКР)

КПКВК: 2201040

Напрям фінансування: 2.2 - прикладні дослідження і розробки

Джерела фінансування

Джерело фінансування: 7713 - кошти держбюджету

Фактичний обсяг фінансування за звітний етап: 559.7 тис. грн.

5. Науково-технічна робота

Назва роботи (укр)

Аналіз стану, визначення основних напрямів розвитку, уніфікація, стандартизація, удосконалення, розробка та впровадження криптографічних систем, включаючи систему ЕЦП на національному рівні та інфраструктури відкритих ключів на міжнародному рівні

Назва роботи (англ)

Analysis, identification of the main development directions, unification, standardization, improvement, development and implementation of cryptographic systems, including the signature at the national level, and public key infrastructure on an international level

Реферат (укр)

Розроблені методи синтезу та аналізу перспективних національних стандартів функції гешування, блокового симетричного шифрування (перетворення) та направленого шифрування, які дозволили створити національні стандарти на функцію гешування та блокове симетричне перетворення, що відповідають міжнародним вимогам. Вирішено низку наукових та практичних задач розвитку теорії та практики побудування системи ЕЦП, в тому числі створення у першій половині 2013 року акредитованого центру сертифікації ключів (АЦСК) з новими форматами Центрального засвідчувального органу (Міністерство юстиції), а також Міністерства зборів та податків.

Реферат (англ)

The methods of synthesis and analysis of prospective national standards hash function, block symmetric encryption and directional encryption, which helped to create national standards for a hash function and a symmetric block cipher in accordance with international requirements. Solved a number of scientific and practical problems of the theory and practice of building a system of electronic signature, including the creation of the first half of 2013 accredited Certification Authority with new formats Central certifying authority and the Ministry of fees and taxes.

Індекс УДК: 004.7, 004.056:061.68;004.375:061.68

Коди тематичних рубрик НТІ: 50.37.23

6. Науково-технічна продукція (НТП)

НТП 1

Назва продукції (укр): Методи синтезу та аналізу блокових симетричних шифрів, асиметричних шифрів, електронних цифрових підписів та функцій гешування по критеріям криптографічної стійкості.

Назва продукції (англ): Methods of synthesis and analysis of block symmetric ciphers, asymmetric ciphers, digital signatures and hash functions for cryptographic security criteria.

Очікувані результати:

Галузь застосування: 73.10.2

Опис продукції (укр): Розроблені методи синтезу та аналізу перспективних національних стандартів функції гешування, блокового симетричного шифру (перетворення) та направленого шифрування дозволили створити національні стандарти на функцію гешування та блокове симетричне перетворення, що відповідають міжнародним вимогам. Криптографічні та

табличні перетворення, що застосовуються в шифрі, відповідають найсучаснішим вимогам щодо рівня криптографічної стійкості та швидкодії.

Соціально-економічна спрямованість НТП:

Стадія завершеності НТП: Звіт по НДДКР

Впровадження НТП: Впроваджено

Строки впровадження: 2014-2015

Виробник продукції: ХНУРЕ

Споживачі продукції: підприємства та установи, які використовують криптографічний захист даних.

Перспективні ринки: УкраЇна

Права інтелектуальної власності: За договорами

Форми та умови передачі продукції: Продаж продукції

7. Бібліографічний опис

1.Долгов В.И. Блочные симметричные шифры. Методология оценки стойкости к атакам дифференциального и линейного криптоанализа // В.И. Долгов, И.В. Лисицкая / Украина, Харьков, издательство "Форт". -2013. - С.456. 2. Семенов С.Г. Методы и средства распределения доступа и защиты данных в компьютеризированных информационных управляющих системах критического применения/ Украина, Харьков, издательство "ХУПС". -2013. -С.360. 3. Горбенко Ю.И. Методы и средства генерации случайных битовых последовательностей // А.А.Торба, А.А. Бобкова, В.А. Бобух, И.Д. Горбенко / Украина, Харьков, издательство "Форт". -2013. - С.232. 4. Долгов В.И. Стойкость блочных шифров к дифференциальному и линейному криптоанализу// И.В.Лисицкая / Германия, Саарбрюкен, "LAP LAMBERT Academic Publishing". -2014. - С.497. 5. Халимов Г.З. Кривые Гурвица. Построение и применение для универсального хеширования. Изд. LAP LAMBERT Academic Publishing, Германия, 2014, С.89. https://www.lap-publishing.com/.../book/978-3-659-54769-0. 6. Долгов В.И. О роли схем разворачивания ключей в атаках на итеративные шифры // А.А.Настенко / Радиотехника, Всеукраинский межведомственный научно-технический сборник. - №171.-С.7-15. 7. Долгов В.И. S-блоки для современных шифров // Е.Д. Мельничук / Радиотехника, Всеукраинский межведомственный научно-технический сборник. - №171.-С.16-23. 8. Олейников Р.В. Криптоанализ шифра Mickey на основе анализа внутренних состояний // А.В.Казимиров / Радиотехника, Всеукраинский межведомственный научно-технический сборник. - №171.-С.24-30. 9. Лисицкая И.В. Вырожденные подстановки / Радиотехника, Всеукраинский межведомственный научно-технический сборник. - №171.-С.31-38. 10. Руженцев В.И. Про доказательство отсутствия эффективных байтовых дифференциальных характеристик для Rijndael-подобных шифров / Радиотехника, Всеукраинский межведомственный научно-технический сборник. - №59.-С.39-42. 11. Горбенко І.Д. Аналіз стійкості обчислювальних задач, що засновані на білінійних відображеннях //Л.В. Макутоніна / Радиотехника, Всеукраинский межведомственный научно-технический сборник. - №171.-С.79-89. 12. Іваненко Д.В. Методи протидії атакам спеціального виду на схеми направленого шифрування у кільцях зрізаних поліномів / Радиотехника, Всеукраинский межведомственный научно-технический сборник. - №171.-С.90-98. 13. Горбенко Ю.И. Сущность и анализ криптографических требований стандарта NIST SP 800-90B // Р.И.Мордвинов / Радиотехника, Всеукраинский межведомственный научно-технический сборник. - №171.-С.99-108. 14. Халимов Г.З. Универсальное хеширование по обобщенным кривым Гурвица // А.Н. Герцог / Радиотехника, Всеукраинский межведомственный научно-технический сборник. -2013. - №1.-С.140-146 15. Горбенко І.Д. Оцінка стійкості направленого шифру NTRU до атаки з адаптивно підібраними шифротекстами // Бубир А.П. / Радиотехника, Всеукраинский межведомственный научно-технический сборник. - №171.-С.147-151. 16. Халимов Г.З. Оценки коллизионной стойкости универсального хеширования по алгебраическим кривым / Системи озброєння і військова техніка, МО України, Харківський університет Повітряних Сил ім. Івана Кожедуба. - 2013. - № 1(33). - С.135-139 17. Олейников Р.В. Метод построения нелинейных узлов замены на основе градиентного спуска // А.В.Казимиров / Радиотехника, Всеукраинский межведомственный научно-технический сборник. - №172.-С.104-108 18. Лисицкая И.В. О криптографической значимости схем разворачивания ключей в обеспечении стойкости БСШ к атакам линейного и дифференциального криптоанализа // А.А. Настенко, К.Е. Лисицький / Радиоелектроника и информатика, Научно-технический журнал. - №3.-С.56-65. 19. Лисицкий К.Е. Уточненная математическая модель случайной подстановки // Е.Д. Мельничук / Автоматизированые системы управления и приборы автоматики. -2013. - №162.-С.22-28. 20. Руженцев В.И. О методе доказательства стойкости блочных симметричных шифров к атаке невыполнимых дифференциалов / Прикладная радиоэлектроника, Х: ХНУРЭ. - 2013. - том 12, №2. стр.215-219. 21. Халимов Г.З. Строго универсальное хэширование/ Прикладная радиоэлектроника, Х: ХНУРЭ. -

2013. - том 12, №2. стр.220-224. 22. Халимов Г.З. Оценка сложности универсального хэширования по алгебраическим кривым / Прикладная радиоэлектроника, Х: ХНУРЭ. - 2013. - том 12, №2. стр.225-229 23. Лисицкий К.Е. О приходе итеративных шифров к стационарному состоянию, свойственному случайной подстановке // Лисицкая И.В. /Прикладная радиоэлектроника, Х: ХНУРЭ. - 2013. - том 12, №2. стр. 230-235. 24.Мельничук Е.Д. Исследование соответствия новым критеріям отбора подстановочных конструкцій современных БСШ / Прикладная радиоэлектроника, Х: ХНУРЭ. - 2013. - том 12, №2. стр.240-246 25. Горбенко І.Д. Аналіз блокових симетричних шифрів міжнародного стандарту ISO/IEC 29192-2 // А.В. Самойлова / Прикладная радиоэлектроника, Х: ХНУРЭ. - 2013. - том 12, №2. стр.247-249. 26. Балагура Д.С. Исследование методов вычисления инверсии в алгоритме NTRU // К.А. Погребняк, Е.Г. Качко, Ю.І. Горбенко / Прикладная радиоэлектроника, Х: ХНУРЭ. - 2013. - том 12, №2. стр.254-257 27. М.Ф. Бондаренко. Обчислювальна складність основних задач на алгебраїчних решітках // Макутоніна Л.В./ Прикладная радиоэлектроника, Х: ХНУРЭ. - 2013. - том 12, №2. стр.258-264 28. Іваненко Д.В. Метод протидії атакам на реалізації, які базуються на аналізі енергоспоживання, схеми направленого шифрування у кільцях зрізаних поліномів. / Прикладная радиоэлектроника, Х: ХНУРЭ. - 2013. - том 12, №2. стр.292-298 29. Горбенко И.Д. О динамике прихода шифров к случайной подстановке при использовании S-блоков с показателями нелинейности близкими к предельным // К.Е. Лисицкий / Радиотехника. - 2014. - №176.-С.27-39. 30. Горбенко І.Д.. Статистичні властивості блокових симетричних шифрів з міжнародного стандарту ISO/IEC 29192-2 // А.В. Самойлова, О.О. Кузнецов / Радиотехника. -2014. - №176.-С.40-44. 31. Кузнецов О.О. Дослідження режимів застосування блокових симетричних шифрів відповідно до ISO/IEC 10116-2006 // Р.І. Мордвінов, Є.П. Колованова, А.В. Самойлова/ Радиотехника. -2014. - №176.-С.45-54. 32. Руженцев В.И. Об условиях отсутствия эффективных усеченных байтовых дифференциалов для блочных симметричных шифров / Радиотехника. -2014. - №176.-С.55-61 33. Горбенко И.Д.. Оценка стойкости направленного шифрования NTRU к атаке, основанной на изменениях времени расшифровани // А.П. Бубырь / Радиотехника. -2014. - №176.-С.68-73. 33. Горбенко Ю.І.. Аналіз можливостей квантових комп'ютерів та квантових обчислень для криптоаналізу сучасних криптосистем // Р.С. Ганзя, БДИРм-13-1 / "Восточно - Европейский журнал передових технологий". -2014. - №1(67).-С.8-15 34. Кузнецов О.О. Аналіз колізійних властивостей режиму вироблення імітовставок із вибірковим гамуванням // Д.В. Іваненко, Є.П. Колованова / Вестник ХНУ серия "Математическое моделирование. Информационные технологии. АСУ". -2014. -С.25-43 35. Oliynykov R. Related-key cryptanalysis of perspective symmetric block cipher // D. Kaidalov / Прикладная радиоэлектроника. -2014. - №3(13).-С.192-201 36. Кузнецов А.А. Моделирование перспективного блочного шифра "Калина" // Д.В. Иваненко, Е.П. Колованова / Прикладная радиоэлектроника. -2014. - №3(13).-С.202-208 37. Горбенко И.Д. Уточнённые показатели прихода шифров к состоянию случайной подстановки // В.И. Долгов, К.Е. Лисицкий / Прикладная радиоэлектроника. -2014. - №3(13).-С.214-217 38. Горбенко І.Д. Дослідження та порівняльний аналіз перспективних потокових шифрів // С.С. Тімохін / Прикладная радиоэлектроника. -2014. - №3(13).-С.218-221. 39. Долгов В.И. Новый взгляд на шифр Мухомор // К.Е. Лисицкий, И.В. Лисицкая / Прикладная радиоэлектроника. -2014. - №3(13).-С.222-226. 40. Руженцев В.И. Вероятности двухцикловых дифференциалов rijndael-подобного шифра с произвольными подстановками / Прикладная радиоэлектроника. -2014. - №3(13).-С.236-239 41. Горбенко Ю.І. Аналіз стійкості постквантових криптосистем // Р.С. Ганзя / Прикладная радиоэлектроника. -2014. - №3(13).-С.269-275 42. Балагура Д.С. Влияние свойств современных процессоров на производительность программ // К.А. Погребняк, Е.Г. Качко / Прикладная радиоэлектроника. -2014. - №3(13).-С.282-286 43. Бойко А.О. Метод протидії перебору паролів, що не створює вразливості порушення доступності / Прикладная радиоэлектроника. -2014. - №3(13).-С.297-298 44. Гриненко Т.А. Применение кодов аутентификации сообщений для обнаружения модификаций данных в региональных системах дифференциальной коррекции навигационных сигналов систем GPS/ГЛОНАСС // А.П. Нарежний / Прикладная радиоэлектроника. -2014. - №3(13).-С.302-311 45. Торба А.А. Быстродействующий детерминированный генератор псевдослучайных последовательностей для потокового шифрования // В.А. Бобух, А.А. Бобкова / Прикладная радиоэлектроника. -2014. - №3(13).-С.317-328 47. Олейников Р.В. Оценка стой кости симметричных блочних шифров на базе цепи фей стеля при использовании несюръективных S-блоков / Научно-практический журнал "Информационное противодействие угрозам терроризма". -2013. - №20.-С.121-127

8. Звітна документація

Кількість сторінок в звіті: 376

Мова звіту: Російська

Кількість файлів у звіті: 1

9. Заключні відомості

Перелік осіб-виконавців

Бобух Всеволод Анатолійович

Бойко Артем Олександрович

Горбенко Юрій Іванович

Гріненко Тетяна Олексіївна

Казимиров Олександр

Макутоніна Лідія

Мельникова Оксана Анатоліївна

Мордвінов Руслан Ігорович

Олійников Роман Васильович

Тоцький Олександр Сергійович

Халімов Геннадій Зайдулович

Чичмар Сергій Володимирович

Шумов Олександр Іванович

Керівник організації:

Сліпченко Микола Іванович

Керівники роботи:

Горбенко Іван Дмитрович

Керівник відділу реєстрації наукової діяльності УкрІНТЕІ

Юрченко Т.А.