Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0413U002332

Особливі позначки: відкрита

Дата реєстрації: 11-04-2013

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Шевчук Олексій Анатолійович
2. Shevchuk Oleksii Anatoliiovych

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 05.13.21

Назва наукової спеціальності: Системи захисту інформації

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 12-03-2013

Спеціальність за освітою: 8.17010102

Місце роботи здобувача: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

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

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): К 64.052.05

Повне найменування юридичної особи: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

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

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Харківський національний університет радіоелектроніки

Код за ЄДРПОУ: 02071197

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

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.37.23

Тема дисертації:

1. Методи та засоби ЕЦП з заданим рівнем захищеності та підвищеною швидкодією

2. Digital signatures with higher speed

Реферат:

1. Об'єкт дослідження - процеси надання послуг електронного цифрового підпису (ЕЦП) із заданим рівнем захищеності та підвищеною швидкодією. Мета дослідження - забезпечення визначеного рівня стійкості та підвищення швидкодії апаратних засобів криптографічного захисту інформації, що реалізують національний алгоритм ЕЦП, який ґрунтується на перетвореннях у групі точок еліптичної кривої. Методи дослідження - теорії складності обчислень під час оцінювання складності атак повного розкриття для перетворень типу ЕЦП, які ґрунтуються на перетвореннях у групі точок еліптичної кривої; теорії ймовірностей та математичної статистики в ході визначення криптографічної стійкості перетворень типу ЕЦП до екзистенційної підробки; криптографічного аналізу під час оцінювання складності атак повного розкриття для перетворень типу ЕЦП та аналізі властивостей схем ЕЦП з відновленням повідомлення; програмного моделювання та профілювання при реалізації процесів криптографічних перетворень, комбінаторики під час дослідження колізійних властивостей окремих елементів криптографічних перетворень; програмного моделювання паралельних процесів для аналізу стійкості запропонованого протоколу. Апаратура - персональний

комп'ютер. Теоретичні і практичні результати досліджень - розв'язано низку актуальних наукових і практичних задач, які стосуються виконання ЕЦП із використанням засобів криптографічного захисту інформації (КЗІ), що забезпечують захист від їх використання несанкціонованим способом та підвищення в ряді випадків їх швидкодії. Наукова новизна - вперше запропоновано метод модифікації алгоритмів скалярного множення у групі точок еліптичної кривої (ЕК), що використовуються для обчислення ЕЦП, який ґрунтується на частковому кешуванні множника та відповідної модифікації генератора псевдовипадкових послідовностей, що дозволяє підвищити швидкодію засобу ЕЦП; вперше запропоновано метод захисту від атаки повного розкриття за відомими результатами криптографічних перетворень, яка здійснюється за умови підміни апаратного засобу КЗІ, що ґрунтується на модифікації алгоритму автентифікації ISO/IEC 9798-2 6.1, шляхом зміни криптографічних перетворень із симетричних на перетворення з відкритим ключем, для обміну користувача з третьою довіреною стороною, що дозволяє забезпечити безпечний розподіл апаратних засобів КЗІ, які реалізують алгоритми ЕЦП, в умовах існування загрози підміни засобу криптографічного захисту; набув подальшого розвитку метод ЕЦП, визначений у Національному стандарті ДСТУ 4145:2002, який на відміну від існуючого використовує функцію створення доданої надлишковості замість функції ґешування повідомлення, що дозволяє зменшити обсяг ЕЦП для групи повідомлень, в залежності від характеристик повідомлення. Основні результати впроваджено у АТ "Інститут інформаційних технологій"; у межах робіт зі створення захищених каналів у корпоративній мережі передавання даних у Національну акціонерну компанію "Нафтогаз України"; у навчальний процес Харківського національного університету радіоелектроніки. Наукові та практичні результати дисертаційної роботи можуть бути використані в апаратних засобах криптографічного захисту інформації, які реалізують електронний цифровий підпис.

2. Object of study - processes of producing digital signatures (DSS) with the requested security level and increasing computational speed. Subject of research - providing requested level of security and increase computational speed of hardware security modules (HSM) that implements Ukrainian national DSS DSTU 4145-2002. Research methods - theory of complexity (evaluation of security level); probability theory and mathematical statistics the cryptographic analysis (evaluation of full disclosure); software modeling and profiling (evaluation of processes of cryptographic transformations), combination theory . The equipment - the personal computer. Theoretical and practical results of researches - solving the number of the actual scientific and practical tasks concerning performance of DSS - HSM union, providing protection against their use by unauthorized way and increases in some cases their speed. Scientific novelty - the method of modification scalar multiplication algorithms (in elliptic curve) which are based on a partial caching and pseudorandom number generator (PRNG) modification. That allows to increase the speed of DSS computation. The method of protection against attack of full disclosure by known results of cryptographic transformations, which is performed with spoofed HSM, is proposed for the first time. The method is based on the modified authentication algorithm ISO/IEC 9798-2 6.1, with changed cryptographic transformations from the symmetric ones to the ones with the public key. That allows the exchanges for the user with the third entrusted party and provides safe distribution of HSM hardware by offering protection from the HSM spoofing attack. Proposed the modification method of the national Ukrainian DSS DSTU 4145-2002 standard for using it in DSS with recovery mode with partial compatibility with existing implementations. The main results are introduced to the JSC "Institute of Information Technologies"; within works is devoted to creation virtual private networks, in NJSC "Naftogaz of Ukraine"; in educational process Kharkov national university. Results can be used for HSM improvements.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки:

Стратегічний пріоритетний напрям інноваційної діяльності:

Підсумки дослідження:

Публікації:

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації:

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Горбенко Іван Дмитрович
2. Gorbenko Ivan Dmytrovych

Кваліфікація: д.т.н., 21.02.01

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Краснобаєв Віктор Анатолійович
2. Краснобаєв Віктор Анатолійович

Кваліфікація: д.т.н., 20.02.14

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Василіу Євген Вікторович
2. Василіу Євген Вікторович

Кваліфікація: д.т.н., 05.13.21

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Горбенко Іван Дмитрович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Горбенко Іван Дмитрович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності Юрченко Т.А.