Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0412U000666

Особливі позначки: відкрита

Дата реєстрації: 30-03-2012

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Баришев Юрій Володимирович
2. Baryshev Yuriy Volodymyrovych

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 05.13.05

Назва наукової спеціальності: Комп'ютерні системи та компоненти

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 17-03-2012

Спеціальність за освітою: 8.160105

Місце роботи здобувача: Вінницький національний технічний університет

Код за ЄДРПОУ: 02070693

Місцезнаходження: 21021 м. Вінниця, вул. Хмельницьке шосе, 95

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): Д 05.052.01

Повне найменування юридичної особи: Вінницький національний технічний університет

Код за ЄДРПОУ: 02070693

Місцезнаходження: вул. Хмельницьке шосе, 95, м. Вінниця, Вінницький р-н., Вінницька обл., 21021, 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: Вінницький національний технічний університет

Код за ЄДРПОУ: 02070693

Місцезнаходження: 21021 м. Вінниця, вул. Хмельницьке шосе, 95

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.10.31

Тема дисертації:

1. Методи та засоби швидкого багатоканального хешування даних в комп'ютерних системах

2. Methods and means for rapid multipipe data hashing within computer systems

Реферат:

1. Об'єктом дослідження є процес криптографічного захисту інформації в комп'ютерних системах. Метою дослідження є підвищення швидкості автентифікації даних та користувачів в комп'ютерних системах шляхом створення нових методів та засобів хешування на основі багатоканальних конструкцій хешування, які забезпечують розпаралелення обчислень. Наукова новизна полягає в тому, що вперше запропоновано узагальнену конструкцію багатоканального хешування, яка на відміну від відомих передбачає можливість керування параметрами перетворень в процесі хешування, що дозволяє розробляти нові методи багатоканального хешування підвищеної швидкості та стійкості до загальних атак. Вперше запропоновано конструкції багатоканального хешування, стійкі до загальних атак на основі мультиколізій, з опосередкованим зав'язуванням всіх каналів один з одним, які порівняно з конструкціями багатоканального хешування з безпосереднім зав'язуванням каналів дозволяють розробляти методи хешування, що забезпечують зменшення часу хешування від 1,4 до 16 раз. Удосконалено методи багатоканального хешування

на основі операції піднесення до степеня за модулем простого числа та структури спеціалізованих процесорів, що їх реалізують, які за рахунок зав'язування каналів дозволяють виконувати операцію піднесення до степеня для чисел в q раз меншої розрядності порівняно з відомими, що забезпечує збільшення швидкості хешування у q раз. Отримали подальший розвиток конструкції багатоканального хешування, стійкі до загальних атак на основі мультиколізій, із безпосереднім зав'язуванням всіх каналів один з одним, які дозволяють, порівняно з відомими, розробляти методи хешування для кількості каналів q>2, що за рахунок розпаралелення обчислень дозволяє досягти підвищення швидкості хешування у q/2 раз. Отримали подальший розвиток методи формування вектора керування параметрами хешування, які забезпечують адаптування до зміни параметрів конструкцій хешування, що дозволяє розробляти програмно-апаратні засоби хешування з різними характеристиками швидкість/стійкість. Практична цінність полягає в створенні програмних засобів для тестування методів багатоканального керованого хешування за допомогою Known Answer Tests, програмних засобів багатоканального керованого хешування із вихідним хеш-значенням довільної довжини та різними параметрами конструкції хешування та рекомендацій щодо побудови спеціалізованих процесорів для швидкого хешування даних в комп'ютерних системах. Ступінь впровадження - результати дисертаційної роботи впроваджені у комп'ютерній системі підприємства ТОВ "ВІАТЕЛ" (м. Вінниця, Україна), підприємства ПП "ВІНБУДІЗОЛ" (м. Вінниця, Україна), а також використовується в навчальному процесі кафедри захисту інформації ВНТУ. Сфера (галузь) використання - в територіально розподілених багатокористувацьких комп'ютерних системах, а також в інших комп'ютерних системах та мережах, де необхідна автентифікація даних та користувачів.

2. The object of research is the process of cryptographic information protection within computer systems. The goal of the research is improving of data and user authentification rapidity within computer systems by developing of new methods and means of hashing based on the multipipe hash constructions, which provide parallelization of computation. The novelty is that the generalized multipipe hash construction, which in contradistinction to known ones provides the ability of data conversion driving during hashing, that allows to develop new multipipe hash methods with increased rapidity and durability against generic attacks, first are proposed. Multipipe hash constructions, which are durable against generic attacks based on multicollisions, with mediate channel interaction, those in contradistinction to multipipe hash constructions with direct channel interaction allow developing of hashing methods, which provide from 1.4 to 16 times hash duration decreasing, first are proposed. Multipipe hashing methods based on modulo prime number exponentiation, which in contradistinction to known ones allow to operate exponentiation of data with q times reduced capacity by channel interaction, that provide q times rapidity increasing, and specialized processors structures, which implement the methods, are improved. Multipipe hash constructions, which are durable against generic attacks based on multicollisions with direct channel interaction, those in contradistinction to known ones allow to develop hashing methods with channel quantity q>2, which provides q/2 times hash rapidity increasing by computation parallelization, are extended. Methods of hashing parameters driving vector generating, which allow to adapt change of hash construction parameters, that allows to develop soft hardware means with different durability/rapidity characteristics, are extended. The practical value concerning software developing for multipipe driven hashing testing by Known Answer Tests, software developing for multipipe hashing with arbitrary output digest length and different hash construction parameters and specialized processors for rapid data hashing in computer systems designing recommendations developing. The degree of the implementation - the results of the dissertation are implemented at the computer system of enterprise "VIATEL" (Vinnytsia, Ukraine), at the computer system of enterprise "VINBUDIZOL" (Vinnytsia, Ukraine) and at the studying process at the information protection department of VNTU. The field of application - geographically distributed multiuser computer systems as well as other computer systems and networks which require data and user authentification.

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. Лужецький Володимир Андрійович
2. Luzhetsky Volodymyr Andriyovych

Кваліфікація: д.т.н., 05.13.05

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. Корченко Олександр Григорович
2. Корченко Олександр Григорович

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

Власне Прізвище Ім'я По-батькові:

1. Рудницький Володимир Миколайович

2. Рудницький Володимир Миколайович

Кваліфікація: д.т.н., 05.13.06

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 Квєтний Роман Наумович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Квєтний Роман Наумович

Відповідальний за підготовку облікових документів

Реєстратор

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