Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0413U001103

Особливі позначки: відкрита

Дата реєстрації: 17-01-2013

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Бойко Артем Олександрович
2. Boiko Artem Oleksandrovych

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: 20-12-2012

Спеціальність за освітою: 8.160101

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): К64.052.05

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

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: 50.41.23

Тема дисертації:

1. Методи побудування кодів автентифікації повідомлення з підвищеною швидкодією

2. Message authentication techniques with higher speed

Реферат:

1. Метою досліджень є аналіз існуючих, удосконалення та розробка нових методів побудування кодів автентифікації повідомлень, які б мали більшу, у порівнянні з існуючими, швидкодію при збереженні заданого рівня стійкості. Об'єктом дослідження є процеси автентифікації даних, які ґрунтуються на використанні універсальних функцій гешування на основі обчислення значення полінома в скінченних полях та кільцях. Предметом досліджень є методи автентифікації даних з заданим рівнем стійкості на основі обчислення значення полінома в скінченних полях та кільцях, які дозволяють виконати вимоги до кодів автентифікації повідомлень, в тому числі обов'язково колізійна стійкість, складність знаходження прообразу та другого прообразу, висока швидкодія, простота реалізації тощо. Методи досліджень: методи теорії ігор та теорії інформації при дослідженні математичної моделі системи з автентифікацією даних та обґрунтування вимог до методів автентифікації даних; методи теорії полів і груп, методи теорії ймовірностей та математична статистика при визначені ймовірності появи слабких ключів; методи теорії паралельних обчислень при побудуванні та оцінці властивостей паралельних алгоритмів гешування; методи системного

аналізу при порівнянні існуючих методів автентифікації повідомлень; програмне моделювання при реалізації процесів універсального гешування. Теоретичні і практичні результати досліджень 1. Удосконалено метод універсального гешування на основі обчислення значення полінома над скінченним полем, який відрізняється від прототипу тим, що передбачає гешування повідомлення у n паралельних потоків суперблоками з n блоків з деяким ключем x з наступним гешуванням отриманих проміжних геш-значень з ключем x^n, що дозволило збільшити швидкодію у n разів, де n - число потоків. 2. Вперше запропоновано метод універсального гешування, який будується на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l, що дозволяє забезпечити імовірність колізії 1/(2^(l-1)) незалежно від довжини повідомлення, збільшити швидкодію приблизно у 2,5 разів у порівнянні з функцією гешування на основі обчислення значення полінома над скінченним полем, забезпечити невразливість до атак спостереження за часом виконання. 3. Вперше запропоновано метод універсального гешування, який будується на основі композиційної каскадної схеми і гешування на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l на обох каскадах, що дозволяє забезпечити більшу кількість ключів, які не належать до класів слабких ключів, у порівнянні з методом універсального гешування на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l. 4. Вперше запропоновано алгоритм паралельного універсального гешування на основі обчислення значення полінома над скінченним полем, який передбачає гешування повідомлення у n паралельних потоків суперблоками з n блоків з деяким ключем x з наступним гешуванням отриманих проміжних геш-значень з ключем x^n. 5. Вперше запропоновано алгоритм універсального гешування на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l, який використовує лише перетворення над кільцем цілих чисел модулю замість перетворень у полях. 6. Вперше запропоновано паралельний алгоритм універсального гешування, що реалізує композиційну каскадну схему і гешування на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l на обох каскадах. 7. Розроблені комплекси програмного забезпечення (програмні моделі), що реалізують розроблені методи універсального гешування в кільці цілих чисел за модулем 2^l. 8. Отримано ряд аналітичних співвідношень, які дозволяють зробити оцінки ймовірностей вибору слабких ключів для універсальних функцій гешування на основі обчислення значення полінома над скінченними полями та над кільцем цілих чисел за модулем 2^l. Наукова новизна. 1. Удосконалено метод універсального гешування на основі обчислення значення полінома над скінченним полем, який відрізняється від прототипу тим, що передбачає гешування повідомлення у n паралельних потоків суперблоками з n блоків з деяким ключем x з наступним гешуванням отриманих проміжних геш-значень з ключем x^n, що дозволило збільшити швидкодію у n разів, де n - число потоків. 2. Вперше запропоновано метод універсального гешування, який будується на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l, що дозволяє забезпечити імовірність колізії 1/(2^(l-1)) незалежно від довжини повідомлення, збільшити швидкодію приблизно у 2,5 разів у порівнянні з функцією гешування на основі обчислення значення полінома над скінченним полем, забезпечити невразливість до атак спостереження за часом виконання. 3. Вперше запропоновано метод універсального гешування, який будується на основі композиційної каскадної схеми і гешування на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l на обох каскадах, що дозволяє забезпечити більшу кількість ключів, які не належать до класів слабких ключів, у порівнянні з методом універсального гешування на основі обчислення значення полінома в кільці цілих чисел за модулем 2^l. Наукові теоретичні та практичні результати дисертаційної роботи можуть використовуватися при проектуванні створенні високошвидкісних засобів захисту інформації у комп'ютерних системах та мережах

2. Aim of research is analysis of existing, improvement and development of methods of new construction of authentication codes messages that would have greater compared with existing, speed while maintaining a given level of security. The object of the study is to process authentication data, based on the use of universal hashing functions based on polynomial value computation over finite fields and rings. The subject of research is the authentication methods of data with a given level of resistance based on polynomial value computation over finite fields and rings that allow to fulfill the requirements for message authentication codes, including the required collision resistance, difficulty finding preimage and second preimage, high performance, ease of implementation.

Research methods: the methods of game theory and information theory in the study of the mathematical model with data authentication and substantiation requirements for data authentication methods, methods of field theory and group methods of probability theory and mathematical statistics in determining the probability of weak keys and the methods of the theory of parallel computing in constructing and evaluation of the properties of parallel algorithms for hashing, methods of system analysis when compared to existing methods of authentication messages; software modeling in the implementation process of universal hashing. Theoretical and practical research results 1. The improvement of method of universal hashing based on polynomial value computation over a finite field, which is different from the prototype that involves hashing messages n in parallel streams superblock with n blocks with some key x followed by hashing the received intermediate hash-value of key x ^ n, which allowed to increase performance in n times, where n - number of threads, was proposed. 2. For the first time the method of universal hashing, which is based on calculating the value of a polynomial in the ring of integers modulo 2 ^ l, thus allowing for the probability of collisions 1 / (2 ^ (l-1)) regardless of the length of the message, increase the speed of approximately 2, 5 times as compared with the function hashing based on polynomial value computation over a finite field, provide invulnerability to attacks observation time performance, was proposed. 3. For the first time the method of universal hashing, which is based on compositional cascade scheme and hashing based on polynomial value computation in the ring of integers modulo 2 ^ l in both stages, which allows a greater number of keys that do not belong to the class of weak keys, in comparison with universal hashing method based on polynomial value computation in the ring of integers modulo 2 ^ l, was proposed. 4. For the first time algorithm of parallel universal hashing based on polynomial value computation over a finite field, involving hashing messages n parallel streams superblock with n blocks with some key x followed by hashing the received intermediate hash-value of key x ^ n, was proposed. 5. For the first time universal hashing algorithm based on calculating the value of a polynomial in the ring of integers modulo 2 ^ l, which uses only the transformation over the ring of integers modulo instead of changes in the fields, was proposed. 6. For the first time parallel algorithm universal hashing, realizing compositional cascade scheme and hashing based on polynomial value computation in the ring of integers modulo 2 ^ l in both stages, was proposed. 7. Software that implement the methods of universal hashing in the ring of integers modulo 2 ^ l was developed. 8. Some analytical relationships, which allows to estimate the probability of choosing weak keys for universal hashing functions based on polynomial value computation over finite fields and over the ring of integers modulo 2 ^ l, were developed. Scientific novelty. 1. The improvement of method of universal hashing based on polynomial value computation over a finite field, which is different from the prototype that involves hashing messages n in parallel streams superblock with n blocks with some key x followed by hashing the received intermediate hash-value of key x ^ n, which allowed to increase performance in n times, where n - number of threads, was proposed. 2. For the first time the method of universal hashing, which is based on calculating the value of a polynomial in the ring of integers modulo 2 ^ l, thus allowing for the probability of collisions 1 / (2 ^ (l-1)) regardless of the length of the message, increase the speed of approximately 2, 5 times as compared with the function hashing based on polynomial value computation over a finite field, provide invulnerability to attacks observation time performance, was proposed. 3. For the first time the method of universal hashing, which is based on compositional cascade scheme and hashing based on polynomial value computation in the ring of integers modulo 2 ^ l in both stages, which allows a greater number of keys that do not belong to the class of weak keys, in comparison with universal hashing method based on polynomial value computation in the ring of integers modulo 2 ^ l, was proposed. Scientific theoretical and practical results of the thesis can be used in the design of high-speed protection of information in computer systems and networks

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. Horbenko Ivan Dmytrovych

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

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Максимович Володимир Миколайович
2. Максимович Володимир Миколайович

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

Власне Прізвище Ім'я По-батькові:

1. Єсін Віталій Іванович

2. Єсін Віталій Іванович

Кваліфікація: к.т.н., 20.02.12

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.