Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0512U000385

Особливі позначки: відкрита

Дата реєстрації: 24-05-2012

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Лисицька Ірина Вікторівна
2. Lysytska Iryna Viktorivna

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор наук

Аспірантура/Докторантура: ні

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: 18-04-2012

Спеціальність за освітою: 7.080402

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): Д 64.052.01

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. Методологія оцінки стійкості блокових симетричних криптоперетворень на основі зменшених моделей

2. Methodology for assessing security of symmetric block crypto transformations based on reduced models

Реферат/анотація:

1. Об'єкт - процеси формування показників стійкості блокових симетричних шифрів (БСШ) до атак лінійного та диференціального крипто аналізу. Мета - розробка нової методології оцінки стійкості БСШ до атак диференціального і лінійного криптоаналізу, що базується на використанні зменшених моделей БСШ та моделюванні шифрувальних перетворень випадковими підстановками для прискореного отримання точних показників доказової стійкості БСШ. Методи: теорія ймовірностей, математична статистика - для дослідження показників випадковості підстановок і підстановочних перетворень (зменшених моделей шифрів) і для обробки результатів статистичних експериментів комбінаторика і системний аналіз - для обґрунтування запропонованої методики криптоаналізу БСШ на основі вивчення і порівняльної оцінки показників стійкості зменшених моделей та під час виконання досліджень комбінаторних властивостей підстановочних конструкцій; методи статистичних випробувань - під час виконання експериментальних досліджень за оцінкою ефективності використання підстановочних конструкцій різних типів у зменшених моделях ряду сучасних шифрів апарат Булевої алгебри ? для оцінки криптографічних показників S-блоків

ряду сучасних шифрів і S-блоків, сформованих за новим методом відбору випадкових підстановок. Апаратура - персональний комп'ютер. Теоретичні та практичні результати - розроблена нова методологія прискореного криптоаналізу, що будується, з одного боку, на основі оцінки властивостей і показників зменшених моделей прототипів, а з іншого - ?на доведеній можливості математичного моделювання шифрів випадковими підстановками та дозволяє вирішити протиріччя між неможливістю безпосереднього виміру показників стійкості БСШ до атак лінійного та диференціального криптоаналізу і необхідністю отримання оцінок відповідних показників з високим рівнем довіри у прийнятні часові терміни. Методологія має велике практичне значення для вдосконалення технологій блокового симетричного шифрування. Наукова новизна - вперше запропоновано та обґрунтовано методологію оцінки стійкості БСШ до атак лінійного та диференціального криптоаналізу, яка передбачає використання сукупності шести методів для формування висновків стосовно рівня доказової безпеки шифрів, що дозволило істотно прискорити процес виконання експертизи і порівняння рішень під час побудови алгоритмів БСШ; вперше запропоновано метод оцінки стійкості БСШ до атак лінійного та диференціального криптоаналізу, який передбачає використання для формування висновків стосовно рівня доказової безпеки шифрів показників їх зменшених моделей, що дозволило на основі аналізу показників зменшених моделей визначити показники стійкості великих прототипів; вперше запропоновано метод оцінки показників доказової безпеки БСШ до атак диференціального й лінійного криптоаналізу, що будується на основі використання показників випадкових підстановок відповідного степеня, який не пов'язаний з показниками нелінійних перетворень (S-блоків) шифрів, що дозволило значно спростити процес знаходження показників доказової безпеки сучасних БСШ до атак лінійного та диференціального криптоаналізу; вперше встановлено принцип формування максимумів повних диференціалів та лінійних корпусів БСШ, який ґрунтується на придбанні шифром властивостей випадкової підстановки зі збільшенням кількості циклів, що дає можливість визначати показники доказової безпеки на основі використання показників випадкових підстановок; вперше запропоновано метод швидкої оцінки лінійних та диференціальних показників сучасних БСШ, який передбачає використання спрощених співвідношень для розрахунку максимальних значень диференціальної та лінійної ймовірностей випадкової підстановки відповідного степеня, що дозволяє підвищити швидкість отримання показників доказової безпеки БСШ до атак диференціального та лінійного криптоаналізу; вперше запропоновано два методи оцінки стійкості БСШ до атак диференціального і лінійного криптоаналізу AMDP та AMLHP, які передбачають розрахунки середнього значення максимуму диференціальної ймовірності та середнього значення максимуму ймовірності лінійного корпусу, що дозволяє більш адекватно відображати показники доказової стійкості шифрів; вперше запропоновано метод оцінки якості криптографічних перетворень на основі визначення кількості циклів, які потрібні БСШ для набуття властивостей випадкової підстановки, що дає можливість порівнювати БСШ під час виконання експертизи та перевірки окремих рішень; набула подальшого розвитку математична модель випадкової підстановки в частині доведення ряду теорем щодо виразу для закону розподілу зміщень таблиць лінійних апроксимацій, що, на відміну від існуючих підходів, дозволило розрахунковим шляхом отримати значення максимумів лінійних корпусів шифрів і за рахунок цього суттєво прискорити процес визначення показників їх доказової безпеки до атак лінійного криптоаналізу; набула подальшого розвитку математична модель випадкової підстановки в частині встановлення зв'язків між сусідніми значеннями законів розподілу переходів XOR таблиць та зміщень таблиць лінійних апроксимацій випадкових підстановок, які подані у вигляді простих співвідношень, що дозволило отримати більш придатне для обчислення подання закону розподілу переходів XOR таблиць, та встановити істотно більш складний рівень проведення атак лінійного криптоаналізу відносно атак диференціального криптоаналізу; набула подальшого розвитку математична модель випадкової підстановки в частині формування додаткових критеріїв відбору підстановок, яка, на відміну від існуючих підходів, використовує порівняння емпіричних законів розподілу переходів диференціальних таблиць та зміщень таблиць лінійних апроксимацій підстановок з теоретичними, що дало можливість посилити вимоги до перевірки шифрувальних перетворень на відповідність властивостям випадкових підстановок. Результати реалізовані в системах криптографічного захисту інформації під час виконання ряду НДР та ДКР у ЗАТ

"Інститут інформаційних технологій" (акт впровадження від 24.10.2011 р.), а також використані в навчальному процесі кафедри безпеки інформаційних технологій Харківського національного університету радіоелектроніки (акт впровадження від 7.10.2011 р.) та при формуванні та реалізації нових навчальних програм кафедри захисту інформації Запорізького національного технічного університету (акт впровадження від 12.10.2011 р.). Наукові та практичні результати роботи можуть бути використані в організаціях: які займаються проектуванням та конструюванням засобів захисту інформації для уточнення показників алгоритмів шифрування, які вже експлуатуються; а також при проектуванні та розробці нових конструкцій БСШ; які займаються експертизою та оцінкою проектних та конструкторських рішень щодо побудови сучасних БСШ, у тому числі комісіями при проведенні конкурсів по відбору перспективних рішень.

2. Object - the formation process of security characteristics for symmetric block cipher (SBC) to linear and differential cryptanalysis. Purpose - a development of a new methodology for the security assessment of SBC to differential and linear cryptanalysis based on the application of scaled models of SBC and simulation of encryption transformations by random permutations for fast obtaining of provable SBC security indicators. Methods include probability theory, mathematical statistics for researching the randomness of permutations and permutation transformations (scaled models of ciphers) and for processing the results of statistical experiments; combinatorics and system analysis for substantiations of proposed cryptanalysis method based on the research and comparative evaluation of security characteristics and reduced models during the research of substitution structures combinatorial properties, methods of statistical tests - during the initial research for evaluation of efficiency substitution designs and different types of reduced models of a number of modern ciphers; Boolean algebra to assess the performance of cryptographic S-blocks of some modern ciphers and S-blocks generated by the new method of selection of random permutations. Equipment - the personal computer. Theoretical and practical results: it is developed a new methodology for fast cryptanalysis, which is based on the one hand, by assessing the characteristics and parameters of model prototypes, on the other, on the proven capabilities of mathematical modeling ciphers and random permutations can solve the contradiction between the impossibility of direct measurement of security characteristics of SBC to linear attacks and differential cryptanalysis and the need to obtain estimates of relevant parameters with a high level of confidence in acceptable time limits. The methodology is of great practical value for improving the technology of block symmetric encryption. Scientific novelty: first proposed and verified methodology for assessing the security of SBC to linear attacks and differential cryptanalysis, which involves the use of combination of six methods for forming opinions on the level of evidence of secure ciphers, thereby greatly accelerate the process of research and comparison of solutions in the building block algorithms for symmetric encryption, first proposed method for assessing the security of SBC to linear attacks and differential cryptanalysis, which involves the application to form opinions on the level of evidence of secure ciphers indicators of reduced models that allowed for the analysis of model performance indicators to determine the security of large prototypes, first proposed method for assessing the performance of evidence-based security SBC to differential attacks and linear cryptanalysis, which is based on random permutations of indices corresponding degree, which is not related to performance of nonlinear transformations (S-block) codes that greatly simplify the process of finding the parameters of evidence security modern SBC to linear and differential attacks crypto analysis first established the principle of formation of maxima of complete differentials and linear hulls symmetric block cipher based on the purchase of a random permutation cipher properties with increasing number of cycles, which makes it possible to determine the parameters of evidence-based security through the use of random parameters substitutions, the first time the method rapid estimation of linear and differential parameters of modern symmetric block ciphers, which involves the use of simplified relations for calculating the maximum values of the differential and linear probabilities of a random permutation corresponding degree, which can increase the speed of obtaining evidence of safety indicators symmetric block cipher to differential attacks and linear crypto analysis, first proposed two methods for evaluating the stability of symmetric block cipher to differential attacks and linear cryptanalysis AMDP and AMLHP, involving calculations of the average maximum differential probability and the average maximum likelihood linear body, allowing more adequately reflect the performance of evidence-based resistance codes, first proposed method of assessing the

quality of cryptographic transformations on the basis of determining the number of cycles required for the acquisition of properties SBC random permutation, which makes it possible to compare SBC during the examination and verification of individual solutions, has acquired the further development of mathematical model of a random permutation in terms of bringing a number of theorems concerning the expression for the law displacement distribution tables of linear approximations, in contrast to existing approaches, allowed calculation obtain the maximum linear buildings codes and thus significantly speed up the determination of their evidence-based security to attack crypto linear analysis came the further development of mathematical model in a random permutation of the set relations between neighboring values of distribution laws XOR conversion tables and linear approximations of displacements tables of random permutations, which are presented in the form of simple ratios, allowing to obtain more suitable for calculating representation of the distribution XOR conversion tables, and set much more difficult level of linear cryptanalysis attacks differential attacks against crypto analysis gained further development of mathematical model in a random permutation of the establishment of additional criteria for selecting substitutions that unlike existing approaches using empirical comparison of distribution laws differential conversion tables and linear approximations of displacements table lookup with the theoretical, making it possible to strengthen the requirements for verification of cryptographic transformations to match the properties of random permutations. The results are implemented in the cryptographic protection of information in the course of several research and development activity in JSC "Institute of Information Technologies" (the act of implementation of 24.10.2011), and also used in the learning process of the information technologies security Department at National University of Radio Electronics (the act of implementation of 10/07/2011 City) and the formation and implementation of new curriculum department of information security Zaporizhzhya National Technical University (act introduction of 12.10.2011). Scientific and practical results of the thesis can be used: in organizations that are engaged in designing and constructing information security for the performance specification encryption algorithms that are already operating, as well as designing and developing new designs SBC, in organizations that are engaged in examination and evaluation of project and design solutions for building modern SBC, including commissions during the competitions for the selection of perspective solutions.

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. Ковальчук Людмила Василівна
2. Ковальчук Людмила Василівна

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. 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. Мороз Борис Іванович

2. Мороз Борис Іванович

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 Бондаренко Михайло Федорович

Власне Прізвище Ім'я По-батькові головуючого на засіданні Бондаренко Михайло Федорович

Відповідальний за підготовку облікових документів

Реєстратор

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