Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0421U102567

Особливі позначки: відкрита

Дата реєстрації: 31-05-2021

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Ігнатенко Сергій Михайлович
2. Ihnatenko Serhii M.

Кваліфікація:

Ідентифікатор ORCHID ID: Не застосовується

Вид дисертації: кандидат наук

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: 22-04-2021

Спеціальність за освітою: Безпека інформації в спеціальних інформаційних системах

Місце роботи здобувача:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Сектор науки: Не застосовується

III. Відомості про дисертацію

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): Д 64.051.29

Повне найменування юридичної особи: Харківський національний університет імені В. Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: майдан Свободи, буд. 4, м. Харків, Харківський р-н., Харківська обл., 61022, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Сектор науки: Не застосовується

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

Повне найменування юридичної особи: Харківський національний університет імені В. Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: майдан Свободи, буд. 4, м. Харків, Харківський р-н., Харківська обл., 61022, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Сектор науки: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 50.37.23

Тема дисертації:

1. Методи розв'язання задачі LPN над скінченними кільцями для оцінювання стійкості симетричних постквантових шифросистем

2. Methods for solving the LPN problem over finite rings to evaluate the security of symmetric post-quantum cryptosystems

Реферат:

1. У дисертації розв'язано актуальну наукову задачу розробки більш ефективних (в порівнянні з перебірним) методів розв'язання задачі LPN над скінченними кільцями для оцінювання стійкості симетричних постквантових шифросистем. Вперше отримано аналітичні оцінки обсягу матеріалу, достатнього для розв'язання із заданою достовірністю задачі LPN над довільним скінченним кільцем, які дозволяють визначити часову складність узагальненого алгоритму BKW. Розроблено два методи підвищення ефективності розв'язання задачі LPN за допомогою ММП. Вперше розроблено метод побудови нових алгоритмів розв'язання СР над кільцем за довільною скінченною сукупністю вхідних таких алгоритмів.

Наведено аналітичні вирази оцінок достовірності та часової складності алгоритмів розв'язання СР, які будуються за допомогою розробленого методу, через відповідні характеристики вхідних алгоритмів. Головним практичним результатом роботи є можливість оцінювати стійкість симетричних шифросистем, які будуються над скінченними кільцями та базуються на складності розв'язання задачі LPN. Ключові слова: симетрична постквантова шифросистема, задача LPN, часова складність алгоритму, метод максимуму правдоподібності, узагальнений алгоритм BKW, скінченне кільце, обґрунтування стійкості, система лінійних рівнянь зі спотвореними правими частинами.

2. This thesis is devoted to solving the actual scientific problem of development more effective methods (in comparison with brute force method) of solving the LPN problem over finite rings for evaluation of the security of post-quantum symmetric cryptosystems. Analysis of available scientific publications was carried out. It showed that in spite of the considerable progress in the development of fast methods (more effective in comparison with brute force method) for solving the LPN problem over a field of two elements or some residue rings, the question of the existence of such methods in case of arbitrary finite ring remains open. To date, there are not even noasymptotic estimates of the amount of material sufficient to solve the LPN problem over an arbitrary finite ring properly. The problem of the noasymptotic time complexity of the generalized BKW algorithm, which is a natural extension of one of the best methods for solving the LPN problem over a two-element field in case of arbitrary finite ring, remains unresolved. As a result, the security of many symmetric cryptosystems over finite rings (by analogy with known cryptosystems based on the complexity of the classical LPN problem solving over the field) remains undefined, which holds back the practical application of these cryptosystems in modern information and telecommunication systems. Analytical estimates of the amount of material sufficient to solve the LPN problem over an arbitrary finite ring properly, that generalize a similar estimate known for the classical LPN problem and allow to determine the time complexity of the generalized BKW algorithm, a known prototype of which is currently one of the most effective algorithms for solving the classical LPN problem are obtained for the first time. The maximum likelihood method for solving the LPN problem over finite Frobenius rings has been improved based on the fast Fourier transform using, which allows to significantly reduce the time complexity of the LPN problem solving over Frobenius rings, using both the MLM itself and other algorithms that use MLM as an auxiliary procedure. The maximum likelihood method for solving the LPN problem over residue rings modulo has been improved based on the Fermat number transforms, which enables to significantly reduce the time complexity of the LPN solving using a generalized BKW algorithm. The method for developing new algorithms for solving the LPN problem over residue rings modulo for an arbitrary finite set of inputs of such algorithms obtained for the first time. It makes it possible to increase the effectiveness of solving this problem by properly selecting a composition of the N number. New scientific and practical results presented in this thesis allow: – to purposefully choose the values of the parameters of post-quantum symmetric cryptosystems over finite rings, which guarantee their security against known attacks; – to reduce (from several times to several dozen orders) the time complexity of solving the LPN problem over finite rings using the maximum likelihood method, as well as the generalized BKW algorithm; – to establish and prove the inexpediency (from the cryptographic security point of view) of the practical application of LPN-C type encryption systems over the residue ring modulo where ; – to increase the effectiveness of known attacks on the Ring-LWE encryption system from to times (depending on the encryption system parameters); – to increase the effectiveness of correlation attacks on SNOW 2.0-like stream ciphers over residue rings modulo from to times (depending on the value and gamma generator length); – to build SNOW 2.0-like stream ciphers over residue rings modulo , which are reasonably secure against known correlation attacks, in particular, to increase the resistance of SNOW 2.0 cipher from to operations (with increasing of the amount of required material from to) by completely replacement from boolean bitwise addition in the gamma generator scheme to addition modulo . Keywords: symmetric post-quantum cryptosystem, LPN problem, time complexity of the algorithm, maximum likelihood method, generalized BKW algorithm, finite ring, security proving, system of linear equations corrupted by noise.

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. Кузнецов Олександр Олександрович
2. Kuznetsov Oleksandr Oleksandrovych

Кваліфікація: 05.13.21

Ідентифікатор ORCHID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Сектор науки: Не застосовується

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Кудін Антон Михайлович
2. Kudin Anton M.

Кваліфікація: 05.13.21

Ідентифікатор ORCHID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Сектор науки: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Василіу Євген Вікторович

2. Vasiliu Yevhen V.

Кваліфікація: 05.13.21

Ідентифікатор ORCHID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Сектор науки: Не застосовується

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Потій Олександр Володимирович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Олійников Роман Васильович
Відповідальний за підготовку облікових документів	
Реєстратор	

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Т.А.