# Облікова картка дисертації

## I. Загальні відомості

**Державний обліковий номер:** 0821U102260

**Особливі позначки:** відкрита

**Дата реєстрації:** 02-09-2021

**Статус:** Захищена

**Реквізити наказу МОН / наказу закладу:**

## II. Відомості про здобувача

**Власне Прізвище Ім'я По-батькові:**

1. Вамболь Олексій Сергійович

2. Vambol Oleksii Serhiiovych

**Кваліфікація:**

**Ідентифікатор ORCID ID:** Не застосовується

**Вид дисертації:** доктор філософії

**Аспірантура/Докторантура:** так

**Шифр наукової спеціальності:** 122

**Назва наукової спеціальності:** Комп'ютерні науки

**Галузь / галузі знань:**

**Освітньо-наукова програма зі спеціальності:** Не застосовується

**Дата захисту:** 27-08-2021

**Спеціальність за освітою:** Спеціалізовані комп'ютерні системи

**Місце роботи здобувача:**

**Код за ЄДРПОУ:**

**Місцезнаходження:**

**Форма власності:**

**Сфера управління:**

**Ідентифікатор ROR:** Не застосовується

## III. Відомості про організацію, де відбувся захист

**Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради):** ДФ 64.062.008

**Повне найменування юридичної особи:** Національний аерокосмічний університет ім. М. Є. Жуковського "Харківський авіаційний інститут"

**Код за ЄДРПОУ:** 02066769

**Місцезнаходження:** вул. Чкалова, буд. 17, м. Харків, Харківський р-н., Харківська обл., 61070, 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:** Національний аерокосмічний університет ім. М. Є. Жуковського "Харківський авіаційний інститут"

**Код за ЄДРПОУ:** 02066769

**Місцезнаходження:** вул. Чкалова, буд. 17, м. Харків, Харківський р-н., Харківська обл., 61070, Україна

**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. Математичні методи криптоаналізу і підвищення продуктивності асиметричних шифрів зі спеціальними властивостями

2. Mathematical methods of cryptanalysis and increasing the performance of asymmetric ciphers with special properties

**Реферат/анотація:**

1. Дисертація присвячена розробленню математичних методів криптоаналізу нових асиметричних шифрів зі спеціальними властивостями, а також створенню математичних методів підвищення продуктивності складових зазначених шифрів. В даній роботі таким шифрами називаються асиметричні схеми шифрування, що мають корисні властивості, які в цілому не притаманні цьому класу шифрів, і, відповідно, ширші сфери застосування у порівнянні з тими, що випливають з визначення асиметричної схеми шифрування. Прикладами цих властивостей є гомоморфність, постквантовість і завадостійкість. Метою дослідження є визначення властивостей і криптостійкості ранцевого шифру на основі матриць, а також підвищення продуктивності складових частин фонтанного QC-MDPC шифру Мак-Еліса. Досягнення цієї мети було

здійснено шляхом вирішення таких задач: визначити кількісні властивості ранцевого шифру на основі матриць, які включають часові складності зашифрування, розшифрування і генерації пари ключів, розміри відкритого та секретного ключів, а також коефіцієнт розширення шифротексту і рівень безпеки проти атак повного перебору; визначити наявність властивості адитивної гомоморфності для ранцевого шифру на основі матриць; розробити метод криптоаналізу ранцевого шифру на основі матриць, ефективніший за атаку повного перебору, та визначити його обчислювальну складність; розробити метод генерації робастного розподілу солітона, продуктивніший за стандартний; впровадити результати досліджень. Ці задачі були вирішені з використанням методів абстрактної алгебри (теорії кінцевих полів, теорії груп), лінійної алгебри, теорії ймовірностей, математичної статистики і теорії складності обчислень. Дисертаційне дослідження має такі наукові результати. Вперше для ранцевого шифру на основі матриць були визначені кількісні властивості, які включають часові складності зашифрування, розшифрування та генерації пари ключів, розміри відкритого і секретного ключів, а також коефіцієнт розширення шифротексту і рівень безпеки проти атак повного перебору. Цей результат необхідний для обґрунтовування рішень про доцільність використання даного шифру. Вперше для ранцевого шифру на основі матриць була доведена властивість адитивної гомоморфності. Даний результат вказує на можливість використання цього шифру для побудови протоколу таємного електронного голосування. Вперше були запропоновані поліноміально-складні методи криптоаналізу ранцевого шифру на основі матриць. Дані атаки роблять можливим відновлення відкритого тексту з шифротексту даної криптосистеми за відсутності секретного ключа. Вказаний результат обґрунтовує висновок про недоцільність використання цього шифру в якості інструменту забезпечення конфіденційності і таким чином дозволяє виключити ризики інформаційної безпеки, обумовлені застосуванням даної криптосхеми. Перелік цих ризиків можна скласти за допомогою перших двох результатів. Вперше був запропонований мажорантно-суперпозиційний метод генерації робастного розподілу солітона. Вказаний метод відрізняється від стандартного середньою часовою складністю, яка становить O(1) за умови невикористання довгої арифметики. Застосування пропонованого методу дозволяє підвищити в декілька разів продуктивність генерації робастного розподілу солітона кодером завадостійких кодів LT, які використовуються фонтанним QC-MDPC шифром Мак-Еліса. Насамперед зазначений результат має практичну цінність для сфери імітаційного моделювання. Ранцевий шифр на основі матриць і запропонована атака на нього були програмно реалізовані у вигляді динамічно приєднуваної бібліотеки MBKCLib та додатків, які надають можливість використовувати та хронометрувати її засоби. Запропонований та стандартний методи генерації робастного розподілу солітона були програмно реалізовані у вигляді динамічно приєднуваної бібліотеки RSDLib та додатку RSDTest, призначеного для перевірки коректності вказаних методів за допомогою критерію узгодженості Пірсона та дослідження їхньої продуктивності. Отримані результати було впроваджено в міжнародному проекті «TEMPUS SEREIN: Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains», двох державних НДР, а також у навчальному процесі кафедри комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут». Матеріали дисертації увійшли в якості складових частин у три звіти з НДР та розділ підручника, розробленого в рамках зазначеного проекту. Матеріали дисертації були опубліковані в періодичних наукових виданнях у вигляді 6 статей, три з яких індексуються в Scopus, та збірниках праць наукових конференцій у формі 2 індексованих в Scopus статей.

2. The thesis is devoted to developing the mathematical methods of cryptanalysis of new asymmetric ciphers with special properties and creating the mathematical methods of increasing the performance of the components of the given ciphers. In accordance with the terminology used in this study, such ciphers are the asymmetric encryption schemes that possess useful properties generally not inherent in this class of ciphers and thus have wider application area in comparison with the one arising from the definition of an asymmetric encryption scheme. Homomorphity, post-quantumness and noise immunity are the examples of these properties. The aim of the thesis is to determine the properties and cryptographic strength of the matrix-based knapsack cipher, as well as to increase the performance of the components of the fountain QC-MDPC McEliece cipher. This aim has been

achieved by means of solving the following tasks: determine the quantitative properties of the matrix-based knapsack cipher, which include the time complexities of encryption, decryption and key pair generation, the sizes of the public and private keys, the ciphertext expansion factor and the level of security against a brute-force attack; determine for the matrix-based knapsack cipher the presence of the property of additive homomorphity; develop such a method of cryptanalysis of the matrix-based knapsack cipher that is more efficient than a brute-force attack and determine the computational complexity of the method developed; develop such a method for generating a robust soliton distribution that has better performance than the standard method; implement research results. These tasks have been solved using the methods of abstract algebra (the theory of finite fields, the group theory), linear algebra, probability theory, mathematical statistics and the theory of computational complexity. The research has yielded the following scientific results. For the first time, the quantitive properties of the matrix-based knapsack cipher have been determined. The properties, which have been considered, include the time complexities of encryption, decryption and key pair generation, the sizes of the public and private keys, the ciphertext expansion factor and the level of security against a brute-force attack. This result is required to substantiate decisions about expediency of using the given cipher. For the first time, the property of additive homomorphity for the matrix-based knapsack cipher has been proved. The given result indicates the possibility of using this cipher to build a protocol of secret e-voting. For the first time, polynomial-time methods of cryptanalysis of the matrix-based knapsack cipher have been proposed. These attacks permit recovering the plaintext from the ciphertext of the given cryptosystem in the absence of the secret key. The aforesaid result substantiates the conclusion about inexpediency of using this cipher as a privacy tool and thus permits eliminating the information security risks, which arise from the use of the given cryptoscheme. A list of these risks can be made using the first two results. For the first time, the majorant-superposition method for generating a robust soliton distribution has been proposed. This method differs from the standard one in time complexity, which is O(1) provided that long arithmetics is not used. Applying the proposed method permits increasing several times the performance of generating a robust soliton distribution by the encoder of the LT error-correction codes, which are used in the fountain QC-MDPC McEliece cipher. First of all, the given result is of practical significance for simulation modeling. The matrix-based knapsack cipher and the proposed attack on it have been software implemented as the dynamic link library MBKCLib and applications, which permit using and timing its facilities. The proposed and standard methods for generating a robust soliton distribution have been software implemented as the dynamic link library RSDLib and application RSDTest, which has been designed for verification of correctness of the given methods by means of the Pearson's goodness-of-fit test and for investigation of their performance. The obtained results have been implemented in the international project «TEMPUS SEREIN: Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains», two state scientific-research works, as well as in the education process of the Department of Computer Systems, Networks and Cybersecurity of National Aerospace University «Kharkiv Aviation Institute». The thesis materials have been included as components in three scientific-research reports and the textbook developed within the framework of the aforementioned project. The thesis materials have been published in scientific periodicals as 6 articles, three of which are Scopus publications, as well as in proceedings of scientific conferences as 2 papers indexed in Scopus.

**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. Харченко Вячеслав Сергійович
2. Kharchenko Vyacheslav Serhiiovych

**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

## VII. Відомості про офіційних опонентів та рецензентів

**Офіційні опоненти**

**Власне Прізвище Ім'я По-батькові:**

1. Кузнецов Олександр Олександрович
2. Kuznetsov Oleksandr Oleksandrovych

**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. Казимир Володимир Вікторович

2. Kazymyr Volodymyr Viktorovych

**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**

**Власне Прізвище Ім'я По-батькові:**

1. Шостак Ігор Володимирович

2. Shostak Igor Volodymyrovych

**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

**Власне Прізвище Ім'я По-батькові:**

1. Морозова Ольга Ігорівна

2. Morozova Olha Ihorivna

**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

## VIII. Заключні відомості

**Власне Прізвище Ім'я По-батькові голови ради** Чухрай Андрій Григорович

**Власне Прізвище Ім'я По-батькові головуючого на засіданні** Чухрай Андрій Григорович

**Відповідальний за підготовку облікових документів**

**Реєстратор**

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