Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0526U000042

Особливі позначки: відкрита

Дата реєстрації: 23-02-2026

Статус: Запланована

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Якименко Ігор Зіновійович
2. Ihor Yakymenko

Кваліфікація: к. т. н., доц., 05.13.21

Ідентифікатор ORCID ID: 0000-0003-2586-6196

Вид дисертації: доктор наук

Аспірантура/Докторантура: ні

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: 05-03-2026

Спеціальність за освітою: Кібербезпека

Місце роботи здобувача: Західноукраїнський національний університет

Код за ЄДРПОУ: 33680120

Місцезнаходження: вул. Львівська, Тернопіль, Тернопільський р-н., 46009, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): Д 26.861.05

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, Київ, 03110, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

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

Повне найменування юридичної особи: Західноукраїнський національний університет

Код за ЄДРПОУ: 33680120

Місцезнаходження: вул. Львівська, Тернопіль, Тернопільський р-н., 46009, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.56.02

Тема дисертації:

1. Методи та засоби криптографічного захисту інформації на основі системи залишкових класів
2. Methods and means of cryptographic information protection based on the residual number system

Реферат:

1. У дисертаційній роботі вирішується науково-прикладна проблема розробки методів, засобів та методології криптографічного захисту інформації на основі цілочисельної, модифікованої досконалої форми, поліноміальної та ієрархічної систем залишкових класів. Проблема вирішується у спосіб розробки та реалізації комплексного наукового підходу, в якому криптографічні перетворення виконуються в СЗК та її похідних формах (цілочисельній, модифікованій досконалій, поліноміальній та ієрархічній), а обчислювально затратні операції множення/піднесення до степеня реалізуються через операції додавання із застосуванням векторно-модульних алгоритмів модулярного множення та експоненціювання. Для вирішення поставлених завдань в дисертаційній роботі застосовуються методи основ алгебри і теорії чисел, теорії алгоритмів, методів криптографії та програмування, теорії множин та статистики. Розроблено симетричний криптоалгоритм у системі залишкових класів, який за рахунок розбиття відкритого повідомлення на залишки по відповідних попарно взаємнопростих модулях (ключах) та використання

китайської теореми про залишки дозволяє розпаралелити обчислювальний процес, зменшити розмірність операндів та на основі побудованих аналітичних виразів встановити розрядність та кількість модулів системи залишкових класів для забезпечення такої ж стійкості, як і сучасний симетричний криптоалгоритм AES-256. Розроблено високопродуктивні симетричні та асиметричні криптоалгоритми на основі системи залишкових класів та її модифікованої досконалої форми, які за рахунок довільної заміни базисних чисел в процесі шифрування на попарно взаємнопрості з відповідними модулями додаткові ключі дозволяють підвищити криптостійкість та забезпечити необхідний рівень захисту інформаційних потоків. Розроблено криптографічний алгоритм, в якому за рахунок шифрування відкритого тексту у вигляді залишків за допомогою китайської теореми про залишки і розшифрування на основі операції пошуку залишків за відповідними модулями забезпечується підвищення швидкості розшифрування інформації без втрати стійкості алгоритму. Розроблено одно- та двоключові симетричні криптографічні методи в поліноміальній системі залишкових класів, які за рахунок заміни в процесі шифрування базисних поліномів на довільно вибрані попарно взаємнопрості з модулями поліноми дозволяють створити додаткову структурну неоднозначність, ускладнити криптоаналіз через необхідність розв'язання NP-повної задачі та збільшити криптографічну стійкість. Розроблено симетричні методи шифрування/розшифрування інформаційних потоків в ієрархічній цілочисельній та поліноміальній системах залишкових класів, які за рахунок представлення зашифрованого тексту наборами залишків за відповідними модулями (ключами) та розпаралелення процесу обчислень дозволяють підвищити стійкість криптоалгоритму та збільшити його швидкодію. Розроблено методологію криптографічного захисту інформації в системі залишкових класів, яка за рахунок застосування векторно-модульних методів модулярного множення та експоненціювання, цілочисельної, модифікованої досконалої форми, поліноміальної та ієрархічної систем залишкових класів дає змогу забезпечити збільшення стійкості, зменшення часової складності, підвищення швидкодії алгоритмів, спеціалізованого програмного забезпечення та побудувати єдину стратегію криптографічного захисту інформаційних потоків на основі системи залишкових класів. Удосконалено методи відновлення полінома за його залишками в кільці Z[x], які за рахунок використання операції додавання добутку модулів або їх залишків за відповідними модулями дозволяють уникнути обчислювально громіздкої процедури пошуку мультиплікативного оберненого полінома, що, в свою чергу, призводить до збільшення швидкодії та зменшення часової складності поліноміальних алгоритмів шифрування. Набув подальшого розвитку метод пошуку оберненого полінома в кільці Z[x] на основі методу невизначених коефіцієнтів, який за рахунок усунення операції пошуку найбільшого спільного дільника двох поліномів дозволив зменшити часову складність та підвищити швидкодію алгоритму при його використанні в поліноміальних криптосистемах. Набули подальшого розвитку поліноміальний, дво- та тримодульний цілочисельні асиметричні криптосистеми Рабіна, які за рахунок заміни операції множення на операцію додавання та використання векторно-модульного методу модулярного множення дозволяють зменшити часову складність криптографічних перетворень і підвищити швидкодію реалізації алгоритмів. Основні результати впроваджено у АТ «Тернопільобленерго» (№5291/24 від 17.12.2025 р.), ТзОВ НВФ «Інтеграл» (№03-07/2025 від 07.03.2025 р.), ТзОВ завод «Ремпобуттехніка» (№ЦКБ/04-25 від 10.02.2025 р.), Управлінні кібербезпеки та цифрового розвитку відділу цифрової трансформації Міністерства енергетики України, Департаменті Бюро економічної безпеки України (від 12.01.2025 р.), використані при виконанні п'яти науково-дослідних робіт у Західноукраїнському національному університеті (ЗУНУ) акт впровадження від 05.12.2025 р.

2. The dissertation addresses a scientific and applied problem focused on the development of methods, tools, and a comprehensive methodology for cryptographic information protection based on integer, modified perfect form, polynomial, and hierarchical residue number systems. The problem is solved through the development and implementation of an integrated scientific approach in which cryptographic transformations are performed within the RNS and its derivative forms (integer, modified perfect, polynomial, and hierarchical), while computationally expensive multiplication and exponentiation operations are implemented via addition using vector–modular algorithms for modular multiplication and exponentiation. To solve the stated tasks, the dissertation employs methods of algebra and number theory, algorithm theory, cryptography and programming, set theory, and

statistics. A symmetric cryptographic algorithm in the residue number system has been developed which, by decomposing the plaintext into residues with respect to corresponding pairwise coprime moduli (keys) and applying the Chinese Remainder Theorem, enables parallelization of the computational process, reduction of operand dimensionality, and, based on derived analytical expressions, determination of the bit-length and the number of RNS moduli required to achieve security equivalent to that of the modern symmetric cryptographic algorithm AES-256. High-performance symmetric and asymmetric cryptographic algorithms based on the residue number system and its modified perfect form have been developed. By allowing arbitrary replacement of basis numbers during the encryption process with additional keys that are pairwise coprime with the corresponding moduli, these algorithms increase cryptographic strength and ensure the required level of protection of information flows. A cryptographic algorithm has been developed in which encryption of the plaintext is performed in the form of residues using the Chinese Remainder Theorem, and decryption is carried out based on the operation of residue reconstruction with respect to the corresponding moduli, thereby increasing decryption speed without loss of algorithmic security. Single-key and dual-key symmetric cryptographic methods in the polynomial residue number system have been developed. Through the replacement, during encryption, of basis polynomials with arbitrarily selected polynomials that are pairwise coprime with the moduli, these methods introduce additional structural ambiguity, complicate cryptanalysis due to the necessity of solving an NP-complete problem, and increase cryptographic strength. Symmetric methods for encryption and decryption of information flows in hierarchical integer and polynomial residue number systems have been developed; by representing the ciphertext as sets of residues with respect to the corresponding moduli (keys) and by parallelizing computations, these methods enhance the security of the cryptographic algorithm and increase its performance. A methodology for cryptographic information protection in residue number systems has been developed. By applying vector–modular methods of modular multiplication and exponentiation, as well as integer, modified perfect, polynomial, and hierarchical residue number systems, the proposed methodology ensures increased security, reduced time complexity, improved algorithmic performance, development of specialized software, and the establishment of a unified strategy for cryptographic protection of information flows based on residue number systems. Methods for reconstructing a polynomial from its residues in the ring Z[x] have been improved. By using the operation of adding the product of moduli or their residues with respect to the corresponding moduli, these methods avoid the computationally intensive procedure of finding a multiplicative inverse polynomial, which in turn increases performance and reduces the time complexity of polynomial encryption algorithms. The method for finding an inverse polynomial in the ring ?[?] based on the method of undetermined coefficients has been further developed; by eliminating the operation of computing the greatest common divisor of two polynomials, the time complexity is reduced and the performance of the algorithm in polynomial cryptosystems is improved. The polynomial, two-module, and three-module integer asymmetric Rabin cryptosystems have been further developed, enabling reduced computational complexity of cryptographic transformations and enhanced algorithmic performance by replacing multiplication with addition and utilizing a vector-modular method for modular multiplication.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки: Інформаційні та комунікаційні технології

Стратегічний пріоритетний напрям інноваційної діяльності: Розвиток сучасних інформаційних, комунікаційних технологій, робототехніки

Підсумки дослідження: Теоретичне узагальнення і вирішення важливої наукової проблеми

Публікації:

- 1. Yakymenko I., Kasianchuk M., Martyniuk O., Martyniuk S. A Symmetric Cryptoalgorithm Based on a Hierarchical Residue Number System. International Journal of Computing, 2025. 24(1), pp. 92-101. https://doi.org/10.47839/ijc.24.1.3880 (Scopus)

- 2. Yakymenko I., Karpinski M., Shevchuk R., Kasianchuk M. Symmetric Encryption Algorithms in a Polynomial Residue Number System. Journal of Applied Mathematics., 2024, pp. 1-12. DOI:10.1155/2024/4894415 (Scopus).
- 3. Nykolaychuk Ya., Yakymenko I., Vozna N., Kasianchuk M. Residue Number System Asymmetric Cryptoalgorithms. Cybernetics and Systems Analysis. 2022, Vol. 58, No. 4, P.611-618. http://jnas.nbuv.gov.ua/article/UJRN-0001335526. https://doi.org/10.1007/s10559-022-00494-7. (Scopus).
- 4. Shevchuk R., Yakymenko I., Karpinski M., Shylinska I., Kasianchuk M. Finding the inverse of a polynomial modulo in the ring Z[x] based on the method of undetermined coefficients. Computer Science. vol. 25. no. 2. 2024. pp.1-14. DOI:10.7494/csci.2024.25.2.5740 (Scopus).
- 5. M. M. Kasianchuk, I. Z. Yakymenko, Ya. M. Nykolaychuk Symmetric Cryptoalgorithms in the Residue Number System. Cybernetics and Systems Analysis, 2021, Vol 57, Issue 2, p.184-189. https://doi.org/10.1007/s10559-021-00358-6
- 6. Nykolaychuk Ya., Kasianchuk M., Yakymenko I. Theoretical Foundations of the Modified Perfect form of Residue Number System. Cybernetics and Systems Analysis. 2016. Vol. 52, №2. pp. 219-223 (Scopus). DOI: 10.1007/s10559-016-9817-2
- 7. Nykolaychuk Ya., Kasianchuk M., Yakymenko I. Theoretical Foundations for the Analytical Computation of Coefficients of Basic Numbers of Krestenson's Transformation. Cybernetics and Systems Analysis. 2014. Vol. 50, № 5. pp. 649-654 (Scopus). DOI: 10.1007/s10559-014-9654-0
- 8. Iakymenko I., Kasianchuk M., Kinakh I., Karpinski M. Construction of distributed thermal or piezoelectric sensor based on residue systems. Przeglad Elektrotechniczny. 2017. №1. pp. 290-294 (Scopus). DOI: 10.15199/48.2017.01.69
- 9. Kasianchuk M., Yakymenko I., Yatskiv S., Gomotiuk O., Bilovus L. The Method of Joint Execution of the Basic Operations of the Rabin Cryptosystem. CEUR Workshop Proceedings, 2023, 3373, pp. 425–436. https://ceur-ws.org/Vol-3373/paper28.pdf (Scopus).
- 10. Kasianchuk M., Yakymenko I., Yatskiv V., Karpinski M., Yatskiv S. Method of Multi-Bit Numbers Multiplication in Residue Number System for Asymmetric Cryptosystems. CEUR Workshop Proceedings, 2022, 3156, pp. 365–377. https://ceur-ws.org/Vol-3156/paper27.pdf . (Scopus).
- 11. Stanislaw Zawislak, Mykhailo Kasianchuk, Igor Iakymenko, Daniel Jancarczyk Methods of Crypto-stable Symmetric Encryption in the Residual Number System. Procedia Computer Science. Volume 207, 2022, pp. 128-137. DOI:10.1016/j.procs.2022.09.045 (Scopus)
- 12. Yakymenko I., Kasianchuk M., Shylinska I. A Method for Polynomial Recovery from its Resudues Based on Addition in Z[x] Ring. Informatics and Mathematical Methods in Simulation Vol.14 (2024), No. 4, pp. 305-313. DOI:10.15276/imms.v14.no4.305.
- 13. Якименко І. З., Касянчук М. М., Івасьєв С. В. Криптосистема Рабіна на основі операції додавання. Математичне та комп'ютерне моделювання. Серія: Технічні науки № 19, 2019. 145–150 с. DOI: https://doi.org/10.32626/2308-5916.2019-19.145-150
- 14. Якименко І. З. Удосконалення реалізації криптоалгоритму Ель-Гамаля на основі системи залишкових класів. Інформатика та математичні методи в моделюванні, 2018, 8, № 1. С. 69-77. DOI: 10.15276/imms.v8.no1.69
- 15. Касянчук М.М., Якименко І.З., Івасьєв С.В., Мандебура Н.М., Неміш В.М. Дослідження часових характеристик апаратної реалізації методів пошуку оберненого елемента за модулем. Вісник Хмельницького національного університету. Технічні науки. 2017. №6 (255). С. 191-197.
- 16. Касянчук М.М., Якименко І.З., Івасьєв С.В., Момотюк О.В. Експериментальне дослідження програмної реалізації методів пошуку оберненого елемента за модулем. Інформатика та математичні методи в моделюванні. 2017. Т.7, №3. С. 178–186.
- 17. Касянчук М.М., Якименко І.З., Івасьєв С.В., Маслияк Б.О. Метод розширення набору модулів модифікованої досконалої форми системи залишкових класів. Математичне та комп'ютерне моделювання: Технічні науки. 2017. В.15. С.73-78.

- 18. Касянчук М.М., Якименко І.З., Паздрій І.Р., Івасьєв С.В. Експериментальне дослідження програмної реалізації сумісного виконання алгоритму Евкліда та множення. Інформатика та математичні методи в моделюванні. 2017. Т.7, №1-2. С. 29–36.
- 19. Касянчук М.М., Якименко І.З., Дубчак Л.О., Рендзеняк Н.А., Мандебура Н.М. Модифікований метод шифрування Рабіна з використанням різних форм системи залишкових класів. Вісник Хмельницького національного університету. Технічні науки. 2017. №1(245). С. 127-131.
- 20. Касянчук М.М., Якименко І.З., Долинюк Т.М., Рендзеняк Н.А. Експериментальне дослідження програмної реалізації методів модулярного експоненціювання. Інформатика та математичні методи в моделюванні. 2015. Т.5, №4. С. 376–382.
- 21. Івасьєв С.В., Якименко І.З., Касянчук М.М. Вдосконалений алгоритм пошуку символів Якобі. Оптико-електронні інформаційно-енергетичні технології. 2015. Том 29, № 1. С. 45-50.
- 22. Касянчук М.М., Якименко І.З., Паздрій І.Р., Николайчук Я.М. Аналітичний пошук модулів досконалої форми системи залишкових класів та їх застосування в китайській теоремі про залишки. Вісник Хмельницького національного університету. Технічні науки. 2015. №1(221). С. 170-176.
- 23. Николайчук Я. М., Касянчук М.М., Якименко І.З., Івасьєв С.В. Ефективний метод модулярного множення в теоретико-числовому базисі Радемахера–Крестенсона. Вісник Національного університету «Львівська політехніка». Комп'ютерні системи та мережі. 2014. № 806. С. 195-199.
- 24. Якименко І.З., Касянчук М.М., Тимошенко Л.М., Гребень Н.Є. Алгоритми опрацювання інформаційних потоків в комп'ютерних системах. Інформатика та математичні методи в моделюванні. 2013. Т.3, №3. С. 266–274.
- 25. Якименко І.З., Касянчук М.М., Кімак В.Л. Теоретичні основи зменшення часової та апаратної складності систем захисту інформаційних потоків на основі еліптичних кривих з використанням теоретико-числового базису Радемахера-Крестенсона. Вісник Національного університету «Львівська політехніка» «Комп'ютерні системи та мережі». 2012. №745. С. 190–197.
- 26. Николайчук Я.М., Касянчук М.М., Якименко І.З., Долинюк Т.М. Теоретичні основи виконання модулярних операцій множення та експоненціювання в теоретико–числовому базисі Крестенсона–Радемахера. Інформатика та математичні методи в моделюванні. 2011. №2. С. 123–130.
- 27. Zadiraka V., Yakymenko I., Kasianchuk M., Ivasiev S. Theoretical and numerical Krestenson's basis and its application to problems of cryptographic protection and factorization of multidigit numbers, Computer technologies in information security: collective monograph, By edited V.Zadiraka, Ya.Nykolaichuk, Ternopil: Kart-blansh, 2015. P. 216-260. Ch. 5.
- 28. Yakymenko I., Kasyanchuk M., Volynskyi O. Fundamental application-oriented tasks in Krestenson base, Methods of effective protection of information flows: collective monograph, By edited V.Zadiraka, Ya.Nykolaichuk, Ternopil: Terno-graf, 2014. P. 149-185. Ch.6.
- 29. Kasianchuk M., Yakymenko I., Ivasiev S. High-Productivity Methods of Finding Residues Multidigital Numbers By Modulo, in Inżynier XXI Wieku: VI Międzynarodowa Konferencja studentow oraz doktorantow, 02.12.2016: monografia, 1st ed., Bielsko – Biała (Poland): Akademia Techniczno-Humanistyczna w Bielsku-Białej. 2016. pp. 123-130. Chapter in monograph.
- 30. Якименко І. Алгоритми побудови модифікованої досконалої форми системи залишкових класів. Спеціалізовані комп'ютерні технології в інформатиці: Колективна монографія. Під ред. В.Задіраки, Я.Николайчука. Тернопіль: Бескиди, 2017. С. 580-604.
- 31. Kasianchuk M., Yakymenko I., Ivasiev S. Theoretical foundations for creating five modular modified perfect form of the system of residual classes, in Inżynier XXI Wieku: VII Międzynarodowa Konferencja studentow oraz doktorantow, 08.12.2017: monografia, 1st ed., Vol.2., Bielsko – Biała (Poland): Akademia Techniczno-Humanistyczna w Bielsku-Białej, 2017, pp. 123-130. Chapter in monograph.
- 32. Yakymenko I., Kasianchuk M., Martyniuk O., Martyniuk S., Martyniuk A., Yakymenko Y. A Symmetric Cryptoalgorithm in a Polynomial Hierarchical Residual Number System. Proceedings International Conference on Advanced Computer Information Technologies, ACIT., 2025, pp. 501-504. DOI:

10.1109/ACIT65614.2025.11185808.
- 33. Yakymenko I., Martyniuk O., Martyniuk S., Yakymenko Y., Kasianchuk M. Hierarchical Encryption in a Residual Number System. Proceedings International Conference on Advanced Computer Information Technologies, ACIT., 2024, pp. 496–499 (Scopus). DOI: 10.1109/ACIT62333.2024.10712567
- 34. Shevchuk R., Yakymenko I., Kasianchuk M. Encryption Using Residue Number System: Research Trends and Future Challenges. Proceedings International Conference on Advanced Computer Information Technologies, ACIT2024, 2024, pp. 552–559 (Scopus). DOI: 10.1109/ACIT62333.2024.10712566
- 35. Shevchuk R., Karpinski M., Kasianchuk Yakymenko I., Melnyk A., Tykhyi R. Software for Improve the Security of Kubernetes-based CI/CD Pipeline. Proceedings International Conference on Advanced Computer Information Technologies, ACIT2023, 2023, pp. 420–425. (Scopus). DOI: 10.1109/ACIT58437.2023.10275654
- 36. Yakymenko I., Kasianchuk M., Shylinska I., Shevchuk R., Yatskiv V., Karpinski M. Polynomial Rabin Cryptosystem Based on the Operation of Addition. 12th International Conference on Advanced Computer Information Technologies, ACIT 2022, 2022, pp. 345–350. DOI:10.1109/ACIT54803.2022.9913089 (Scopus).
- 37. Yakymenko I., Kasianchuk M., Yatskiv V., Shevchuk R., Koval V., Yatskiv S. Sustainability and Time Complexity Estimation of Cryptographic Algorithms Main Operations on Elliptic Curves. 2021 11th International Conference on Advanced Computer Information Technologies (ACIT). pp. 494-498 (Scopus). DOI: 10.1109/ACIT52158.2021.9548534
- 38. Mykhailo Kasianchuk, Ihor Yakymenko, Vasyl Yatskiv, Stepan Ivasiev, Andriy Sverstiuk. Same Bit-Size Moduli Formation of Residue Number System for Application in Asymmetric Cryptography. IntelITSIS 2021. pp. 301-308.
- 39. Yakymenko I., Shylinska I., Kasianchuk M., Bilovus L., Gomotiuk O. Algorithmic Support for Rabin Three-Modular Cryptosystem Based on the Operation of Addition. IEEE 15th International Conference on Computer Sciences and Information Technologies (CSIT). 2020. pp. 328-331 (Scopus).
- 40. Kasianchuk M., Yakymenko I., Karpinski M., Shevchuk R., Karpinskyi V., Shylinska I. Theoretical Bases for Reducing the Time Complexity of the Rabin Cryptosystem. Conference on Computer Science and Information Technologies. 2020. pp. 628-639. (Scopus). DOI: 10.1007/978-3-030-63270-0_43
- 41. Ivasiev S., Kasyanchuk M., Yakymenko I., Gomotiuk O., Shylinska I., Bilovus L. Algorithmic support for Rabin cryptosystem implementation based on addition.10th International Conference on Advanced Computer Information Technologies (ACIT). 2020. pp. 779-782. (Scopus). DOI: 10.1109/ACIT49673.2020.9208923
- 42. Yakymenko I., Kasianchuk M., Ivasiev S., Shevchuk R., Batko Y., Vasylkiv V. Method for Determining Prime and Relatively Prime Numbers of 2n+k Type Based on the Periodicity Property. 10th International Conference on Advanced Computer Information Technologies (ACIT), Deggendorf, Germany. 2020. pp. 751–754. https://doi.org/10.1109/ACIT49673.2020.9208812 (Scopus).
- 43. Yakymenko I., Kasianchuk M., Gomotiuk O., Tereshchuk G., Ivasiev S., Basistyi P. Elgamal cryptoalgorithm on the basis of the vector-module method of modular exponentiation and multiplication. IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET). 2020. pp. 926-929. (Scopus). DOI: 10.1109/TCSET49122.2020.235572
- 44. Karpinski M., Rajba S., Zawislak S., Warwas K., Kasianchuk M., Ivasiev S., Yakymenko I. A method for decimal number recovery from its residues based on the addition of the product modules, 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). Metz, France. 2019. pp.13-17. https://doi.org/10.1109/IDAACS.2019.8924395. (Scopus).
- 45. Kasianchuk M., Yakymenko I., Ivasiev S., Shevchuk R., Tymoshenko L. The method of factorizing multi-digit numbers based on the operation of adding odd numbers. CEUR Workshop Proceedings 8th International Conference Advanced Computer Information Technologies ACIT. June 2018. 2018, pp. 232-235, (Scopus).
- 46. Ivasiev S., Yakymenko I., Kasianchuk M., Shevchuk R., Karpinski M., Gomotiuk O. Effective algorithms for finding the remainder of multi-digit numbers. Advanced Computer Information Technology (ACIT–2019): Proceedings of the International Conference. 2019, pp. 175-178. (Scopus). DOI: 10.1109/ACITT.2019.8779899

- 47. Yakymenko I., Kasianchuk M., Ivasiev S., Melnyk A., Nykolaichuk Y. Realization of RSA cryptographic algorithm based on vector-module method of modular exponention. In Proceedings of the 2018 14th International Conference on Advanced Trends in Radioelecrtronics. Telecommunications and Computer Engineering (TCSET), Lviv-Slavske, Ukraine, 20–24 February 2018. 2018. pp. 550–554.
- 48. Якименко І.З., Касянчук М.М., Кінах Я.І., Власюк І.М., Суслін В.В. Удосконалення реалізації асиметричних криптоалгоритмів на основі системи залишкових класів. Матеріали VI Всеукраїнської школи-семінару молодих вчених і студентів «Сучасні комп'ютерні інформаційні технології» (ACIT). 2018. с. 79.
- 49. Карпінський, М. П., Кінах, Я. І., Яциковська, У. О., Якименко, І. З., Касянчук, М. М. Удосконалення архітектури комп'ютерної мережі для програмної реалізації криптоаналітичних алгоритмів. Матеріали □ науково-технічної конференції „Інформаційні моделі, системи та технології". 2018. С. 93.
- 50. Карпінський М. П., Кінах Я. І., Войтенко, О. С., Паславсьий, В. Р., Якименко, І. З., Касянчук, М. М. Теоретичний аналіз інформаційної безпеки в комп'ютерних мережах. Збірник тез доповідей □ Міжнародної науково-технічної конференції молодих учених та студентів „Актуальні задачі сучасних технологій". 2, 2017. С.81-82.
- 51. Rajba T., Klos-Witkowska A., Ivasiev S., Yakymenko I., Kasianchuk M. Research of time characteristics of search methods of inverse element by the module in: Proc. IEEE 9th Intern. Conf. on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS-2017) (Bucharest, Romania. 21–23 Sept, 2017), 2017. pp. 82–85. https://doi.org/10.1109/IDAACS.2017.8095054. (Scopus).
- 52. Kasianchuk M., Yakymenko I., Pazdriy I., Melnyk A., Ivasiev S., Rabin's modified method of encryption using various forms of system of residual classes. 14th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM), 2017. pp. 222-224. (Scopus). DOI: 10.1109/CADSM.2017.7916120
- 53. Якименко І.З. Методологія криптографічного захисту інформації на основі цілочисельної, модифікованої досконалої та поліноміальної систем залишкових класів, Матеріали XIV Міжнародної науково-технічної конференції ITSec-2025 Безпека інформаційних технологій, 22-24 травня 2025, м. Тернопіль (Україна). 2025. С. 224-228.
- 54. Karpiński M., Ivasiev S., Yakymenko I., Kasianchuk M., Gancarczyk T. Advanced method of factorization of multi-bit numbers based on Fermat's theorem in the system of residual classes. International Conference on Control, Automation and Systems (ICCAS–2016): Proceedings. Gyeongju, Korea. V.1. 2016. pp.1484–1486 (Scopus). DOI: 10.1109/ICCAS.2016.7832500
- 55. Nykolaychuk Ya., Ivas'ev S., Yakymenko I., Kasianchuk M. Test of verification of multidigit numbers on simplicity on the basis of method of vector and modular multiplication. Modern Problems of Radio Engineering, Telecommunica-tions and Computer Science (TCSET–2016): Proceedings of the XIII–th International Conference. L'viv–Slavske. 2016. pp.534-536 (Scopus). DOI: 10.1109/TCSET.2016.7452107
- 56. Kozaczko D., Ivasiev S., Yakymenko I., Kasianchuk M. Vector Module Exponential in the Remaining Classes System. Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS–2015): Proceedings of the 2015 IEEE 8th International Conference. Warsaw, Poland. V.1. 2015. pp.161–163 (Scopus). DOI: 10.1109/IDAACS.2015.7340720
- 57. Kasianchuk M., Yakymenko I., Pazdriy I., Zastavnyy O. Algorithms of findings of perfect shape modules of remaining classes system. The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM-2015): Proceedings of the XIII International Conference. Polyana-Svalyava. 2015. pp.168-171 (Scopus). DOI: 10.1109/CADSM.2015.7230866
- 58. Ivas'ev S., Kasyanchuk M., Yakymenko I., Nykolaychuk Ya. Fundamental Backgrounds of the Discrete Logarithms Theory in the Rademacher–Krestenson's Basis. Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET–2012): Proceedings of the XI–th International Conference. L'viv–Slavske. 2012. 93 P. (Scopus).

- 59. Касянчук М.М., Якименко І.З., Тимошенко Л.М., Івасьєв С.В., Николайчук Я.М. Векторно-модульний метод модулярного множення. Сучасні інформаційні та електронні технології: Матеріали Міжнародної науково-практичної конференції. Одеса. 2014, С. 152.
- 60. Пат. 159225 Україна МПК G06F 7/00 (2025.01). Накопичуючий синхронізований двійковий суматор / Николайчук Я.М., Грига В.М., Якименко І.З., Грига Л.П., № u 2024 04320 заявл. 03.09.2024; опубл. 08.05.2025, Бюл. №19/2025.
- 61.Пат. 160091 Україна МПК G06F7/04. Пристрій порівняння даних, представлених у непозиційній системі залишкових класів / Николайчук Я.М., Якименко І.З., Івасьєв С.В, Грига В.М. № u202404328 заявл. 03.09.2024; опубл. 06.08.2025, Бюл. № 32/2025.

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами: 01220001497, 01210109485, 0120U102040, 0117U000410, 0114U000569, 0112U000078, 01230103785, 0114U006089, 0112U003917

VI. Відомості про наукового керівника/керівників (консультанта)

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Євсеєв Сергій Петрович
2. Serhii P. Yevseiev

Кваліфікація: д. т. н., професор, 21.05.01

Ідентифікатор ORCID ID: 0000-0003-1647-6444

Додаткова інформація:

Повне найменування юридичної особи: Національний технічний університет "Харківський політехнічний інститут"

Код за ЄДРПОУ: 02071180

Місцезнаходження: вул. Кирпичова, Харків, Харківський р-н., 61002, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Смірнов Олексій Анатолійович

2. Oleksii Smirnov

Кваліфікація: д.т.н., професор, 21.05.01

Ідентифікатор ORCID ID: 0000-0001-9543-874X

Додаткова інформація:

Повне найменування юридичної особи: Центральноукраїнський національний технічний університет

Код за ЄДРПОУ: 02070950

Місцезнаходження: просп. Університетський, Кропивницький, Кропівницький р-н., 25006, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Рудницький Володимир Миколайович
2. Volodymyr Rudnytskyi

Кваліфікація: д. т. н., професор, 05.13.06

Ідентифікатор ORCID ID: 0000-0002-7362-3263

Додаткова інформація:

Повне найменування юридичної особи: Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки

Код за ЄДРПОУ: 26614573

Місцезнаходження: вул. Стрілецька, Чернігів, Чернігівський р-н., 14033, Україна

Форма власності: Державна

Сфера управління: Міністерство оборони України

Ідентифікатор ROR:

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Корченко Олександр Григорович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Корченко Олександр Григорович
Відповідальний за підготовку облікових документів	Корецька В.О.
Реєстратор	Юрченко Тетяна Анатоліївна

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Тетяна Анатоліївна