

Облікова картка ДіР

I. Загальні відомості

Державний обліковий номер: 0225U005204

Особливі позначки: відкрита

Дата реєстрації: 27-12-2025



II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Тригонометричні суми в теорії чисел і криптографії

Початок етапу: 06.2023

Закінчення етапу: 12.2025

Вид звітнього документа: Остаточний звіт

III. Відомості про виконавця ДіР

Повне найменування юридичної особи: Одеський національний університет імені І. І. Мечникова

Код за ЄДРПОУ: 02071091

Місцезнаходження: вул. Дворянська, Одеса, 65082, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Розмір організації: Понад 250 співробітників

Телефон: 380487235254

IV. Відомості про співвиконавців ДіР

V. Відомості про замовника ДіР

Повне найменування юридичної особи: Одеський національний університет імені І. І. Мечникова

Код за ЄДРПОУ: 02071091

Місцезнаходження: вул. Дворянська, Одеса, 65082, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Розмір організації: Понад 250 співробітників

Телефон: 380487235254

VI. Джерела, напрями та обсяги фінансування ДіР

Підстава для проведення ДіР: 43 - Власна ініціатива (якщо ДіР виконується з власної ініціативи за кошти виконавця або безкоштовно)

Напрямок фінансування: 2.1 - Фундаментальні дослідження

Джерела фінансування

7706 - Безоплатно (договір про науково-технічне співробітництво, тощо)

VII. Відомості про ДіР

Назва роботи українською:

Тригонометричні суми в теорії чисел і криптографії

Назва роботи англійською:

Exponential sums in Number Theory and Cryptography

Реферат українською:

Досліджено властивості сум Клоостермана над кільцем цілих елементів уявного квадратичного поля $\mathbb{Q}(-d_1/2)$. Отримано оцінки сум Клоостермана і їх узагальнення для задач розподілу розв'язків деяких конгруенцій. Досліджені спеціальні конгруенції для генерування послідовностей псевдовипадкових чисел та досліджені нелінійні конгруентні генератори псевдовипадкових чисел. Досліджено властивості сум Клоостермана на еліпсі над скінченим розширенням уявного квадратичного розширення поля раціональних чисел в арифметичній прогресії. Розроблені методи генерування псевдовипадкових чисел, породжених аналогами еліптичних кривих над алгебраїчним розширенням поля раціональних чисел. Досліджено спеціальні конгруенції на еліптичних кривих для генерування послідовностей псевдовипадкових чисел. Побудована хеш-функція на еліптичній кривій і розглянуто її використання в криптографії. Досліджено спеціальні конгруенції для генерування послідовностей псевдовипадкових чисел. Розроблені методи генерування псевдовипадкових чисел, породжених аналогами еліптичних кривих над скінченим кільцем.

Реферат англійською:

The properties of Kloosterman sums over the ring of integers of the imaginary quadratic field $\mathbb{Q}(-d_1/2)$ have been investigated. Sharp bounds for Kloosterman sums, as well as their generalizations, have been obtained in connection with problems concerning the distribution of solutions to certain congruences. Special congruences relevant to the construction of pseudorandom number sequences have been studied, together with nonlinear congruential pseudorandom number generators. Furthermore, the behavior of Kloosterman sums on an elliptic curve defined over a finite extension of the imaginary quadratic extension of the rational field, arranged in an arithmetic progression, has been examined. Methods have been developed for constructing pseudorandom number generators derived from analogues of elliptic curves over algebraic extensions of the rational field. Special congruences on elliptic curves used for generating pseudorandom sequences have been analyzed. An elliptic-curve-based hash function has been constructed, and its cryptographic applications have been discussed. Additional special congruences relevant to pseudorandom sequence generation have been investigated. Moreover, methods have been designed for constructing pseudorandom number generators based on elliptic-curve analogues defined over a finite ring.

Індекс УДК: 002:651.928(083.73), 511.33 , 517.955.8 , УДК 511.33, УДК 511.333, УДК 511.321, УДК 517.955.8, УДК 002:651.928(083.73), УДК 004.056.55, УДК 00

Коди тематичних рубрик: 20.51.35, 27.15.19, 27.31.19

Керівники роботи

Власне Прізвище Ім'я По-батькові: Варбанець Сергій Павлович

Науковий ступінь: д. ф.-м. н.

Наукове звання: професор

Ідентифікатор ORCID ID:

Додаткова інформація: Scopus ID: 51562903900 ;

<https://www.scopus.com/authid/detail.uri?authorId=51562903900>

VIII. Наукова (науково-технічна) продукція (НТП)

Назва НТП українською: Тригонометричні суми в теорії чисел і криптографії

Назва НТП англійською: Exponential sums in Number Theory and Cryptography

НТП, яку передбачалося створити: Створено

Причини, через які НТП не було створено:

Отримані результати: Методи, теорії, гіпотези

Галузь застосування: 73.10 - Дослідження і розробки в галузі природничих і технічних наук

Реєстраційний номер картки технології:

Опис НТП: Отримано результати, що описують класи інверсних генераторів та їх узагальнень, а також оцінки для обґрунтування їх рівномірності. Висновки про структуру одиниць і системи конгруенцій з [1] дають підхід до вибору стану генератора та контролю його порядку. Побудовані раніше інверсні генератори забезпечують готові формули оновлення стану, для яких наведено оцінки експоненційних сум і дискріпансії. Методи аналізу природно переносяться на послідовності точок еліптичних кривих над $\mathbb{Z}_p$. Сформульовано умови на коефіцієнти кривої, що гарантують щільність орбіт і відсутність коротких циклів. Запропоновано схему генератора $P_{n+1} = kP_n + Q$ і доведено оцінку дискріпансії. Створено конструкцію хеш-функції на еліптичній кривій та алгоритм аналітичного наближення дискріпансії.

Соціально-економічна спрямованість НТП: Інше (Має наукове та соціально-економічне значення як фундаментальне дослідження)

Вплив НТП на довкілля: не впливає на довкілля

Впровадження НТП: Впроваджено

Практична реалізація НТП

Початок етапу: 06.2023

Закінчення етапу: 12.2025

Споживачі продукції: заклади вищої освіти

Перспективні ринки: Україна

Характер співробітництва з інвестором

Потрібний обсяг інвестицій, тис. грн.:

Права, що надаються інвестору після завершення роботи:

Наявність бізнес-плану:

Техніко-економічне обґрунтування:

Потенціальний обсяг продажу, тис. грн.:

Очікуваний термін окупності (років):

Додаткова інформація:

IX. Бібліографічний опис

1. Sergey Varbanets and Yakov Vorobyov, The Kloosterman sums on the ellipse // Algebra and Discrete Mathematics, Vol. 35 (2), 2023, P. 251-270.
2. Pavel Varbanets, Sergey Varbanets, Yakov Vorobyov, Divisor function of the Gaussian integers weighted by the Kloosterman sum // Algebra and Discrete Mathematics, Vol. 40 (2), 2025 (to appear).
3. Mykyta Klishyn, Pavel Varbanets, The distribution of the points of elliptic curve over the finite ring // The XIV International Algebraic Conference in Ukraine, July 03-07, 2023, Sumy, Ukraine, p. 75.
4. Pavel Varbanets, Yakov Vorobyov, Weighed multiplicative function over $\mathbb{Z}[i]$ // The XIV International Algebraic Conference in Ukraine, July 03-07, 2023, Sumy, Ukraine, p. 131.
5. P. Varbanets, Exponential sums on the manyfolds over finite field // Ukraine Algebra Conference "At the End of the Year 2023, 26-27 December, 2023, Kyiv, Ukraine, 2023, p. 54.
6. Павло Варбанець, Микита Клішин, Псевдовипадкові числа на кривих $Ax^m + By^k = 1 \pmod{p^n}$ // VI Всеукраїнській науково-практичній конференції "Освітні інновації у закладах освіти: проблеми та перспективи", 12 грудня 2023 року, Ізмаїл, Україна.
7. Sergey Varbanets, Exponential sums over the sequences of PRN's // The XIV International Algebraic Conference in Ukraine, July 03-07, 2023, Sumy, Ukraine, p. 132.
8. Sergey Varbanets, Yakov Vorobyov, Norm Kloosterman sums and its applications // The XIV International Algebraic Conference in Ukraine, July 03-07, 2023, Sumy, Ukraine, p. 133.
9. Klishin M., Varbanets S., Kloosterman sum on the ellipse // Ukraine Algebra Conference "At the End of the Year 2023, 26-27 December, 2023, Kyiv, Ukraine, 2023, p. 29.
10. Варбанець С., Нормені суми Клоостермана // VI Всеукраїнській науково-практичній конференції "Освітні інновації у закладах освіти: проблеми та перспективи", 12 грудня 2023 року, Ізмаїл, Україна.
11. Варбанець С. П., Функція в арифметичній прогресії // 78 Наукова конференція професорсько-викладацького складу і наукових працівників. Підсекція алгебри «Аналітична теорія чисел», 2023.
12. Belozero G., Klishin M., Varbanets S., Vorobiova A., Analogue of the ternary divisor problem in an arithmetic progression // XXIX International Scientific and Practical Conference "Business culture in the conditions of socio-cultural transformation of society", Lyon, France July 23 – 26, 2024, Sect. Physical and mathematical sciences, 2024, pp. 175-176.
13. Сергій Варбанець. Послідовності псевдовипадкових чисел на еліптичних кривих // VII Всеукраїнська науково-практична-конференція з міжнародною участю «Освітні інновації у закладах освіти: проблеми та перспективи», 18 грудня 2024р., Ізмаїл, 2024. С. X.
14. Pavel Varbanets, Sergey Varbanets, Yakov Vorobyov, Multiplicative functions weighted with Kloosterman sums over $\mathbb{Z}[i]$ // Ukraine Mathematics Conference At the End of the Year 2024, December 16-18, 2024, Kyiv, Ukraine, p. 51.
15. Belozero G., Klishin M., Varbanets S., Vorobiova A., On numbers of the type $mn = (m^2 + n^2)k$ in arithmetic progression // VI International Scientific and Practical Conference "Perspectives of contemporary science: theory and practice", Lviv, Ukraine 22-24 July 2024, Sect. Physical and mathematical sciences, 2024, pp. 167-170.

Х. Заключні відомості

Керівник юридичної особи

Труба Вячеслав Іванович
д. ю. н., професор, 12.00.03

Перелік осіб-виконавців

Варбанець Сергій Павлович
(д. ф.-м. н., 01.01.08)

**Відповідальний за підготовку
облікових документів**

Райко Ірина Володимирівна, Волювач Ольга Вячеславівна

Телефон

(048)723-04-10

Реєстратор

Юрченко Тетяна Анатоліївна

**Керівник відділу УкрІНТЕІ, що є
відповідальним за реєстрацію наукової
діяльності**



Юрченко Тетяна Анатоліївна