Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0416U000249

Особливі позначки: відкрита

Дата реєстрації: 28-01-2016

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Чан Тхе Вінь

2. Tran The Vinh

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: кандидат наук

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 01.01.08

Назва наукової спеціальності: Математична логіка, теорія алгоритмів і дискретна математика

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 18-01-2016

Спеціальність за освітою: 8.04020402

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): Д 26.001.18

Повне найменування юридичної особи: Київський національний університет імені Тараса Шевченка

Код за ЄДРПОУ: 02070944

Місцезнаходження: вул. Володимирська, 60, м. Київ, Київська обл., 01033, 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: Київський національний університет імені Тараса Шевченка

Код за ЄДРПОУ: 02070944

Місцезнаходження: 01033, м. Київ, вул. Володимирська, 64

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 27.03.19

Тема дисертації:

1. Застосування сумм Клостермана в криптографії і кодуванні

2. Applications of the Kloosterman sums in cryptography and coding

Реферат/анотація:

1. У дисертаційній роботі розглядаються застосування сум Клостермана та їх узагальнень над кільцем цілих раціональних та цілих гаусових чисел у криптографії і кодуванні. Знайдені нові результати про властивості цих сум. Для мультиплікативних функцій спеціального вигляду, що зважені сумами Клостермана, побудовані зображення суматорних функцій у термінах дзета-подібних функцій. Для неповних сум Клостермана над кільцем цілих чисел знайдені оцінки відповідних білінійних форм. Для побудови послідовностей псевдо-випадкових чисел введені нові конгруентні лінійно-інверсні генератори. Дискрепантні функції псевдо-випадкових чисел породжених лінійно-інверсними генераторами оцінюються за допомогою оцінок тригонометричних Клостерманівських сум. Доведено, що такі послідовності псевдо-випадкових чисел проходять серіальний тест на рівнорозподіленість та непередбачуваність. Побудовано аналог степеневого конгруентного генератора послідовності комплексних чисел одиничного кола на норменій підгрупі кільця

класів лишків за модулем. Досліджено розподіл значень вагової функції коду Клостермана над кільцем класів лишків , в кільці цілих гаусових чисел.

2. The thesis deals with applications of the Kloosterman sums and its generalizations over the ring of rational integers and Gaussian integers in cryptography and coding. There are obtained the new results on properties these sum. For multiplicative function of special type whict weighted by the Kloosterman sums it is constructed the representations of summatory functions in terms of zeta-similarly functions. For the incomplete Kloosterman sums over the ring of integers there are obtained estimates of adequate belinear forms. For construct of the sequences of pseudorandom numbers there are embedded new congruential linear-inversive generators. The discrepancy of pseudorandom numbers that produced by linear-inversive generators estimate there is estimated with the help of the estimates of the Kloosterman sums. It is proved that such sequences of pseudorandom numbers passe the serial test on equidistribution and unpredictability. And analogue of power congruential generator of the sequence of complex numbers from unit circl there is constructed on the norm subgroup of the residue ring modulo , . It is investigated a distribution of values of the weight function of the Kloosterman code over the residue ring modulo , of the Gaussian numbers.

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. Варбанець Павло Дмитрович
2. Varbanets Pavlo Dmytrovych

Кваліфікація: д.ф.-м.н., 01.01.08

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. Глазунов Микола Михайлович

2. Глазунов Микола Михайлович

Кваліфікація: д.ф.-м.н., 01.05.01

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. Левитська Аліна Олександрівна

2. Левитська Аліна Олександрівна

Кваліфікація: д.ф.-м.н., 01.01.05

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 Петравчук Анатолій Петрович

Власне Прізвище Ім'я По-батькові головуючого на засіданні

Петравчук Анатолій Петрович

Відповідальний за підготовку облікових документів

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності



Юрченко Т.А.