Облікова картка ДіР

I. Загальні відомості

Державний обліковий номер: 0225U002383

Державний реєстраційний номер: 0118U007356

Особливі позначки: відкрита

Дата реєстрації: 06-03-2025

II. Етап виконання ДіР

Номер етапу: 1

Назва етапу: Розробка та дослідження криптостійких генераторів псевдовипадкових послідовностей і генераторів пуассонівських імпульсних потоків

Початок етапу: 01.2019

Закінчення етапу: 12.2024

Вид звітного документа: Остаточний звіт

III. Відомості про виконавця ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. Степана Бандери, буд. 12, м. Львів, Львівська обл., 79013, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 380322582111

IV. Відомості про співвиконавців ДіР

V. Відомості про замовника ДіР

Повне найменування юридичної особи (або ПІБ фізичної особи): Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. Степана Бандери, буд. 12, м. Львів, Львівська обл., 79013, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Розмір організації:

Телефон: 380322582111

VI. Джерела, напрями та обсяги фінансування ДіР

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

Напрям фінансування: 2.2 - прикладні дослідження і розробки

Джерела фінансування

7704 - власні кошти, кошти підприємств, установ, організацій, фізичної особи на виконання ініціативних робіт

Фактичний обсяг фінансування (тис. грн.): 0.000

VII. Відомості про ДіР

Назва роботи українською:

Розробка та дослідження криптостійких генераторів псевдовипадкових послідовностей і генераторів пуассонівських імпульсних потоків

Назва роботи англійською:

Development and research of cryptographically secure pseudorandom sequences generators and Poisson pulse sequence generators

Реферат українською:

Запропоновано метод подолання недоліків модифікованих адитивних генераторів Фібоначчі, побудованих на основі примітивних поліномів у полі GF(p); запропоновано криптостійкі генератори псевдовипадкових послідовностей на основі модифікованого алгоритму BBS та генератора Джиффі; запропоновано генератори пуассонівських імпульсних послідовностей на основі модифікованих адитивних генераторів Фібоначчі із заданим модулем рекурентного рівняння та на основі цифрових синтезаторів частоти, що дозволяють оперативно керувати вихідною частотою; розроблено синтезатори частоти з покращеними метрологічними характеристиками; оптимізовано метод зменшення нерівномірності імпульсних послідовностей, що дозволяє підвищити точність синтезаторів; теоретичні результати також застосовано для створення засобів моделювання дозиметричних детекторів; окремі генератори були реалізовані на FPGA. Наукова та науково-технічна значущість роботи підтверджена порівняльним аналізом характеристик запропонованих пристроїв з існуючими аналогами та публікаціями у провідних наукових виданнях. Соціально-економічне значення роботи полягає в можливості використання результатів роботи у військовій та цивільній сферах, зокрема, у засобах захисту інформації.

Реферат англійською:

A method for overcoming the shortcomings of modified additive Fibonacci generators built on the basis of primitive polynomials in the field GF(p) was proposed; crypto-resistant generators of pseudo-random sequences based on the modified BBS algorithm and the Jiffy generator were proposed; Poisson pulse sequence generators based on modified additive Fibonacci generators with a given modulus of the recurrent equation and digital frequency synthesizers that allow for operational control of the output frequency have been proposed; frequency synthesizers with improved metrological characteristics have been developed; a method for reducing the non-uniformity of pulse sequences has been optimized, which allows for increasing the accuracy of synthesizers; theoretical results have also been applied to create means of modeling dosimetric detectors; individual generators have been implemented on FPGA. The scientific and scientific and technical significance of the work is confirmed by a comparative analysis of the characteristics of the proposed devices with existing analogues and publications in leading scientific publications. The socio-economic significance of the work lies in the possibility of using the results of the work in the military and civilian spheres, in particular in information protection means.

Індекс УДК: 004.7, 004; 519.6, 004.056; 004.421.5

Коди тематичних рубрик: 50.37.23, 50.05.19

Керівники роботи

Власне Прізвище Ім'я По-батькові: Войтусік Степан Степанович

Науковий ступінь: к. ф.-м. н.

Вчене звання:

Ідентифікатор ORCID ID:

Додаткова інформація:

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

Назва НТП українською: Спосіб подолання недоліків модифікованих адитивних генераторів Фібоначчі, побудованих на основі примітивних поліномів в полі GF(p). Генератори пуассонівських імпульсних послідовностей на основі модифікованих адитивних генераторів Фібоначчі із заданим модулем рекурентного рівняння. Синтезатори частоти з покращеними метрологічними характеристиками. Оптимізований метод зменшення нерівномірності імпульсних послідовностей, що дозволяє покращити точність синтезаторів.

Назва НТП англійською: A method for overcoming the shortcomings of modified additive Fibonacci generators built on the basis of primitive polynomials in the field GF(p). Proposed generators of Poisson pulse sequences based on modified additive Fibonacci generators with a given modulus of the recurrent equation. Frequency synthesizers with improved metrological characteristics. Optimized method for reducing the non-uniformity of pulse sequences, which allows for improving the accuracy of synthesizers.

НТП, яку передбачалося створити:

Причини, через які НТП не було створено:

Отримані результати: Методи, теорії, Аналітичні матеріали

Галузь застосування: 72.19. Дослідження й експериментальні розробки у сфері інших природничих і технічних наук

Реєстраційний номер картки технології:

Опис НТП: Запропоновано спосіб подолання недоліків модифікованих адитивних генераторів Фібоначчі, побудованих на основі примітивних поліномів в полі GF(p); запропоновано генератори пуассонівських імпульсних послідовностей на основі модифікованих адитивних генераторів Фібоначчі з заданим модулем рекурентного рівняння на основі цифрових синтезаторів частоти, що дозволяють оперативно керувати вихідною частотою; розроблено синтезатори частоти з покращеними метрологічними характеристиками; оптимізовано метод зменшення нерівномірності імпульсних послідовностей, що дозволяє покращити точність синтезаторів; теоретичні результати також застосовані для створення імітаційних засобів дозиметричних детекторів; аналіз автокореляційної функції шумоподібних сигналів показав її ефективність у використанні лише для аналізу широкосмугових генераторів шуму; створено моделі на основі прикладу корисного сигналу, що дають можливість підібрати необхідні робочі характеристики: частоту та потужність, що важливо для подальшого вибору передавача, підсилювача, антени та системи охолодження; досліджено, що необхідною умовою для створення ефективних генераторів шуму є точна конфігурація частот, що підвищує вимоги до передачі та пристрою управління; імплементовано окремі генератори на ПЛІС.

Соціально-економічна спрямованість НТП: Забезпечення промисловості чи населення новим видом інформаційно-комунікаційних послуг

Вплив НТП на довкілля:

Впровадження НТП: Не впроваджено

Практична реалізація НТП

Початок етапу: 01.2019

Закінчення етапу: 12.2024

Споживачі продукції: Інформаційно-комунікаційні системи державних установ і критичної інфраструктури, де потребується високий рівень захищеності інформації

Перспективні ринки: Іноземні та внутрішні ринки

Характер співробітництва з інвестором

Потрібний обсяг інвестицій, тис. грн.:

Права, що надаються інвестору після завершення роботи:

Наявність бізнес-плану:

Техніко-економічне обгрунтування:

Потенціальний обсяг продажу, тис. грн.:

Очікуваний термін окупності (років):

Додаткова інформація:

IX. Бібліографічний опис

X. Заключні відомості

Керівник юридичної особи Чухрай Наталія Іванівна
д. е. н., 08.00.04

Перелік осіб-виконавців

Ісаков Олександр Володимирович

Гарасимчук Олег Ігорович
(к. т. н., 05.13.05)

Малогловець Андрій Сергійович

Цебак Олег Анатолійович

Шабатура Марія Миколаївна
(к. т. н.)

Шевчук Микола Сергійович

Відповідальний за підготовку облікових документів Приставська М.М.

Телефон +38 (032) 258-26-37

Реєстратор

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

