ВІДГУК

на автореферат дисертації
«Генератори пуассонівських імпульсних послідовностей
з покращеними характеристиками»
здобувача Костіва Юрія Михайловича, яка подана на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – Комп'ютерні системи та компоненти.

Дисертаційна робота «Генератори пуассонівських імпульсних послідовностей з покращеними характеристиками», яка подана Ю.М.Костівим на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – «Комп'ютерні системи та компоненти», присвячена розробленню нових методів побудови генераторів пуассонівських імпульсних послідовностей (ГПІП) аналізу їх характеристик та розробленню методів оцінювання їх якості. Автором було виконано аналіз існуючих підходів до вирішення проблем, пов'язаних зі створенням сучасних генераторів, що використовуються у моделюванні та криптографії, виявлені недоліки, що існують на даний момент та запропоновані нові перспективні підходи у цій галузі.

Виходячи зі сказаного, автором роботи виконана постановка наукової задачі, яка полягає у створенні нових алгоритмів для формулювання імпульсних послідовностей, що відповідають заданому закону розподілення ймовірностей, і задовольняють сучасним вимогам. В рамках вирішення цієї задачі здобувачем було виконано аналіз методів та засобів генерування імпульсних пуассонівських послідовностей, а також запропоновано удосконалену методику обчислення показників якості таких послідовностей на основі критерію хі-квадрат Персона. В рамках виконаних наукових досліджень за допомогою цієї методики було досліджено конгруентні генератори, генератори Фібоначчі, генератори на регістрах зсуву з лінійним зворотним зв'язком та виявлена їх придатність для створення на їх основі генераторів пуассонівськх послідовностей. Особливо цінним є те, що автором було напрацьовано і запропоновано досконалу методику, проектування ГПІП та хороший варіант такого генератору.

На основі аналізу існуючих методів оцінки послідовностей, що формуються на виході генераторів псевдовипадкових чисел, зроблено висновок про непридатність тестових пакетів NIST STS, та інших їм подібних, через те, що вони розраховані виключно на перевірку послідовностей з рівномірним розподіленням ймовірностей. Оскільки в роботі поставлена задача перевірки послідовності на відповідність її Пуассонівському закону, автор запропонував свою власну методику і довів її до стану опрацьованого інструментарію, який може бути використаний при вирішенні відповідних дослідницьких задач. Автор абсолютно обґрунтовано обрав у якості основи створеного критерію оцінки послідовностей критерій Пірсона, оскільки він є одним з тих критеріїв, що детально описаний у науковій літературі і входить до складу майже всіх відомих пакетів, зокрема NIST. В роботі надається розроблений автором математичний апарат, що дозволяє шляхом відповідних обчислень визначати розмір обчислювальних статистичних інтервалів, величин емпіричних і теоретичних частот символів на виході генераторів, а також число ступенів свободи, обґрунтовано розмір необхідної статистичної вибірки.

Запропонована автором методика оцінки генераторів була випробувана на генераторах, побудованих за схемою, що включає джерело імпульсного потоку з досить рівномірним розподіленням ймовірностей та джерело корегуючого коду, який перетворює рівномірну послідовність на послідовність, що описується законом Пуассона. У якості джерел імпульсного потоку розглядались майже всі відомі типи елементарних генераторів, що використовуються для формування псевдо випадкових числових послідовностей. Зокрема було розглянуто генератори, побудовані на основі регістрів з лінійним зворотним зв'язком. В процесі виконання досліджень була визначена сукупність утворюючих поліномів, які дають найкращі Пуассонівські послідовності. Автором було запропоновано гібридну схему, яка включає комбінацію таких генераторів, частина з яких задіяна для формування опорної послідовності, а частина для формування керуючого коду. Для формування вихідної послідовності пропонується використання операції мультиплексії. Також запропоновано інструментарій для визначення набору складових генераторів та їх характеристик в залежності від вимог до вихідного Пуассоновського потоку.

Крім того, було запропоновано схеми генераторів, побудованих на аналітичних принципах формування рекурентних послідовностей. Зокрема це конгруентні лінійні генератори та генератори Фібоначчі. Результатом виконаних досліджень стали величини параметрів рекурентних рівнянь, при яких середня частота імпульсів зостається у визначеному діапазоні значень.

Так само, як і у випадку з генераторами на регістрах, запропоновано комбінаційну схему, до складу якої входять різноманітні елементарні генератори псевдо випадкових послідовностей з параметрами, визначеними у відповідності до запропонованої методики. Розроблений генератор автором було названо модифікованим генератором Фібоначчі. Він містить у своєму складі декілька регістрів, охоплених системою зворотних зв'язків і забезпечує формування Пуассонівського потоку із заданими характеристиками. В роботі наведені аналітичні залежності, на основі яких формуються вихідні імпульси та сукупність коефіцієнтів, що визначають модифікований алгоритм Фібоначчі.

Усі запропоновані технічні рішення і методики були автором випробувані у рамках задач, поставлених на дослідження у роботі. Результатом таких досліджень стала методика проектування ГПІП, яка дозволяє визначити:

- тактову частоту створеного генератора;
- період повторення випадкових чисел на виході генератора;
- максимально можливе число на виході генератора;
- структуру генератора;
- параметри структурних елементів генератора.

Для випробувань створеного генератора в роботі запропонована методика утворення імітаційної моделі генератора та порядок роботи з нею.

Як видно із автореферату, здобувачем отримано результати, які дають змогу зробити висновок, про те, що найкращим варіантом ГПІП є схема, до складу якої входять опорний генератор і система порівняння вихідного та еталонного потоків із засобами корекції. Також автором обґрунтована необхідність пошуку нових методів оцінювання якості вихідного Пуассонівського потоку, оскільки існуючі методі розраховані виключно на оцінювання імпульсних потоків з рівномірним розподіленням ймовірностей. На основі цього висновку автор розробив і запропонував власний тест, побудований на основі критерію Пірсона що дає можливість визначати статистичні характеристики символів на виході генератору, а також методику його використання.

Виконані автором статистичні дослідження різноманітних складних генераторів довели можливість формування Пуассонівської імпульсної послідовності на основі псевдовипадкової бітової послідовності Голдмана.

Таким чином, результатом наукових досліджень, виконаних автором є науково обґрунтована методика розроблення та випробування складних генераторів Пуассонівського потоку, їх статистичного випробування, яка уявляє собою цінний інструментарій, що може бути використаний в галузі імітаційного моделювання та при вирішені питань, пов'язаних із захистом інформації.

Зі змісту автореферату слідує, що при виконанні роботи здобувачем була використана сучасна математична база, яка є адекватною до проведених досліджень. Використані засоби розроблення та моделювання відповідають меті роботи, є сучасними та не суперечить загально прийнятим підходам. Отримані результати є достовірними, відображені у публікаціях здобувача, обговорені на фахових науково-технічних конференціях на багатьох з яких автор цього відгуку був присутній особисто, а також підтверджені актами впровадження результатів у науково-дослідні роботи та у виробництво.

До достоїнств та переваг роботи, що відрізняє її від подібних робіт у галузі інформаційних технологій, можна віднести нові теоретико-практичні підходи до рішення науково-прикладних проблем, пов'язаних з формуванням псевдовипадкових послідовностей із заданим законом розподілення символів на виході генератору. Вважаю, що відмічене надало можливості отримати результати, які раніше не були досягнуті іншими дослідниками в прикладній галузі, тобто у галузі моделювання процесів, пов'язаних із будуванням систем інформаційної безпеки. Вони є новим внеском автора у науку про інформаційні процеси, що відбуваються у сучасних комп'ютерних системах.

Структура автореферату, повнота та достовірність матеріалів, зібраних в ході проведення наукових досліджень та які приведені в ньому, відповідають вимогам, які встановлені до кваліфікаційних робіт на здобуття наукового ступеня кандидата технічних наук. Зміст автореферату суть теми роботи відображає повністю.

Зауваження

1) Автореферат містить занадто багато загальновідомих положень в галузі статистики та способів оцінки потоків псевдовипадкових послідовностей. Автору слід би було зосередитись на більш детальному описанні своїх особистих наукових результатів.

2) У якості складових частин опорних генераторів автором були обрані конгруентні лінійні генератори, генератори Фібоначчі та регістри зі зворотним лінійним зв'язком, які були ретельно досліджені Дональдом Кнутом ще в 60-х роках і визнані недостатньо якісними. Очевидно, було б доцільно розглянути і більш досконалі сучасні варіанти генераторів.

Зазначені недоліки носять рекомендаційний характер та не знижують наукової цінності роботи в цілому, а також не впливають на отримані результати. Робота Ю.М. Костіва є повноцінним науковим дослідженням, яке виконане ним самостійно. У авторефераті відображені всі етапи дослідження. Отримані результати є обґрунтованими з математичної точки зору і дають можливість зробити висновок про їх наукову достовірність.

Вважаю, що робота «Генератори пуассонівських імпульсних послідовностей з покращеними характеристиками», відповідає вимогам до кандидатських дисертацій, які передбачені Постановою Кабінету Міністрів України №567 від 24 липня 2013 року «Про затвердження Порядку присудження наукових ступенів і присвоєння звання старшого наукового співробітника», а її автор, Костів Юрій Михайлович, заслуговує присвоєння наукового ступеня кандидата технічних наук зі спеціальності 05.13.05 – «Комп'ютерні системи та компоненти».

Завідувач кафедри Інформаційних систем в економіці
Одеського національного економічного університету

доктор технічних наук ***О.О.Скопа***

Доцент кафедри Інформаційних систем в економіці
Одеського національного економічного університету

кандидат технічних наук ***Ю.В. Щербина***

Підпис: Щербина
Засвідчую
Нач. відділу кадрів
"19" 03 2018

Підпис: Скопа
Засвідчую
Нач. відділу кадрів
"19" 03 2018