Голові разової спеціалізованої вченої ради
Національного університету «Львівська політехніка»
д.т.н., професору Нємковій Олені Анатоліївні

ВІДГУК

офіційного рецензента – к.т.н., доцента, Совина Ярослава Романовича,
доцента кафедри захисту інформації
Національного університету «Львівська політехніка»
на дисертаційну роботу
Горячого Олега Ярославовича
«Розроблення генераторів псевдовипадкових чисел на основі покращених методів обчислення елементарних функцій для задач кібербезпеки»,
подану до захисту на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека та захист інформації»
(галузь знань 12 «Інформаційні технології»)

Актуальність теми дисертаційної роботи.

Актуальність цієї дисертаційної роботи полягає в необхідності підвищення точності та швидкодії обчислення елементарних функцій, поширених у задачах кібербезпеки та захисту інформації, зокрема операцій ділення (DIV), функцій оберненого значення (RCP), квадратного кореня (SQRT) та зворотного квадратного кореня (RSQRT) в арифметиці з рухомою комою. Потреба в покращенні таких методів та їх оптимізації є особливо актуальною у випадках, коли відповідні реалізації недоступні на цільовій платформі у вигляді бібліотечних функцій або апаратних інструкцій, або ж не задовольняють вимог щодо точності, швидкодії чи підтримуваного формату. Крім того, критичним елементом більшості систем кібербезпеки та захисту інформації щодо безпеки, надійності та продуктивності є генерація випадкових та псевдовипадкових послідовностей високої якості. Це питання набуває особливої важливості для систем реального часу або у випадку обмежених ресурсів – зокрема для задач автентифікації, криптографії, стеганографії, симуляції, прийняття рішень і реагування на інциденти інформаційної безпеки.

Основна частина дослідження спрямована на розроблення та практичне тестування швидких і простих генераторів псевдовипадкових чисел (ГПВЧ), реалізованих на основі запропонованих чисельних алгоритмів в арифметиці з рухомою комою, що демонструють хороші статистичні властивості та є придатними для застосування в сфері інформаційної безпеки. Детальне тестування та порівняння генераторів випадкових і псевдовипадкових послідовностей має критичне значення насамперед для моделювання й

симуляції, криптографічних і стеганографічних систем та протоколів, а також для задач, пов'язаних із безпекою об'єктів критичної інформаційної інфраструктури. Відомо, що чимало поширених ГПВЧ можуть містити статистичні недоліки, мати криптографічні чи алгоритмічні вразливості, помилки реалізації або навіть містити криптографічні бекдори (наприклад, як у випадку генератора Dual_EC_DRBG).

Для більшості застосувань у сфері кібербезпеки та захисту інформації визначальними є простота, швидкодія та висока якість генераторів щодо статистичних властивостей згенерованих послідовностей. Для оцінювання випадковості істинно випадкових і псевдовипадкових послідовностей для криптографічних застосувань найбільш поширеним інструментом наукових досліджень є пакет тестів NIST Statistical Test Suite (STS), який також застосовується в даному дослідженні як основа аналізу статистичних характеристик.

Зв'язок теми дисертації з державними програмами, науковими напрямами університету та кафедри.

Дисертаційні дослідження виконувались у відповідності до наукового напрямку кафедри безпеки інформаційних технологій Інституту комп'ютерних технологій, автоматики та метрології Національного університету «Львівська політехніка», а також у межах науково-дослідних робіт кафедри безпеки інформаційних технологій за темами «Розробка та дослідження генераторів псевдовипадкових чисел і послідовностей» (№ держреєстрації 0113U005267), «Розробка та покращення ефективності алгоритмів обчислення елементарних функцій для задач захисту інформації» (№ держреєстрації 0120U103215) та «Розроблення стеганографічних методів приховування даних у цифрових зображеннях» (№ держреєстрації 0120U100024).

Наукова новизна основних результатів дисертації.

Наукова новизна результатів та основних положень даної роботи полягає у тому, що:

- ***Вперше*** запропоновано новий клас ГПВЧ на основі чисельних методів в арифметиці з рухомою комою, що демонструють максимальний період до $5{,}3 \cdot 10^9$ бітів, високу швидкодію (до 40 МБ/с на Intel i5) та задовільні статистичні характеристики. Близько 75–81% згенерованих послідовностей успішно проходять усі 188 тестів пакету NIST STS, що зіставно або краще ніж у відомих реалізацій бібліотеки random чи апаратних генераторів на ESP32 та Intel. Вони призначені, в першу чергу, для стеганографії, криптографії, комп'ютерних ігор, моделювання та симуляції.

- ***Вперше*** запропоновано адаптивні методи переключення магічних констант, зокрема для функцій RSQRT та SQRT, що передбачає розбиття області визначення функцій на піддіапазони з вибором оптимізованих констант.

Розроблені для задач захисту інформації методи мають невелику надлишковість порівняно з алгоритмом FISR та забезпечують необхідний компроміс між точністю, розміром таблиці пошуку та швидкодією, використовуючи пам'ять для зберігання констант. Вони призначені, в першу чергу, для мікроконтролерів, персональних комп'ютерів та ПЛІС. Порівняно з методом Вальчика та ін. для функції RSQRT метод переключення магічних констант для двох та восьми піддіапазонів (методи DC та 8DC) має в 11,8 та в 101,2 раза меншу максимальну відносну похибку.

- ***Вперше*** досліджено вплив запропонованих ГПВЧ на основі чисельних методів в арифметиці з рухомою комою на стеганографічні методи. Запропоновані генератори використано для вдосконалення методів LSB-стеганографії у випадку приховування даних у цифрових зображеннях. Застосування вдосконаленої моделі стеганосистеми дозволило підвищити рівень безпеки стеганографічних методів шляхом аналізу висококонтрастних і граничних ділянок зображень, а також зменшити розмір стеганоключа на 94% без послаблення конфіденційності, цілісності та стійкості до виявлення вбудованих даних.

- ***Вперше*** запропоновано методи покращення точності та швидкодії функцій RSQRT та RCP на основі алгоритму FISR, що через використання додаткових магічних констант (методи 2MC та 3MC) на основі цілочислових операцій дозволяють зменшити на 1–2 порядки кількість використаних операцій множення в арифметиці з рухомою комою. Вони забезпечують спрощення апаратної реалізації та підвищення продуктивності обчислень, зокрема для пристроїв з обмеженими ресурсами, мікроконтролерів, ПЛІС та високопродуктивних систем. Запропоновані методи двох та трьох магічних констант дозволяють зменшити максимальні відносні похибки в 11,9 та в 21,2 рази порівняно з відомими алгоритмами.

- ***Удосконалено*** методи апроксимації елементарних функцій в арифметиці з рухомою комою, зокрема для обчислення функцій RCP, RSQRT, RCBRT, SQRT, DIV, CBRT, EXP, LOG2 тощо, що поєднують методи Ньютона-Рафсона, Хаусхолдера, мінімаксної апроксимації, застосування наближених апаратних інструкцій Intel та ARM, методи магічної константи, оптимізовані параметри алгоритмів. Запропоновані вдосконалені методи забезпечують високу точність (зменшення максимальних відносних похибок в 2,2–32,9 рази, наприклад, похибка до 1 ULP або повна точність для чисел одинарної та подвійної точності) та швидкодію (зменшення кількості операцій, зокрема множень з рухомою комою, або використання таблиць пошуку) для задач кібербезпеки та захисту інформації. Отримали подальший розвиток методи модифікації та вдосконалення, а також вимірювання продуктивності алгоритмів обчислення елементарних функцій в арифметиці з рухомою комою.

- ***Вдосконалено*** методи чисельного багатовимірного пошуку на основі застосування ГПВЧ, методу багатовимірного прямого пошуку та методу золотого перетину, що використовуються для визначення таких практичних значень параметрів, що мінімізують максимальну відносну похибку алгоритмів. Наприклад, запропонований метод рандомізованої багатовимірної жадібної оптимізації, порівняно з іншими методами, дозволяє підвищити швидкість оптимізації параметрів та покращити їх результати, а також в перспективі може застосовуватись для інших задач кібербезпеки. Для функції RCP застосовані методи оптимізації дали змогу отримати варіанти алгоритмів із повною точністю для типів float і double.

- ***Отримала подальший розвиток*** методика автоматизації статистичного тестування псевдовипадкових послідовностей для задач кібербезпеки, що включає використання пакету тестів NIST STS, визначення періоду повторення, застосування графічних тестів, оцінку ентропії, аналіз кореляції, аналіз продуктивності ГПВЧ і генераторів істинно випадкових послідовностей на різних платформах. Запропоновані методи призначені для комплексної оцінки якості генераторів та криптографічних алгоритмів.

Ступінь обґрунтованості наукових положень дисертації, їх достовірність та новизна.

Автором було застосовано професійний підхід до постановки завдань та цілей дослідження. Також автором було проведено аналіз достатньої кількості наукових праць та одержано великий масив практичних результатів дослідження, що забезпечує високий ступінь обґрунтованості досліджень.

Наведені в дисертації результати є достатньо обґрунтованими, що підтверджується даними моделювання, експериментальних досліджень, розрахунків, практичними результатами тестування та актами впровадження. Наведені результати тестування алгоритмів на кількох різних платформах (Intel i-5, Intel i-7, Raspberry Pi 3, ESP-WROOM-32). Результати досліджень представлені у вигляді достатньої кількості таблиць, графіків та рисунків, що підтверджують отримані автором результати та зроблені висновки.

Основна ідея дисертації, що визначає її наукову новизну та актуальність, полягає у дослідженні можливості застосування арифметики з рухомою комою та вдосконалених методів швидкої апроксимації нелінійних елементарних функцій (RCP, SQRT, RSQRT тощо) на основі методу FISR для проєктування ГПВЧ, придатних для задач кібербезпеки та захисту інформації, які відповідають вимогам статистичних тестів NIST STS.

Наукове значення виконаного дослідження.

Отримані здобувачем наукові положення, висновки та практичні результати можуть бути використані під час проектування вдосконалених методів обчислення як розглянутих в роботі, так й інших елементарних функцій

в арифметиці з рухомою комою, зокрема на основі алгоритму FISR, а також для розробки на їх основі ГПВЧ із поліпшеними статистичними властивостями та потенційною криптостійкістю.

Запропоновані методи обчислення функцій та генерації псевдовипадкових чисел можуть бути використані під час побудови стеганографічних систем, біометричних систем, систем виявлення вторгнень, нейронних мереж, збереження конфіденційності баз даних, а також протоколів захищеного багатокористувацького обчислення. Одержані результати наукового дослідження є значущими для галузі 12 «Інформаційні технології» та спеціальності 125 «Кібербезпека та захист інформації».

Практичне значення одержаних результатів.

На основі отриманих алгоритмів можна реалізувати спеціалізовану математичну бібліотеку, що буде підтримувати ефективні обчислення елементарних функцій з різною точністю (наприклад, 13 або 14 біт для функції RCP; 10, 13 або 15 коректних біт для функції RSQRT). Також можна розробити відповідну бібліотеку запропонованих легких та швидких ГПВЧ на їх основі для застосувань у сфері кібербезпеки та захисту інформації, що мають задовільні статистичні характеристики відповідно до тестів NIST. Наведені в дисертації методи та програмні коди алгоритмів можна реалізувати як в програмному, так і в апаратному вигляді на інших платформах, зокрема на мікроконтролерах, CPU, FPGA та GPU.

Розроблено універсальні методи автоматизації статистичного тестування ГПВЧ на основі NIST STS, визначення періоду повторення, вимірювання швидкодії та продуктивності алгоритмів, придатні для застосування у криптографії, чисельних методах і задачах кібербезпеки.

Запропоновані алгоритми були реалізовані мовою C++ на платформах Intel i-5 та i-7, ESP-32 та Raspberry Pi, здійснено практичне тестування їх точності, швидкодії, а також згенерованих псевдовипадкових послідовностей. Зокрема, наукові та практичні результати виконаних досліджень використані у навчальному процесі кафедри безпеки інформаційних технологій Національного університету «Львівська політехніка» для студентів спеціальності 125 «Кібербезпека та захист інформації», зокрема з курсів «Комп'ютерні методи дослідження інформаційних процесів і систем», «Технології програмування», «Прикладна криптологія» та «Архітектура комп'ютерних систем», а також використовувались при виконанні науково-дослідних робіт кафедри. Отримані теоретичні та практичні результати досліджень впровадженні в ПП НВПП «Спаринг-Віст Центр».

Повнота оприлюднення результатів дисертаційної роботи.

Основні наукові результати за темою дисертації опубліковано у **15** наукових працях: **1** стаття у науковому періодичному виданні іншої держави,

яке включено до міжнародних наукометричних баз **Scopus** та **Web of Science**, **3** статті у періодичних фахових виданнях України з технічних наук, одна з яких входить до міжнародної наукометричної бази **Scopus**, **1** стаття в науковому нефаховому виданні України, **1** розділ колективної монографії та **9** публікацій в збірниках матеріалів та тез наукових конференцій, дві з яких включені до міжнародних наукометричних баз даних **Scopus** та **Web of Science**. Загалом, автором представлено **5** особистих доповідей на міжнародних конференціях, симпозіумах та консорціумах. Також, матеріали дисертації неодноразово обговорювались на наукових семінарах кафедри «Безпека інформаційних технологій» Національного університету «Львівська політехніка».

Вважаю, що основні положення та результати проведеного дисертаційного дослідження висвітлені у публікаціях в достатньому обсязі, а особистий внесок здобувача у колективно опублікованих працях є вагомим, полягає у формуванні та розробці ключових ідей, програмних реалізацій та результатів практичних досліджень.

Зауваження до дисертації.

Поряд із позитивними особливостями роботи, можна виділити наступні зауваження та дискусійні положення щодо змісту дисертації:

1. Формулювання наукової новизни дисертації є занадто детальним та містить ієрархічну структуру, зокрема щодо розробки покращених методів обчислення елементарних функцій. Окремі близькі елементи наукової новизни можна об'єднати.

2. Як було показано в роботі, вимога криптографічної стійкості генераторів псевдовипадкових чисел для сфери кібербезпеки та захисту інформації є надзвичайно актуальною поряд із статистичними характеристиками, особливо для блокового та потокового шифрування, а також з метою мінімізації можливих вразливостей інформаційних систем, що їх використовують. Проте, в роботі недостатньо уваги приділено забезпеченню криптографічної стійкості запропонованих генераторів на основі арифметики з рухомою комою, зокрема основний їх недолік – висока кореляція вихідних послідовностей. Проходження генераторами статистичних тестів NIST не гарантує криптографічної стійкості.

3. Запропоновані здобувачем генератори є перспективними для реалізації на 64-бітних платформах, що показано в 4-му розділі (пп. 4.2.3, 4.2.4 та 4.3.1), а також у додатках Е та Ж дисертації, на прикладі процесорів Intel Core 5-го та 7-го покоління на основі детального статистичного дослідження та тестування продуктивності. Практичну цінність та перспективність застосування запропонованих генераторів підвищило б також наведення аналогічних результатів для одноплатного 64-бітного мінікомп'ютера Raspberry Pi 3, що працює на основі процесора ARM Cortex A53.

4. У розділі 4.2.1 дисертації наведено перелік стандартних некриптостійких генераторів псевдовипадкових послідовностей, зокрема з бібліотеки random мови C++, та апаратних генераторів випадкових послідовностей, доступних на платформах Intel та ESP-WROOM-32 (наприклад, rdrand та esp_random), що використовувались для тестування та порівняння як альтернативні методи генерації. Варто було б навести також результати експериментального порівняння та дослідження запропонованих алгоритмів з відомими криптостійкими ГПВЧ, зокрема на основі криптографічних алгоритмів та протоколів (наприклад, ГПВЧ Fortuna). Серед популярних методів побудови криптографічно стійких генераторів можна навести наступні: на основі блокових шифрів (AES-CTR, ГОСТ 28147-89 та ANSI X9.17), потокових шифрів (RC4, SEAL, Salsa20, ChaCha20 та SNOW 3G), односторонніх функцій (BBS та RSA) та хеш-функцій (SHA-256 та SHA-3).

5. На початку розділу 4 дисертації наведено використані опції та параметри компіляції під час експериментальних досліджень на різних платформах. Зокрема, для персональних комп'ютерів та міні-комп'ютера Raspberry Pi було використано прапорець компіляції "–ffp=contract=on", а для мікроконтролера ESP-WROOM-32 – вже значення "–ffp-contract=fast", що може впливати на результати обчислень в арифметиці з рухомою комою, а відповідно на генерацію псевдовипадкової послідовності розглянутим методом. При цьому, у роботі не наводиться порівняння статистичних характеристик запропонованих генераторів при зміні параметрів компіляції.

6. У роботі описано недостатньо детально механізм вибору конкретних алгоритмів апроксимації елементарних функцій, наведених в додатку Д, що використовувались для проєктування генераторів псевдовипадкових чисел. Зокрема, не аргументовано вибір функцій RCP, RSQRT та SQRT у випадку вхідних значень, що не є простими числами, а також конкретних параметрів a і b у рекурентному рівнянні (3.3).

Слід відзначити, що наведені зауваження не знижують загальної позитивної оцінки дисертаційної роботи.

Висновок.

Незважаючи на виявлені неточності та зазначені зауваження дисертаційна робота Горячого Олега Ярославовича на тему «Розроблення генераторів псевдовипадкових чисел на основі покращених методів обчислення елементарних функцій для задач кібербезпеки» є цілісною, завершеною науково-дослідною роботою, виконаною здобувачем самостійно, що представлена на здобуття наукового ступеня доктора філософії за спеціальністю 125 «Кібербезпека та захист інформації» (галузь знань 12 «Інформаційні технології»). За своїм змістом, структурою, обсягом, науковою новизною та практичним значенням відповідає спеціальності

125 «Кібербезпека та захист інформації» та вимогам «Порядку присудження ступеня доктора філософії та скасування рішень разової спеціалізованої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого постановою Кабінету Міністрів України від 12 січня 2022 року № 44 зі змінами згідно з Постановою КМ №9341 від 21.03.2022, а її автор Горячий Олег Ярославович заслуговує на присудження йому наукового ступеня доктора філософії за спеціальністю 125 – Кібербезпека та захист інформації.

Офіційний рецензент:
кандидат технічних наук, доцент
доцент кафедри захисту інформації
Національного університету
«Львівська політехніка» Ярослав СОВИН

Підпис к.т.н., доцента Совина Я.Р. засвідчую:

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ • НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ "ЛЬВІВСЬКА ПОЛІТЕХНІКА" • ЗКПО 02071010

Проректор Микола ЛОГОЙДА