ВІДГУК

офіційного опонента - к.т.н., доцента кафедри захисту інформації Інституту комп'ютерних технологій, автоматики та метрології Національного університету "Львівська політехніка" Гарасимчука Олега Ігоровича

на дисертаційне дослідження

Дячука Ростислава Любомировича

на тему

«Розробка та дослідження інформаційної системи генерування високоентропійної послідовності випадкових чисел»

подану на здобуття наукового ступеня доктора філософії за спеціальністю 121 – Інженерія програмного забезпечення галузь знань 12 – Інформаційні технології

Актуальність дисертаційного дослідження.

Генерація послідовностей випадкових чисел (ПВЧ) є ключовим елементом сучасних криптографічних систем, адже саме від рівня ентропії та непередбачуваності залежить стійкість ключів, протоколів автентифікації та цифрових підписів. Використання слабких генераторів створює загрозу компрометації даних та відкриває можливості для криптоаналітичних атак. У контексті програмної інженерії ця проблема набуває особливої актуальності, оскільки розробка безпечних програмних продуктів вимагає інтеграції криптографічно стійких генераторів ПВЧ у процеси проектування, тестування та експлуатації систем. Забезпечення якісної генерації ПВЧ є невід'ємною частиною життєвого циклу програмного забезпечення, що включає моделювання загроз, розробку архітектури безпеки та впровадження стандартів захисту інформації. Таким чином, дослідження методів генерації ПВЧ та їх застосування у криптографії має не лише теоретичне, а й практичне значення для програмної інженерії, сприяючи створенню надійних і стійких до атак інформаційних систем.

Представлене дисертаційне дослідження розглядається саме цей напрямок, зокрема генерації ПВЧ на основі набору природних хаотичних процесів. А саме фотоелектричних явищ. Дослідження, проведені Дячуком Р.Л. створюють засади для покращення організації генерації високоентропійних

ПВЧ, призначених для захисту даних методами шифрування та кодування, а саме розробкою та дослідженням нових алгоритмів, програмних та інформаційних системна їх основі.

Серед існуючих та активно діючих в цьому напрямі технології генерації ПВЧ, залишають недостатньо опрацьованими ряд питань. Зокрема, як забезпечити співвідношення між швидкодією (продуктивністю) генерації ПВЧ і їх криптостійкістю та надійністю. Не достатньо вивченим є питання ефективності застосування відповідних правил клітинних автоматів для покращення рівня хаотичності згенерованої ПВЧ. Актуальним є завдання експрес оцінки ступені хаотичності ПВЧ без застосування тестування на ступінь хаотичності у відповідності до стандартів NIST. Надзвичайно актуальним є питання створення нових, або використання існуючих природних джерел, які можуть бути основою для генерації ПВЧ з максимально доступним рівнем хаотичності, а також інші питання, які досі не розв'язані.

Враховуючи вище зазначені виклики і питання, актуальним є розробка та дослідження інформаційної системи генерування високоентропійної послідовності випадкових чисел, чому і присвячено дисертаційне дослідження Дячука Р.Л. Тому, з точки зору розв'язання вище перелічених завдань, актуальність тематики дослідження не викликає сумніву.

Аналіз змісту дисертації та основні результати дослідження.

Дисертаційна робота включає анотації українською та англійською мовами, зміст, перелік умовних позначень, чотири розділи з підрозділами, висновки, список використаних джерел та додатки.

У вступі обґрунтовано актуальність теми, визначено предмет і об'єкт дослідження, сформульовано мету та завдання, описано методи, наукову новизну, теоретичне й практичне значення результатів, наведено дані про апробацію та структуру роботи.

Перший розділ містить огляд теоретичних аспектів генерації високоентропійних ПВЧ та характеристики апаратних генераторів. Розглянуто їхні переваги й недоліки, відомі підходи до створення джерел ентропії та програмно-апаратного середовища генераторів. Досліджено теоретичні основи

оцінювання випадковості та ентропії, проведено порівняльний аналіз сучасних генераторів ПВЧ для систем криптографічного захисту. Обґрунтовано доцільність використання фотоелектричних явищ, які можуть бути джерелами ентропії. Матеріали розділу висвітлено повно й ґрунтовно, що підтверджує актуальність та завдання дослідження.

Другий розділ присвячено експериментам із фотоелектричними явищами як джерелами ентропії: інтенсивність пікселів відеозображення, фотострум та темновий струм фотодіода. Встановлено, що ПВЧ, отримані з відеозображення, мають непередбачуваний характер, але продуктивність (85–288 Мбіт/с) є недостатньою для сучасних систем і не відповідає стандартам NIST. Генерація ПВЧ на основі фотоструму забезпечує до 2 Мбіт/с і частково проходить тести NIST. Використання темнового струму фотодіода як джерела ПВЧ дає до 980 Мбіт/с із високим рівнем непередбачуваності, а продуктивність можна підвищити завдяки високочастотним компонентам. Такі ПВЧ рекомендовано використовувати як вектори ініціалізації для гібридних генераторів.

Досліджено гібридний генератор, що поєднує три згадані джерела на основі фотоелектричних явищ із технологіями клітинних автоматів. Це дозволяє вирішити проблеми швидкодії, надійності, відповідності статистичним вимогам та стабільності постобробки. Програмна частина забезпечує масштабування, паралелізацію та можливість застосування нейронних мереж для навчання системи.

Третій розділ описує створення інформаційної системи для генерації ПВЧ із використанням гібридного підходу, заснованому на фотоелектричних явищах та клітинних автоматів (КА). Система забезпечує непередбачуваність, хаотичність і криптостійкість послідовностей. Інтерфейс дозволяє обирати джерело ПВЧ, діапазон значень, баланс між швидкістю та безпекою, а також зберігати й аналізувати результати. Продуктивність системи становить 0,980–288 Мбіт/с і може бути збільшена при використанні високочастотних компонентів. Масштабування та розпаралелення програмної частини дозволили підвищити продуктивність у 4 рази на прикладі генерації з відеозображення.

Четвертий розділ висвітлює практичне застосування системи: формування вхідних векторів для хеш-функцій, використання у стеганографічних системах та створення криптографічних ключів із високою ентропією. Розробки впроваджено на підприємствах галузі, зокрема у ТДВ «Завод Кварц», Kaskad Developers Group та компанії «Datawiz».

У висновках узагальнено результати дослідження, які чітко сформульовані та відповідають вимогам до дисертаційних робіт на здобуття ступеня доктора філософії. Список джерел охоплює достатню кількість українських та зарубіжних праць. Додатки містять перелік публікацій, дані про апробацію, акти впровадження та лістинг частини програмного коду.

Наукова новизна, оцінка обґрунтованості наукових положень дисертаційного дослідження та їх достовірності.

Дисертаційна робота містить ряд нових цікавих теоретичних та практичних результатів, розробку інформаційної системи та аналіз її параметрів на основі розроблених методів та алгоритмів. Зокрема, **вперше** ***запропоновано метод генерації ПВЧ, на основі фотоелектричних явищ, який забезпечує швидкість генерації ПВЧ до 1 Гбіт/сек при високому рівні випадковост***, який є доступними, придатними для гнучкого налаштування , що дозволяє підвищити ефективність генерації ПВЧ; ***розроблено інформаційну систему екстракції ПВЧ з стохастичних фізичних явищ, а саме, інтенсивності пікселів зображення веб-камери, фото- та темнового струму фотодіода***, яка містить модуль обробки отриманих ПВЧ за допомогою технології КА та аналітичний модуль інтелектуальної спрощеної статистичної оцінки згенерованих ПВЧ, що дозволяє пройти перевірку 12 тестів NIST з 15 можливих; ***запропоновано метод балансу між продуктивністю та якістю генерації ПВЧ***, яка може працювати у режимі неперервного потоку, що дозволяє у процесі генерації ПВЧ віддавати перевагу або швидкодії, або випадковості, що дозволяє керувати рівнем надійності згенерованої ПВЧ. Також, **дістали подальшого розвитку** ***методика використання КА***, зокрема створено бібліотеку на мові програмування Java по роботі з лінійними КА на основі примітивних побітових операцій низького рівня, запропоновано і експериментально доведено високу продуктивність, низьке

ресурсоспоживання і високу якість генерації і обробки ПВЧ запропонованим функціоналом лінійних клітинних автоматів хаотичного типу (правила 30, 90, 105), що дозволило скоротити час обробки майже на порядок у порівнянні з парадигмою об'єктноорієнтованого програмування; ***оптимізація балансу між високою продуктивністю і низькою ресурсоємності функціоналу на КА***; ***технологія генерації ПВЧ***, що переходить на якісний рівень – неперервна генерація ПВЧ заданої продуктивності та якості.

На підставі вище наведеного вважаю, що наукові результати, отримані дисертантом під час виконання дисертаційного дослідження, є вагомим науковим внеском у технології та засоби генерації високоентропійних ПВЧ.

Дисертаційна робота Дячука Р.Л. має чітку та логічну структуру і є цілісним та завершеним науковим дослідженням.

Зв'язок роботи з науковими програмами, планами, темами.

Дисертаційне роботу виконано в межах науково-дослідних робіт Чернівецького національного університету імені Юрія Федьковича, зокрема згідно з планами ***кафедри програмного забезпечення комп'ютерних систем*** за держбюджетною темою «Дослідження, моделювання та розробка програмного забезпечення складних динамічних систем» (Державний реєстраційний номер 0121U109232), а також у рамках акредитованої аспірантської програми «Інженерія програмного забезпечення», яку закінчив дисертант. Тематика дослідження, висвітленого у дисертаційній роботі, що опонується повністю відповідає згаданій освітньо-наукової програми III рівня вищої освіти та вище зазначеної теми науково-дослідної роботи кафедри.

Практична цінність одержаних результатів.

Робота має яскраво виражений практичний характер, хоча і містить ряд теоретичних положень. Її результати впроваджені та використовуються сучасними українськими підприємствами, про що свідчать відповідні акти впровадження від компаній ТДВ ЗАВОД «Кварц», Kaskad Developers Group та «Datawiz». Зокрема впроваджено технологію екстракції ПВЧ з інтенсивності пікселів веб-камери, фото- та темнового струму фотодіода, оброблених за

технологією КА та технологію генерації вхідного вектора хеш-функцій, стеганографічних алгоритмів та алгоритмів генерації криптографічних ключів.

Результатів дисертаційного дослідження застосовано у навчальних курсах кафедри програмного забезпечення комп'ютерних систем та кафедри радіотехніки та інформаційної безпеки Чернівецького національного університету імені Юрія Федьковича. А саме: «Криптографічний захист інформації», «Безпека в цифровому просторі», «Безпека програм та даних». Це дозволило підвищити якість навчального процесу та науково-дослідної роботи студентів та аспірантів.

Достовірність отриманих результатів та висновків.

Достовірність отриманих результатів та висновків, показаних в дисертаційній роботі Дячука Р.Л., забезпечується коректним формулюванням вихідних даних – мети та завдань дослідження, аргументованим вибором методів досліджень. Достовірність наукових положень обґрунтовано сучасними методами досліджень, які відповідають поставленій задачі, а також успішною апробацією отриманих результатів на всеукраїнських та міжнародних конференціях.

Оформлення результатів, дотримання вимог академічної доброчесності, повнота викладу наукових положень та результатів у публікаціях.

Дисертація має повний обсяг 260 сторінок друкованого тексту, при чому основна частина викладена на 137 сторінках. Список використаних джерел є репрезентативним.

Дисертаційна робота має логічну структуру, висновки та рекомендації відповідають отриманим у розділах результатам. Оформлення дисертації задовільних усім вимогам до такого роду кваліфікаційних наукових праць.

Результати перевірки на наявність академічного плагіату показують високий індивідуальний рівень дисертаційної роботи про що говорить і авторський викладення матеріалу по всьому тексту дисертації. Використання результатів інших авторів здійснюється із суворим посиланням на їхні джерела.

Тому, можна упевнено стверджувати, що дисертаційна робота Дячука Р.Л. відповідає нормам академічної доброчесності.

Основні положення дисертації та найважливіші її результати опубліковано у науковій періодиці та апробовані на наукових конференціях.

Зокрема дисертантом опубліковано 1 стаття у науковому виданні, що індексується у наукометричній базі SCOPUS; 4 статті – у виданнях, включених до переліку наукових фахових видань України; 7 робіт – у збірниках матеріалів міжнародних та всеукраїнських наукових конференцій. Отже, вимоги щодо кількості та якості наукових публікації автором виконано.

Дискусійні положення та зауваження до змісту дисертаційного дослідження.

До дискусійних положень та зауважень можна віднести наступне:

1. Автор розглядає веб-камеру як джерело ентропії, але не вказує, чи будь-яка веб-камера підходить для генерації ПВЧ? Які самі характеристики потрібно перевірити перед прийняттям рішення про доцільність її використання?

2. Стверджувати про "лавинний ефект" при кореляціїії сусідніх кадрів не зовсім коректно згідно визначення. Лавинний ефект це максимальна зміна наслідків (до 50%) при мінімальному відхиленні вхідних параметрів. Чи можна у вашому випадку стверджувати, що вхідним параметром є проміжок часу між сусідніми кадрами – досить хитка позиція, що потребує подальшої аргументації. На мій погляд краще ввести інший термін дуже близький до "лавинного ефекту".

3. Не продекларовано технічні вимоги для функціонування інформаційної системи (об'єм оперативної пам'яті, об'єм жорсткого диску, роздільна здатність монітора, швидкодія процесора, ширина USB каналу).

Однак, наведені недоліки та зауваження не є принциповими, не впливають на загальну позитивну оцінку дисертаційної роботи, не зменшують її наукової новизни та практичної цінності.

Загальні висновки.

Оцінюючи дисертаційну роботу у цілому, є усі підстави стверджувати, що за актуальністю теми, обсягом виконаних досліджень, їх обргунтованості, науковою новизною і цінністю одаржаних в ній результатів, а також її науково-теоретичним рівнем, дисертаційна робота Дячука Ростислава Любомировича на тему «Розробка та дослідження інформаційної системи генерування високоентропійної послідовності випадкових чисел», подана до захисту, є завершеним науковим дослідженням, що вносить значний внесок у розвиток методів генерації високоентропійних ПВЧ, оцінки ступінь їх хаотичності і визначення балансу між продуктивністю на надійністю створених ПВЧ.

Дисертація є завершеною науковою працею, яка цілком відповідає вимогам пунктів 6 – 9 «Порядку присудження степеня доктора філософії та скасування рішення разової вченої ради закладу вищої освіти, наукової установи, про присудження ступеня доктора філософії», затвердженого Постановою Кабінету Міністрів України від 12 січня 2022 р. № 44 (зі змінами), а її автор Дячук Ростислав Любомирович заслуговує на присудження степеня доктора філософії за спеціальністю 121 – «Інженерія програмного забезпечення» галузі знань 12 – «Інформаційні технології».

Офіційний опонент:

Доцент кафедри захисту інформації
Інституту комп'ютерних технологій,
автоматики та метрології
Національного університету
"Львівська політехніка" к.т.н., доцент Олег ГАРАСИМЧУК

Підпис доцента Гарасимчука О.І.

засвідчую

Учений секретар _____ /Р.Брилинський/

«____»_____ 2026р.