РЕЦЕНЗІЯ

кандидата технічних наук, директора навчально-наукового інституту фізико-технічних та комп'ютерних наук Чернівецького національного університету імені Юрія Федьковича, доцента

ШПАТАРА ПЕТРА МИХАЙЛОВИЧА

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.

Актуальність дисертаційного дослідження Дячука Ростислава Любомировича визначається швидким зростанням вимог до захисту інформаційних потоків у криптографії. Одним із ключових аспектів цього захисту є використання послідовностей випадкових чисел (ПВЧ). Генерація ПВЧ відіграє фундаментальну роль у сучасних криптографічних системах, адже рівень ентропії та непередбачуваності безпосередньо впливає на стійкість ключів, протоколів автентифікації та цифрових підписів. Використання ненадійних генераторів створює ризик компрометації даних і відкриває шлях для криптоаналітичних атак.

У сфері програмної інженерії ця проблема є особливо значущою, оскільки розробка безпечних програмних продуктів потребує інтеграції криптографічно стійких генераторів ПВЧ на всіх етапах життєвого циклу програмного забезпечення – від моделювання загроз і проектування архітектури безпеки до тестування та експлуатації.

Таким чином, дослідження методів генерації ПВЧ та їх застосування у криптографії має як теоретичну, так і практичну цінність, сприяючи створенню надійних інформаційних систем, стійких до атак.

У дисертації розглядається саме цей напрям, зокрема генерація ПВЧ на основі природних хаотичних процесів, зокрема фотоелектричних явищ. Дослідження Дячука Р.Л. закладають основу для вдосконалення процесів створення високоентропійних ПВЧ, призначених для захисту даних шляхом шифрування та кодування. Це включає розробку нових алгоритмів, програмних рішень та інформаційних систем.

Попри наявність сучасних технологій генерації ПВЧ, низка питань залишається недостатньо опрацьованою. Серед них – пошук оптимального балансу між швидкодією генерації та її криптостійкістю, дослідження ефективності застосування клітинних автоматів для підвищення рівня хаотичності, а також розробка методів експрес-оцінки хаотичності без використання стандартних тестів NIST. Особливо актуальним є питання створення нових або використання існуючих природних джерел для генерації ПВЧ з максимально можливим рівнем хаотичності.

З огляду на ці виклики, розробка та дослідження інформаційної системи генерації високоентропійних ПВЧ є надзвичайно важливим завданням, якому й присвячено дисертацію Дячука Р.Л. Актуальність теми дослідження не викликає сумнівів.

Аналіз змісту дисертації та основні результати дослідження.

Структура дисертаційної роботи 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, а також наведено дані про апробацію та структуру роботи.

У вступі дисертації аргументовано актуальність обраної теми, визначено предмет та об'єкт дослідження, сформульовано мету й завдання, окреслено

методи, наукову новизну, а також теоретичну та практичну значущість отриманих результатів. Подано інформацію про апробацію роботи та описано її структуру.

Перший розділ присвячено теоретичним аспектам генерації високоентропійних ПВЧ та аналізу апаратних генераторів. Розглянуто їхні переваги й недоліки, наведено відомі підходи до створення джерел ентропії та програмно-апаратного середовища генераторів. Описано теоретичні основи оцінювання випадковості та ентропії, здійснено порівняльний аналіз сучасних генераторів ПВЧ для систем криптозахисту. Обґрунтовано доцільність дослідження фотоелектричних явищ як потенційних джерел ентропії. Матеріали розділу подано комплексно, предметна галузь проаналізована глибоко й всебічно.

Другий розділ містить результати дослідження фотоелектричних явищ, запропонованих як джерела ентропії. Розглянуто використання інтенсивності пікселів відеозображення з камер, фотоструму та темнового струму фотодіода. Встановлено, що ПВЧ, отримана з інтенсивності пікселів, має непередбачуваний характер, але продуктивність у межах 85–288 Мбіт/с є недостатньою, а результати не відповідають стандартам NIST. Генерація на основі фотоструму фотодіода забезпечує до 2 Мбіт/с і частково відповідає вимогам NIST. Використання темнового струму фотодіода дає продуктивність до 980 Мбіт/с із високим рівнем непередбачуваності, причому цей показник можна підвищити за рахунок високочастотної апаратної частини. Такі ПВЧ рекомендовано застосовувати як вектори ініціалізації для гібридних генераторів. Автор також дослідив гібридний генератор, що поєднує три джерела на основі фотоелектричних явищ із клітинними автоматами. Це забезпечує вирішення проблем швидкодії, надійності, відповідності статистичним вимогам та стабільності постобробки. Програмна частина створює можливості для масштабування, паралелізації та використання нейронних мереж.

Третій розділ присвячено розробці інформаційної системи генерації ПВЧ, яка інтегрує три типи генераторів із подальшою обробкою клітинними автоматами. Такий підхід дозволяє забезпечити непередбачуваність,

хаотичність, криптостійкість та ізольованість послідовностей. Інтерфейс системи дає змогу керувати процесом генерації: обирати джерело ПВЧ, діапазон значень, баланс між швидкістю та рівнем безпеки, зберігати та аналізувати результати. Продуктивність системи становить 0,980–288 Мбіт/с і може бути збільшена завдяки високочастотним апаратним рішенням. Передбачено масштабування та розпаралелення програмної частини, що дозволило, наприклад, підвищити продуктивність генерації на основі відеозображення у чотири рази.

У четвертому розділі наведено результати практичного застосування системи: для формування вхідних векторів хеш-функцій, у стеганографічних системах із підвищеними вимогами до прихованості та стійкості, а також для створення криптографічних ключів із високим рівнем ентропії. Розробки впроваджено у виробництво на підприємствах галузі, зокрема на ТДВ «Завод Кварц», у Kaskad Developers Group та компанії «Datawiz».

У висновках узагальнено основні результати дослідження, які чітко сформульовані та відповідають вимогам до дисертаційних робіт на здобуття ступеня доктора філософії.

Список використаних джерел охоплює широкий спектр літератури, включно з працями українських та зарубіжних авторів.

Додатки містять перелік публікацій за темою, дані про апробацію, акти впровадження та частину програмного коду.

Наукова новизна та обґрунтованість результатів

Дисертаційне дослідження містить низку нових теоретичних і практичних напрацювань, включно з розробкою інформаційної системи та аналізом її параметрів на основі запропонованих методів і алгоритмів.

Вперше:

- розроблено метод генерації ПВЧ на основі фотоелектричних явищ, що забезпечує швидкість до 1 Гбіт/с при високому рівні випадковості та можливості гнучкого налаштування, що підвищує ефективність процесу.

- створено інформаційну систему екстракції ПВЧ зі стохастичних фізичних явищ (інтенсивність пікселів веб-камери, фото- та темновий струм фотодіода),

яка включає модуль обробки даних за технологією клітинних автоматів (КА) та аналітичний модуль статистичної оцінки, що дозволяє успішно пройти 12 із 15 тестів NIST.

- запропоновано метод балансування між продуктивністю та якістю генерації ПВЧ у режимі неперервного потоку, що дає змогу керувати рівнем надійності результатів.

Подальшого розвитку набули:

- методи використання КА: створено бібліотеку на Java для роботи з лінійними КА на основі низькорівневих побітових операцій, доведено їхню високу продуктивність, низьке ресурсоспоживання та якість генерації ПВЧ, використання хаотичних правил (30, 90, 105) дозволило скоротити час обробки майже у десять разів порівняно з об'єктно-орієнтованим підходом.

- оптимізація балансу між продуктивністю та ресурсоємністю, що вивело технологію генерації ПВЧ на якісно новий рівень – неперервна генерація із заданими параметрами продуктивності та якості.

Отримані результати становлять вагомий внесок у розвиток технологій генерації високоентропійних ПВЧ.

Дисертація Дячука Р.Л. має чітку структуру та є завершеним науковим дослідженням.

Зв'язок із науковими програмами

Робота виконана в межах науково-дослідних проектів Чернівецького національного університету імені Юрія Федьковича, відповідно до планів кафедри програмного забезпечення комп'ютерних систем за держбюджетною темою «Дослідження, моделювання та розробка програмного забезпечення складних динамічних систем» (№ 0121U109232), а також у рамках акредитованої аспірантської програми «Інженерія програмного забезпечення». Тематика дисертації повністю відповідає освітньо-науковій програмі III рівня та зазначеній темі кафедральних досліджень.

Практична цінність

Робота має виражений прикладний характер. Її результати впроваджені на українських підприємствах («Кварц», Kaskad Developers Group, «Datawiz»), що

підтверджується актами впровадження. Зокрема, реалізовано технологію екстракції ПВЧ із сигналів веб-камери та фотодіода, а також технологію генерації вхідних векторів для хеш-функцій, стеганографічних алгоритмів і криптографічних ключів.

Результати використано у навчальних курсах кафедри програмного забезпечення комп'ютерних систем та кафедри радіотехніки й інформаційної безпеки, зокрема «Криптографічний захист інформації», «Безпека в цифровому просторі», «Безпека програм та даних», що сприяло підвищенню якості освітнього процесу та наукової роботи студентів і аспірантів.

Достовірність результатів

Достовірність забезпечується коректним формулюванням мети й завдань, аргументованим вибором методів та їх відповідністю поставленим задачам. Результати апробовані на всеукраїнських і міжнародних конференціях, що підтверджує їх наукову надійність.

Оформлення та академічна доброчесність

Дисертація обсягом 260 сторінок (основна частина – 137 сторінок) має логічну структуру, висновки узгоджуються з отриманими результатами. Список джерел є репрезентативним. Перевірка на плагіат засвідчила високий рівень індивідуальності роботи, використання чужих результатів здійснено з належним посиланням. Таким чином, дисертація відповідає нормам академічної доброчесності.

Основні положення та результати опубліковано у наукових виданнях і презентовано на конференціях: 1 стаття у виданні, що індексується в SCOPUS; 4 статті у фахових виданнях України; 7 робіт у збірниках матеріалів міжнародних та всеукраїнських конференцій. Вимоги щодо кількості та якості публікацій виконано.

Дискусійні положення та зауваження до змісту дисертаційного дослідження.

До дискусійних положень та зауважень можна віднести наступне:

1. Автор згадує, що в якості джерела ентропії використовує фотодіод з високою кантовою ефективністю, але не обґрунтовує це положення. А саме, як

пов'язана квантова ефективність фотодіода із якістю (непередбачуваністю) створеної на його основі ПВЧ.

2. При розгляді темнового струму фотодіода як джерела ентропії, показано, що найкращі результати отримані про 50 °С. Але не досліджено як випливають на якість ПВЧ більші температури. Було би доцільно вивчити це питання.

3. Щодо вимірювання темнового струму фотодіоду. На рис. 2.8 є позиція 4 "вольтметр постійного струму", а на рис. 2.11 присутній ППТН (поз. 7). З якою метою здійснені зміни і як вони впливають на генерацію ПВЧ?

4. Добре би було проаналізувати можливість роботи створеної інформаційної системи з існуючими криптографічними приладами, які використовують інші джерела ентропії.

У цілому, перелічені питання та зауваження не є суттєвими і принциповими, не зменшують наукової новизни та практичної цінності роботи і не впливають на загальну цілком позитивну оцінку дисертаційної роботи.

Загальні висновки.

Оцінюючи дисертаційну роботу у цілому, є усі підстави стверджувати, що за актуальністю теми, обсягом виконаних досліджень, їх обргунтованості, науковою новизною і цінністю одержаних 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 ступеня 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 ступеня доктора

філософії за спеціальністю 121 – «Інженерія програмного забезпечення» галузі знань 12 – «Інформаційні технології».

Рецензент:

Директор навчально-наукового інституту
фізико-технічних та комп'ютерних наук
Чернівецького національного університету
імені Юрія Федьковича, к.т.н., доцент Петро ШПАТАР