ВІДГУК

офіційного опонента – доктора технічних наук, професора кафедри математичного моделювання та аналізу даних навчально-наукового інституту комп'ютерних наук та штучного інтелекту Харківського національного університету імені В.Н. Каразіна БАРАННІКА Володимира Вікторовича на дисертаційну роботу 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.

Сучасне суспільство оперує інформаційними потоками, які повинні бути захищені з точки зору кибербезпеки. Тому створення алгоритмів та програмного забезпечення методами програмної інженерії для кібербезпеки, є актуальним завданням. Один з напрямків такого захисту ґрунтується на генерації послідовеностей випадкових чисел (ПВЧ). Дослідження в цьому напрямку сприяє покращенню розуміння організації безпеки потоків даних шляхом шифрування та кодування.

Існуючі алгоритми та технології захисту інформації, в яких застосовуються ПВЧ, залишають нерозв'язаними такі питання, як оптимальний вибір співвідношення між продуктивністю генерації ПВЧ і їх надійністю, ефективністю застосування клітинних автоматів з метою підвищення рівня хаотичності ПВЧ, експрес діагностика рівня хаотичності згенерованих ПВЧ, створення джерел ПВЧ з максимальним рівнем хаотичності ті інші.

Тому, дисертаційна робота Дячука Ростислава Любомировича «Розробка та дослідження інформаційної системи генерування високоентропійної послідовності випадкових чисел», яка зорієнтована на розв'язання вище зазначених питань, є безумовно актуальною.

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

Дисертаційне дослідження виконано на кафедрі програмного забезпечення комп'ютерних систем Чернівецького національного університету імені Юрія Федьковича. Її зміст відповідає тематиці науково-дослідної роботи: «Дослідження, моделювання та розробка програмного забезпечення складних динамічних систем» (Державний реєстраційний номер 0121U109232). Доцільно зазначити, що кафедра проводить діяльність за акредитованою аспірантською програмою «Інженерія програмного забезпечення», яку закінчив дисертант. Тематика дослідження опонованої дисертаційної роботи повною мірою відповідає зазначеній освітньо-науковій програми III рівня вищої освіти та вище зазначеної теми науково-дослідної роботи кафедри.

Структура дисертації.

Дисертація є завершеної науково-дослідною роботою, що складається з анотації (українською та англійською мовами), змісту, переліку умовних скорочень, чотирьох розділів, висновків, списку використаних джерел та додатків.

У *вступі* обґрунтовано актуальність теми дисертаційного дослідження, визначено предмет і об'єкт дослідження, сформульовано мету та завдання дослідження, методи дослідження, наукову новизну, теоретичне та практичне значення отриманих результатів, подано відомості про апробацію роботи та наведено її структуру.

Перший розділ містить ключові відомості з теорії генерації високоентропійних ПВЧ, а також відомості про апаратні генератори ПВЧ. Розглянуто різні підходи до створення джерела ентропії та програмно-конструкторського оточення. Розглянуто теоретичні основи оцінювання випадковості та ентропії, а також проведено порівняльний аналіз сучасних найбільш відомих генераторів ПВЧ в системах криптобезпеки. Обґрунтовано доцільність дослідження фото-електричних явищ (ФЕЯ) та квантових як джерела ентропії для генерації ПВЧ.

Матеріали розділу висвітлено повно, проведений ґрунтовний аналіз предметної галузі, ретельно та всебічно обґрунтовано актуальність та завдання дисертаційного дослідження.

У *другому розділі* дисертаційного дослідження наведено результати дослідження ПВЧ, джерелом яких є природні явища, а саме - інтенсивність пікселів зображення з веб-камери, або цифрової відеокамери, фото- та темнового струму фотодіода з високою квантовою ефективністю. Показано, що найкращі властивості мають ПВЧ згенеровані на основі фотоструму фотодіода. Вони є непередбачуваними, їх продуктивність досягає 2 Мбіт/сек. При цьому вони частково відповідають тестам NIST. А ПВЧ створені за допомогою темнового струму фотодіода, мають абсолютно непередбачуваний характер і продуктивність до 980 Мбіт/сек. Така продуктивність може бути збільшена при застосування високочастотної апаратної частини. Також вивчено властивості гібридного генератора ПВЧ. Він поєднує у собі генератор на основі відео або веб-камери і клітинних автоматів (КА). Це об'єднання вирішує питання по швидкодії, надійності, контрольованості, відповідності статистичним вимогам та вимогам до безпеки і стабільності пост-обробки. Також програмна частина гібридного генератора відкриває теоретично необмежені можливості по масштабованості та паралелізації процесу генерації, а також машинного навчання за допомогою нейронної мережі.

У *третьому розділі* описано створення інформаційної системи для генерації ПВЧ на основі усіх трьох генераторів із обробкою отриманих ПВЧ за допомогою клітинних автоматів. Таке об'єднання повністю забезпечує вимоги до непередбачуваності та хаотичності ПВЧ, їх криптостійкості та ізольованості послідовностей. Інформаційна система дозволяє обирати:

- джерело ПВЧ (база даних, файл, на основі відео-, або веб-камери, фото- та темнового струму фотодіода з високою квантовою ефективністю, гібридного з обробкою числових послідовностей за допомогою клітинних автоматів);
- діапазони значень (біти 0-1, стандартний діапазон 1-256, або користувацький діапазон);
- баланс між швидкістю генерації та рівнем безпеки, зберігати її та аналізувати.

Досягнута продуктивність інформаційної системи знаходиться у межах 0,980 - 288 Мбіт/с. Продуктивність може бути суттєво збільшена при використанні високочастотної апаратної частини. Вона передбачає можливість масштабувати всю програмну частину генератора, або ж розпаралелити процес обробки «сирої» числової послідовності всередині блоку програмної частини. Це, на прикладі ПВЧ, згенерованої з відео-зображення та веб-камери, дозволило підвищити продуктивність у 4 рази.

Четвертий розділ присвячено результатам застосування створеної інформаційної системи для формування вхідного вектора хеш-функції, для стеганографічних систем із підвищеними вимогами до прихованості та стійкості, а також для формування криптографічних ключів із високим рівнем ентропії та криптостійкості. Ці результати впроваджено у ТДВ ЗАВОД «Кварц», Kaskad Developers Group та компанії «Datawiz» для підвищення криптостійкості їх програмного забезпечення.

Висновки дисертаційної роботи сформульовано чітко, вони повністю охоплюють отримані результати і повністю задовольняють вимоги, що ставляться до результатів дисертації на здобуття наукового ступеня доктора філософії.

Список використаних джерел повністю охоплює предметну галузь і вказує на аналіз значної кількості літературних джерел, як українських, так і закордонних авторів.

Додатки містять список публікацій за темою дисертації, відомості про апробацію, акти впровадження результатів дисертаційної роботи та лістинг частини коду програмного забезпечення.

Наукова новизна одержаних результатів.

До найсуттєвіших та нових наукових результатів дисертаційної роботи Дячука Р.Л., на мою думку, можна віднести наступне:

1. Автором вперше:

- запропоновано метод генерації ПВЧ, особливістю якого є використання фотоелектричних явищ, що, на відміну від існуючих методів, забезпечує швидкість генерації ПВЧ від 0,288 до 1 Гбіт/сек при високому рівні випадковості, є доступними, високопродуктивними, здатними 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, на відміну від аналогів, містить модуль обробки отриманих ПВЧ за допомогою технології КА та аналітичний модуль інтелектуальної спрощеної статистичної оцінки згенерованих ПВЧ. Це дозволяє пройти перевірку 12 тестів NIST з 15 можливих;

- запропоновано метод балансу між продуктивністю та якістю генерації ПВЧ, яка на відміну від аналогів, 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;

2. Набуло подальшого розвитку:

- методика використання КА: 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 ресурсо-споживання і високу якість генерації і обробки ПВЧ запропонованим функціоналом лінійних клітинних автоматів хаотичного типу (правила 30, 90, 105). Це дозволило скоротити час обробки майже на порядок у порівнянні з парадигмою об'єктно-орієнтованого програмування;

- оптимізація балансу між високою продуктивністю і низькою ресурсо-ємністю функціоналу на КА;

- технологія генерації ПВЧ, що переходить на якісний рівень – неперервна генерація ПВЧ заданої продуктивності та якості.

Вважаю, що отримані дисертантом наукові результати є вагомим внеском у методи та засоби генерації високоентропійних ПВЧ.

Достовірність отриманих результатів та висновків.

Достовірність результатів, отриманих в дисертаційній роботі Дячука Р.Л., забезпечено коректною постановкою задачі, мети та завдань дослідження, послідовним їх розв'язанням та аргументованим вибором методів та засобів розробки програмного забезпечення.

Достовірність наукових положень, висновків та рекомендацій, підтверджуються сучасними методами досліджень, які відповідають поставленій задачі, глибоким аналізом об'єкта та предмета дослідження за

допомогою адекватних методів, а також успішною апробацією на всеукраїнських та міжнародних конференціях.

Практична цінність одержаних результатів.

Практична цінність наукових результатів дисертаційної роботи Дячука Р.Л. полягає у практичному застосуванні теоретичних положень методів та технологій. Це підтверджуються актами про впровадження результатів дисертації. Зокрема у компаніях ТДВ ЗАВОД «Кварц», Kaskad Developers Group та «Datawiz» використовують: технологію екстракції ПВЧ з інтенсивності пікселів веб-камери, фото- та темнового струму фотодіода, оброблених за технологією клітинних автоматів та технологію генерації вхідного вектора хеш-функцій; стеганографічних алгоритмів та алгоритмів генерації криптографічних ключів.

Варто зазначити, що результати дисертаційного дослідження використовуються у:

- навчальних курсах кафедри програмного забезпечення комп'ютерних систем Чернівецького національного університету імені Юрія Федьковича, пов'язаних з крипто захистом;
- методичних розробках;
- навчальних посібниках, які застосовуються в освітньому процесі і науково-дослідній роботі студентів та аспірантів.

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 дисертаційної роботи на наявність академічного плагіату свідчать про високу індивідуальність роботи. Авторський стиль простежується по всьому тексту дисертації. Відсутні запозичення і використання результатів інших авторів без посилання на їхні джерела. Це підтверджує, 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.

Однак, дисертаційна робота Дячука Р.Л. не позбавлена деяких недоліків. До них можна віднести наступне:

1. При викладенні матеріалу бажано пояснити принципову різницю між генерацією випадкових чисел та генерацією саме послідовностей випадкових чисел. Зокрема сучасні вимоги до довжини послідовності, продуктивність генерації, питанням безпеки, надійності та зручності використання (usability).

2. У заявленій у розділі 2 пункт 2.1 (стор. 46) цифровій веб-камері відсутні: технічні характеристики, які унеможливлюють стверджувати про відсутність первинної пост-обробки всередині самої камери; дані про довгий час неперервної надійної роботи веб-камери. Бажано було б провести дослідження на веб-камері відомої марки смартфона чи айфона.

3. Аналізуючи відповідність сгенерованої послідовності випадкових чисел вимогам NIST (SP 800-22) табл.3.1 не пояснено низький рівень проходження тесту 7. Non-overlapping Template Matching та тесту 15. Random Excursions Variant. Не вказано можливі причини, критичність та шляхи подолання.

4. Перевірка якості хешування проводились на коротких фразах. Проте саме об'єкти великого розміру представляють науково-дослідницький інтерес. Логічно допустити, що запропонований алгоритм успішно справиться з таким завданням. Однак необхідні дослідження не були проведені.

5. Деякі англійські наукові терміни перекладені не однозначно коректно. Наприклад, «seed» в одному місці трактується як «затравка», а в іншому як «початковий вектор».

Вважаю, що викладені зауваження не є визначальними і не зменшують загальної наукової новизни та практичної значущості результатів дисертаційної роботи та не впливають на її загальну позитивну оцінку.

Загальні висновки.

Подана до захисту дисертаційна робота є завершеною науковою працею, яка містить нові, добре обгрунтовані результати. Дисертація розвязує актуальну науково-прикладну задачу розробка інформаційної системи для генерації

високоентропійних ПВЧ, оцінювання ступеня їх хаотичності та визначення балансу між продуктивністю на надійністю створених ПВЧ.

Тема, зміст та результати дисертації повністю відповідають спеціальності 121 – інженерія програмного забезпечення.

Зважаючи на актуальність теми, обґрунтованість наукових положень, поданих у дисертації, їх новизну та практичну цінність, вважаю, що дисертаційна робота за темою «Розробка та дослідження інформаційної системи генерування високоентропійної послідовності випадкових чисел» 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).

Автор дисертації Дячук Ростислав Любомирович заслуговує на присудження ступеня доктора філософії за спеціальністю 121 – інженерія програмного забезпечення галузі знань 12 «Інформаційні технології».

Офіційний опонент:

професор кафедри математичного моделювання та аналізу даних навчально-наукового інституту комп'ютерних наук та штучного інтелекту Харківського національного університету імені В.Н. Каразіна

доктор технічних наук, професор Володимир БАРАННІК

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ В. Н. КАРАЗІНА * КОД 02071205

ПІДПИС ЗАСВІДЧУЮ
Начальник відділу кадрів