РЕЦЕНЗІЯ

кандидата технічних наук, доцента
Миронець Ірини Валеріївни
на дисертаційну роботу Скуцького Артема Борисовича
«Метод і моделі системи захищеного інформаційного обміну з нероздільним факторіальним кодуванням даних»
подану на здобуття ступеня доктора філософії
за спеціальністю 123 Комп'ютерна інженерія
галузі знань 12 Інформаційні технології

1. Актуальність теми дисертаційної роботи

Забезпечення надійного передавання інформації в умовах зашумленого каналу зв'язку залишається однією з ключових задач сучасної інформаційної інженерії. Ця проблема є особливо гострою для систем з обмеженими ресурсами та відсутністю зворотного каналу, таких як, безпілотні засоби зв'язку, сенсорні мережі та компоненти військових комунікацій. Втрата синхронізації або помилка під час декодування інформації в таких системах може мати незворотні наслідки.

У класичних підходах до організації інформаційного обміну функції синхронізації, захисту та кодування реалізуються окремо, що призводить до збільшення загальної складності системи, потребує додаткових обчислювальних ресурсів та знижує її адаптивність до завад. Така архітектурна роздільність є обмеженням у випадках, коли необхідне одночасне досягнення синхронізації, завадостійкості та криптографічного захисту в реальному часі.

У роботі автор дисертації використовує методи нероздільного факторіального кодування (НФКД), що передбачає використання перестановок як засіб представлення інформації і відкриває можливості для інтеграції зазначених функцій синхронізації та захисту. Використання НФКД для забезпечення надійного та достовірного обміну вже продемонстрував значний потенціал у роботах інших дослідників. Однак запропоновані методи кадрової синхронізації на основі НФКД є далеко не ідеальними та потребують подальшого розвитку та вдосконалення.

У роботі Скуцький А.Б. вирішує важливу науково-технічну задачу що полягає у забезпеченні захищеного інформаційного обміну в системах з нероздільним факторіальним кодуванням зашумленим каналом зв'язку. Особливу увагу зосереджено на ситуаціях, коли початковий момент передавання інформаційної послідовності невідомий, що унеможливлює застосування відомих засобів підтвердження прийому та ініціалізації

синхронізації. Саме ця задача визначає актуальність розробки нових методів кадрової синхронізації, які були б стійкими до шумів та не потребували зворотного каналу зв'язку.

Поєднання скінченних полів квадратних матриць із нероздільним факторіальним кодуванням відкриває перспективні можливості для побудови уніфікованих криптографічних і синхронізаційних рішень. Водночас, зазначений напрям досі залишається недостатньо дослідженим як у контексті формалізації відповідних математичних конструкцій, так і з точки зору їх практичного впровадження в реальні системи інформаційного обміну.

У роботі автором дисертаційного дослідження визначено початковий напрямок формування математичного підґрунтя для побудови скінченних полів матриць другого порядку у полі простих чисел і поєднання з НФКД.

З огляду на викладене, дисертаційне дослідження, присвячене розробці методу та моделей системи захищеного інформаційного обміну з НФКД, є актуальним, науково обґрунтованим і цілком відповідає сучасним викликам в галузі комп'ютерної інженерії та інформаційної безпеки.

2. Наукова новизна результатів

Наукові результати, отримані в результаті виконання дисертаційного дослідження:

- *набув подальшого розвитку* метод кадрової синхронізації нероздільних факторіальних кодів, що використовує як синхрокомбінацію перестановку чисел, яка має максимальне значення мінімальної відстані Хеммінга від її двійкового представлення до всіх її циклічних зсувів, а також кореляційну та мажоритарну обробку прийнятих фрагментів, де довжина фрагмента дорівнює довжині синхрокомбінації, який за рахунок використання ковзного вікна фіксованого розміру та врахування серії спрацювань підсистеми синхронізації дозволяє встановити кадрову синхронізацію приймальної та передавальної станцій системи інформаційного обміну за високої ймовірності бітової помилки та невідомого моменту початку приймання синхрокомбінацій передавача, забезпечуючи необхідні показники ймовірності правильної та хибної синхронізації;
- *набула подальшого розвитку* математична модель процесу виявлення синхрокомбінації систем передавання інформації з нероздільним факторіальним кодуванням даних, що використовують кореляційну та мажоритарну обробку прийнятих фрагментів, яка за рахунок дослідження механізмів перетворення синхрокомбінації в її

зсув в умовах застосування приймачем ковзного вікна фіксованого розміру дозволяє оцінити ймовірності правильної та хибної кадрової синхронізації;

– *вперше розроблено* математичну модель скінченного поля квадратних матриць порядку 2 над скінченним полем простих чисел $\mathbb{Z}_p$, яка за рахунок збільшення порядку поля квадратних матриць до значення p^2, проте збереження порядку p поля $\mathbb{Z}_p$, в якому виконують операції перетворення, дозволяє підвищити стійкість криптографічних систем, які базуються на операціях у скінченому полі.

3. Практичне значення результатів, отриманих у результаті виконання дисертаційного дослідження:

– *розроблено* алгоритм кадрової синхронізації на основі ковзного вікна та серії спрацювань підсистеми синхронізації, що може використовуватися для організації захищеного інформаційного обміну у симплексних каналах із високою імовірністю бітових помилок без попереднього узгодження моменту приймання кадрової синхрокомбінації. Розроблений алгоритм забезпечив успішне встановлення кадрової синхронізації в кожному з 1000 випробувань імітаційної моделі за довжини перестановки-синхрокомбінації $M = 8$. Кожне випробування передбачало встановлення кадрової синхронізації для ймовірностей бітової помилки в каналі від $p_0 = 0.1$ до $p_0 = 0.4$ та процедури надійного передавання блоку корисних даних при відсутності попереднього узгодження початкового моменту інформаційного обміну;

– *розроблено* імітаційну модель системи обміну перестановками, що дозволяє досліджувати вплив різних значень імовірності бітової помилки в каналі зв'язку p_0 і структури синхрокомбінації на імовірнісні показники синхронізації. Отримані результати проведення 10000 випробувань дозволили експериментально визначити максимальну довжину серії хибних спрацювань підсистеми синхронізації $l_{false\_synch} = 4$ для довжини ковзного вікна 75 фрагментів і $p_0 = 0.4$. Отримане значення максимальної довжини серії хибних спрацювань підсистеми синхронізації дозволило задати мінімальний поріг серії спрацювань підсистеми

синхронізації, тим самим забезпечуючи необхідні показники ймовірності встановлення правильної кадрової синхронізації;

- *розроблено* алгоритм перетворення матриць у перестановки, що може бути використаний для перетворення квадратних матриць у перестановки при генерації ключів-перестановок та інтегрувати матричні обчислення і нероздільне факторіальне кодування (НФКД);
- *створено* макетний зразок системи інформаційного обміну, побудований на базі мікроконтролера nRF52840 із використанням ISM-радіоканалу. Макет може бути застосований як прототип для побудови безпечних IoT-рішень або навчальний стенд. Розроблені алгоритми обробки та перетворення текстових повідомлень у перестановки дозволяють стискати текстові повідомлення, що підлягають передаванню в вигляді перестановок. Кількість бітів, що необхідна для передавання двох текстових символів латинського алфавіту (закодовані в перестановку), становить 3 байти замість $M = 8$ байтів, необхідних у звичайному поданні ASCII. Введена надлишковість у текстовому повідомленні забезпечує криптографічний захист , дає можливість перевіряти цілісність інформації шляхом застосування додаткових методів НФКД. Створені приймально-передавальні пристрої побудовані на базі системи на кристалі (System on Chip, SoC) nRF52840 від виробника Nordic Semiconductor і не залежать від архітектури операційної системи комп'ютерної системи, де необхідно реалізувати захищений обмін, можуть бути використані IoT рішеннях;
- *розроблено* програмний код для операцій над перестановками з використанням GPU (CUDA). Розроблені алгоритми множення перестановок дозволили оцінити доцільність використання GPU для прискорення криптографічних операцій над перестановками у системах криптографічного захисту на основі НФКД в порівнянні з обчисленнями на CPU і можуть застосовуватися для оцінки стійкості криптографічних протоколів до атак методом перебору, а також для реалізації високопродуктивних обчислень у серверних системах і системах захищеного інформаційного обміну. Результати дослідження ефективності GPU обчислень, можуть бути використані під час вибору апаратної платформи для реалізації криптографічних протоколів.

4. Структура дисертаційної роботи, оцінка змісту дисертації та її завершеність

Дисертаційна робота Скуцького А.Б. має логічно витриману структуру, що відповідає змісту та послідовності наукового дослідження. Робота складається зі вступу, чотирьох основних розділів, висновків, списку використаних джерел та додатків. Загальний обсяг становить 237 сторінок, включає 62 рисунки, 11 таблиць і 197 найменувань у списку літератури.

Структура роботи логічно відображає послідовність дослідження: від постановки проблеми та аналізу стану наукової розробки теми до обґрунтування теоретичних положень, розробки математичних моделей, алгоритмів та практичного впровадження результатів.

У вступі подано обґрунтування актуальності теми, сформульовано мету, об'єкт, предмет і завдання дослідження, а також визначено положення, що виносяться на захист.

Перший розділ містить огляд сучасного стану предметної області, аналіз переваг і обмежень наявних методів синхронізації, зокрема в контексті симплексних каналів зв'язку з високим рівнем шуму. Окремо розглянуто ситуацію невизначеності початку передавання синхрокомбінацій, яка може спричинити некоректне спрацювання приймальної частини системи. Підкреслено недоліки існуючих методів кадрової синхронізації з НФКД у таких умовах та сформульовано потребу в новому підході.

У другому розділі описано математичну модель процесу синхронізації з використанням ковзного вікна, здійснено її імовірнісну оцінку в умовах дії завад. Розроблено метод кадрової синхронізації для симплексних каналів зв'язку з використанням ковзного вікна і серії спрацювань синхронізуючої підсистеми. Ефективність методу підтверджено результатами імітаційного моделювання.

Третій розділ містить теоретичне обґрунтування побудови скінченних полів квадратних матриць другого порядку над простим полем. Досліджено алгебраїчні властивості множини таких матриць, доведено її комутативність. Створено програмні імітаційні моделі представлення квадратних матриць у вигляді перестановок та наведено опис алгоритму перетворення матриць у перестановки.

Четвертий розділ містить прикладну частину дослідження. Представлено реалізацію прототипу системи інформаційного обміну текстовими повідомленнями на основі мікроконтролера nRF52840 в ISM-діапазоні. Реалізовано алгоритми обробки повідомлень у форматі перестановок. Проведено експериментальні дослідження порівняння продуктивності виконання операції множення над перестановками на

центральному та графічному процесорах за допомогою CUDA, що підтвердило ефективність застосування паралельної обробки перестановок на графічному процесорі з зазначеними в роботі особливостями.

Зміст дисертації є цілісним, завершеним і відображає самостійність автора в проведенні дослідження. Робота виконана на високому теоретичному та прикладному рівні, повністю відповідає вимогам до дисертацій на здобуття ступеня доктора філософії.

5. Повнота викладення отриманих результатів дисертації в наукових публікаціях

Результати дисертаційного дослідження Скуцького Артема Борисовича висвітлено у наукових публікаціях у повному обсязі, що дозволяє розглядати роботу як завершене і апробоване наукове дослідження. Загалом опубліковано 11 праць, які охоплюють усі ключові аспекти дисертації від теоретичних основ і математичних моделей до прикладної реалізації запропонованих методів.

Серед оприлюднених результатів: 4 статті у виданнях, індексованих у міжнародних наукометричних базах (Scopus), 4 публікації у фахових наукових виданнях України, 3 публікації тез доповідей, представлених на конференціях всеукраїнського та міжнародного рівня. У публікаціях послідовно відображено логіку виконання дослідження: постановку проблеми, формалізацію моделей, розробку алгоритмів, результати моделювання та експериментальної перевірки.

Такий рівень публічності і наукової апробації свідчить про відкритість дослідження, відповідність академічним вимогам і готовність результатів до практичного впровадження.

6. Відсутність порушень принципів академічної доброчесності

За результатами перевірки дисертаційної роботи на наявність плагіату порушень академічної доброчесності не виявлено. Робота є оригінальною за змістом і оформленням.

7. Зауваження та недоліки дисертації, щодо її оформлення і змісту

1. У розділі 2 автором розглянуто підхід до зменшення кількості хибних спрацювань шляхом накопичення синхрокомбінацій у окремі блоки. Згідно з даними таблиці 2.1, для досягнення імовірності правильної синхронізації на рівні 2.9e-6 достатньо використання чотирьох таких блоків. Разом із цим, у результатах на рисунку 2.15 також зафіксовано чотири хибні спрацювання. Автор не пояснює, чи

є ця відповідність чисел випадковою, чи вона зумовлена властивостями застосованого методу. Доцільно надати уточнення щодо наявності або відсутності причинно-наслідкового зв'язку між кількістю блоків та кількістю хибних спрацювань.

2. У підрозділі 2.4 представлено графіки залежності ймовірності хибної синхронізації від кількості біт синхрокомбінації в ковзному вікні. Водночас, графіки демонструють лише моменти правильної та хибної синхронізації, без відображення випадків, коли синхрокомбінація взагалі не розпізнається. Відсутність цього показника обмежує повноту інтерпретації результатів. Доцільним було б додати кількісну оцінку ймовірності відсутності розпізнавання, що дозволило б більш об'єктивно оцінити ефективність розробленого підходу.
3. У підрозділі 4.3 автор застосовує особливості подання ASCII-кодів символів латинського алфавіту для побудови відповідних перетворень. Проте варто зазначити, що запропонований підхід не охоплює символи кириличного алфавіту, які виходять за межі стандартної ASCII-таблиці й належать до розширених наборів кодування (наприклад, Windows-1251, UTF-8 тощо). Відсутність аналізу або адаптації методу до кодувань, що підтримують кирилицю, обмежує універсальність і застосовність запропонованого рішення. Доцільним було б або розширити дослідження з урахуванням кириличних символів, або чітко обґрунтувати обмеження виключно латиницею.
4. У підрозділі 4.4 доцільно було б конкретизувати, чи застосовувався одновимірний чи двовимірний блок ниток у GPU-реалізації, а також вказати його розмір, оскільки ці параметри можуть суттєво впливати на ефективність обчислень.
5. У лістингу імітаційних моделей, що наведено в додатках, частково відсутні коментарі, щодо параметрів налаштування імітаційних моделей.
6. У деяких твердженнях наявні загальні або недостатньо конкретизовані формулювання (наприклад: *«значно підвищується ефективність», «суттєво зменшується похибка»*), без уточнення, наскільки саме або за якими критеріями це визначено.

8. Висновок щодо відповідності дисертації вимогам, які висуваються до ступеня доктора філософії

Дисертаційна робота Скуцького Артема Борисовича на тему «Метод і моделі системи захищеного інформаційного обміну з нероздільним факторіальним кодуванням даних» є завершеним науковим дослідженням, яке містить самостійно отримані результати, що мають наукову новизну та практичну цінність.

Результати дослідження пройшли апробацію на наукових конференціях та опубліковані в фахових виданнях, у тому числі індексованих у міжнародних наукометричних базах. Дисертація відповідає вимогам до наукових кваліфікаційних робіт за рівнем новизни, глибини опрацювання матеріалу, обґрунтованості висновків та відповідності результатів заявленій меті.

Таким чином, зміст і рівень виконання дисертаційної роботи відповідають вимогам Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, а її автор – Скуцький Артем Борисович – заслуговує на присудження ступеня доктора філософії за спеціальністю 123 «Комп'ютерна інженерія» галузі знань 12 «Інформаційні технології».

Рецензент:
кандидат технічних наук, доцент,
учений секретар, доцент кафедри
інформаційної безпеки
та комп'ютерної інженерії
Черкаського державного
технологічного університету _____ Ірина МИРОНЕЦЬ