РЕЦЕНЗІЯ

кандидата технічних наук, доцента Чепиноги Анатолія Володимировича на дисертаційну роботу Скуцького Артема Борисовича на тему «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

Актуальність теми дисертаційної роботи

Інформаційна безпека в умовах розвитку цифрових технологій, суттєвого зростання обсягів даних і ускладнення комунікаційних мереж є ключовим фактором стабільності інформаційної інфраструктури. Одним із перспективних напрямів розвитку сучасних криптографічних систем є використання матричних структур і перестановок, що поєднують високу обчислювальну складність з ефективністю реалізації. Такі протоколи знаходять застосування в захисті баз даних, банківських транзакцій, безпечному волевиявленні, IoT-системах та інших критичних інформаційних об'єктах.

Окреме місце в контексті кіберзахисту посідає нероздільне факторіальне кодування даних, яке забезпечує надлишковість і дозволяє ефективно виявляти та виправляти помилки, що виникають у зашумлених каналах зв'язку. Таким чином, в роботі обґрунтовується актуальність задачі забезпечення конгруентності взаємодії двох інформаційних систем через канал зв'язку з високою імовірністю бітової помилки.

У дисертаційній роботі сформульовано і розв'язано завдання розробки методу збільшення достовірності передавання інформації в системах з нероздільним факторіальним кодуванням даних, включаючи побудову моделей кадрової синхронізації за невідомого початкового моменту передавання та перетворення матриць у перестановки. Обґрунтовано використання імітаційного моделювання для перевірки ефективності запропонованих рішень та можливість їх реалізації на сучасних програмно-апаратних платформах.

На сучасному етапі практично відсутні системні дослідження з побудови математичних моделей скінченних полів квадратних матриць над простими полями, а також способів їх інтеграції з методами факторіального кодування. Ці напрями мають значний потенціал для створення нових засобів захищеного обміну в умовах завад.

Таким чином, тема дослідження автора дисертації Скуцького Артема Борисовича є актуальною і відповідає потребам сучасної інформаційної інженерії та має важливе теоретичне і прикладне значення.

Наукова новизна результатів

У роботі дисертантом отримано такі наукові результати:

- 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 $\square_p$, яка за рахунок збільшення порядку поля квадратних матриць до значення p^2, проте збереження порядку p поля $\square_p$, в якому виконують операції перетворення, дозволяє підвищити стійкість криптографічних систем, які базуються на операціях у скінченому полі.

Практичне значення одержаних результатів

Практична цінність результатів проведеного 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, де необхідно реалізувати захищений обмін, і можуть бути використані в IoT рішеннях.
- Розроблено програмний код для операцій над перестановками з використанням графічного процесора (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 «грубої сили», 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.

Структура дисертаційної роботи, оцінка змісту дисертації та її завершеність

Дисертаційна робота має чітку структуру, яка містить: вступ, чотири основні розділи, висновки, список використаних джерел і додатки. Загальний обсяг дисертації становить 237 сторінок. Робота містить 62 рисунки, 11 таблиць і 197 найменувань у списку використаних літературних джерел. Дослідження супроводжується теоретичним аналізом проблематики, математичним моделюванням і практичною реалізацією.

У першому розділі обґрунтовано актуальність теми, визначено мету, об'єкт, предмет і завдання дослідження, а також подано аналітичний огляд сучасного стану проблеми. Особливу увагу приділено аналізу існуючих методів кадрової синхронізації з нероздільним факторіальним кодуванням даних та сучасному стану досліджень, присвячених використанню матричних структур у криптографічних застосуваннях.

Другий розділ присвячено: формалізації математичної моделі процедури синхронізації за умов невизначеного початкового моменту надходження послідовності з урахуванням ковзного вікна фіксованої довжини; розробці методу кадрової синхронізації з кореляційною обробкою на основі ковзного вікна та серії спрацювань підсистеми синхронізації з нероздільним факторіальним кодуванням даних; експериментальним оцінкам розробленого методу.

Запропонований автором метод ґрунтується на використанні існуючого методу кадрової синхронізації з кореляційною обробкою, додаванням ковзного вікна фіксованого розміру і врахуванням серії спрацювань підсистемою синхронізації. Автором дисертаційного дослідження запропоновано відслідковувати мінімальний поріг кількості спрацювань синхронізації. Визначення порогу встановлення синхронізації базується на оцінці максимальної можливої довжини серії хибних спрацювань, що виникають під дією завад під час синхронізації. У цьому ж розділі автором визначено узагальнену структуру інформаційного обміну та описано взаємодію між передавачем, каналом зв'язку і приймачем. Наведено структурну схему формування інформаційного фрагмента, який містить синхронізаційний блок та блок даних. У підсумку виконано перевірку ефективності розроблених методів кадрової синхронізації, шляхом проведення імітаційного моделювання, що засвідчує їхню доцільність в завадостійких системах на основі НФКД.

У третьому розділі автором дисертаційного дослідження здійснено математичне обґрунтування побудови скінченних комутативних полів квадратних матриць другого порядку над полем простих чисел. Обґрунтовано шість сімейств матриць 2 порядку, що є комутативними за операцією множення. Запропоновано алгоритм перетворення матриць у перестановки, що дозволяє використовувати їх для генерації ключів.

У четвертому розділі автором дисертації розглянуто питання практичних аспектів реалізації систем інформаційного обміну із застосуванням НФКД. Продемонстровано етапи побудови імітаційної моделі обміну перестановками через двійковий симетричний канал. Наведено архітектуру та функціональні компоненти макетного зразка системи обміну перестановками, реалізованої на базі чипа nRF52840. Описано алгоритми кодування та декодування текстових повідомлень, порівняно ефективність обчислення перестановок при виконанні на CPU та GPU, проаналізовано

часові витрати та ресурсну доцільність використання обчислень операції множення перестановок на графічних прискорювачах.

У висновках узагальнено основні результати дисертаційного дослідження, сформульовано положення, що виносяться на захист, а також окреслено перспективні напрями подальших досліджень у сфері використання скінченних полів матричних структур і використання факторіального кодування в захищених системах інформаційного обміну.

Повнота викладення отриманих результатів дисертації в наукових публікаціях.

Отримані в дисертаційній роботі наукові результати висвітлено у низці фахових публікацій, що свідчить про їхню завершеність, відповідність вимогам академічної доброчесності та наукової апробації. У співавторстві з іншими дослідниками опубліковано 11 наукових праць, серед яких 8 статей, включно з публікаціями у виданнях, що індексуються у міжнародних наукометричних базах (Scopus), а також у фахових наукових журналах України, які входять до переліку МОН.

Окремі результати дисертаційного дослідження оприлюднено на міжнародних науково-технічних конференціях, що дало змогу здійснити апробацію запропонованих методів та отримати фахову оцінку від наукової спільноти. У публікаціях послідовно висвітлено ключові етапи дослідження: постановку проблеми, формулювання математичних моделей, розробку алгоритмів та імітаційне моделювання, що свідчить про логічну завершеність виконаної роботи.

Результати дисертації викладено у повному обсязі, належним чином апробовано та презентовано в рецензованих наукових джерелах, що відповідає вимогам до дисертаційних робіт на здобуття наукового ступеня доктора філософії.

Відповідність принципам академічної доброчесності.

Порушень принципів академічної доброчесності автором дисертаційного дослідження не виявлено.

Зауваження та недоліки дисертації.

Зауваження до дисертаційної роботи Скуцького А.Б. наступні:

- Розроблені автором моделі є офлайн-імітаційними, тобто побудованими в середовищі MATLAB/Simulink та призначеними для попереднього аналізу ефективності методів синхронізації без інтеграції в реальну апаратну систему. Питання роботи алгоритму в реальному часі лишається відкритим.
- Не в усіх підрозділах наведено загальні висновки щодо доцільності чи обмежень запропонованих рішень.
- У розділі 3.5 висловлено лише гіпотетичну ідею використання матриць для формування ключових перестановок, але бракує формалізації обмежень простору в залежності від розмірності матриць та довжини перестановок.
- Пропонується лише оцінка часу перебору ключа під час проведення обчислень на GPU, однак відсутній аналіз того, наскільки рівномірно розподілені ключі перестановок.
- Вибір платформи Raspberry Pi 4 Model B для побудови макетних зразків не був достатньо обґрунтований, оскільки наявність у складі системи модуля з мікроконтролером nRF52840 відкриває можливості реалізації алгоритмів обробки даних безпосередньо на ньому, що могло б забезпечити більш раціональний розподіл обчислювальних ресурсів.
- Велика кількість графічних зображень, що стосуються імітаційних моделей могла би бути винесена в додатки.
- У тексті основних розділів відсутні чіткі посилання на додатки або вони трапляються епізодично. Це ускладнює розуміння, які саме результати

чи реалізації деталізуються в додатках. Рекомендується більш системно інтегрувати додатки в основну структуру роботи.

Зазначені зауваження не зменшують наукову значущість отриманих результатів.

Висновки щодо відповідності дисертації вимогам, які висуваються до дисертацій на здобуття ступеня доктора філософії.

Дисертаційна робота Скуцького Артема Борисовича на тему «Метод і моделі системи захищеного інформаційного обміну з нероздільним факторіальним кодуванням даних» відповідає в повній мірі вимогам до дисертаційного дослідження на здобуття ступеня доктора філософії, наведеним у Постанові Кабінету Міністрів України №44 від 12.01.2022 «Про затвердження порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії». Автор дисертації заслуговує на присудження ступеня доктора філософії за спеціальністю 123 «Комп'ютерна інженерія» галузі знань 12 «Інформаційні технології».

Рецензент:
кандидат технічних наук, доцент,
декан факультету інформаційних
технологій і систем,
доцент кафедри інформаційної безпеки
та комп'ютерної інженерії
Черкаського державного
технологічного університету _____ Анатолій ЧЕПИНОГА

Учений секретар
Черкаського державного
технологічного університету Ірина МИРОНЕЦЬ