

ВІДГУК

офіційного опонента

доктора технічних наук, професора

Заліського Максима Юрійовича

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 дисертаційного дослідження

Сучасний етап розвитку інформаційно-комунікаційних технологій характеризується зростанням обсягів переданої інформації, збільшенням кількості пристроїв у мережах зв'язку, а також ускладненням умов функціонування каналів передавання даних. У таких умовах актуалізується необхідність у нових методах захищеного обміну, які одночасно забезпечують синхронізацію та стійкість до дії завад.

Забезпечення достовірного та захищеного передавання даних в умовах впливу завад і відсутності зворотного каналу залишається однією з найважливіших задач сучасної теорії та практики інформаційної безпеки. Ця проблема є особливо гострою для систем, що працюють у симплексному режимі, де неможливо використати традиційні методи повторного передавання або підтвердження прийому.

Забезпечення надійного та захищеного інформаційного обміну в умовах зашумлених каналів зв'язку є особливо важливою задачею для сучасних комунікаційних систем і кіберфізичних об'єктів. Використаний дисертантом підхід на основі нероздільного факторіального кодування даних (НФКД) і перестановок як носіїв інформації дозволяє поєднати функції синхронізації та шифрування, що є новітнім напрямом у розвитку інтегрованих криптографічних протоколів. Висока обчислювальна складність перетворень, притаманна перестановкам, забезпечує високий рівень захисту, а їхня структура може бути ефективно використана для реалізації кадрової синхронізації. Такий підхід є перспективним для застосування в умовах інформаційного обміну з високою ймовірністю бітових помилок у каналі зв'язку.

Активне використання матричних структур у криптографічних протоколах зайняло важливу нішу в сучасних дослідженнях інформаційної безпеки завдяки їх здатності відображати складні алгебраїчні залежності, які важко піддаються зворотному аналітичному відновленню. Нероздільне

факторіальне кодування в поєднанні зі скінченними полями квадратних матриць слугують ефективним засобом представлення та перетворення ключових даних, відкриваючи нові можливості для побудови шифрувальних схем з підвищеним рівнем складності.

Запропонована в дисертаційній роботі математична модель скінченного поля квадратних матриць другого порядку над полем простих чисел є актуальною. Вона дозволяє формалізувати та уніфікувати операції з перестановками, забезпечуючи основу для побудови ефективних схем формування ключів для НФКД.

У дисертаційному дослідженні Скуцького А.Б. розв'язується актуальне науково-технічне завдання забезпечення захищеного інформаційного обміну в системах із нероздільним кодуванням у зашумлених каналах зв'язку. Для досягнення поставленої мети було сформульовано низку наукових завдань, зокрема: подальший розвиток методу кадрової синхронізації в умовах невідомого початкового моменту прийому синхрокомбінації приймачем; побудова математичної моделі процесу кадрової синхронізації за таких умов; побудова математичної моделі скінченного поля квадратних матриць другого порядку над простим скінченим полем цілих чисел; розробка методики його застосування для узгодження ключів-перестановок.

Враховуючи зазначені аспекти, тема дисертаційного дослідження Скуцького Артема Борисовича «Метод і моделі системи захищеного інформаційного обміну з нероздільним факторіальним кодуванням даних» є актуальною.

2. Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації та їх достовірність

Основні наукові результати дисертаційного дослідження – метод і моделі системи захищеного інформаційного обміну з нероздільним факторіальним кодуванням даних – обґрунтовані математично та підтверджені програмно-імітаційними моделями. Отримані результати коректно формалізовані, ґрунтуються на відомих положеннях теорії ймовірностей, кодування та комбінаторики, що свідчить про достатню глибину теоретичного та практичного опрацювання поставленого завдання.

Достовірність наукових положень і висновків дисертації забезпечується:

- аргументованим використанням методів імітаційного моделювання, зокрема перевіркою результатів у програмному середовищі MATLAB і Simulink, що дозволяє оцінити ефективність синхронізації в умовах зашумленого каналу;

- використанням коректних математичних апаратів, таких як теорія скінченних полів, теорія кодування, статистичне групування, методи перевірки гіпотез та аналізу достовірності прийнятих рішень;
- відповідністю результатів моделювання теоретичним оцінкам, а також наявністю порівняльного аналізу помилок за різних рівнів шуму, що дозволяє зробити обґрунтовані висновки щодо переваг запропонованих підходів.

Отримані результати є відтворюваними, верифікованими, та можуть бути використані як основа для подальшого вдосконалення алгоритмів синхронізації та захисту інформації у каналах зв'язку з високим рівнем завад.

3. Наукова новизна отриманих результатів

У дисертаційному дослідженні Скуцького А.Б. визначено такі пункти наукової новизни:

1. ***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;
2. ***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.
3. ***вперше розроблено*** математичну модель скінченного поля квадратних матриць порядку 2 над скінченним полем простих чисел, яка дозволяє підвищити стійкість криптографічних систем, що базуються на операціях у скінченному полі.

4. Практична цінність отриманих результатів

До практично значущих аспектів роботи, автором Скуцьким А.Б. винесено:

- 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 0.1 до 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 і структури синхрокомбінації на імовірнісні показники 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 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 nRF52840 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.

5. Повнота викладу в наукових публікаціях, зарахованих за темою дисертації

Результати дисертаційного дослідження знайшли належне відображення у публікаціях автора. Основні положення роботи опубліковано в одинадцяти наукових працях, серед яких вісім наукових статей, зокрема у виданнях, що індексуються в міжнародних наукометричних базах, а також у фахових наукових журналах, включених до переліку МОН України. Окремі результати оприлюднено на наукових конференціях, а також у складі колективної наукової монографії. Такий рівень публікаційної активності свідчить про наукову зрілість здобувача та відповідність представлених матеріалів вимогам до дисертаційних робіт.

6. Дотримання норм академічної доброчесності

Аналіз змісту дисертаційної роботи Скуцького А.Б., її структури, стилю викладу та оформлення, а також проведена перевірка посилань на використані джерела дають підстави стверджувати, що автор дотримався принципів академічної доброчесності. У роботі належним чином наведено посилання на праці інших дослідників, не виявлено фактів плагіату чи несанкціонованого використання результатів сторонніх авторів. Текст дисертації є оригінальним за змістом, а наукові положення, висновки й запропоновані методи мають чітке авторське обґрунтування. Ознак порушення академічної доброчесності не виявлено.

7. Зауваження та недоліки

Дисертаційна робота є масштабною, актуальною, добре структурованою та ґрунтується на значному обсязі проведених досліджень. Проте, попри наукову новизну й практичну значущість, у роботі є низка недоліків, які потребують або виправлення, або чіткого обґрунтування в процесі захисту:

1. Не зовсім чітко обґрунтовано, чому саме використано метод кадрової синхронізації на основі кореляційної обробки, хоча у першому розділі розглянуто також метод кадрової синхронізації на основі поділу на префіксну та суфіксну частини.
2. Не подано узагальненої картини взаємозв'язку запропонованих методів із класичними методами шифрування/кодування/синхронізації (наприклад, на основі Markov decision process або VCH-кодів). Введення порівняльної таблиці в розділі 1.6 було би доцільним.
3. У другому розділі дисертаційного дослідження автором розглянуто теоретичну оцінку встановлення синхронізму на основі НФКД з довжиною синхрокомбінації $M=8$ за ймовірності бітової помилки $p_0=0.4$. Проте не проведено обґрунтування вибору саме цієї довжини перестановки та значення ймовірності бітової помилки.
4. Автором не показано, чому саме для формування матричних полів обрано структуру 2×2 .
5. У третьому розділі автором здійснено математичне обґрунтування побудови скінченних полів, зокрема подано підхід до формування перестановок на основі матричних представлень. Водночас, незважаючи на потенційно важливу роль структури отриманого множини перестановок у подальшому застосуванні, у роботі не представлено аналізу їх статистичних або структурних властивостей. Зокрема, не досліджено характер розподілу перестановок, згенерованих за допомогою скінченного комутативного поля матриць: чи мають вони рівномірний розподіл, чи спостерігаються певні закономірності або скупчення. Відсутність такого аналізу ускладнює оцінку ефективності та стійкості запропонованого підходу, особливо з огляду на можливе використання отриманих перестановок у задачах шифрування або побудови псевдовипадкових послідовностей. Доцільно розширити дослідження оцінкою ентропії, циклічної структури або інших метричних характеристик множини згенерованих перестановок.
6. Імітаційні моделі побудовано на базі BSC (Binary Symmetric Channel) з фіксованою ймовірністю помилки. У роботі автором правильно зазначено, що це спрощення, але відсутня навіть спроба чисельного порівняння результатів із іншими моделями каналу передачі Гілберта–Елліота або іншими реалістичними каналами (AWGN, релеєвським).
7. У розділі 4.3 автором запропоновано практичне застосування прототипу захищеного інформаційного обміну текстовими даними через радіоканал ISM-діапазону для IoT-систем. Використано nRF52840, однак важливо оцінити не лише швидкодію, а й енергоспоживання побудованої системи інформаційного обміну.

8. У роботі зустрічаються варіативні формулювання для одних і тих самих понять (наприклад: «система передавання», «система обміну»; «канал передавання», «канал зв'язку»). Доцільно дотримуватися єдиної термінології в межах одного розділу або всієї роботи.

Виявлені зауваження та окремі недоліки дисертаційної роботи мають уточнювальний характер і не знижують наукової та практичної цінності отриманих результатів. Вони не впливають на загальну позитивну оцінку дисертації та не ставлять під сумнів обґрунтованість основних положень, сформульованих автором, а також достовірність представлених висновків.

8. Висновок

Дисертаційна робота Скуцького Артема Борисовича є завершеним науковим дослідженням, присвяченим актуальному завданню забезпечення захищеного інформаційного обміну в умовах зашумленого каналу передавання даних. Отримані результати спрямовані на підвищення достовірності передавання перестановок у системах із нероздільним факторіальним кодуванням за відсутності зворотного каналу зв'язку та за високої ймовірності бітової помилки.

Дисертація відповідає освітньо-науковій програмі «Комп'ютерні системи та мережі» спеціальності 123 «Комп'ютерна інженерія» та змістовно охоплює проблематику захищеного передавання даних, синхронізації, теорії перестановок і побудови скінченних матричних структур.

Подана до захисту дисертаційна робота відповідає вимогам Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії, затвердженому постановою КМУ від 12 січня 2022 р. № 44. Автор роботи – Скуцький Артем Борисович – заслуговує на присудження ступеня доктора філософії за спеціальністю 123 «Комп'ютерна інженерія».

Офіційний опонент:

доктор технічних наук,
професор, професор кафедри
телекомунікаційних та
радіоелектронних систем
Державного університету
«Київський авіаційний інститут»

Максим ЗАЛІСЬКИЙ

Підпис Заліського Максима Ярославовича
Вчений секретар КАН



Тина Набук