

ВІДГУК

офіційного опонента

доктора технічних наук, професора

Опірського Івана Романовича

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

У сучасних умовах цифрової трансформації, стрімкого розвитку засобів бездротового зв'язку та постійного зростання обсягів даних, що передаються в інформаційних мережах, суттєво зростають вимоги до надійності, безпеки та стійкості обміну інформацією. Забезпечення надійного, швидкого та достовірного передавання даних між компонентами інформаційної взаємодії стає критично важливим завданням, особливо в умовах воєнного часу, що актуалізує потребу в захищених каналах зв'язку для систем з обмеженими ресурсами та відсутністю зворотного зв'язку.

Проблема забезпечення достовірного передавання повідомлень у таких умовах тісно пов'язана з задачами кадрової синхронізації, завадостійкого кодування, а також з інтеграцією криптографічних механізмів у загальну структуру інформаційного обміну. У цьому контексті зростає інтерес до нових підходів до представлення даних — зокрема, заснованих на використанні нероздільного факторіального кодування та структур, побудованих на основі матриць над скінченними полями, що розглянуто в дисертаційному дослідженні.

Особливої уваги заслуговують дослідження, в яких факторіальне кодування поєднується з використанням скінченних полів квадратних матриць. Запропонований підхід дозволяє не лише ускладнити процедуру

зворотного аналізу інформації (що підвищує криптостійкість), а й уніфікувати механізми кодування та синхронізації в межах єдиної обчислювальної моделі.

Дисертаційне дослідження Скуцького А.Б., присвячене завданню захищеного інформаційного обміну в системах з нероздільним факторіальним кодуванням у зашумлених симплексних каналах зв'язку і повною мірою відповідає актуальним викликам сучасної інформаційної інженерії. Отримані результати можуть бути використані в різноманітних сферах: від критично важливих об'єктів інфраструктури та систем Інтернету речей (IoT) до спеціалізованих військових застосувань, де вимагається завадостійке передавання повідомлень без потреби організації зворотного зв'язку. Таким чином, тематика дисертаційної роботи є обґрунтовано своєчасною та науково перспективною.

2. Наукова новизна отриманих результатів

У результаті виконання дисертаційного дослідження Скуцьким А.Б. сформульовано такі положення, що становлять наукову новизну роботи:

- **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{F}_p , яка за рахунок збільшення порядку поля квадратних матриць до значення p^2 , проте збереження порядку p поля \mathbb{F}_p , в якому виконують операції перетворення, дозволяє підвищити стійкість криптографічних систем, які базуються на операціях у скінченному полі.

3. Практична цінність отриманих результатів

У роботі автором визначено такі практичні можливості застосування отриманих результатів:

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

Скуцький А.Б. у достатній мірі висвітлив основні наукові положення дисертаційної роботи в публікаціях. Опубліковано 11 наукових праць, серед яких 8 наукових статей, зокрема 4 у виданнях, індексованих у базі Scopus, та 4 – у фахових наукових виданнях України. Апробація отриманих результатів здійснювалася на ряді міжнародних та всеукраїнських науково-практичних конференцій, зокрема:

- XII Міжнародна науково-технічна конференція «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління» (Баку–Харків–Жиліна, 27–28 квітня 2022 року);

- Міжнародна науково-практична конференція «Information Technology for Education, Science and Technics» (ITEST 2022);

- II Міжнародна науково-практична конференція «Виклики та загрози об'єктам критичної інфраструктури» (Київ, 29–30 червня 2023 року);

- Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II-2023) (Київ, 26 жовтня 2023 року);

- Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II-2024) (Київ, 26 жовтня 2024 року);

- III Міжнародна науково-практична інтернет-конференція «Інновації та перспективні шляхи розвитку інформаційних технологій» (ІПШРІТ-2024) (Черкаси, 22 листопада 2024 року).

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

Результати дисертаційної роботи є науково обґрунтованими та узгоджуються з фундаментальними положеннями теорії інформації, теорії кодування та математичної криптографії. У процесі виконання дослідження коректно застосовано математичну апарат теорії перестановок, елементів теорії скінченних полів, комбінаторики, а також методи математичної статистики, теорії випадкових процесів і засоби імітаційного моделювання. Розроблені моделі й алгоритми підтверджені числовими експериментами на імітаційних моделях, що свідчить про їхню внутрішню узгодженість і працездатність у запропонованих умовах застосування.

6. Дотримання норм академічної доброчесності

Дисертаційна робота виконана з дотриманням принципів академічної доброчесності. Текст є оригінальним, належним чином оформлено посилання на використані джерела. Ознак плагіату чи інших порушень не виявлено. Отримані результати належать автору та підтверджені публікаціями.

7. Зауваження та недоліки

У дисертаційній роботі наявні окремі недоліки.

- Наведений опис методу кадрової синхронізації з кореляційною обробкою на основі ковзного вікна в другому розділі є детальним і завантаженим деталями реалізації. Варто було б опустити несуттєві деталі реалізації для покращення сприйняття суті методу.

- У розділі 2.5 використано емпірично обрані пороги для визначення хибної синхронізації. Методика вибору цих порогів потребує узагальнення (можливо, через варіаційне числення або байєсівський підхід).

- Не вказано, чи всі введені сімейства матриць задовольняють умови поля. Якщо використовується лише абелева група, варто чітко відмежувати це від поняття поля.

- Автором не показано позитивний ефект від використання розроблених структур матричних полів в схемах криптографічного перетворення інформації.

- У розділі 4.1 під час побудови моделі інформаційного обміну перестановками використано BSC (Binary Symmetric Channel), що є надто спрощеною моделлю. У сучасних дослідженнях зазвичай застосовують модель Гілберта-Елліота або Rayleigh-фейдінг. Варто додати хоча б одне випробування з більш складною моделлю каналу.

- У розділі 4 створено макетні зразки приймально-передавальних пристроїв захищеного інформаційного обміну текстовими повідомленнями через радіоканал ISM діапазону з використанням перестановок. Однак запропонований автором метод з 2 розділу не використовувався, а вплив шуму на процес інформаційного обміну між макетними зразками був відсутнім.

- У наведених імітаційних моделях імітується лише процеси передавання/приймання перестановок у двійковому представленні, без врахування реального прийому на PHY-рівні (затримки, jitter, RSSI, тощо).

- Відсутність чіткої формалізації термінології. Іноді одна й та сама сутність іменується по-різному ("синхролітера", "синхрокомбінація"). Це потребує уніфікації.

Зазначені зауваження не знижують загального рівня виконаної роботи.

8. Висновок

Дисертаційна робота Скуцького Артема Борисовича на тему «Метод і моделі системи захищеного інформаційного обміну з нероздільним факторіальним кодуванням даних» є завершеним науковим дослідженням, у межах якого запропоновано низку нових рішень для підвищення достовірності обміну інформацією в умовах зашумлених симплексних каналів зв'язку. Розроблений метод кадрової синхронізації на основі кореляційної обробки з використанням ковзного вікна та серії спрацювань підсистеми синхронізації, математичне обґрунтування побудови скінченних полів квадратних матриць другого порядку над полем цілих чисел, а також алгоритм формування перестановок на основі матриць становлять науковий інтерес і мають потенціал для практичного впровадження у сучасні засоби захищеного зв'язку.

Представлена робота повністю відповідає змісту освітньо-наукової програми «Комп'ютерні системи та мережі» спеціальності 123 «Комп'ютерна інженерія» та охоплює актуальні напрями досліджень у галузях захисту інформації, математичного моделювання та теорії кодування. За актуальністю теми, рівнем теоретичних напрацювань і результатами практичного моделювання дисертація відповідає встановленим вимогам до наукових кваліфікаційних робіт такого рівня.

Враховуючи наукову новизну, повноту реалізації поставленої мети, обґрунтованість висновків і практичну значущість отриманих результатів, можна стверджувати, що дисертаційна робота Скуцького Артема Борисовича відповідає 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 заслуговує на присудження ступеня доктора філософії за спеціальністю 123 «Комп'ютерна інженерія» галузі знань 12 «Інформаційні технології».

Офіційний опонент:

доктор технічних наук,
професор, завідувач кафедри
захисту інформації
Національного університету
«Львівська політехніка»

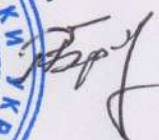


Іван ОПІРСЬКИЙ

Підпис д.т.н., професора Опірьського І.Р. засвідчую

Вчений секретар Національного університету

«Львівська політехніка», д.т.н., доцент

Роман БРИЛИНСЬКИЙ