

ВІДГУК

офіційного опонента кандидата технічних наук, доцента,
доцента кафедри захисту інформації,
Національного університету «Львівська політехніка»

Гарасимчука Олега Ігоровича

на дисертаційну роботу

Халявки Віктора Володимировича

на тему «Методи вибору параметрів скінченних полів матриць другого порядку
та їх примітивних елементів для криптографічних застосувань у комп'ютерних
системах і мережах»

подану на здобуття ступеня доктора філософії
за спеціальністю 123 Комп'ютерна інженерія
галузі знань 12 Інформаційні технології

1. Актуальність теми дисертаційного дослідження

Сучасний розвиток комп'ютерних систем і мереж характеризується постійним збільшенням обсягів даних, що передаються, обробляються та зберігаються в електронному вигляді, а також зростанням вимог до криптографічної стійкості засобів захисту інформації. У таких умовах особливого значення набувають методи побудови математично строгих і водночас практично реалізованих криптографічних платформ, здатних забезпечувати належний рівень захисту в розподілених обчислювальних середовищах, мобільних мережах, вбудованих системах, хмарних сервісах та IoT-рішеннях.

Теоретичною основою значної частини сучасних криптографічних протоколів є арифметика скінченних полів та обчислювальна складність задач дискретного логарифмування. Водночас подальше вдосконалення криптографічних механізмів потребує розширення простору допустимих параметрів, пошуку нових алгебраїчних середовищ і конструктивних процедур вибору елементів великого порядку. Одним із перспективних напрямів є

використання скінченних полів квадратних матриць над простими полями, що дозволяє поєднати апарат теорії скінченних полів із додатковими можливостями матричного подання.

Дисертаційна робота Халявки В.В. присвячена розв'язанню актуального науково-прикладного завдання, яке полягає у розробленні методів вибору параметрів скінченних полів матриць другого порядку та їх примітивних елементів для криптографічних застосувань у комп'ютерних системах і мережах. Актуальність роботи підсилюється тим, що примітивні елементи є генераторами мультиплікативних груп і можуть використовуватися як базові параметри у протоколах узгодження ключів, схемах електронного цифрового підпису та інших криптографічних механізмах.

Отже, обрана тема є своєчасною, відповідає пріоритетним напрямкам розвитку інформаційних та комунікаційних технологій і має як теоретичне, так і прикладне значення для комп'ютерної інженерії, кібербезпеки та захисту інформації.

2. Наукова новизна отриманих результатів

У дисертації сформульовано та обґрунтовано результати, що мають ознаки наукової новизни. До найбільш вагомих положень належать такі:

- *вперше розроблено* метод вибору примітивних елементів скінченного поля квадратних матриць другого порядку над простим скінченим полем цілих чисел, який за рахунок послідовної перевірки дискримінанта характеристичного рівняння, максимального періоду матриці в квадратичному розширенні та примітивності її визначника в базовому полі дозволяє конструктивно формувати множину примітивних елементів поля матриць без повного перебору всіх його елементів;
- *вперше розроблено* метод вибору параметрів скінченного поля квадратних матриць другого порядку над простим скінченим полем цілих чисел Z_p і примітивного елементу в цьому полі матриць для довільного простого p , який за рахунок детального дослідження й використання

властивостей суми квадратичних лишків і нелишків у Z_p дозволяє перейти від окремого розв'язання завдання вибору поля та завдання пошуку примітивного елемента в цьому полі до їх узгодженого алгоритмічного розв'язання в межах єдиної процедури, а також суттєво звужити множину пошуку допустимих параметрів поля й забезпечити можливість знаходження примітивного елемента без повного перебору всіх елементів поля матриць;

– *удосконалено* метод вибору параметрів скінченного поля квадратних матриць другого порядку над простим скінченним полем цілих чисел Z_p і примітивного елемента в цьому полі матриць для випадку, коли p є числом Мерсенна або $(p+1)/2$ є простим числом, який за рахунок обчислення символу Лежандра замість процедури розв'язання квадратичного рівняння в Z_p дає змогу точно знаходити параметричне сімейство примітивних елементів поля матриць.

3. Практична цінність отриманих результатів

Практичне значення результатів дисертаційного дослідження полягає в можливості їх використання під час розроблення програмних і програмно-апаратних засобів криптографічного захисту інформації в комп'ютерних системах і мережах. Отримані результати мають прикладну орієнтацію, оскільки вони формалізовані у вигляді методик, алгоритмів та імітаційних програмних моделей.

До основних практичних результатів роботи можна віднести такі:

– розроблено методику вибору примітивних елементів скінченних полів матриць другого порядку, орієнтовану на практичну й програмну реалізацію. Методика охоплює формування множини матриць-кандидатів, обчислення їх сліду, визначника та дискримінанта, перевірку умови максимального періоду, визначення порядку визначника та побудову примітивних елементів за допомогою скалярних коефіцієнтів із базового поля. Встановлено співвідношення, які дозволяють контролювати повноту

сформованої множини примітивних елементів і уникати дублювання результатів під час обчислень. Розроблена методика дає змогу формувати всі примітивні елементи скінченного поля матриць другого порядку для їх подальшого використання в криптографічних алгоритмах комп'ютерних систем і мереж. Використання поля матриць порядку 2 над Z_p забезпечує збільшення порядку мультиплікативної групи з $p-1$ до p^2-1 порівняно з базовим полем, що створює передумови для розширення можливостей криптографічних перетворень і потенційного підвищення їх криптографічної стійкості;

– розроблено алгоритми вибору параметрів скінченного поля квадратних матриць другого порядку над простим скінченим полем цілих чисел Z_p і примітивного елементу в цьому полі матриць. Для спеціального випадку, коли p є числом Мерсенна або $(p+1)/2$ є простим числом, побудовано алгоритм, у якому основні обчислювальні кроки зводяться до знаходження первісного кореня, перевірки квадратичної нелишковості за символом Лежандра, розв'язання допоміжного рівняння та обчислення параметрів матриці. Для загального випадку побудовано алгоритмічну процедуру, що включає факторизацію чисел $p-1$ та p^2-1 , перевірку умов максимального порядку циклічної підгрупи та примітивності визначника, внаслідок чого забезпечується конструктивний вибір параметрів поля і примітивного елемента в ньому.

Отримані оцінки складності підтверджують, що визначальним чинником часу виконання є факторизація відповідних чисел, а самі алгоритми придатні до використання в задачах комп'ютерної інженерії, пов'язаних із математичним моделюванням обчислювальних процесів, програмною реалізацією криптографічних перетворень і захистом інформації в комп'ютерних системах і мережах.

Модельний приклад застосування алгоритмів вибору параметрів скінченного поля квадратних матриць другого порядку свідчить, що ймовірність

вибору потрібної примітивної матриці збільшується порівняно з випадком повного перебору: 0,667 проти 0,132 для $p = 11$; 0,75 проти 0,166 для $p = 17$; 0,8 проти 0,133 для $p = 19$;

– розроблено імітаційні програмні моделі запропонованих схем узгодження ключів Діффі-Хеллмана та електронного цифрового підпису Ель-Гамала на скінченних полях квадратних матриць другого порядку, що забезпечує відтворення всіх основних етапів роботи криптографічних схем: генерації ключів, формування відкритих параметрів, узгодження спільного ключа, створення електронного цифрового підпису та його перевірки – і можуть бути використані для переносу в програмне середовище.

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

Основні наукові результати дисертаційної роботи достатньою мірою висвітлені в публікаціях здобувача. За темою дисертації опубліковано 5 наукових праць, серед яких 2 статті у виданнях, що індексуються у Scopus та/або Web of Science, зокрема одна стаття у виданні кuartилію Q2, а також 3 публікації у матеріалах міжнародних науково-практичних конференцій.

Апробація результатів дисертації здійснювалася на таких наукових заходах:

- VII Міжнародна науково-практична конференція «Інформаційні технології в освіті, науці і техніці» (ІТОНТ-2024), Черкаси, 23–24 травня 2024 року;
- IV Міжнародна науково-практична конференція «Інновації та перспективні шляхи розвитку інформаційних технологій» (ІПШРІТ-2025), Черкаси, 25 листопада 2025 року;
- V International Conference on Electrical, Computer and Energy Technologies (ICECET 2025), Paris, France, 3–6 July 2025.

Зміст публікацій відповідає темі дисертації, а опубліковані результати відображають основні наукові положення, методи, алгоритми та приклади

практичного застосування, подані в дисертаційній роботі. Це свідчить про належний рівень апробації одержаних результатів у науковому середовищі.

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

Наукові положення, висновки та рекомендації, сформульовані в дисертаційній роботі, є достатньо обґрунтованими. Достовірність результатів забезпечено використанням адекватного математичного апарату теорії скінченних полів, лінійної алгебри, теорії чисел, методів алгоритмічного аналізу, обчислювального експерименту, статистичного аналізу та криптографічного моделювання.

У роботі послідовно розглянуто теоретичні засади побудови скінченних полів квадратних матриць другого порядку, сформульовано умови, за яких матриця може бути генератором мультиплікативної групи, розроблено методи вибору примітивних елементів і параметрів матричного поля, а також наведено алгоритмічні процедури їх реалізації. Важливим є те, що автор не обмежується загальною постановкою задачі, а переходить до конкретних критеріїв, обчислювальних процедур, модельних прикладів і оцінювання складності.

Висновки дисертації логічно випливають із поставленої мети, завдань дослідження та отриманих результатів. Структура дисертаційної роботи є послідовною: від аналізу предметної області та постановки задачі – до розроблення методів, алгоритмів, імітаційних моделей і оцінювання придатності запропонованих рішень для криптографічних застосувань.

6. Дотримання норм академічної доброчесності

Дисертаційна робота виконана з дотриманням принципів академічної доброчесності. Використані ідеї, результати та тексти інших авторів супроводжуються посиланнями на відповідні джерела. У дисертації наведено список використаних джерел, а також зазначено особистий внесок здобувача у працях, опублікованих у співавторстві.

За результатами ознайомлення з дисертаційною роботою ознак академічного плагіату, фабрикації чи фальсифікації результатів не виявлено. Основні результати, подані в роботі, належать здобувачу та підтверджуються публікаціями за темою дисертації.

7. Зауваження та недоліки

Позитивно оцінюючи дисертаційну роботу в цілому, доцільно висловити такі зауваження і побажання:

- у першому розділі дисертації варто було б детальніше зіставити запропонований підхід із практично використовуваними криптографічними платформами, зокрема з реалізаціями над $GF(p^2)$, еліптичними кривими та сучасними варіантами «matrix power function». Це дозволило б чіткіше окреслити межі застосування матричних полів саме як криптографічної платформи;
- запропоновані методи вибору параметрів у загальному випадку залежать від факторизації чисел $p-1$ та p^2-1 . У роботі доцільно було б більш докладно розглянути масштабованість цих процедур для параметрів, актуальних для сучасних криптографічних застосувань, і надати практичні рекомендації щодо вибору значення p з урахуванням сучасних рівнів безпеки;
- розгляд протоколів Діффі-Хеллмана та Ель-Гамала в матричному полі демонструє працездатність запропонованої ідеї, проте безпековий аналіз міг би бути поглиблений через формалізацію зв'язку між задачею дискретного логарифмування в матричному полі та відомими задачами в класичних розширеннях скінченних полів, а також через аналіз можливих спеціалізованих атак;
- у четвертому розділі досліджено статистичні властивості піднесення матриці до степеня, однак доцільно було б ширше описати параметри експериментів: обсяг вибірок, критерії прийнятності, використані набори статистичних тестів і межі інтерпретації отриманих результатів;

– імітаційні програмні моделі є корисним практичним результатом, однак у роботі можна було б детальніше подати вимоги до програмного середовища, особливості реалізації модульної арифметики, питання відтворюваності експериментів і потенційні ризики реалізаційного характеру, зокрема пов'язані з обчисленнями зі змінним часом виконання;

– у роботі доцільно було б розширити прикладні рекомендації для розробників щодо інтеграції запропонованих алгоритмів у реальні криптографічні протоколи: процедури перевірки параметрів, формат представлення матриць, вимоги до генерації випадкових показників і контроль коректності відкритих параметрів.

Зазначені зауваження не знижують загальної позитивної оцінки дисертаційної роботи, не ставлять під сумнів достовірність основних наукових результатів і можуть розглядатися як напрями подальших досліджень та вдосконалення запропонованих підходів.

Висновок

Дисертаційна робота Халявки Віктора Володимировича на тему «Методи вибору параметрів скінченних полів матриць другого порядку та їх примітивних елементів для криптографічних застосувань у комп'ютерних системах і мережах» є завершеним науковим дослідженням, у якому розв'язано актуальне науково-прикладне завдання розроблення методів вибору параметрів скінченних полів матриць другого порядку та їх примітивних елементів для використання в криптографічних протоколах комп'ютерних систем і мереж.

У роботі отримано нові науково обґрунтовані результати, зокрема розроблено метод вибору примітивних елементів скінченних полів матриць другого порядку, метод вибору параметрів матричного поля та примітивного елемента в ньому, а також удосконалено метод вибору параметрів для спеціальних класів простих чисел. Практична цінність роботи підтверджується наявністю алгоритмічних процедур, імітаційних програмних моделей і

прикладів використання матричних полів у протоколах узгодження ключів та електронного цифрового підпису.

Дисертація відповідає спеціальності 123 «Комп'ютерна інженерія» галузі знань 12 «Інформаційні технології», а її зміст відповідає профілю досліджень у галузі комп'ютерних систем і мереж, криптографічного захисту інформації, математичного моделювання та алгоритмічного забезпечення криптографічних перетворень.

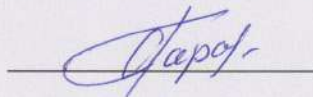
За актуальністю теми, науковою новизною, рівнем обґрунтованості отриманих результатів, практичною значущістю, повнотою апробації та відповідністю вимогам до кваліфікаційних наукових праць дисертаційна робота відповідає вимогам «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого постановою Кабінету Міністрів України від 12 січня 2022 року № 44, а її автор Халявка Віктор Володимирович заслуговує на присудження наукового ступеня доктора філософії за спеціальністю 123 «Комп'ютерна інженерія» галузі знань 12 «Інформаційні технології».

Офіційний опонент:

Доцент кафедри захисту інформації

Національного університету «Львівська політехніка»,

к.т.н., доцент



Олег ГАРАСИМЧУК

Підпис к.т.н. доцента О. І. Гарасимчука засвідчую:

Вчений секретар

Національного університету «Львівська політехніка»,

к.т.н., доцент



Роман БРИЛИНСЬКИЙ