

РЕЦЕНЗІЯ

кандидата технічних наук, доцента

Миронець Ірини Валеріївни

на дисертаційну роботу *Халявки Віктора Володимировича*

«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*

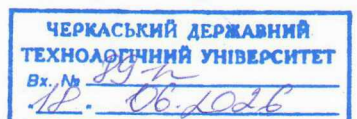
1. Актуальність теми дисертаційної роботи.

У криптографічних системах рівень захищеності визначається не лише самим алгоритмом, а й коректністю вибору його параметрів. Навіть математично стійкий протокол може втратити свої захисні властивості, якщо використані в ньому параметри мають недостатній порядок, належать до небажаних підмножин або обрані без належної перевірки алгебраїчних властивостей. Тому питання формування, перевірки та обґрунтованого вибору криптографічних параметрів є самостійною важливою задачею комп'ютерної інженерії та інформаційної безпеки.

Особливої ваги ця задача набуває для криптографічних операцій, у яких використовуються не скалярні, а структурно складніші алгебраїчні об'єкти. Перехід від звичайних елементів простого поля до матриць відкриває додаткові можливості для побудови криптографічних перетворень, однак одночасно ускладнює контроль за властивостями використовуваних елементів. Для практичного застосування недостатньо лише задати множину допустимих матриць; необхідно мати формальні критерії, за якими можна визначити, чи утворює відповідна структура придатне алгебраїчне середовище, чи має вибраний елемент потрібний порядок і чи може він виконувати роль генератора в криптографічному протоколі.

У цьому контексті дисертаційна робота Халявки Віктора Володимировича є актуальною, оскільки вона спрямована на розв'язання саме цього завдання – не на декларативне використання матриць у криптографії, а на розроблення методів їх параметризації та вибору примітивних елементів. Такий підхід має принципове значення для побудови криптографічних протоколів, де помилковий вибір базового елемента може призвести до зменшення ефективного простору ключів або появи вразливостей, пов'язаних із роботою в підгрупах меншого порядку.

Важливість теми також полягає в тому, що вибір параметрів скінченного поля матриць другого порядку не є суто допоміжною процедурою. Він



безпосередньо впливає на можливість практичної реалізації криптографічної схеми, складність підготовчого етапу, повноту множини допустимих елементів і відтворюваність результатів. Розроблення конструктивних методів такого вибору дозволяє перейти від випадкового або перебірного підходу до керованої процедури формування криптографічних параметрів.

Отже, актуальність дисертаційного дослідження визначається потребою в створенні методів, які забезпечують контрольований вибір параметрів матричних алгебраїчних структур для криптографічного застосування. Запропонований напрям є важливим для подальшого розвитку математичного апарату криптографічних протоколів і для підвищення обґрунтованості їх реалізації в комп'ютерних системах і мережах.

2. Наукова новизна результатів роботи.

Наукова новизна дисертаційної роботи полягає в наступному:

- 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 і примітивного елементу в цьому полі матриць для довільного простого p , який за рахунок детального дослідження й використання властивостей суми квадратичних лишків і нелишків 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 знизити 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 скінченим полем цілих чисел і примітивного елементу в цьому полі матриць для випадку, коли порядок поля p є числом Мерсенна або $(p+1)/2$ є простим числом, який за рахунок обчислення символу Лежандра замість процедури розв'язання квадратичного рівняння в скінченному полі цілих чисел дає змогу точно знаходити параметричне сімейство примітивних елементів поля матриць.

3. Практичне значення одержаних результатів.

Практична цінність роботи полягає в наступному:

– 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 скінченним 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.

Моделльний 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. Структура роботи, оцінка змісту дисертації та її завершеність.

Дисертаційна робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел і додатків. Загальний обсяг роботи становить 178 сторінок машинописного тексту, робота містить 6 рисунків, 22 таблиці та 101 найменування у списку використаних джерел.

У вступі обґрунтовано актуальність теми, визначено мету, задачі, об'єкт і предмет дослідження, наведено методи дослідження, сформульовано наукову новизну та практичне значення отриманих результатів, подано відомості про особистий внесок здобувача, апробацію результатів і публікації.

У першому розділі проведено аналіз сучасного стану предметної області, розглянуто використання скінченних полів і матричних структур у криптографічних застосуваннях комп'ютерних систем і мереж, досліджено комутативні сімейства квадратних матриць другого порядку над полем простих лишків та сформульовано передумови подальшого розроблення методів вибору параметрів матричних полів.

У другому розділі розроблено метод вибору примітивних елементів скінченних полів квадратних матриць другого порядку. У розділі встановлено умови, за яких матриця може бути генератором мультиплікативної групи скінченного поля матриць, наведено опис методу, досліджено особливості його застосування та сформовано методика, придатну для практичної реалізації.

У третьому розділі розроблено метод вибору параметрів поля квадратних матриць другого порядку та примітивного елемента в ньому. Значну увагу приділено аналізу властивостей квадратичних лишків і нелишків у простому полі, побудові алгоритмічних процедур для спеціального та загального випадків, а також порівняльному аналізу запропонованих методів вибору примітивних елементів.

У четвертому розділі розглянуто криптографічні протоколи у скінченних полях квадратних матриць другого порядку. Автором наведено реалізацію

протоколу узгодження ключів та протоколу електронного цифрового підпису у матричному полі, досліджено статистичні властивості піднесення матриці до степеня, а також проаналізовано обчислювальну складність запропонованих криптографічних перетворень у порівнянні з класичним випадком.

Висновки дисертації відображають основні наукові та практичні результати, отримані здобувачем. Зміст розділів узгоджується з поставленою метою та завданнями. Дисертаційна робота є завершеною науковою працею, у якій отримано результати, що мають теоретичне й прикладне значення для розвитку криптографічних застосувань у комп'ютерних системах і мережах.

5. Відсутність (наявність) порушень принципів академічної доброчесності.

За результатами ознайомлення зі змістом дисертаційної роботи можна зробити висновок, що робота виконана з дотриманням принципів академічної доброчесності. У тексті дисертації наведено посилання на використані джерела, результати інших авторів відокремлено від результатів здобувача, а наукові положення та висновки мають авторське обґрунтування. Ознак порушення академічної доброчесності не встановлено.

6. Повнота викладення дисертації в опублікованих працях.

Основні результати дисертаційної роботи опубліковано в 5 наукових публікаціях, серед яких 2 статті у виданнях, що індексуються у Scopus та/або Web of Science, одна з яких належить до квартиля Q2, а також 3 доповіді на міжнародних науково-практичних конференціях. Результати роботи доповідалися та обговорювалися на міжнародних науково-практичних конференціях, зокрема ІТОНТ-2024, ІПШРІТ-2025 та ICESCT 2025.

Вважаю, що основні положення дисертаційної роботи достатньо повно відображені в опублікованих наукових працях здобувача, а рівень апробації результатів відповідає вимогам до дисертаційних робіт на здобуття ступеня доктора філософії.

7. Зауваження та недоліки дисертації щодо її вмісту й оформлення.

Варто відзначити деякі недоліки дисертаційної роботи:

1. У дисертаційній роботі доцільно було б чіткіше формалізувати для основних алгоритмів вхідні дані, вихідні дані, передумови застосування та умови завершення. Зокрема, це стосується методики вибору примітивних елементів, поданої у розділі 2 (с. 71-78), та алгоритмічних процедур вибору параметрів поля у розділі 3 (с. 111-130). Наявність такої специфікації у вигляді

окремих алгоритмічних блоків або таблиць полегшила б незалежну програмну реалізацію запропонованих методів і перевірку коректності їх виконання.

2. У роботі значну увагу приділено формуванню повної множини примітивних елементів, проте окремо не розглянуто практичну задачу вибору одного або обмеженої кількості примітивних елементів для конкретного криптографічного протоколу. Доцільно було б навести рекомендації щодо того, коли потрібно формувати всю множину примітивних елементів, а коли достатньо конструктивно отримати один придатний генератор.

3. Потребують додаткової систематизації виняткові та граничні випадки роботи запропонованих алгоритмів: малі значення простого модуля, виродження матриці-кандидата, повторне отримання еквівалентних елементів, відсутність виконання окремих умов на дискримінант або визначник. Подання таких випадків у вигляді окремої таблиці відмов або сценаріїв відхилення параметрів зробило б методики більш придатними для інженерної реалізації.

4. У четвертому розділі наведено приклади реалізації протоколу узгодження ключів і схеми електронного цифрового підпису у матричному полі (с. 136-140), однак недостатньо окремо розкрито питання комунікаційних витрат: довжини відкритих параметрів, відкритих ключів, підписів і проміжних повідомлень у матричному поданні. Такий аналіз є важливим для оцінювання застосовності запропонованих схем у мережах з обмеженою пропускнуою здатністю.

5. У дисертації бажано було б детальніше описати процедури життєвого циклу ключових параметрів для запропонованих криптографічних схем: періодичне оновлення параметрів, повторне використання або заборону повторного використання окремих елементів, дії у разі компрометації секретного показника та розділення параметрів між різними сеансами взаємодії.

6. У теоретичній частині роботи варто було б чіткіше відокремити властивості скінченного поля матриць другого порядку, що використовуються як відомі або попередньо встановлені, від тих положень, які безпосередньо становлять внесок здобувача у методи вибору параметрів і примітивних елементів. Це підвищило б прозорість подання наукового результату та полегшило б сприйняття логіки дослідження.

7. Окремі графічні матеріали потребують більш уніфікованого подання. Зокрема, для алгоритмічних схем на рисунках 3.1-3.3, 4.1 (с. 113, 124, 130, 139) доцільно було б застосувати єдиний підхід до структури блоків, позначень і деталізації умов переходів, а для рисунків 4.2-4.3 (с. 145) – додати більш розгорнуті пояснення щодо інтерпретації наведених результатів

тестування. Це підвищило б наочність представлення експериментальних і алгоритмічних результатів.

Незважаючи на вказані недоліки, дисертаційна робота є важливим науковим дослідженням та заслуговує на позитивну оцінку.

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

Дисертаційна робота Халявки Віктора Володимировича «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 у криптографічних протоколах комп'ютерних систем і мереж.

За актуальністю теми, науковою новизною, теоретичною обґрунтованістю, практичним значенням отриманих результатів, повнотою їх апробації та відповідністю спеціальності 123 Комп'ютерна інженерія дисертаційна робота відповідає вимогам до дисертацій на здобуття ступеня доктора філософії, встановленим «Порядком присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженим постановою Кабінету Міністрів України від 12 січня 2022 р. № 44 та «Порядком присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради про присудження ступеня доктора філософії в Черкаському державному технологічному університеті», затвердженим вченою радою Черкаського державного технологічного університету 18.04.2022 (протокол № 14) зі змінами та доповненнями.

Дисертація може бути представлена для офіційного захисту в разовій спеціалізованій вченій раді, а її автор, *Халявка Віктор Володимирович*, заслуговує на присудження ступеня доктора філософії за спеціальністю *123 Комп'ютерна інженерія галузі знань 12 Інформаційні технології*.

Рецензент:

кандидат технічних наук, доцент,
доцент кафедри інформаційної безпеки
та комп'ютерної інженерії
Черкаського державного
технологічного університету



Ірина МИРОНЕЦЬ