

РЕЦЕНЗІЯ

кандидата технічних наук, доцента

Розломій Інни Олександрівни

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

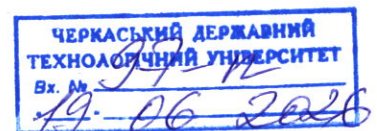
галузі знань 12 Інформаційні технології

1. Актуальність теми дисертаційної роботи.

Ефективність криптографічного механізму значною мірою визначається не лише складністю покладеної в його основу математичної задачі, а й тим, наскільки коректно сформовано алгебраїчне середовище для виконання криптографічних операцій. У практичних реалізаціях криптографічних протоколів саме етап вибору параметрів часто є критичним: невдалий вибір базового елемента, недостатній порядок елементів або наявність прихованих структурних обмежень можуть істотно знизити фактичний рівень стійкості навіть формально коректної схеми.

З цієї позиції особливого значення набувають дослідження, спрямовані на створення процедур контрольованого вибору параметрів для нетрадиційних алгебраїчних платформ. Використання матричних об'єктів у криптографії є привабливим з огляду на можливість розширення множини параметрів і ускладнення структури перетворень. Разом з тим, такий підхід потребує підвищеної уваги до формального опису властивостей відповідних матричних множин, оскільки довільне використання матриць без належного контролю їх алгебраїчних характеристик не гарантує необхідного рівня криптографічної стійкості.

У цьому контексті актуальною є задача побудови методів, які дозволяють не просто використовувати скінченні поля матриць другого порядку, а цілеспрямовано обирати їх параметри та примітивні елементи. Примітивний елемент у такому середовищі має принципове значення, оскільки саме він забезпечує можливість формування мультиплікативної групи. За відсутності конструктивної процедури його вибору практичне застосування матричних полів



у криптографії ускладнюється або зводиться до обчислювально витратного перебору.

Актуальність дисертаційної роботи Халявки Віктора Володимировича полягає в тому, що вона орієнтована на розв'язання саме цієї прикладної криптоінженерної проблеми – формування придатних параметрів скінченних полів матриць другого порядку та визначення їх примітивних елементів для подальшого використання в протоколах захисту інформації. Такий напрям дослідження є важливим для переходу від теоретичної можливості застосування матричних алгебраїчних структур до алгоритмічно визначених процедур, які можуть бути реалізовані в комп'ютерних системах і мережах.

Отже, тема дисертаційного дослідження є актуальною, оскільки вона стосується однієї з ключових передумов побудови надійних криптографічних засобів – обґрунтованого вибору параметрів алгебраїчного середовища. Запропоновані в роботі підходи мають значення для розвитку математичного забезпечення криптографічних протоколів і можуть бути використані як основа для подальшого вдосконалення засобів захисту інформації в комп'ютерних системах і мережах.

2. Наукова новизна результатів роботи.

Наукова новизна дисертаційної роботи:

- *вперше розроблено* метод вибору примітивних елементів скінченного поля квадратних матриць другого порядку над простим скінченним 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 скінченним полем цілих чисел \mathbb{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 \mathbb{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 звузити 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 \mathbb{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 \mathbb{Z}_p дає змогу точно знаходити параметричне сімейство примітивних елементів поля матриць..

3. Практичне значення одержаних результатів.

Практична цінність результатів дисертаційного дослідження полягає у наступному:

1. Розроблено методику вибору примітивних елементів скінчених 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 \mathbb{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.

2. Розроблено алгоритми вибору параметрів скінченного поля квадратних матриць другого порядку над простим скінченним полем цілих чисел \mathbb{Z}_p і примітивного елемента 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 $p=19$.

3. 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.

Отримані результати можуть бути корисними для дослідників і розробників, які працюють над математичним забезпеченням криптографічних протоколів, програмною реалізацією алгоритмів над скінченними полями та побудовою нових алгебраїчних платформ для захисту інформації в комп'ютерних системах і мережах.

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, 6 рисунків, 22 таблиці, список використаних джерел із 101 найменування.

У першому розділі розглянуто сучасний стан використання скінченних полів і матричних структур у криптографічних застосуваннях, проаналізовано комутативні сімейства квадратних матриць другого порядку та обґрунтовано постановку задач дисертаційного дослідження.

У другому розділі розроблено метод вибору примітивних елементів скінченних полів квадратних матриць другого порядку. Розділ містить умови, за яких матриця може бути генератором мультиплікативної групи, опис методу та методу вибору примітивних елементів, орієнтовану на програмну реалізацію.

У третьому розділі розглянуто задачу вибору параметрів поля квадратних матриць другого порядку та примітивного елемента в ньому. Значну увагу приділено використанню властивостей квадратичних лишків і нелишків, а також побудові алгоритмів для спеціального й загального випадків вибору параметрів.

У четвертому розділі наведено застосування запропонованих результатів у криптографічних протоколах. Розглянуто реалізацію протоколу узгодження ключів та електронного цифрового підпису в матричному полі, досліджено статистичні властивості піднесення матриці до степеня та виконано аналіз обчислювальної складності.

Висновки дисертації узагальнюють отримані наукові та практичні результати. Загалом структура роботи є логічною, матеріал викладено послідовно, а дисертаційне дослідження справляє враження завершеної наукової праці, у якій поставлену мету досягнуто, а основні задачі вирішено.

Дисертаційна робота є завершеною науковою працею. Мету роботи досягнуто, поставлені задачі вирішено.

5. Відсутність (наявність) порушень принципів академічної доброчесності.

Ознак порушень здобувачем принципів академічної доброчесності не встановлено. У роботі наведено посилання на використані праці, а результати, що становлять наукову новизну, сформульовано як авторський внесок здобувача.

6. Повнота викладення дисертації в опублікованих працях.

Основні положення дисертаційної роботи опубліковано в 5 наукових працях, серед яких 2 статті у виданнях, що індексуються в міжнародних наукометричних базах Scopus та/або Web of Science, одна з яких належить до квартиля Q2, а також 3 публікації у матеріалах міжнародних науково-практичних конференцій. Наведений перелік публікацій свідчить про достатню апробацію

основних результатів дисертаційного дослідження та їх оприлюднення в науковому середовищі.

7. Зауваження та недоліки дисертації щодо її оформлення і змісту.

Зауваження до роботи:

1. У розділах 2 і 3 значна кількість тверджень спирається на взаємозв'язок між параметрами матриці, характеристичним поліномом, дискримінантом і порядком відповідного елемента. Для полегшення сприйняття матеріалу доцільно було б додати окрему узагальнювальну схему або таблицю, яка показувала б послідовність переходів від матриці-кандидата до висновку про її придатність як примітивного елемента.

2. У дисертації розглянуто обчислювальну складність запропонованих процедур, проте меншою мірою розкрито питання потреби в пам'яті під час формування множин матриць-кандидатів, зберігання проміжних результатів і можливого попереднього обчислення окремих параметрів. Такий аналіз був би корисним для практичної реалізації методів за великих значень p .

3. У дисертаційній роботі недостатньо розкрито питання збереження властивостей при зміні розміру простого модуля p . Основні теоретичні положення сформульовано для довільного простого p , однак у практичних прикладах і числових ілюстраціях переважно використовуються відносно невеликі значення параметрів. Доцільно було б окремо показати, як змінюються кількість допустимих параметричних сімейств, частка примітивних елементів, обсяг проміжних обчислень і практична зручність реалізації при переході до значень p , характерних для реальних криптографічних застосувань.

4. У четвертому розділі наведено приклади застосування запропонованих підходів у протоколах узгодження ключів і електронного цифрового підпису, однак доцільно було б окремо сформулювати модель порушника для цих протоколів. Зокрема, варто було б зазначити, чи враховуються атаки з підміною відкритих параметрів, передаванням некоректних матриць або навмисним вибором параметрів із небажаними алгебраїчними властивостями.

5. Для практичної перевірки програмних реалізацій запропонованих методів корисно було б навести набір тестових векторів: значення p , параметри поля, приклад примітивного елемента, секретні параметри, відкриті ключі, спільний ключ або приклад підпису. Це спростило б відтворення результатів іншими дослідниками та розробниками.

Зазначені зауваження не знижують наукової новизни та практичної значущості дисертаційної роботи. Вони можуть розглядатися як напрями уточнення, подальшого розвитку та інженерного вдосконалення запропонованих результатів.

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

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, пов'язане з вибором параметрів матричних скінченних полів і примітивних елементів для криптографічних протоколів.

За актуальністю, науковою новизною, практичним значенням, повнотою опублікування основних результатів і рівнем обґрунтованості висновків дисертація відповідає вимогам до дисертаційного дослідження на здобуття ступеня доктора філософії, визначеним чинним порядком присудження ступеня доктора філософії.

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



Інна РОЗЛОМІЙ

Підпис к.т.н., доцента Інни РОЗЛОМІЙ засвідчую:

Учений секретар

Черкаського державного

технологічного університету,

к.т.н., доцент



Ірина МИРОНЕЦЬ