

ВІДГУК

офіційного опонента

доктора технічних наук, професора

Одарченка Романа Сергійовича

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 дисертаційного дослідження

Сучасні комп'ютерні системи та мережі функціонують в умовах інтенсивного зростання обсягів даних, розширення розподілених обчислювальних середовищ, поширення хмарних сервісів, мобільних платформ, вбудованих пристроїв та Інтернету речей. За таких умов криптографічний захист інформації залишається ключовим засобом забезпечення конфіденційності, цілісності, автентичності та стійкості електронних сервісів до несанкціонованого доступу й обчислювальних атак.

Теоретичною основою значної частини сучасних криптографічних протоколів є арифметика у скінченних полях. Водночас подальший розвиток засобів криптографічного захисту потребує пошуку нових алгебраїчних платформ, які зберігають математичну строгість класичних скінченних полів, але дають змогу розширити простір криптографічних параметрів, підвищити варіативність генераторів і сформувані додаткові можливості для побудови протоколів узгодження ключів, шифрування, цифрового підпису.

У цьому контексті дослідження скінченних полів квадратних матриць другого порядку над простими скінченними полями є науково обґрунтованим і перспективним напрямом. Використання матричного подання дозволяє перейти від скалярного середовища до алгебраїчної структури з більшою кількістю параметрів, а застосування примітивних елементів таких полів створює основу для реалізації криптографічних перетворень, орієнтованих на складність дискретного логарифмування в розширеному середовищі.

Дисертаційна робота Халявки В.В. присвячена розробленню методів вибору параметрів скінченних полів матриць другого порядку та їх примітивних елементів для криптографічних застосувань у комп'ютерних системах і мережах. Актуальність теми додатково обґрунтовано ще й тим, що практична придатність матричних криптографічних платформ визначається не лише самим фактом використання матриць, а насамперед можливістю конструктивно обирати параметри поля, знаходити генератори

мультиплікативної групи та забезпечувати контроль властивостей таких параметрів у реальних криптографічних протоколах.

Отже, тема дисертаційного дослідження є своєчасною, відповідає сучасним потребам розвитку криптографічних засобів захисту інформації та узгоджується з актуальними завданнями спеціальності 123 «Комп'ютерна інженерія» та освітньо-наукової програми «Комп'ютерні системи та мережі».

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

Наукові положення дисертації, висновки та рекомендації є достатньо обґрунтованими. Автором послідовно сформульовано мету дослідження, визначено об'єкт і предмет, обрано релевантні методи дослідження та логічно пов'язано завдання роботи з отриманими результатами.

Достовірність результатів забезпечено використанням коректного математичного апарату теорії скінченних полів, лінійної алгебри, теорії чисел, комбінаторного аналізу, алгоритмічного моделювання та аналізу обчислювальної складності. У роботі досліджено умови, за яких матриця може бути генератором мультиплікативної групи скінченного поля матриць, розглянуто критерії примітивності, властивості характеристичного полінома, дискримінанта, сліду та визначника матриці-кандидата.

Обґрунтованість запропонованих методів підтверджено тим, що автор не обмежується декларативним описом матричного поля, а формує алгоритми вибору примітивних елементів і параметрів поля, розглядає спеціальний та загальний випадки вибору, виконує порівняльний аналіз із підходами повного перебору та оцінює обчислювальну складність відповідних процедур.

Додатковим підтвердженням достовірності є наведені приклади застосування отриманих результатів у криптографічних протоколах узгодження ключів Діффі-Хеллмана та електронного цифрового підпису Ель-Гамала в матричному середовищі. Виконані програмні імітаційні моделі дають змогу відтворити основні етапи формування параметрів, генерації ключів, узгодження спільного секрету, створення та перевірки підпису.

Висновки дисертації відповідають поставленим завданням, є логічним узагальненням результатів, отриманих у розділах роботи, та загалом підтверджують досягнення сформульованої мети дослідження.

3. Наукова новизна отриманих результатів

У дисертаційній роботі Халаявки В.В. отримано низку результатів, що мають ознаки наукової новизни та розвивають математичний апарат криптографічних застосувань у комп'ютерних системах і мережах. До основних результатів наукової новизни належать такі положення:

- 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 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 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 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.

4. Практична цінність отриманих результатів

Практична значущість дисертаційної роботи полягає в можливості використання розроблених методів і алгоритмів під час створення програмних та програмно-апаратних засобів криптографічного захисту інформації. Найбільш вагомими практичними результатами є наступні.

- 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 скінчених 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.

Одержані результати можуть бути використані в задачах криптографічного моделювання, побудови протоколів узгодження ключів, реалізації схем електронного цифрового підпису, а також у подальших дослідженнях щодо застосування матричних алгебраїчних структур у комп'ютерних системах і мережах.

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

Основні положення дисертаційної роботи достатньо повно відображені в наукових публікаціях здобувача. За темою дисертації опубліковано 5 наукових праць, 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 Scopus, а також 3 публікації за матеріалами міжнародних науково-практичних конференцій.

Публікації відповідають змісту дисертації та висвітлюють основні результати, пов'язані з вибором примітивних елементів у скінченних полях матриць другого порядку, вибором параметрів таких полів, а також застосуванням отриманих результатів у криптографічних протоколах. Апробація результатів на міжнародних конференціях підтверджує науковий інтерес до тематики роботи та достатній рівень оприлюднення основних положень дисертаційного дослідження.

6. Дотримання норм академічної доброчесності

Дисертаційна робота має самостійний характер і містить результати власних досліджень здобувача. У тексті роботи наведено посилання на використані джерела, коректно відображено попередні наукові результати інших авторів, а також зазначено особистий внесок здобувача у працях, виконаних у співавторстві.

Ознак порушення академічної доброчесності, зокрема академічного плагіату, фабрикації або фальсифікації результатів, у межах аналізу представлених матеріалів не виявлено. Наукові положення, винесені на захист, пов'язані зі змістом дисертації та підтверджені опублікованими працями.

7. Зауваження та недоліки

Дисертаційна робота є завершеним науковим дослідженням і, загалом, справляє позитивне враження. Разом з тим, до її змісту можна висловити такі зауваження та побажання:

- порівняння обчислювальної складності алгоритмів і протоколів наведено переважно на рівні аналітичних оцінок і модельних прикладів.

Було б корисно доповнити роботу ширшим експериментальним бенчмаркінгом на різних програмних і апаратних платформах, зокрема для вбудованих систем та IoT-пристроїв;

- у роботі доцільно було б ширше зіставити запропоновані матричні підходи з усталеними криптографічними платформами за рівнем еквівалентної криптографічної стійкості у бітах для різних значень параметру p , оскільки саме така форма порівняння є найбільш зручною для практичного вибору параметрів;
- у тексті роботи трапляються окремі місця, де варто було б уніфікувати термінологію та позначення, зокрема щодо використання понять «електронний цифровий підпис», «електронний підпис», «поле матриць» і «матричне подання квадратичного розширення». Такі уточнення полегшили б сприйняття матеріалу читачем;
- у роботі доцільно було б детальніше розглянути питання вибору та перевірки випадкових параметрів під час реалізації запропонованих криптографічних протоколів. Зокрема, недостатньо повно висвітлено вимоги до джерел випадковості, процедур генерації секретних показників, контролю їх належності до допустимих діапазонів та запобігання повторному використанню випадкових значень у схемах електронного цифрового підпису. Для практичного застосування таких протоколів ці аспекти є принциповими, оскільки навіть математично коректна схема може втратити стійкість у разі некоректної генерації або використання випадкових параметрів;
- у дисертації варто було б окремо проаналізувати питання сумісності та можливості інтеграції запропонованих матричних криптографічних схем у наявні інфраструктури захисту інформації. Робота демонструє теоретичну й алгоритмічну придатність скінченних полів матриць другого порядку для протоколів узгодження ключів та електронного цифрового підпису, однак меншою мірою розкриває, як такі рішення можуть бути представлені у форматах ключів, сертифікатів, протокольних повідомлень або програмних інтерфейсів, сумісних із наявними криптографічними бібліотеками та мережевими протоколами. Це уточнення посилило б практичну орієнтованість результатів.

Наведені зауваження мають уточнювальний характер. Вони не знижують загальної наукової новизни, практичної значущості та позитивної оцінки дисертаційної роботи.

8. Висновок

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, пов'язане з розробленням методів вибору параметрів скінченних полів матриць другого порядку та їх примітивних елементів для використання в криптографічних протоколах.

У роботі отримано науково обґрунтовані результати, що мають значення для розвитку математичного апарату криптографії, побудови нових підходів до вибору параметрів алгебраїчних структур і практичного моделювання криптографічних протоколів у комп'ютерних системах і мережах. Запропоновані методи та алгоритми мають наукову новизну, практичну цінність і достатній рівень апробації у наукових публікаціях.

За актуальністю теми, обсягом і рівнем виконаних досліджень, науковою новизною, практичною значущістю та повнотою оприлюднення результатів 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 р. № 44.

Автор дисертаційної роботи – Халявка Віктор Володимирович – заслуговує на присудження ступеня доктора філософії за спеціальністю 123 «Комп'ютерна інженерія» галузі знань 12 «Інформаційні технології».

Офіційний опонент:

доктор технічних наук,
професор, декан факультету аеронавігації,
електроніки та телекомунікацій
Національного університету
«Київський авіаційний інститут»

Роман ОДАРЧЕНКО



Віктор Халявка
Менеджер секретаріату
Ірина Кобза