Потенціал Нерозвязаних Проблем у Груповій Криптографії

Євген Котух
2-а кафедра 2-го навчального інституту
Воєнна Академія імені Євгенія Березняка
Київ, Україна
yevgenkotukh@gmail.com

Геннадій Халімов
Кафедра безпеки інформаційних технологій
Харківський Національний Університет
Радіоелектроніки
Харків, Україна
hennadii.khalimov@nure.ua

Групова криптографія все ще перебуває на ранніх етапах розвитку, хоча за останнє десятиліття продуктивно просувається вперед [1]. Більшість протоколів, що ґрунтуються на теорії груп, базуються на пошукових задачах, які походять з традиційних вирішувальних задач в комбінаторній теорії груп.

Проблема слова стала одним з перших прикладів нерозв'язної задачі [2]. Через її нерозв'язність декілька інших задач у комбінаторній теорії груп також виявилися нерозв'язними. Важливо зазначити, що встановлення NP-повноти для проблеми слова в конкретних групах залежить від детального аналізу структури та властивостей цих груп. Скінченно наведені групи є надзвичайно складними об'єктами. Зі скінченими групами та проблемою слова пов’язано багато структур і теорій.

Проста група – це нетривіальна група, єдиними нормальними підгрупами якої є сама тривіальна група. Практичний інтерес також мають деякі квазіпрості групи: G є квазіпростою, якщо вона є досконалою, тобто дорівнює власній підгрупі-комутатору $G=[G,G]$, а її група внутрішніх автоморфізмів $Inn(G)$ – проста. Для практичного застосунку в криптографії прикладне значення мають скінченні групи, оскільки перспективні напрями вимагають кінцевих структур даних. Існує класифікація [3] всіх скінченних простих груп, докази якої було завершено в 2000-х роках після багатьох років роботи великої кількості математиків. Для розуміння скористаємось Теоремою 1.

Теорема 1. Якщо G є скінченною простою групою, то або G є абелевою, у цьому випадку вона є циклічною групою простого порядку, або G є неабелевою, у цьому випадку виконується одна з умов:

- або $G \cong A_n$ – знакозмінна група на $n > 5$ символів;
- або G – група типу Лі;
- або G – одна з 26 спорадичних груп.

Групи типу Лі, які включають як класичні, так і виняткові групи, є важливим елементом сучасної алгебраїчної теорії. Вони визначені над скінченними полями із характеристикою поля p, яка є простим числом, та порядком поля q, що є степенем p. Основною особливістю цих груп є порядок групи. Використання неабелевих груп у криптографії має декілька переваг порівняно з абелевими групами. Неабелеві групи мають більш складну структуру, ніж абелеві, оскільки в них порядок виконання операцій є суттєвим.

Властивість некомутативності неабелевих груп ускладнює певні види атак, такі як атаки з використанням методів лінійної алгебри, які можуть бути ефективними проти криптосистем, заснованих на абелевих групах [4]. В неабелевих групах можливе використання більшої кількості операцій для конструкції криптосистем, що надає додаткову гнучкість у дизайні криптографічних протоколів.

Неабелеві групи можуть використовуватися у протоколах обміну ключами, де складність обчислення оберненого елемента або вирішення проблеми кон'югації може забезпечити додатковий рівень безпеки. Дослідження в області постквантової криптографії також виявили, що певні криптосистеми, засновані на неабелевих групах, можуть бути стійкими до атак з використанням квантових комп'ютерів. Всебічний аналіз та опис цих унікальних алгебраїчних структур наведено в [5].

Проблема слова може бути NP-повною для певних спеціальних класів груп або в певних умовах, але важливо зазначити, що у загальному випадку для абстрактних груп проблема слова не класифікується як NP-повна. Це мотивує зазначити групи як напрями досліджень, де проблема слова представляє практичний інтерес та може бути NP-повною:

Групи Дена були введені Максом Деном у 1910-х роках. Вони є прикладами фундаментальних груп певних 2-вимірних многовидів і мають властивість, що для деяких з них проблема слова розв'язна, тоді як для інших – ні. Ці групи дозволили глибше зрозуміти, як структура групи впливає на обчислювальні аспекти проблеми слова.

Групи Григорчука введені у 1980-х роках Ростиславом Григорчуком, ці групи є прикладами груп, що мають властивість проміжного росту. Проблема слова для груп Григорчука була розв’язана.

Групи Баумслага – Солітара задаються дуже простими відношеннями, але мають складну структуру та багато властивостей, що забезпечують складність реалізації. Для деяких параметрів конструкції групи Баумслага – Солітара проблема слова є розв'язною, тоді як для інших – вона залишається відкритою або нерозв'язною.

Коксетерові групи, що генеруються відбиттями, які задовольняють певним відношенням. Для деяких класів Коксетерових груп проблема слова розв'язна.

Групи Тарського - незліченні групи, введені Альфредом Тарським, для яких проблема слова є нерозв'язною. Складність відношень у цих групах призводить до того, що не існує загального алгоритму для визначення, чи дорівнюють один одному два дані слова.

Гіперболічні групи були визначені Громовим, ці групи мають складні відношення, які відображають їх геометричні властивості. Проблема слова в гіперболічних групах наразі досліджена недостатньо.

Автоматні групи можуть бути представлені за допомогою автоматів, що дозволяє моделювати динаміку групових операцій. Складність відношень у таких групах є предметом інтенсивного дослідження, оскільки вона має важливі наслідки для розуміння динамічних систем в математиці.

Спорадичні групи – це особливий клас скінченних простих груп, які не належать до жодного з великих сімейств скінченних простих груп, таких як циклічні групи, альтернативні групи або групи Лі. Всього існує 26 спорадичних груп, і вони є досить рідкісні та особливі у світі алгебраїчних структур.

Кожна з цих спорадичних груп має унікальні властивості та структуру; вивчення цих груп дозволило математикам зробити значний прогрес у розумінні скінченних простих груп та їх застосуваннях у різних областях математики та фізики.

Вагнер та Маг'ярік [6] розробили протокол відкритого ключа, заснований на нерозв'язності проблеми слова для скінченно представлених спорадичних Сузукі 2-груп. Це демонструє, що ідея використання складності неабелевих груп у криптографії не нова. В останні роки ця ідея отримує нові напрями досліджень [7-9].

Кілька протоколів некомутативної криптографії, наприклад некомутативний протокол Діффі – Хеллмана Ко-Лі, протокол обміну ключами Аншеля – Аншеля — Голдфельда (AAG Commutator), схема цифрового підпису Кахробай – Коуппаріс і Кахробай – Хан – схема некомутативного шифрування з відкритим ключем Ель-Гамаля, базуються на складності проблеми пошуку спряженості в певних запропонованих групах.

Асиметрична криптографія використовує односторонні функції. NP-повні задачі вважаються оптимальними для таких функцій, оскільки вони дозволяють відносно легко генерувати складні для вирішення приклади. Однак застосування NP-повних задач у криптографії обмежене через труднощі у створенні задач, які були б обґрунтовано складними. У статті детально розглянуто класи NP проблем, визначено основні терміни та концепції, проаналізовано властивості та критерії NP-повноти. Особлива увага приділяється складності NP-повних проблем в контексті квантових обчислень, а також визначенню неабелевих груп, в яких проблема слова вважається NP-повною. Дослідження підкреслює потенційні переваги використання неабелевих груп у криптографії, оскільки проблема слова для цих груп відноситься до класу NP-повних проблем. Зроблено огляд останніх досліджень у галузі розробки асиметричних криптографічних примітивів, заснованих на використанні складних для розв'язання проблем у кінцевих групах. Обґрунтовано перспективність цього напрямку в груповій криптографії.

Література References

[1] Alamati, Navid, et al. "Cryptographic group actions and applications." Advances in Cryptology–ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7–11, 2020, Proceedings, Part II 26. Springer International Publishing, 2020.

[2] Verschaffel, L., Schukajlow, S., Star, J., & Van Dooren, W. (2020). Word problems in mathematics education: A survey. *ZDM, 52*, 1–16.

[3] van Veldhuizen, Toon, and Hans Cuypers. "Investigating finite simple groups."Master Thesis

[4] Singh, Priyanka, Manju Khari, and Nikhil S. Kaundanya. "Impact of group theory in cryptosystem." *Functional encryption*. Cham: Springer International Publishing, 2021. 19–36.

[5] Lanel, G. H., Jinasena, T. M. K. K., & Welihinda, B. A. (2021). A survey of public-key cryptography over non-abelian groups.

[6] N.R. Wagner and M.R. Magyarik. A public-key cryptosystem based on the word problem // Proc. Advances in Cryptology–CRYPTO 1984, LNCS 196, Springer-Verlag (1985), pp. 19–36.

[7] Khalimov G., Kotukh Y. et al. Towards advance encryption based on a Generalized Suzuki 2-groups // 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME). Mauritius, 2021, pp. 1–6. doi: 10.1109/ICECCME52200.2021.9590932.

[8] Khalimov G., Kotukh Y., Khalimova S. MST_3 Cryptosystem Based on a Generalized Suzuki 2-Groups [Electronic resource]. Access mode : http://ceur-ws.org/Vol-2711/paper1.pdf

[9] Khalimov G., Kotukh Y., Didmanidze I., Sievierinov O., Khalimova S. and Vlasov A. Towards three-parameter group encryption scheme for MST3 cryptosystem improvement // 2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4), London, United Kingdom, 2021, pp. 204–211. doi: 10.1109/WorldS451998.2021.9514009.