УДК 621.391:519.2 **DOI:10.30837/rt.2024.1.216.05**

Є.В. КОТУХ, канд. техн. наук, Г.З. ХАЛІМОВ, д-р техн. наук,
М.В. КОРОБЧИНСЬКИЙ, д-р техн. наук, М.М. РУДЕНКО, канд. техн. наук,
В.О. ЛЮБЧАК, канд. фіз.-мат. наук, С.М. МАЦЮК, канд. техн. наук, М.В. ЧАЩИН

ГОРИЗОНТИ ДОСЛІДЖЕНЬ В ГРУПОВІЙ КРИПТОГРАФІЇ В КОНТЕКСТІ РОЗРОБКИ ПОСТКВАНТОВИХ КРИПТОСИСТЕМ

Постановка задачі

Основним елементом криптографії з відкритим ключем є односторонні функції. У криптографії така функція використовується для шифрування, тоді як її інверсія – для дешифрування. Важливо, що дешифрування має бути простим лише для особи з секретним ключем, яка відкриває "люк" для легкого розшифрування. Цей секретний ключ відомий лише одержувачу та дозволяє легко розшифровувати повідомлення, зашифровані відкритим ключем. Відсутність інформації про "люк" у третіх осіб робить розшифрування обчислювально нездійсненним.

Інтуїтивно обґрунтованим припущенням є, що NP-повні проблеми в області теоретичної інформатики можуть бути ідеальними кандидатами для використання як односторонніх функцій у криптографії з відкритим ключем [1]. Проблема, що належить до множини NP-повних проблем, визначається тим, що перевірка правильності її рішення є простою, у той час як знаходження самого рішення є складним без наявності секретної інформації про "люк". Тут "простота" означає можливість обчислення за поліноміальний час, а "складність" – це неполіноміальний час обчислень, зазвичай експоненціальний.

Припускаючи, що $P \neq NP$, здається, що використання NP-повних проблеми задовольнило ці критерії. Загалом легко генерувати NP приклади належні до множини NP-повних проблем, але за умови, що $P \neq NP$ такі приклади залишаються такими, що важко розв'язуються.

Іншою привабливою особливістю NP-повних проблем є те, що, на відміну від задачі цілочисельної факторизації та проблеми дискретного логарифмування, вирішення NP-повних проблем є потенційно складним для квантового прискорення обчислень. Це залишається відкритим питанням, навіть за умови припущення, що $P \neq NP$. Таким чином, цікавою науковою задачею є розгляд можливості використання NP-повних проблем для побудови криптосистем відкритого ключа, стійких до атак, що реалізуються на квантових комп'ютерах [2].

Існують технічні складнощі для створення криптосистеми на основі NP-повних проблем, що завадило використанню цієї множини задач як основи для безпеки в таких криптосистемах. Концепція використання NP-повних проблеми для створення криптосистеми з відкритим ключем спочатку здавалася перспективною, але на практиці не продемонструвала результатів. Перша така криптосистема з відкритим ключем була побудована на базі проблеми цілочисельного рюкзака, яка згодом була скомпрометована за допомогою потужних універсальних атак. Зауважимо, що атаки були спрямовані на конкретну реалізацію люка, а не безпосередньо на проблему рюкзака. Задача побудови стійкої реалізації люка для криптосистеми на основі проблеми рюкзака залишається актуальною.

Проблема слова і проблема рюкзака мають схожість, оскільки обидві представляють собою "природні" задачі для криптосистем з відкритим ключем та можуть бути безпосередньо застосовані для побудови криптосистеми з відкритим ключем. Зрозуміло, що основною проблемою для розробки стійкої до атак конструкції є реалізація люка, що забезпечує розшифрування. Коли люк існує, він може стати вразливим місцем для криптоаналітичних атак [2].

Для розуміння ієрархії задач прийняття рішень запропонуємо візуалізацію множин складності проблем (рис. 1), що починається з проблем, які вирішуються за поліноміальний час,

проходить через множину NP-повних проблем і завершується NP-складними нерозв'язними проблемами, які є найскладнішими з усіх.

NP-повні проблеми вважаються такими, що знаходяться на грані розв'язності та є найпростішими з відомих "природних" проблем, які все ще вважаються нерозв'язними. Якщо NP-повна проблема буде трохи послаблена, вона може стати вже розв'язною.

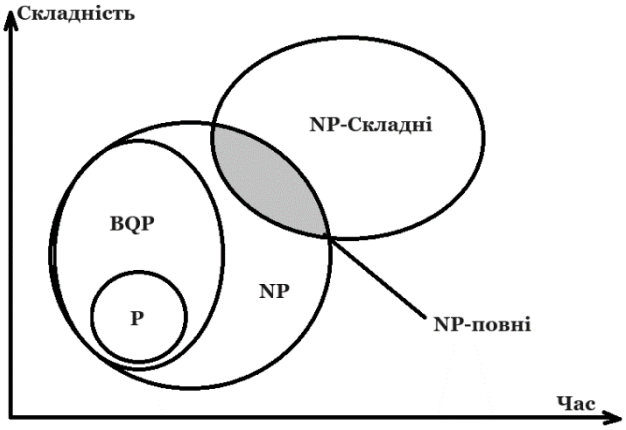

Рис. 1. Класи складності нерозв’язаних проблем

У контексті побудови квантово стійкої асиметричної криптосистеми необхідно враховувати саме дизайн люка. Це додає складності у використанні класичних NP-повних проблем та зумовлює, що NP-повна проблема може бути більш ускладнена задля забезпечення постквантових властивостей. Вважається, що більш складна проблема може ускладнити безпосередні атаки та надати більше можливостей для інтеграції люків, зберігаючи при цьому стійкість криптосистеми.

Аналіз поточного стану проблем, складних для розв’язання

Брассард в роботі [3] продемонстрував, що з певними обмеженнями, якщо б криптосистема була доведено NP-повною для атаки, це б теоретично означало, що NP=NP-повна. Однак ця теорія вважається невірною, хоч і доказів цьому немає. Тому криптоаналіз асиметричних криптосистем, що засновані на NP-повних проблемах, буде легшим, та, ймовірно, обчислено ймовірним.

Існує багато теорій про NP-повноту, але вони стосуються лише аналізу найгіршого випадку та певних прикладів проблеми. Наприклад, проблема цілочисельного рюкзака не є NP-повною за умов, якщо у проблемі не використовуються "експоненційно великі" числа. Для цього випадку для цієї проблеми існують алгоритми поліноміального часу [4].

Існують також розумні алгоритми наближення, що дозволяють обчислити приблизне рішення, яке не є точним. Також існують недетерміновані алгоритми, які можуть надати точну відповідь або з великою ймовірністю також можуть не дати відповіді зовсім. Хоча немає відомого алгоритму поліноміального часу для класичних обчислювачів, що вирішує найгірші випадки великих екземплярів, алгоритми, подібні до описаних, можуть запускати великі екземпляри NP-повної проблеми, які є неприйнятними, якщо асиметрична криптосистема має бути безпечною.

Проблема факторизації стала основою для декількох криптографічних систем, генерації криптографічно безпечних генераторів випадкових чисел та алгоритмів обміну секретними ключами без участі арбітра. Для цього випадку кожен протокол із повним підтвердженням безпеки базується на припущенні, що факторизація залишається складним завданням. Сама криптосистема RSA, хоча й не є прямо еквівалентною , все ж залежить від складності цього процесу для забезпечення своєї безпеки. Нові напрями в розробці та дослідженні криптосистем відкритого ключа, що використовують факторизацію, з’являються постійно.

В роботах [5 – 10] розглянуто використання логарифмічних підписів – особливого типу факторизації в групах. Факторизація залишається нерозв'язною проблемою для класичних

комп’ютерів. Проблеми, які можуть вирішити квантові комп'ютери за поліноміальний час, відносяться до класу BQP. До них відносяться всі проблеми P і багато проблем NP (див. рис. 1). В роботі [11] теоретично обґрунтовано можливість зниження криптографічної стійкості криптосистем, що використовують факторизацію чи проблему дискретного логарифму з використанням квантових обчислень. Отже, квантовому комп’ютеру потрібно більше ніж поліноміальна кількість кроків для вирішення NP-повної проблеми. Зрозуміло, що справжній статус складності завдання факторизації, особливо за умов факторизації в групах, залишається невизначеним.

Лю та Пас представили NP-повну задачу, складність випадку якої, у середньому, еквівалентна існуванню односторонніх функцій [1]. Отже, складна проблема в множині NP-повних проблем існує, якщо існує справжня одностороння функція та $P \neq NP$. Однак це не робить криптосистему, що використовує в основі таку проблему, криптографічно стійкою, бо реалізація функціональності люка матиме критичне значення.

Відповідно розгляд більш складних проблем як основи для криптосистем з відкритим ключем є важливим науково значущим підходом. Існують різноманітні проблеми, доведено нерозв'язні, а також задачі, для яких неможливо знайти загальне алгоритмічне рішення. Важливо , що для асиметричних криптосистем може бути застосований лише специфічний приклад однієї з цих складних задач. Складність криптоаналізу все одно залишиться в межах класу NP.

Розглянемо основні визначення та поняття. Перш за все, необхідно дослідити та обґрунтувати, за яких умов проблема, що визначається, належить до NP-повних проблем.

Визначення 1. Нехай A – детермінований алгоритм, який зупиняється на всіх входах. Функція $f: \mathbb{N} \to \mathbb{N}$, де $f(n)$ – максимальна кількість кроків, яка A використовується для будь-якого введення довжини n, є визначенням часу виконання (часової складності) A. Якщо $f(n)$ є час роботи A, вважаємо, що A виконується в часі $f(n)$, і це A є $f(n)$ часовим алгоритмом.

Визначення 2. Нехай f та g є функціями $f, g: \mathbb{N} \to \mathbb{R}^+$. Визначимо, що $f(n) = O(g(n))$, якщо існують такі позитивні цілі числа c і n_0, що для кожного цілого $n \geq n_0$, $f(n) \leq cg(n)$. Коли $f(n) = O(g(n))$, то $g(n)$ – це асимптотична верхня межа для $f(n)$.

Визначення 3. Нехай $t: \mathbb{N} \to \mathbb{R}^+$ функція. Визначимо клас часової складності, $TIME(t(n))$ як множину усіх проблем, які розв’язуються за допомогою $O(t(n))$ часового алгоритму.

Визначення 4. $P = \bigcup_{k \in \mathbb{N}} TIME(n^k)$ або P – це клас задач, які можна розв’язати за поліноміальний час за допомогою детермінованого алгоритму.

Визначення 5. NP – це клас задач, рішення яких може бути перевірено за поліноміальний час.

Визначення 6. Проблема A – це поліноміальне відображення часу, яке зводиться до проблеми B, визначеної як $A \leq_P B$, якщо існує функція f – поліноміальна обчислювана за часом, де для кожного w, $w \in A \Leftrightarrow f(w) \in B$. Функція f називається поліноміальним скороченням часу A до B.

Визначення 7. Проблема B є NP-повною, якщо вона задовольняє двом умовам: B знаходиться в NP, і будь-яке A в NP є обчислюваною за поліноміальний час, що зводиться до B.

З визначення NP-повноти випливає, якщо якась NP-повна проблема знаходиться в P, то всі ці проблеми належать до множини P. Маємо наступний висновок – якби алгоритм

вирішення проблеми за поліноміальний час можна було знайти для будь-якої NP-повної проблеми, то кожну NP-повну проблему можна вирішити за поліноміальний час.

Наразі не визначено жодної NP-повної проблеми, що можна вирішити за поліноміальний час. Також не доведено зворотне. Однак щоб це довести, треба довести, що $P \neq NP$; це наразі є найважливішою невирішеною проблемою в теоретичній інформатиці. Теоретично обґрунтовано, що класи P і NP не є рівними. Саме це обґрунтування лежить в основі припущення, що NP-повні проблеми не можуть бути розв'язані за поліноміальний час [12]. Хоча відсутність доказів цієї гіпотези може розглядатися як явна слабкість у використанні NP-повних проблем як основи для асиметричних криптосистем, важливо зазначити, що наразі не доведено, що факторизацію цілих чисел та обчислення дискретних логарифмів не можна виконати за поліноміальний час з використанням класичного обчислювача. Докази на користь $P \neq NP$ не наведено, але факт недоведеності $P \neq NP$ не є сильним запереченням проти використання NP-повних проблем як основи для криптосистем з відкритим ключем. Однак, навіть якщо це насправді так – $P \neq NP$, все ще не зрозуміло, чи можна використовувати NP-повні проблеми як платформу для криптосистем з відкритим ключем. Причиною цього є те, що класи складності P і NP визначаються в термінах найгіршого випадку часу роботи алгоритмів, які вирішують проблеми, що містяться в них. Отже, можливо, що за умов належності проблеми до NP з $P \neq NP$ є багато прикладів таких проблем, що можуть бути розв'язані за поліноміальний час. Саме з цих причин було проведено дослідження середньої складності NP-повних проблем [13].

За декілька десятиріч визначено перелік актуальних проблем, для яких переважна більшість прикладів таких проблем є простою для розв'язання. Наприклад, важливо зазначити, що проблема слова є NP-повною проблемою та є розв'язуваною для багатьох груп. Тільки незначна частина прикладів потребує часу, більшого за поліноміальний. Такі проблеми визначені як ті, що мають «чорну діру», та їх подальше використання у якості кандидатів для криптографії з відкритим ключем не розглядається. Вочевидь, існують проблеми, що мають «білу діру», де переважна більшість випадків є складною. Такі проблеми в множині NP-повних проблем мають перспективу для побудови постквантових криптосистем відкритого ключа.

Критерії належності проблеми слова в групах до NP-повних проблем

Наступні проблеми прийняття рішень були введені ще у 1911 р. та визначаються таким чином.

Проблема слова: для будь-якого $g \in G$ визначте, чи g є тотожним елементом G.

Проблема спряженості: для будь-якого $x, y \in G$ визначте, чи x та y спряжені, тобто чи існує елемент $c \in G$ (кон'югатор), такий, що $c^{-1}xc = y$.

Проблема ізоморфізму: Нехай G і G' – групи, задані кінцевими представленнями, визначте, чи G ізоморфна G'.

В 1912 р. Ден розробив алгоритм, що вирішує як проблему слова, так і проблему спряженості для фундаментальних груп замкнутих орієнтованих двовимірних многовидів роду, який більший або дорівнює 2. Такий підхід був значно розширений та адаптований для широкого спектру задач у теорії груп.

Проблема слова для загальних груп не класифікується як NP-повна, оскільки її властивості суттєво відрізняються в залежності від конкретної групи, для якої вона формулюється. Хоча для деяких специфічних класів груп проблема слова може бути розв'язана за поліноміальний час, для інших вона може бути нерозв'язною. Для того щоб проблема вважалася NP-повною, вона має задовольняти двом умовам: бути в множині NP (тобто для кожної вірної відповіді існує "свідок", який може бути перевірений за поліноміальний час), а також умові зведення кожної NP проблеми до NP-повної за поліноміальний час.

Проблема слова не завжди відповідає цим умовам, оскільки її складність може істотно варіювати залежно від структури групи. Проблема слова може бути NP-повною для певних

спеціальних класів груп або в певних умовах. Тому, проблема слова в контексті теорії груп не вважається NP-повною, хоча її варіанти для деяких конкретних груп або у спеціалізованих контекстах можуть мати різні обчислювальні властивості. Стислий аналіз таких класів груп допомагає визначити наступні конструкції.

Графові групи: для певних графових груп проблема слова може бути NP-повною. Це пов'язано зі структурою групи, яка визначається графом, та складністю визначення, чи можна рядок, сформований з генераторів та їх інверсій, звести до порожнього слова.

Групи з особливо складними відношеннями: у деяких групах, де визначення відношень між генераторами є особливо складним, проблема слова може стати NP-повною. Це стосується ситуацій, коли відношення в групі настільки складні, що перевірка еквівалентності двох рядків вимагає значних обчислювальних зусиль.

Специфічні конструкції: для деяких специфічних конструкцій груп, особливо тих, що штучно створені для демонстрації певних обчислювальних властивостей, проблема слова може бути NP-повною. Ці конструкції зазвичай розробляються так, щоб ілюструвати певні теоретичні аспекти проблеми слова.

Як було зазначено вище, проблема слова є розв'язуваною для багатьох груп G. Наприклад, для поліциклічних груп існують розв'язки проблеми слова, оскільки можна легко обчислити нормальну форму будь-якого слова в поліциклічному представленні; інші алгоритми також можуть вирішити проблему слова в певних умовах, зокрема алгоритм Тодда – Коксетера [14] і алгоритм завершення Кнута – Бендікса [15]. З іншого боку, неможливість розв'язання проблеми слова для конкретної групи деяким алгоритмом не означає, що в цій групі проблема слова є нерозв'язною. Наприклад, алгоритм Дена не розв'язує проблему слова для фундаментальної групи тора, але оскільки ця група є прямим добутком двох нескінченних циклічних груп, проблема слова для неї є розв’язною. У більш конкретних термінах проблему з уніфікованим словом можна виразити як питання про переписування літеральних рядків. Для представлення P групи G, P буде вказувати певну кількість генераторів $x, y, z, ...$ для G. Потрібно ввести одну букву для x і іншу (для зручності) – для елемента групи, представленого x^{-1}. Назвемо ці букви алфавітом $\sum$ нашої задачі. Тоді кожен елемент у G певним чином представляється добутком символів алфавіту $\sum$ певної довжини, помножених в G. Рядок довжиною 0 (нульовий рядок) означає одиничний елемент групи e з G. Суть усієї проблеми полягає в тому, щоб мати можливість розпізнати всі способи представлення e, враховуючи деякі співвідношення.

Вплив відношень у G полягає в тому, що вони дозволяють різним рядкам представляти один і той самий елемент групи. Відношення надають перелік рядків (слів), які можна вставляти або видаляти у виразі без зміни значення виразу, тобто елемента групи, що отримується в результаті множення слів. Це означає, що за наявності певних відношень можемо перетворити одне представлення елемента на інше, зберігаючи при цьому ідентичність елемента в контексті групової операції.

Для простого прикладу візьмемо презентацію $\{a \mid a^3\}$. Подання $\{a \mid a^3 = e\}$ описує циклічну групу порядку 3, де e – одиничний елемент групи. У цій групі кожен елемент можна представити як ступінь a та $a^3 = e$, тобто представити a як одиничний елемент групи. Записуючи A для зворотного до a, ми маємо можливі рядки, що поєднують будь-яку кількість символів a та A. Щоразу, коли бачимо aaa, або aA чи Aa, можемо їх викреслити. Ми також повинні пам’ятати про те, щоб викреслити AAA; це говорить, що оскільки куб a є одиничним елементом G, то таким же є і куб, обернений a. За цих умов проблема слова стає легкою. Спочатку скоротимо рядки до порожнього рядка a, aa, A або AA. Потім, щоб перетворити A в aa і перетворити AA в a, помножимо на aaa. Таким чином, проблема слова для циклічної групи третього порядку є розв’язною.

Однак це не типовий випадок, оскільки у якості прикладу маємо доступну канонічну форму, яка зменшує будь-який рядок з трьох до довжиною щонайбільше одного шляхом

монотонного зменшення довжини. В загальному випадку не можна отримати канонічну форму для елементів шляхом поетапного скорочення. Ймовірно, доведеться використовувати відношення для багаторазового розширення рядка, щоб зрештою знайти скорочення, яке зменшує довжину. У гіршому випадку відношення між рядками, що свідчить що вони рівні, в G є нерозв'язною проблемою .

Петро Новіков показав, що існує скінченно представлена група G, така що проблема визначення слова для G є нерозв'язною [16]. Звідси випливає, що проблема однорідного слова також є нерозв'язною. Інший доказ отримано авторами у [17] та досі не спростовано.

Існують нерозв'язні задачі для скінченно заданих груп і для напівгруп. В [18 – 20] розглянуто основні результати. Скінченно представлена група G складається з генераторів $x_1, x_2, ..., x_n$, які є просто абстрактними символами, і реляторів $r_1 \neq e\ r_1 \neq e, r_2 \neq e, ..., r_m \neq e$, які будуть визначені нижче. Кожному твірному відповідає x_i зворотний x_i^{-1}. Слово в G – це кінцевий рядок, що складається із символів x_i і x_i^{-1}. Порожній рядок e також є словом, ідентифікатором групи. Кожне з r_i перераховане вище, є словом. Груповою операцією об'єднання слів є конкатенація. Для кожного слова w зворотне слово w^{-1} складається з усіх символів w, записаних у зворотному порядку, де кожен x_i замінюється на x_i^{-1}, а кожен x_i^{-1} замінюється на x_i.

Група G складається з класів еквівалентності всіх можливих слів. Два слова w і v еквівалентні, якщо ми можемо перетворити w на v за допомогою кінцевої послідовності правил зміни форми.

Правило 1: зміна $x_i x_i^{-1}$ або $x_i^{-1} x_i$ на e, тобто виключення $x_i x_i^{-1}$ або $x_i^{-1} x_i$;

Правило 2: представлення $x_i x_i^{-1}$ або $x_i^{-1} x_i$ будь-який момент;

Правило 3: зміна r_j або r_j^{-1} на e, тобто виключення r_j або r_j^{-1};

Правило 4: представлення r_j або r_j^{-1}.

Існує більш формальний спосіб визначення цих понять. Спочатку вільна група F на генераторах $x_1, x_2, ..., x_n$ визначається як набір усіх слів у x_i і x_i^{-1}, які скорочуються шляхом повторної відміни $x_i x_i^{-1}$, $x_i^{-1} x_i$ доки подальші відміни не стануть можливими. Це дозволяє R бути нормальною підгрупою, породженою словами $r_1, r_2, ... r_m$ (R є перетином усіх нормальних підгруп, що містять r_j). Нарешті, G є фактор-групою F / R.

Проблема зі словом для групи G – це проблема з рішенням, яка запитує w, чи кожне слово w є еквівалентним тотожності G. Виявляється, що існують певні групи, для яких проблема зі словом є нерозв'язною. Як і будь-яка нерозв'язна проблема, проблема слова може бути нерозв'язною лише як питання, яке ставлять про нескінченну кількість слів, – будь-яка кінцева колекція слів повинна мати розв'язну проблему зі словами.

Таким чином, проблема слова в теорії груп може мати значний вплив на розробку криптографічно стійких алгоритмів в постквантову еру. Оскільки проблема слова може бути нерозв'язною для деяких груп, це створює потенціал для використання таких груп у розробці криптографічних систем, де визначення еквівалентності двох слів (або рядків) є критично важливим. Дослідження проблеми слова може сприяти створенню нових криптографічних схем, де безпека базується на складності обчислень у певних групах, а обґрунтування використання цих груп буде відігравати ключову роль у розробці алгоритмів, стійких до квантових атак.

Потенціал нерозв'язаних проблем у груповій криптографії

Групова криптографія все ще перебуває на ранніх етапах розвитку, хоча за останнє десятиліття продуктивно просувається вперед [21]. Більшість протоколів, що ґрунтуються на теорії груп, базуються на пошукових задачах, які походять з традиційних вирішувальних

задач в комбінаторній теорії груп. У наших застосуваннях ми використовуємо обидва типи цих задач. Задано властивість P та об'єкт O, вирішувальна задача для P та O полягає в визначенні, чи має O властивість P, тоді як пошукова задача для P полягає в знаходженні принаймні одного конкретного об'єкта O з властивістю P з множини об'єктів S, коли є інформація про те, що існують об'єкти з властивістю P. Наприклад, проблема пошуку спряженості, проблема пошуку гомоморфізму, проблема пошуку розкладу та проблема пошуку приналежності підгрупі є деякими з запропонованих примітивів на основі пошуку.

Проблема слова стала одним з перших прикладів нерозв'язної задачі, яка була виявлена не в області математичної логіки чи теорії алгоритмів, а у ключовій сфері класичної математики – алгебрі [22]. 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. Наприклад, вільна група на двох твірних без зв’язків містить у собі як підгрупу вільну групу на злічено нескінченній кількості твірних. З такими 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 [23] 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. Ця додаткова складність робить процес аналізу і розкриття приватних ключів у криптосистемах більш складним.

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 [24]. 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. Загалом, використання неабелевих груп в криптографії дозволяє розробляти складніші та потенційно більш безпечні криптографічні схеми, які можуть пропонувати кращий захист від різноманітних типів криптоаналітичних атак. 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 [25].

Класичні групи – це групи природних матриць. Існує чотири типи для кожного цілого числа $n \geq 2$ і ступеня простого числа q. Наприклад, проективна спеціальна лінійна група $n \times n$ матриць над полем порядку q, позначена $PSL_n(q)$, має ранг $n-1$ і є простою, за винятком випадків, коли $n=2$ і $q=2,3$. Інші класичні групи – це групи унітарних, ортогональних і симплектичних матриць над скінченними полями. Інтерес мають також скінченні квазіпрості класичні групи, наприклад спеціальна лінійна група $SL_n(q)$. З $n=2$ маємо, що $SL_n(2^k) = PSL_n(2^k)$, що є простим для $k>1$. Виняткові групи не мають таких природних представлень, як групи матриць, і всі мають порядок не більше 8. Існує 10 нескінченних сімейств, індексованих ступенями простого числа q, одним з цих сімейств є групи Сузукі, що визначені над полями порядку 2^{2n+1}, які ми позначаємо $Sz(2^{2n+1})$.

З огляду на розв'язання проблеми групової факторизації автори в [26] припустили, що короткі шляхи існують у графах Кейлі кінцевих простих груп. Гіпотеза Бабая полягає в тому, що існує константа $c>0$ така, що для будь-якого h у скінченній простій неабелевій групі G і будь-якій породжуючій множині S існує шлях від 1 до h у $\Gamma(G,S)$ довжиною не більше $(\log|G|)^c$. Тобто кожен елемент G може бути записаний як слово довжини щонайбільше $(\log|G|)^c$ в елементах S. Гіпотеза Бабая для груп Лі обмеженого рангу була доведена. В інших випадках гіпотеза залишається недоведеною. Існують часткові результати, що підтверджують гіпотезу Бабая для певних генеруючих наборів. Зокрема, було доведено гіпотезу Бабая для більшості генеруючих множин знакозмінних груп та продемонстровано що гіпотеза Бабая вірна для груп великого рангу типу Лі з майже всіма достатньо великими множинами S. Гіпотеза Бабая передбачає, що для кожного елемента $h \in G$ існує шлях довжиною $(\log|G|)^{O(1)}$ від 1 до h на графі Кейлі. Важливість цієї гіпотези полягає в її наслідках для криптоаналізу в завданні пошуку таких коротких шляхів.

У області дослідження генеративних наборів, що ускладнюють пошук коротких шляхів, в останні роки отримано багато результатів: оптимізовано алгоритм Шраєра – Сімса для вирішення проблеми факторизації в групах перестановок; запропоновано алгоритм Лас-Вегас, заснований на випадковому блуканні, здатний розкладати на множники елементи A_n для майже всіх множин, а також запропоновано алгоритм, який припускається та експериментально надає ще коротші слова [27].

Було доведено, що кожна скінченна проста неабелева група G має генеруючий набір S розміром не більше семи. Для цього набору існує алгоритм, здатний знайти слова довжиною $O(\log|G|)$ за час, що дорівнює $O(\log|G|)$. Цей результат доводить необхідність пошуку таких генеруючих наборів, які роблять процес побудови коротких шляхів складнішим, збільшуючи складність криптоаналізу.

Групи Лі $PSL_n(q)$ і $SL_2(2^k)$ детально розглянуто в [25], де розроблено ефективні алгоритми для декількох спеціально вибраних генеруючих наборів. Інший підхід включає представлення класичних груп як "груп чорного ящика" та використання алгоритму Лас-Вегас для спроби побудови стандартних генеруючих наборів, які дозволяють вирішувати проблему факторизації. Для всіх генеруючих наборів $SL_2(2^k)$ існує субекспоненціальний алгоритм, що забезпечує слова субекспоненціальної довжини.

Вже було зауважено, що 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. Прикладами скінченно породжених лінійних груп є: скінченно породжені поліциклічні групи, групи Кокстера, групи кіс і групи графів. Отже, для всіх цих груп проблему зі словом можна розв'язати в логарифмічно-

му просторі. Це мотивує зазначити групи, як напрями досліджень, де проблема слова представляє практичний інтерес та може бути NP-повною:

Групи Дена: 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: ці групи 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: це групи, що генеруються відбиттями, які задовольняють певним відношенням. Для деяких класів Коксетерових груп проблема слова розв'язна.

Групи Тарського: це 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: визначені Громовим, ці групи мають складні відношення, які відображають їх геометричні властивості. Проблема слова в гіперболічних групах наразі досліджена недостатньо.

Автоматні групи: ці 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: 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, і вивчення цих груп дозволило математикам зробити значний прогрес у розумінні скінченних простих груп та їх застосуваннях у різних областях математики та фізики.

Однак єдиного ефективного алгоритму, який би працював для всіх груп і генераторних наборів, наразі не знайдено. Дослідження груп переважно як комбінаторних структур, що використовують представлення груп через генератори та релятори, є відгалуженням теорії груп, відомої як комбінаторна теорія груп.

Вагнер та Маджарік [28] 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 [5 – 10].

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. У [30] автори стверджують, що ця криптосистема з відкритим ключем безпечна, оскільки немає достатньо інформації для визначення ключа w. Криптосистема, представлена вище, була вперше атакована Гофхайнцем і Стейнвандтом у [31]. Однак їхній алгоритм в основному заснований на грубій силі. Пізніше в 2003 р. Петрідес [32] заявив, що цей протокол вразливий, оскільки наданий відкритий ключ дає занадто багато інформації та дозволяє зловмиснику легко отримати закритий ключ. Схема узгодження ключів на основі задачі одночасного пошуку спряженості. Протокол Аншеля – Аншеля – Голдфельда добре відома і базується на складності проблеми одно-

часного пошуку спряженості. У 2019 р. Григорчук і Григор'єв запропонували певні класи груп автоматів для протоколу AAG. Конкретними прикладами, які вони запропонували, є перша група Григорчука та група Базиліка. Безпека цієї системи в цілому полягає в складності варіації проблеми пошуку сполученості в певних групах. Наприклад, Ко-Лі запропонував групи кіс, а Ейк та Кахробай в [33] запропонували поліциклічні групи.

Висновки

Асиметрична криптографія використовує односторонні функції. NP-повні задачі вважаються оптимальними для таких функцій, оскільки вони дозволяють відносно легко генерувати складні для вирішення приклади для яких рішень є складним. Однак, застосування NP-повних задач у криптографії обмежене через труднощі у створенні задач, які би були 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. Проведено 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.

Список літератури:

1. Liu, Yanyi, and Rafael Pass. On one-way functions from NP-complete problems // Cryptology ePrint Archive (2021).
2. Luckow, Andre, Johannes Klepsch, and Josef Pichlmeier. Quantum computing: Towards industry reference problems // Digitale Welt 5 (2021): 38–45.
3. Gilles Brassard. Relativized cryptography // Proceedings of the 20th Annual Symposium on Foundations of Computer Science. 1979. pp. 383–391.
4. Baldo A., Boffa M., Cascioli L., Fadda E., Lanza C., & Ravera A. The polynomial robust knapsack problem // European Journal of Operational Research. 2023. 305(3). 1424–1434.
5. Kotukh Y., Khalimov G. Towards practical cryptoanalysis of systems based on word problems and logarithmic signatures // Proceedings of II International Conference Information security: problems and prospects, 25 Nov 2022, Baku, Azerbaijan, pp. 55–58.
6. 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.
7. 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
8. 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.
9. Khalimov G., Kotukh Y., Didmanidze I., Khalimova S. 2021. Encryption scheme based on small Ree groups // Proceedings of the 2021 7th International Conference on Computer Technology Appli-cations (ICCTA '21). ACM, New York, NY, USA, 33–37. https://doi.org/10.1145/3477911.3477917
10. Khalimov G., Kotukh Y., Shonia O., Didmanidze I., Sievierinov O., Khalimova S. Encryption Scheme Based on the Automorphism Group of the Suzuki Function Field // 2020 IEEE PIC S&T, Kharkiv, Ukraine, 2020, pp. 383–387. doi: 10.1109/PICST51311.2020.9468089.
11. Suo J., Wang L., Yang S., Zheng W., & Zhang J. Quantum algorithms for typical hard problems: a perspective of cryptanalysis // Quantum Information Processing. 2020. 19. P. 1–26.
12. Vega F. (2023). On Feasibly Solving NP-complete Problems.
13. Causey C. J. (2023). NP-Complete Problems and Public Key Cryptography.
14. Todd J.A., Coxeter H.S.M. A practical method for enumerating cosets of a finite abstract group // Proc. Edinb. Math. Soc., II. Ser. 5, 26-34 (1936). Zbl 0015.10103, JFM 62.1094.02
15. Ball W. W. R., & Coxeter H. S. (2022). Knuth-Bendix Completion Algorithm.
16. Novikov P. S. Algorithmic Unsolvability of the Word Problem in Group Theory.. L. Britton, 1958 // Journal of Symbolic Logic 23 (1):50–52.
17. William W. Boone, Frank B. Cannonito, Roger C. Lyndon, Word Problems, Decision Problems and Burnside Problem in Group Theory. C. R. J. Clapham, 1976 // Journal of Symbolic Logic 41 (4):785–788.

18.Nyberg Brodda, Carl-Fredrik. The word problem and combinatorial methods for groups and semigroups. Diss. University of East Anglia, 2021.
19.Rybalov A. (2020, May). A generic algorithm for the word problem in semigroups and groups // Journal of Physics: Conference Series (Vol. 1546, No. 1, p. 012100). IOP Publishing.
20.Hooshmand M. H. Basic results on an unsolved problem about factorization of finite groups // Communications in Algebra 49.7 (2021): 2927–2933.
21.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.
22.Verschaffel L., Schukajlow S., Star J., & Van Dooren W. (2020). Word problems in mathematics education: A survey. ZDM, 52, 1-16.
23.van Veldhuizen, Toon, and Hans Cuypers. Investigating finite simple groups. Master Thesis
24.Singh, Priyanka, Manju Khari, and Nikhil S. Kaundanya. Impact of group theory in cryptosystem // Functional encryption. Cham: Springer International Publishing, 2021. 19–36.
25.Lanel G. H., Jinasena T. M. K. K., & Welihinda, B. A. (2021). A survey of public-key cryptography over non-abelian groups.
26. Kahrobaei D., Flores R., & Noce, M. (2023). Group-based cryptography in the quantum era. Not. Am. Math. Soc, 70(5), 752–763.
27.Vasco, María Isabel González, Delaram Kahrobaei, and Eilidh McKemmie. Applications of Finite non-Abelian Simple Groups to Cryptography in the Quantum Era // arXiv preprint arXiv:2308.14725 (2023).
28.Wagner N.R. and Magyarik M.R. A public-key cryptosystem based on the word problem // Proc. Advances in Cryptology–CRYPTO 1984, LNCS 196, Springer-Verlag (1985), pp. 19–36.
29.Sconza S., & Wildi, A. (2024). Knot-based Key Exchange protocol // Cryptology ePrint Archive.
30.Kahrobaei D., Khan B. A non-commutative generalization of ElGamal key exchange using polycyclic groups // IEEE GLOBECOM Global Telecommunications Conference [4150920], 2006. doi: 10.1109/glocom.2006.
31.Hofheinz D., & Steinwandt R. (2002). A practical attack on some braid group based cryptographic primitives // Public Key Cryptography—PKC 2003: 6th International Workshop on Practice and Theory in Public Key Cryptography Miami, FL, USA, January 6–8, 2003 Proceedings 6 (pp. 187–198). Springer Berlin Heidelberg.
32.Petrides G. (2006). Cryptographic applications of non-commutative algebraic structures and investigations of nonlinear recursions. The University of Manchester (United Kingdom).
33.Eick B., & Kahrobaei D. (2004). Polycyclic groups: a new platform for cryptology? // arXiv preprint math/0411077.
34.Kuperberg G. (2005). A subexponential-time quantum algorithm for the dihedral hidden subgroup problem // SIAM Journal on Computing. 35(1). 170–188.

Надійшла до редколегії 10.03.2024

Відомості про авторів:
Котух Євген Володимирович – канд. техн. наук, доцент, професор кафедри кібербезпеки; Національний технічний університет «Дніпровська політехніка»; Дніпро, Україна; e-mail: yevgenkotukh@gmail.com; ORCID: https://orcid.org/0000-0003-4997-620X
Халімов Геннадій Зайдулович – д-р техн. наук, професор, завідувач кафедри безпеки інформаційних технологій; Харківський національний університет радіоелектроніки; Харків, Україна; e-mail: hennadii.khalimov@nure.ua; ORCID: https://orcid.org/0000-0002-2054-9186
Коробчинський Максим Володимирович – д-р техн. наук, професор, начальник 2-ї кафедри технічних видів розвідки та інформаційних технологій 2-го навчального інституту Воєнної академії імені Євгенія Березняка Міністерства оборони України; Київ, Україна; e-mail: mars_kor@ukr.net; ORCID: https://orcid.org/0000-0001-8049-4730,
Руденко Михайло Миколайович – канд. техн. наук, доцент, доцент 2-ї кафедри технічних видів розвідки та інформаційних технологій 2-го навчального інституту Воєнної академії імені Євгенія Березняка Міністерства оборони України; Київ, Україна; e-mail: ruminik33@ukr.net; ORCID:https://orcid.org/0000-0002-9180-1510
Любчак Володимир Олександрович – канд. фіз.-мат. наук, доцент, завідувач кафедри кібербезпеки Сумського державного університету; e-mail: v.liubchak@dcs.sumdu.edu.ua; ORCID: https://orcid.org/0000-0002-7335-6716
Мацюк Сергій Михайлович – канд. техн. наук, доцент, доцент кафедри кібербезпеки; Національний технічний університет «Дніпровська політехніка»; Дніпро, Україна; e-mail: matsiuk.s.m@nmu.one; ORCID: https://orcid.org/0000-0001-6798-5500
Чащин Максим В'ячеславович – аспірант; Національний технічний університет «Дніпровська політехніка»; Дніпро, Україна; e-mail: mchaschin@gmail.com; ORCID: https://orcid.org/0009-0004-4671-0443