УДК 004.056.55 **DOI:10.30837/rt.2025.2.221.10**

Є.В. КОТУХ, канд. техн. наук, Г.З. ХАЛІМОВ, д-р техн. наук, І.Є. ДЖУРА

КРИПТОГРАФІЧНА КОНКУРЕНТОСПРОМОЖНІСТЬ КРИПТОСИСТЕМ НА ОСНОВІ НЕКОМУТАТИВНИХ ГРУП

Вступ

Сучасна криптографія стоїть на порозі фундаментальних змін, зумовлених стрімким розвитком квантових обчислень. Побудова повномасштабного квантового комп'ютера несе пряму загрозу для більшості криптографічних систем, що використовуються сьогодні. Алгоритм Шора, запропонований у 1994 р., дозволяє розв'язувати задачі факторизації цілих чисел та дискретного логарифмування за поліноміальний час [1]. Саме на складності цих задач базується безпека таких поширених систем, як RSA, DSA та криптографія на еліптичних кривих (ECC).

Поточний стан розробки квантових комп'ютерів демонструє неухильний прогрес. Компанії IBM, Google, IonQ та інші досягли значних успіхів у створенні квантових процесорів з десятками та сотнями кубітів. Експертні оцінки щодо появи криптографічно релевантного квантового комп'ютера (CRQC) – системи, здатної зламати сучасні криптографічні стандарти, – варіюються від 10 до 30 років [2]. Однак принцип "збирай сьогодні, розшифровуй завтра" змушує вже зараз переходити до постквантової криптографії, оскільки конфіденційні дані, зашифровані сьогодні, можуть зберігати свою цінність протягом десятиліть.

Усвідомлення цієї загрози стимулювало глобальний рух до розробки та стандартизації постквантових криптосистем (Post-Quantum Cryptography, PQC) – алгоритмів, стійких до атак як з боку класичних, так і квантових комп'ютерів. Національний інститут стандартів і технологій США (NIST) з 2016 р. проводить міжнародний конкурс з відбору стандартів PQC [3]. У 2022 р. було завершено перший раунд стандартизації, в результаті якого було обрано чотири алгоритми: CRYSTALS-Kyber (інкапсуляція ключів), CRYSTALS-Dilithium та FALCON (цифрові підписи), а також SPHINCS+ (резервний алгоритм підписів). Усі ці рішення базуються на решітчастій криптографії та криптографії геш-функцій.

Серед основних напрямів досліджень у галузі PQC виділяють криптографію на основі кодів, що виправляють помилки (code-based), геш-функцій (hash-based), решіток (lattice-based), багатовимірних поліномів (multivariate) та некомутативних груп (non-commutative group-based) [4]. Примітно, що алгоритми на основі некомутативних груп не увійшли до першого набору стандартів NIST, що частково пояснюється їх відносною новизною та складністю аналізу безпеки. Однак четвертий раунд конкурсу NIST, який триває, розглядає альтернативні підходи, включаючи системи на некомутативних групах [5].

Криптосистеми на основі некомутативних груп представляють особливий інтерес завдяки унікальним властивостям некомутативних алгебраїчних структур. Некомутативність – властивість, за якої результат операції залежить від порядку операндів – забезпечує природний захист від квантових алгоритмів, які ефективно працюють з комутативними структурами. Основними представниками цього напряму є групи кіс (braid groups), матричні групи над кінцевими кільцями, групи автоморфізмів та поліциклічні групи. Ці системи демонструють привабливі характеристики: компактність ключів, високу швидкість криптографічних операцій та потенційну стійкість до як класичних, так і квантових атак.

Однак розробка практичних криптосистем на некомутативних групах стикається з низкою викликів. По-перше, це складність ретельного аналізу криптографічної стійкості через нестандартні математичні основи порівняно з класичними підходами. По-друге, необхідність забезпечення балансу між безпекою, продуктивністю та розміром ключів/підписів відповідно до сучасних практичних вимог. По-третє, важливість забезпечення сумісності з існуючою інфраструктурою та підтримки криптографічної гнучкості (crypto-agility) – здатності швидко переходити між різними алгоритмами у разі виявлення вразливостей [6].

Актуальність дослідження криптосистем на некомутативних групах зумовлена кількома факторами. Насамперед, принцип диверсифікації криптографічних підходів вимагає розробки альтернативних рішень, заснованих на різних математичних засадах. Монокультура в постквантовій криптографії, коли усі системи базуються на решітчастих задачах, створює ризик одночасного компрометування всіх алгоритмів у випадку прориву в методах їх аналізу. Некомутативні групи можуть слугувати як резервне або доповнююче рішення, забезпечуючи криптографічну стійкість навіть у разі компрометування основних постквантових стандартів.

Метою даного дослідження є комплексний аналіз криптографічної конкурентоспроможності систем на основі некомутативних груп, оцінка їх переваг і недоліків порівняно з існуючими постквантовими рішеннями, а також визначення перспектив їх практичного застосування в умовах квантової загрози.

Групова криптографія на основі некомутативних груп

Криптографія на основі некомутативних груп є одним з найстаріших і водночас найменш досліджених напрямів PQC. Її привабливість полягає у використанні математичних структур, де задачі, аналогічні задачі дискретного логарифма, вважаються обчислювально складними навіть для квантових комп'ютерів. Прикладами таких задач є задача пошуку спряженого елемента (Conjugacy Search Problem, CSP), задача розкладу елемента за множиною твірних (Decomposition Problem, DP) або проблеми слова (Word Problem, WP) [6].

Безпека криптосистем на некомутативних групах базується на уявній складності цих специфічних задач, на основі яких було розроблено низку протоколів обміну ключами. Відомим прикладом є протокол Аншеля–Аншеля–Гольдфельда (AAG). Це один з перших протоколів, що базується на складності одночасного розв'язання задачі CSP. Два користувачі, Аліса та Боб, обирають секретні елементи з певних комутуючих підгруп і обмінюються публічними ключами, які є результатом спряження. Спільний секретний ключ обчислюється як результат послідовного застосування секретних елементів. Безпека протоколу критично залежить від вибору платформної групи [7]. Протокол Ко–Лі використовує властивості комутаторів. Аліса обирає секретний елемент a, а Боб – b. Вони обмінюються спряженими елементами, і спільний ключ обчислюється як комутатор $[a,b]=aba^{-1}b^{-1}$. Цей протокол також виявився вразливим у багатьох групах [8].

Вибір «правильної» платформної групи є центральною проблемою в некомутативній груповій криптографії. Ідеальна група повинна поєднувати високу складність обчислювальних задач з ефективністю групових операцій та стійкістю до відомих атак [9].

Історично групи кіс (Braid Groups) були першими і найпопулярнішими кандидатами на роль платформних груп. Вони мають інтуїтивну геометричну інтерпретацію, а групова операція (композиція кіс) є відносно простою. Протоколи AAG та Ко–Лі початково пропонувалися саме для груп кіс. Однак з часом було знайдено низку ефективних атак. Атака лінійного розкладу (Linearization attacks) використовує гомоморфні відображення групи кіс в матричні групи, де задача CSP стає значно простішою. Атака на основі довжини (Length-based attacks)

використовує специфічні метрики та властивості нормальних форм (наприклад, нормальна форма Гарсайда) для отримання інформації про секретний ключ. Через ці атаки більшість криптосистем на групах кіс сьогодні вважаються зламаними або небезпечними [10].

Поліциклічні групи (Polycyclic Groups) мають перевагу в ефективному представленні елементів та швидких групових обчисленнях. Це дозволило розробити практичні криптосистеми. Проте, структура цих груп виявилася занадто "регулярною". Атака Усова (Usov's attack) продемонструвала, як можна ефективно лінеаризувати задачу CSP у поліциклічних групах, що робить їх непридатними для криптографії, що використовує проблему CSP [11].

Група Томпсона F (Thompson's Group F) має низку унікальних властивостей, зокрема, вона є нескінченною, скінченно породженою та не містить вільних підгруп. Були спроби побудувати на ній криптосистеми, але задача CSP в цій групі виявилася тривіальною [12]. Дослідження продовжуються, але наразі Група Томпсона F не вважається надійним кандидатом для «платформної» групи.

Групи матриць, такі як $GL(n,q)$, були запропоновані як платформи для протоколів, що базуються на задачі розкладу (DP). Перевагою є швидкі матричні операції. Однак багато таких схем вразливі до атак, що використовують методи лінійної алгебри, наприклад обчислення власних векторів та значень. Протокол MOR виявився вразливим саме через такі методи [13].

Дослідження, результати якого представлено в даній роботі, дало новий імпульс використанню кінцевих простих груп та груп автоморфізмів, що пов'язані з максимальними кривими Деліня–Люстига (Ерміта, Сузукі, Рі) [14 – 23].

Незважаючи на теоретичну привабливість, некомутативна групова криптографія поки не досягла значного успіху в процесі стандартизації PQC NIST. Подані пропозиції не дійшли до фінальних раундів конкурсу NIST PQC. Так, схема цифрового підпису WalnutDSA була одною з найвідоміших кандидатів у першому раунді NIST PQC. Однак схему WalnutDSA, що базується на групах кіс та використовує нову обчислювальну задачу E-Multiplication, було незабаром зламано за допомогою атаки лінійного розкладу [24]. Інші пропозиції на основі груп також були атаковані або не змогли продемонструвати достатню ефективність порівняно з кандидатами на основі решіток чи кодів. Проаналізуємо основні причини, що гальмують стандартизацію криптопримитивів на основі групової криптографії. По-перше, це проблеми з доведенням безпеки, бо формально складно довести складність базових задач для конкретних груп в поєднанні до складної проблеми, що застосовується як «платформне» рішення. По-друге, швидкі реалізації атак на початкові пропозиці підірвали довіру до напряму в цілому. По-третє, багато з опублікованих групових протоколів мають великий розмір ключів та/або повільні операції порівняно з лідерами PQC, такими як Kyber та Dilithium. І хоча, на думку автора, великий розмір ключів в постквантову еру не є фактором, що міг би заблокувати рішення від подальшого розгляду в поєднанні з висвітленими проблемами, це визивало скепсіс у експертів NIST.

Сучасний стан криптографії на основі некомутативних груп можна охарактеризувати як період обережного оптимізму та інтенсивного пошуку. Після хвилі успішних атак на перше покоління протоколів спільнота усвідомила, що вибір платформної групи та дизайну протоколу є надзвичайно складним завданням. Проаналізуємо основні виклики для створення успішного PQC кандидата на основі групової некомутативної криптографії. По-перше, зрозуміло, що основним викликом є пошук надійних платформ – груп, що не допускають «простих» гомоморфізмів у лінійні групи та є стійкими до атак на основі структурних властивостей. По-друге, формальний аналіз безпеки та доведення складності обчислювальних задач

для кандидатних груп має бути наведено з урахуванням сучасного уявлення про побудову та реалізацію атак з використанням квантового компьютера. По-трете, проблема підвищення ефективності, а саме зменшення розміру ключів або реалізація прискоренних обчислень, мала б на меті демонстрацію криптографічної конкурентоспроможності з іншими PQC-напрямами.

Одним із підходів у цьому напряму є використання криптосистем на основі логарифмічних підписів (Logarithmic Signatures, LS), зокрема сімейства MST [25 – 29]. Історично реалізації, такі як криптосистема MST3, використовували для криптографічних перетворень, переважно центр скінченної некомутативної групи (наприклад, групи Сузукі). Такий підхід має суттєвий недолік: потужність (порядок) центру групи значно менша за потужність самої групи. Це обмежує як розмір простору повідомлень, так і варіативність криптографічних перетворень, що потенційно звужує простір ключів та може створювати вразливості.

Дане дослідження узагальнює результати розробки та аналізу нового підходу до побудови криптосистем на некомутативних групах. В якості математичної платформи було обрано групи автоморфізмів функціональних полів, асоційованих з максимальними кривими Деліня–Люстига, а саме кривими Ерміта, Сузукі та Рі. Ці групи є багатопараметричними, мають надзвичайно великий порядок та складну внутрішню структуру, що робить їх привабливими кандидатами для побудови стійких постквантових криптосистем.

Метою статті є представлення узагальненої моделі для класу криптосистем на основі логарифмічних підписів, проведення порівняльного аналізу різних платформних груп (Сузукі, Ерміта, Рі) та оцінка їхньої криптографічної конкурентоспроможності з погляду безпеки та затрат на реалізацію.

Результати дослідження криптосистем на основі груп з використанням логарифмічних підписів

В основі дослідження груп лежить теорія алгебраїчних кривих над скінченними полями. Важливим класом максимальних кривих є так звані криві Деліня–Люстига, що виникають у теорії представлень скінченних груп типу Лі [30]. У дослідженні було розглянуто три родини таких кривих – Ерміта, Сузукі та Рі. Ці групи автоморфізмів є скінченними простими або майже простими групами типу Лі. Вони мають великий порядок та неабелеву структуру, що робить їх ідеальними кандидатами для побудови криптосистем. На відміну від груп кіс, ці групи є 3-х або 4-параметричними, що ускладнює їх аналіз та потенційно робить обчислювальні задачі складнішими. Порядок цих груп зростає поліноміально з високим степенем від розміру поля, що створює великий простір для ключів. Замість класичних протоколів AAG/Ко–Лі для цих груп було розроблено метод направленого шифрування на основі логарифмічних підписів. Концепція логарифмічного підпису є центральною для криптосистем сімейства MST. На практиці він реалізується у вигляді представлення, де кожному елементарному блоку повідомлення ставиться у відповідність певний елемент групи. У класичній криптосистемі MST3 повідомлення відображалося в центр групи $Z(G)$, що обмежувало як простір повідомлень, так і варіативність перетворень.

Ключова ідея дослідження полягає у відмові від обмеження центром групи та використанні для шифрування значно більших її підструктур – ядра гомоморфізму або повної групи. Запропонований метод направленого шифрування дозволяє подолати головний недолік старих систем MST – обмеженість центром групи. Таким чином, вдалося значно збільшити розмір повідомлення та потенційну криптостійкість.

Загальний алгоритм можна представити у вигляді блок-схеми:

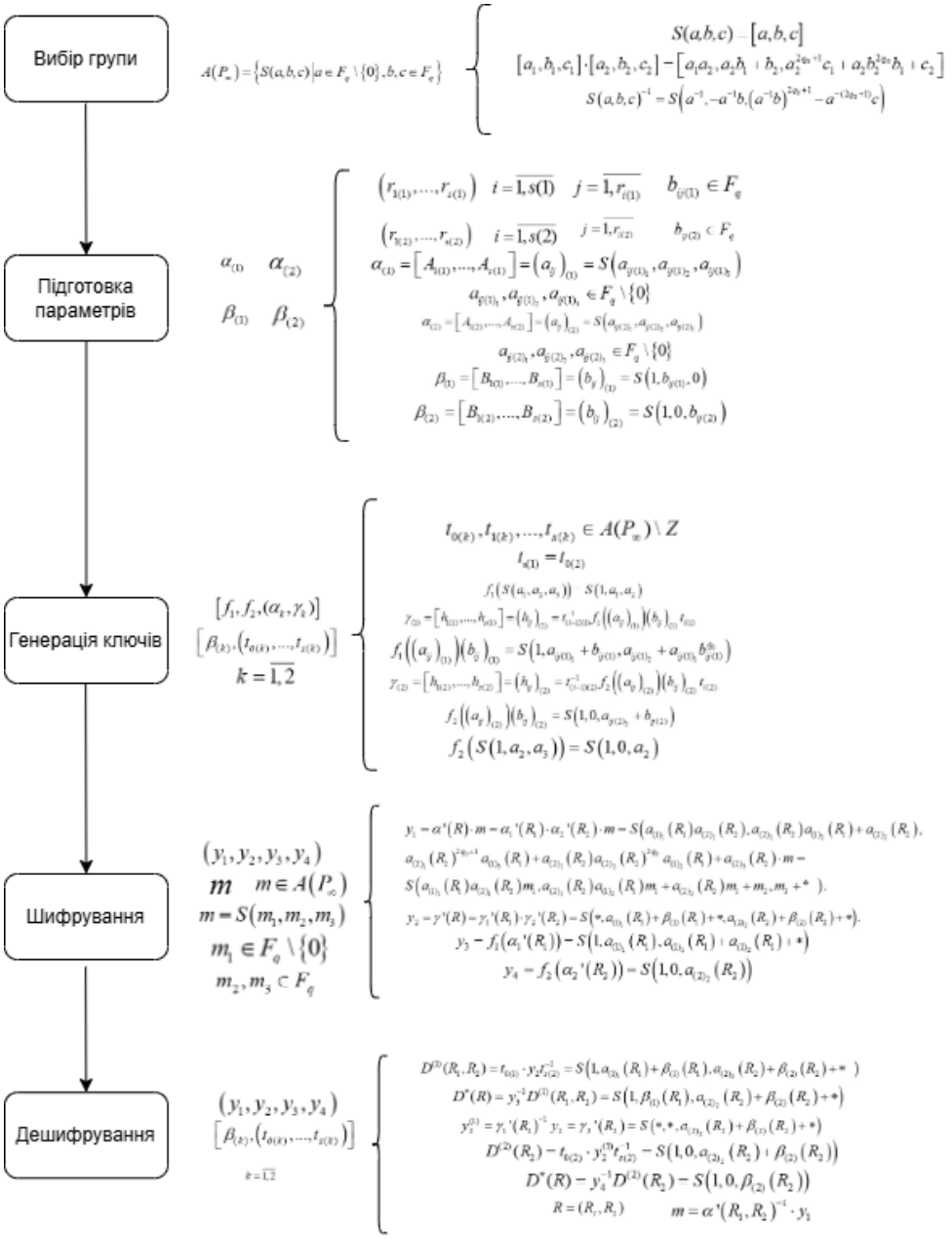

Рис. 1. Блок-схема загального алгоритму направленого шифрування на максимальних групах Деліня–Люстига

В якості математичної платформи було обрано групи автоморфізмів функціональних полів, асоційованих з максимальними кривими Деліня–Люстига: кривими Ерміта, Сузукі та Рі. Ці групи є скінченними простими або майже простими групами типу Лі. Вони мають великий порядок та складну неабелеву структуру, що робить їх ідеальними кандидатами для побудови стійких криптосистем. На відміну від груп кіс, ці групи є 3-х або 4-параметричними, що ускладнює їх аналіз та потенційно робить обчислювальні задачі складнішими.

ISSN 0485-8972 Radiotekhnika No. 221 (2025)
eISSN 2786-5525

Таблиця 1

Порівняльні характеристики платформних груп

Артефакти	**Автоморфізми функціонального поля групи Сузукі**	**Автоморфізми функціонального поля групи Ерміта**	**Автоморфізми функціонального поля групи Рі**
Група	$A(P_\infty)=\{S(a,b,c)\mid a\in F_q\setminus\{0\}, b,c\in F_q\}$	$A(P_\infty)=\{S(a,b,c)\mid a\in F_q\setminus\{0\}, b,c\in F_q\}$	$A(P_\infty)=\{a(x),\beta(x),y(x),h(\lambda),I^{-}\mid x\in F_q,\lambda\in F_q^{x}\}$
Порядок	$OrdA(P_\infty)=q^2$	$OrdA(P_\infty)=q^3(q^2-1)$	$OrdA(P_\infty)=q^3$
Кількість параметрів	3-параметрична	3-параметрична	4-параметрична
Скінченне поле	F_q	F_q	F_q
Структура центра			
Елемент групи	$S(a,b,c)=[a,b,c]$	$S(a_1,b_1,c_1)\cdot S(a_2,b_2,c_2)=S(a_1a_2,a_2b_1+b_2,a_2^{q+1}c_1+a_2b_2^qb_1+c_2)$	$S(a,b,c)=a(a)\beta(b)\gamma(c)$
Зворотній елемент групи	$S(a,b,c)^{-1}=S(a^{-1},-a^{-1}b,(a^{-1}b)^{2q_0+1}-a^{-(2q_0+1)}c)$	$S(a,b,c)^{-1}=S(a^{-1},-a^{-1}b,-a^{-(g+1)}c+a^{-(g+1)}b^{q+1})$	$S(a,b,c)^{-1}=S(-a,-b-a^{3t+1},-c-ab+a^{3t+2})$
Гомоморфізми	$f_1(S(a_1,a_2,a_3))=S(1,a_1,a_2)$ $f_2(S(1,a_2,a_3))=S(1,0,a_2)$	$f_1(S(a_1,a_2,a_2^{q+1}/2))=S(1,a_2,a_2^{q+1}/2)$ $f_2(S(a_1,a_2,a_2^{q+1}/2))=S(1,0,a_2)$	$f((a_{ij})_{(1)})(b_{ij})_{(1)}=S(0,a_{ij(1)_1},a_{ij(1)_2})S(0,b_{ij(1)},0)=S(0,a_{ij(1)_1}+b_{ij(1)},a_{ij(1)_2})$, $f((a_{ij})_{(2)})(b_{ij})_{(2)}=S(0,0,a_{ij(2)_2})S(0,0,b_{ij(2)})=S(0,0,a_{ij(2)_2}+b_{ij(2)})$
Розмір логарифмічного підпису	<256 записів по 128 біт	<256 записів по 128 біт	256 записів по 64 біти
Особливості	Просте представлення при непарній характеристиці	Ефективні обчислення в полях характеристики 2	Найбільший порядок та кількість параметрів серед груп на кривих Деліня–Люстіга
Атака грубою силою на зашифрований текст	$O(q^2)$, визначається повним порядком групи	$O(q^3)$, визначається вичерпним пошуком по всій групі	$O(q^2)$, визначається повним порядком групи
Атака грубою силою на $R=(R_1,R_2)$.	$O(q)$, забезпечується зв'язуванням ключів	$O(q^l)$, забезпечується зв'язуванням ключів та гомоморфним шифруванням	$O(q^2)$, забезпечується зв'язуванням ключів та гомоморфним шифруванням
Атака грубою силою на $(t_{0(k)},\dots,t_{s(k)})$.	$O(q)$	$O(q^5)$	$O(q^3)$
Атака на алгоритм	$O(q^2)$	$O(q^5)$	$O(q^2)$
Оцінка PQC стійкості	Висока, оскільки для задачі WP невідомі ефективні квантові алгоритми	Висока, оскільки невідомі ефективні квантові алгоритми	Найвища з розглянутих, зважаючи на максимальний порядок та складність структури

У класичній криптосистемі MST3 повідомлення відображається в центр групи Z(G), який є абелевою підгрупою. Це дозволяє легко виконувати обчислення, але обмежує простір зашифрованих значень. Гіпотеза дослідження полягала в тому що використання логарифмічних підписів з відображенням на всю групу, а не тільки в центр групи як в базовій конструкції MST3 не в центр, дозволяє суттєво збільшити довжину повідомлення, яке можна зашифрувати за одну ітерацію та розширити простір ключів та підвищити загальну криптографічну стійкість системи за рахунок використання складнішої структури всієї групи. Практичні результати, що викладені в табл. 1, підтверджують гипотезу.

Використовуючи всю групу для шифрування, вдалося значно збільшити розмір повідомлення та потенційну криптостійкість. Як показано у дослідженні, початкові версії направленого шифрування були вразливі до атак послідовного відновлення. Цю проблему було вирішено шляхом зв'язування ключів та застосування гомоморфного шифрування до випадкових покриттів, що є важливим кроком до створення практично безпечної системи.

Використання багатопараметричних груп дозволяє досягати високого рівня безпеки при відносно менших розмірах скінченного поля. Це прямо впливає на затрати на ключі та загальні параметри. Застосування розроблених контрзаходів дозволяє довести складність атаки на криптосистему до повного перебору по всій групі. Продемонструємо отримані в роботах [14 – 23] результати.

Результати дослідження платформних груп

Дослідження дозволило отримати низку вагомих наукових та практичних результатів, що підсумовано нижче.

Привабливими групами є групи з центром, який визначається елементарною 2 абелевою групою, що досягається на скінченних полях характеристики 2. Застосування логарифмічних підписів та випадкових покриттів призводить до низьких витрат на загальні параметри криптосистеми.

Таким класом груп, з накриттям Галуа ступеня *m* та з характеристикою 2, є узагальнені 2-групи Сузукі. Узагальнені 2-групи Сузукі є багатопараметричними групами і можуть мати довільний великий порядок. Криптосистеми MST на основі узагальненої 2-групи Сузукі потенційно мають перевагу над іншими реалізаціями схем у секретності та реалізації. Використання багатопараметричних груп потенційно забезпечує кращі характеристики в реалізації за рахунок оптимізації обчислення по параметрах групи та розміру скінченного поля. Максимальна підгрупа повної групи автоморфізмів $A(P_\infty)$ ототожнюється з трійкою $A(P_\infty)=\left\{[a,b,c]\,|\,a,b,c\in K, a\neq 0,\ ma\ c^{q_0}+c=b^{q_0+1}\right\}$, має порядок більший ніж порядок групи Сузукі, що дорівнює $ordH(P_\infty)=q^3\left(q^2-1\right)$. Для непарної характеристики поля F_{q^2} група автоморфізмів $A(P_\infty)$ визначається як $A(P_\infty)\left\{\left[a,b,\frac{b^{q+1}}{2}+c\right]\middle| a\in F_{q^2}^*, b\in F_{q^2}\ \ and\ \ c^q+c=0\right\}$. Для непарного характеристичного поля група автоморфізмів $A(P_\infty)$ функціонального поля Ерміта має просте представлення. Обчислювальні вектори з використанням матриць логарифмічних підписів і випадкових покриттів легко транскодуються в координати підгрупи $A(P_\infty)$.

Вперше запропонований метод направленого шифрування по групі автоморфізмів функціонального поля функцій Сузукі має переваги у високій секретності схеми шифрування на основі групи автоморфізмів $A(P_\infty)$ функціонального поля Сузукі над F_q, що дорівнює q^2. При цьому довжина зашифрованого тексту визначається значенням $3\log q$ для обчислення в скінченному полі над F_q, довжина логарифмічного масиву підпису визначається кінцевим полем понад F_q і значно менше порівняно з криптосистемою MST3, а обчислення в кінцевому полі простіші, в порівнянні з криптосистемою MST3 по групі Сузукі, за рахунок обчислення оберненого елемента в кінцевому полі розмірності, яка в два рази більша.

Вперше запропоновано метод направленого шифрування на групах автоморфізмів функціонального поля Ерміта. Було розроблено та обгрунтовано нове рішення, яке полягає в тому, щоб побудувати логарифмічний підпис поза центром групи для реалізації шифрування по всім координатам групи. Таке рішення дало можливість зменшити розмір кінцевого поля F_{q^2}, складність обчислення при фіксованій секретності криптосистеми. Практично це реалізується за рахунок обчислень в квадратичному полі непарної характеристики. Для перекодування значень обчислювальних векторів в координати групи Ерміта вимагається вирішення рівняння $c^q + c = 0$. Для непарної характеристики квадратичного поля такі рішення знаходяться за виразом $c_i = \gamma^{(q+1)/2+i(q+1)}$, $i = 0,1,...q-1$. Функціональне поле Ерміта є розширенням Галуа над $\mathrm{F}_{q^2}(x)$ з великою групою автоморфізмів, фіксовані поля підгруп групи автоморфізмів надають багате джерело максимальних функціональних полів. Для функціонального поля Ерміта існує кілька сімейств підгруп $A(P_\infty)$.

Метод направленого шифрування на групах функціонального поля Ерміта було вдосконалено використанням гомоморфного перетворення. Складність атаки відновлення ключа в такій криптосистемі визначається вичерпним пошуком по всій групі. У запропонованій криптосистемі з гомоморфним шифруванням випадкові покриття є секретом для криптоаналітика. У цьому випадку відомі атаки на основі слабкості логарифмічних підписів неможливі. Криптосистема MST3, що заснована на групі автоморфізму функціонального поля Ерміта, має перевагу над реалізаціями по групі Сузукі в секретності та реалізації.

Вперше побудовано метод направленого шифрування по малій групі Рі, який, на відміну від MST3 по групі Сузукі, використовує шифрування по ядру групи, що дозволило збільшити розмір повідомлення для зашифрування до значення $|m| = q^2$. Розроблено удосконалення методу направленого шифрування по малій групі Рі на основі шифрування по повній групі $U(q) = \left\{ S(a,b,c) \middle| a,b,c \in F_q \right\}$ зі зв'язаними ключами $R = (R_1, R_2, R_3)$, що дозволило захиститися від атаки послідовного відновлення та забезпечити складність атаки грубої сили q^3.

Криві Рі є максимальними кривими найбільшого роду і мають найбільші групи, що породжуються кривою. Група автоморфізмів по кривій Рі є 4-параметричною групою над полем F_q. Це найбільша група по максимальним кривим Деліня–Люстіга.

Вперше побудовано метод направленого шифрування по групі автоморфізмів функціонального поля Рі, який, на відміну від MST3 по групі Сузукі, використовує шифрування по ядру групи, що дозволило збільшити розмір повідомлення для зашифрування до значення $|m| = q^4$. Розроблено удосконалення методу направленого шифрування по групі автоморфізмів функціонального поля Рі на основі шифрування на повній групі зі зв'язаними ключами, що дозволило захиститися від атаки послідовного відновлення на основі зв'язування ключів логарифмічних підписів та забезпечити складність атаки грубої сили q^4. Група автоморфізмів по кривій Рі $A(P_\infty)$ з $\left|A(P_\infty)\right| = q^3(q-1)$ є максимальною підгрупою і це більше в q рази потужності групи автоморфізмів по кривій Сузукі, та в $q^{3/2}$ рази більше в порівнянні з групою автоморфізмів по кривим Ерміта. Побудова криптосистем на малих групах Рі та автоморфізмах групи Рі має кращі характеристики по секретності та реалізації.

Запропоновано удосконалення методу направленого шифрування по групі автоморфізмів функціонального поля Рі на основі секретного гомоморфного перетворення для випадкових покриттів, що забезпечує захист від послідовних атак відновлення та атак з вибраним текстом, і складність атаки відновлення ключа буде визначатися вичерпним перебором по всій групі автоморфізмів. Реалізація криптосистеми на групі автоморфізмів $A(P_\infty)$ функціонального поля Рі вимагає побудови логарифмічного підпису β на векторах 2^h, де h визначається розміром типу $r_i = 2^h$. Всі блоки B_i є підгрупами $U(q) = \left\{ S(1,b,c) \middle| b,c \in F_q \right\}$. Розмір

масивів β і α визначається типом $(r_1,...,r_s)_b$ і $(r_1,...,r_s)_c$ по координатам b,c для підгруп $U(q)$. Для 128-бітної криптографії, яка еквівалентна обчисленням над полем, $q=2^{64}$, якщо r_i тип $r_i=2^2$, $s=32$, для криптографії в групі потрібні лише 256 записів по 64 біти. У порівнянні з MST3 у Сузукі 2-групі матиме 256 записів по 128 біт для $r_i=2^2$, $s=64$ і 512 записів для $r_i=4^2$, $s=32$. Таким чином, побудова криптосистем на логарифмічних підписах по багатопараметричним групам потенційно забезпечує кращі характеристики в реалізації за рахунок оптимізації обчислення по параметрах групи та розміру скінченного поля.

Висновки

Фактично розроблено новий клас криптосистем. Створено та формалізовано метод «направленого шифрування», який ефективно використовує всю структуру великих некомутативних груп, долаючи обмеження класичних підходів, що базувалися на центрі групи. Проведено порівняльний аналіз платформ. Дослідження підтвердило, що збільшення кількості параметрів групи та її порядку напряму впливає на потенційну секретність та ефективність криптосистеми. Група Рі, як чотирипараметрична група найбільшого порядку, виявилася найбільш потужною та перспективною платформою. Досягнуто високого рівня безпеки. Запропоновані удосконалення (зв'язування ключів та гомоморфне шифрування покриттів) ефективно нейтралізують відомі атаки. Складність атаки методом грубої сили на посилені системи оцінюється повним порядком відповідної групи (наприклад, O(q8) для групи Рі), що за умови правильного вибору параметра q забезпечує надійний захист, в тому числі в постквантовій ері. Оптимізовано практичну реалізацію. Використання багатопараметричних груп дозволяє досягати високого рівня безпеки при відносно менших розмірах скінченного поля. Як зазначено в аналізі, для 128-бітного рівня безпеки система на групі автоморфізмів Сузукі вимагає ключів меншого розміру порівняно з класичною MST3, що знижує вимоги до пам'яті та обчислювальних ресурсів. Створено фундамент для постквантової криптографії. Розроблені криптосистеми базуються на задачі WP у групах автоморфізмів, для яких невідомі ефективні квантові алгоритми. Це, в поєднанні з доведеною стійкістю до класичних атак, робить їх надійними кандидатами для подальших досліджень та можливої стандартизації у якості PQC-протоколів.

Запропонований у дослідженні підхід до розробки схем направленого шифрування на групах автоморфізмів функціональних полів максимальних кривих відкриває новий шлях у розвитку криптографії на основі некомутативних груп. Виходом за межі обчислень у центрі групи вдалося не лише значно збільшити пропускну здатність шифрування, але й, після низки удосконалень, побудувати криптосистеми з високим рівнем безпеки, стійкі до відомих атак. Ключовими досягненнями є розробка методів зв'язування ключів та застосування гомоморфного шифрування, що робить запропоновані схеми надійними кандидатами для епохи постквантової криптографії. Найбільш перспективною платформою виявилися групи Рі завдяки їхній чотирипараметричній структурі та значно більшому, у порівнянні з класичними групами, порядку.

Напрямом подальших досліджень може стати аналіз інших родин некомутативних груп, зокрема узагальнених 2-груп Сузукі, які також є багатопараметричними і можуть мати довільно великий порядок, що потенційно відкриває нові можливості для побудови ще більш ефективних та безпечних криптосистем. Інтерес представляють також дослідження інших груп, таких як групи Григорчука, та інші, які можуть відповідати більшим вимогам з огляду на криптографічну стійкість. Цікавим напрямом є розробка нових задач, які не зводяться до CSP або DP і можуть бути стійкішими до відомих атак. Відкритим залишається питання напрямів удосконалення протоколів та розвиток підходів, що максимально використовують складність усієї групи, а не її окремих частин. В дослідженні представлено нові методи, зокрема зв'язування ключів та гомоморфне перетворення, які є важливим кроком у пошуку перспективних напрямів удосконалення. Іноваційним підходом може бути створення гібрід-

них схем за рахунок комбінування властивостей групової криптографії з іншими постквантовими підходами для створення систем, безпека яких базується на складності задач різної природи.

Криптографія на основі некомутативних груп залишається багатою та глибокою галуззю, що пропонує унікальний підхід до побудови безпечних систем в епоху квантових комп'ютерів. Хоча шлях до практичного застосування та стандартизації виявився складнішим, ніж очікувалося, проведене дослідження демонструє невичерпний потенціал групової криптографії з використанням логарифмічних підписів.

Список літератури:

1. Shor P. W. Algorithms for quantum computation: Discrete logarithms and factoring // Proceedings 35th Annual Symposium on Foundations of Computer Science. 1994. P. 124–134 // IEEE Computer Society Press. https://doi.org/10.1109/SFCS.1994.365700
2. Mosca M., & Piani M. Quantum threat timeline report 2024. Global Risk Institute in Financial Services & evolutionQ. https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/
3. National Institute of Standards and Technology. (2016, December). Post-quantum cryptography standardization: Call for proposals / U.S. Department of Commerce. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/call-for-proposals
4. Khalimov G., Kotukh Y., Kolisnyk M., Khalimova S., & Sievierinov O. LINE: Cryptosystem based on linear equations for logarithmic signatures // Cryptology ePrint Archive. 2024. P. 2024/697. https://eprint.iacr.org/2024/697
5. Kotukh Y., Severinov E., Vlasov O., Tenytska A., & Zarudna E. Some results of development of cryptographic transformations schemes using non-abelian groups // Radiotekhnika. 2021. No 204. P. 66–72.
6. Kotukh Y., & Khalimov G. Hard Problems for Non-abelian Group Cryptography // Fifth International Scientific and Technical Conference" Computer and Information systems and technologies". 2021. https://doi.org/10.30837/csitic52021232176.
7. Anshel I., Anshel M., & Goldfeld D. An algebraic method for public-key cryptography // Mathematical Research Letters. 1999. No 6(3-4). P. 287–291.
8. Myasnikov A. G., & Ushakov A. Random subgroups and analysis of the length-based and quotient attacks // Journal of Mathematical Cryptology. 2008. No 2(1). P. 29–61. https://doi.org/10.1515/JMC.2008.003
9. Kotukh Y., & Khalimov G. Towards practical cryptoanalysis of systems based on word problems and logarithmic signatures // Information security: problems and prospects. 2022. P. 55.
10. Hofheinz D., & Steinwandt R. A practical attack on some braid group based cryptographic primitives // Public Key Cryptography – PKC 2003. P. 187–198. Springer. https://doi.org/10.1007/3-540-36288-6_14
11. Kotov M., & Ushakov A. Analysis of a certain polycyclic-group-based cryptosystem // Journal of Mathematical Cryptology. 2015. No 9(3). P. 161–167. https://doi.org/10.1515/jmc-2015-0013
12. Ruinskiy D., Shamir A., & Tsaban B. Cryptanalysis of group-based key agreement protocols using subgroup distance functions // Public Key Cryptography – PKC 2007. P. 61–75. Springer. https://doi.org/10.1007/978-3-540-71677-8_5
13. Monico C. Cryptanalysis of a matrix-based MOR system // Communications in Algebra. 2016. No 44(1). P. 348–363. https://doi.org/10.1080/00927872.2014.974254
14. Khalimov G., & Kotukh Y. (2025). Cryptographic strengthening of MST3 cryptosystem via automorphism group of Suzuki function fields [2504.07318] Cryptographic Strengthening of MST3 cryptosystem via Automorphism Group of Suzuki Function Fields // arXiv preprint arXiv:2504.07318. https://arxiv.org/abs/2504.07318
15. Khalimov G., & Kotukh Y. (2025). MST3 encryption improvement with three-parameter group of Hermitian function field [2504.15391] MST3 Encryption improvement with three-parameter group of Hermitian function field // arXiv preprint arXiv:2504.15391. https://arxiv.org/abs/2504.15391
16. Khalimov G., & Kotukh Y. (2025). Advanced MST3 encryption scheme based on generalized Suzuki 2-groups [2504.11804] Advanced MST3 Encryption scheme based on generalized Suzuki 2-groups // arXiv preprint arXiv:2504.11804. https://arxiv.org/abs/2504.11804
17. Khalimov G., & Kotukh Y. (2025). Improved MST3 encryption scheme based on small Ree groups [2504.10947] Improved MST3 Encryption scheme based on small Ree groups // arXiv preprint arXiv:2504.10947. https://arxiv.org/abs/2504.10947
18. Khalimov G., Kotukh Y., & Khalimova S. Encryption scheme based on the automorphism group of the Ree function field // IEEE 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS). 2020. P. 1–8.
19. Khalimov G., Didmanidze I., Sievierinov O., Kotukh Y., & Shonia O. Encryption scheme based on the automorphism group of the Suzuki function field // IEEE International Conference on problems of infocommunications. Science and technology PIC ST2020. 2020. P. 383–387.
20. Khalimov G., Kotukh Y., & Khalimova S. Improved encryption scheme based on the automorphism group of the Ree function field // IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS). 2021.

21.Khalimov G., Kotukh Y., & Khalimova S. MST3 cryptosystem based on the automorphism group of the Hermitian function field // IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T). 2019. P. 865–868.

22.Khalimov G., Kotukh Y., Didmanidze I., Sievierinov O., Khalimova S., & Vlasov A. Towards three-parameter group encryption scheme for MST3 cryptosystem improvement // IEEE Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4). 2021. P. 204–211.

23.Khalimov G., Kotukh Y., Didmanidze I., & Khalimova S. Encryption scheme based on small Ree groups // Proceedings of the 2021 7th International Conference on Computer Technology Applications (ICCTA '21). 2021. P. 33–37.

24.Hart D., Kim D., Micheli G., Pascual-Perez G., Petit C., & Quek Y. A practical cryptanalysis of WalnutDSA™ // Public-Key Cryptography – PKC 2018. P. 381–406. Springer. https://doi.org/10.1007/978-3-319-76578-5_13

25.Котух Є. В., Охріменко Т. О., Дяченко О. Ф., Ротаньова Н. Ю., Козіна Л. С., Зеленський Д. В. Криптоаналіз систем на основі проблеми слова з використанням логарифмічних підписів // Радіотехніка. 2021. Вип. 206. С. 106–114. Режим доступу: http://nbuv.gov.ua/UJRN/rvmnts_2021_206_11

26.Котух Є. В., Сєвєрінов О. В., Власов А. В., Козіна Л. С., Теницька А. О., Зарудна Е. О. Методи побудови та властивості логарифмічних підписів // Радіотехніка. 2021. Вип. 205. С. 94–99. Режим доступу: http://nbuv.gov.ua/UJRN/rvmnts_2021_205_11

27.Kotukh Y., & Khalimov H. Advantages of logarithmic signatures in the implementation of crypto primitives // Challenges and Issues of Modern Science. 2024. №2. P. 296–299.

28.Kotukh E., Severinov O., Vlasov A., Kozina L., Tenytska A., & Zarudna E. Methods of construction and properties of logariphmic signatures // Radiotekhnika. 2021. No 205. P. 94–99.

29.Котух Є., Халімов Г. Оцінки секретності та витрат на реалізацію криптосистеми на основі лінійних рівнянь з використанням логарифмічних підписів // Theoretical and applied cybersecurity. 2024. P. 149.

30.Deligne P., & Lusztig G. Representations of reductive groups over finite fields // Annals of Mathematics. 1976. No 103(1). P. 103–161. https://doi.org/10.2307/1971021

Надійшла до редколегії 26.04.2025

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

Джура Ілля Євгенович – студент 4-го курсу, Національний Авіаційний Університет; Київ, Україна; e-mail: illya773823@gmail.com; ORCID: https://orcid.org/0009-0002-5470-4479