УДК 621.391:519.2 **DOI:10.30837/rt.2025.1.220.08**

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

АНАЛІЗ ОБМЕЖЕНЬ КВАНТОВИХ ОБЧИСЛЕНЬ У ЗАДАЧАХ КРИПТОАНАЛІЗУ

Вступ

Ера NISQ (Noisy Intermediate-Scale Quantum) визначає поточний стан розвитку квантових обчислень та характеризується квантовими процесорами, які містять від десятків до тисяч кубітів, але не мають механизмів повноцінної корекції помилок, що зумовлює недосяжність стабільної квантової переваги над класичними комп'ютерами. Розвиток технологій квантових обчислень в умовах обмежених ресурсів у період з 2020 по 2025 р. демонструє поступовий перехід від теоретичних досліджень до прикладного застосування, а також підготовку до впровадження повноцінних обчислень із виправленням помилок. Починаючи з 2020–2021 рр. основна увага була зосереджена на фундаментальних дослідженнях і розробці базових алгоритмів, що працюють у шумному квантовому середовищі. Протягом цього етапу відзначалося стабільне зростання кількості наукових публікацій у галузі квантових обчислень, що зумовлено загальним технологічним проривом у галузі після 2015 р. та його суттєвим прискоренням з 2020 р. Дослідницькі ініціативи зосереджувалися на пошуку шляхів ефективного використання обмежених квантових ресурсів, зокрема через адаптацію алгоритмів до шуму, що притаманний апаратному забезпеченню проміжного рівня. У період 2021–2022 рр. відбувся перехід до практичної демонстрації можливостей квантових алгоритмів на фізичних пристроях. Значущим кроком стало виконання алгоритму квантової приблизної оптимізації (QAOA) на квантовому комп’ютері Google Sycamore із 53 кубітами [1]. Цей експеримент продемонстрував здатність NISQ-систем виконувати обчислювальні задачі з реальним практичним значенням навіть за умов суттєвого рівня шуму та обмеженого контролю над квантовими станами. Це також стало свідченням того, що квантова перевага можлива до досягнення повної толерантності до помилок. Наступний етап в 2023–2024 рр. демонстрував рішення щодо зниження рівня шуму та масштабування архітектури. Було досягнуто важливих результатів у підвищенні точності квантових операцій, зокрема двокубітних гейтів, що перевищили 99,9 % точності. Водночас активно розроблялися нові варіанти алгоритмів, оптимізованих для наявного квантового заліза, які краще враховують фізичні обмеження кубітів, їх зв’язність та топологію. Значну увагу було приділено розробці методів гібридних обчислень, що поєднують класичні та квантові ресурси, а також методам мітігації шуму без використання повноцінної корекції помилок. У 2024–2025 рр. спостерігається стратегічний зсув у напрямку початкової реалізації квантових комп’ютерів із виправленням помилок (FTQC). Це позначає завершення етапу суто шумних обчислень і поступовий перехід до більш стабільних архітектур, здатних підтримувати тривале квантове когерентне обчислення. Провідні компанії у сфері квантових технологій все частіше спрямовують свої зусилля на розробку систем квантової корекції помилок (QEC), що підтверджується зростаючою кількістю інвестицій у відповідні дослідження. За деякими оцінками, близько двох третин індустріальних гравців активно працюють у цьому напрямку або вже інтегрують QEC у свої розробки, що свідчить про нову фазу у розвитку квантових технологій. Таким чином, період 2020–2025 рр. можна охарактеризувати як критично важливий перехідний етап у формуванні основ майбутніх квантових обчислень з повною корекцією помилок та масштабованими архітектурами.

Мета статті – проведення аналізу щодо обмежень поточних квантових архитектур та підходів до організації квантових обсчилень в задачах квантового криптоаналізу.

Етапи розвитку квантових обчислень

NISQ-ера є перехідною фазою розвитку квантових обчислень, що характеризується наявністю пристроїв із обмеженою кількістю кубітів та високим рівнем шуму, що унеможливлює повноцінну реалізацію алгоритмів із квантовою корекцією помилок. У відповідь на ці обмеження в рамках NISQ-парадигми було розроблено низку спеціалізованих алгоритмів та обчислювальних стратегій, здатних працювати в умовах нестабільного квантового середовища. Одним із найбільш поширених підходів є варіаційний квантовий алгоритм знаходження власних значень (VQE), який базується на гібридному квантово-класичному циклі оптимізації. Цей алгоритм знайшов широке застосування у квантовій хімії для моделювання молекулярних структур та визначення енергетичних рівнів, що становить значний інтерес як для наукових, так і для промислових задач.

Іншим перспективним алгоритмом, розробленим спеціально для пристроїв NISQ-типу, є QAOA, призначений для вирішення складних комбінаторних оптимізаційних задач, зокрема задач на графах, маршрутизації та розміщення ресурсів. QAOA вирізняється здатністю досягати хороших апроксимаційних результатів навіть за обмеженої кількості квантових операцій, що робить його одним із провідних кандидатів на демонстрацію так званої квантової переваги в реальних умовах. Оскільки пристрої NISQ характеризуються високим рівнем помилок, важливим напрямом досліджень стали методи зниження впливу шуму на обчислення. Серед найбільш ефективних стратегій можна виділити рандомізовану компіляцію (RC), яка перетворює квантові схеми у форму, більш стійку до шуму, та екстраполяцію до нульового шуму (ZNE), що дозволяє оцінити результат імовірного обчислення за ідеального (безшумного) середовища. Синергічне застосування цих методів, зокрема в контексті алгоритмів на кшталт VQE, дало змогу значно підвищити точність результатів без потреби в повноцінній реалізації системи квантової корекції помилок [2].

У межах NISQ-епохи також активно розвивалися гібридні квантово-класичні підходи. Ці архітектури поєднують квантову частину, яка відповідає за генерацію та маніпуляцію квантовими станами з класичними методами оптимізації та обробки результатів. Серед них вирізняються варіаційні методи, техніки схемного "плетіння" (Circuit Knitting), розділення великих задач на менші підзадачі, а також використання класичної постобробки для зменьшення помилок. Такі інтегровані підходи дозволяють розширити можливості квантових обчислень в умовах апаратних обмежень та слугують основою для подальшого переходу до квантової толерантності до помилок.

Потенційні сфери застосування технологій NISQ є надзвичайно широкими, охоплюють як фундаментальні наукові дослідження, так і прикладні галузі з високим економічним потенціалом. У сфері оптимізації квантові обчислення вже застосовуються до логістичних задач, фінансового моделювання та оптимізації ланцюгів постачання. Алгоритми на кшталт QAOA дозволяють шукати оптимальні або близькі до оптимальних рішення для складних задач, таких як маршрутні задачі, розміщення виробничих потужностей або вибір інвестиційних стратегій, що раніше вимагали значних обчислювальних ресурсів. Квантова перевага в таких випадках може виявлятися у пришвидшеному знаходженні глобальних екстремумів у багатовимірних і складних просторах рішень.

Стратегічною галуззю, де активно розвиваються квантові підходи, є криптографія. Хоча NISQ-пристрої наразі не здатні зламати стійкі класичні криптографічні схеми, вони стимулюють розвиток квантово-стійких (post-quantum) алгоритмів шифрування, які залишатимуться захищеними навіть у випадку появи потужних квантових комп’ютерів [3–6]. Окрім цього, активно досліджується вплив квантових обчислень на надійність сучасних протоколів, що зумовлює перегляд криптографічних стандартів на міжнаціональному рівні.

Попри стрімкий прогрес у сфері квантових обчислень, ера NISQ супроводжується низкою фундаментальних викликів, які досі обмежують практичне застосування цих технологій. Однією з ключових проблем є обмежена масштабованість існуючих систем. Хоча значні інвестиції з боку університетів, урядових структур та індустрії дозволили досягти поточного

рівня розвитку, квантові комп'ютери NISQ-класу ще не демонструють переваг над класичними системами у вирішенні реальних задач. Водночас оптимістичні оцінки припускають, що перехід до пост-NISQ технологій відбудеться вже найближчими роками.

Одним із головних технічних бар'єрів залишається проблема шуму та помилок у квантових системах. Через надзвичайну чутливість кубітів до навколишніх впливів результати обчислень можуть бути суттєво спотворені. Гібридні підходи, що поєднують класичну обробку даних з квантовими обчисленнями, дозволяють досягати значного зменшення похибок, що підтверджується числовими експериментами.

Паралельно з цим триває активний пошук нових квантових архітектур, які можуть забезпечити подолання поточних обмежень. У 2024 р. було оголошено про створення першого у світі топологічного кубіта, важливого кроку на шляху до реалізації відмовостійких квантових комп'ютерів. Крім того, інновації у вигляді «скляних» чіпів, що забезпечують більш стабільне середовище для роботи кубітів, вказують на прагнення до "чистої" і стійкої квантової інфраструктури. Важливо, що у квантовій галузі спостерігається технологічне розмаїття: від надпровідникових схем і пасток для іонів до фотонних і топологічних систем. Саме така різноманітність дозволяє компаніям створювати рішення, придатні до використання в умовах існування ринку квантових обчислень – фази, коли квантові комп'ютери виконуватимуть реальні прикладні задачі з економічною ефективністю.

Однією з найважливіших тенденцій у сучасному розвитку квантових обчислень є поступовий перехід до ери квантових комп'ютерів із повноцінною толерантністю до помилок (FTQC). Очікується, що в період з 2025 по 2029 рр. з'являться перші FTQC-машини, здатні працювати в обчислювальних режимах масштабу MegaQuops або навіть GigaQuops, використовуючи декілька сотень логічних кубітів. У рамках NISQ-парадигми основна увага приділяється методам зниження та пом'якшення шумів, включаючи рандомізовану компіляцію, екстраполяцію до нульового шуму та різні стратегії класичної постобробки результатів. У свою чергу, FTQC базується на реалізації повноцінної квантової корекції помилок (Quantum Error Correction, QEC), що дозволяє масштабувати обчислення без втрати точності за умови дотримання суворих вимог до точності фізичних операцій і надлишковості кубітів для побудови логічних одиниць.

Із технічної точки зору, сучасні NISQ-пристрої зазвичай оперують кількома сотнями до кількох тисяч фізичних кубітів із типовою двокубітною точністю в діапазоні 99–99,9 %. Ці параметри дозволяють виконувати демонстраційні обчислення та тестувати нові алгоритми, але не забезпечують масштабованості для обробки складних задач. Натомість, ранні FTQC-системи, навіть із порівняно невеликою кількістю (~100) логічних кубітів, демонструватимуть значно вищу надійність – із точністю понад 99,9999 % завдяки використанню кодів квантової корекції, таких як поверхневі коди (surface codes) або LDPC-коди (Low-Density Parity-Check).

Важливо зазначити, що найближчим часом кінцеві користувачі опиняться перед вибором між двома платформами: з одного боку NISQ-пристрої з великою кількістю (до 10000) фізичних кубітів і вдосконаленими методами пом'якшення шуму, а з іншого – FTQC-пристрої з меншою, але більш надійною кількістю логічних кубітів. Цей вибір буде залежати від характеру задачі. Деякі наукові проблеми (особливо пов'язані з хімічним моделюванням або квантовою симуляцією) можуть залишатися ефективно вирішуваними на NISQ-архітектурах, тоді як інші, зокрема криптографічні обчислення, великомасштабна оптимізація або точне моделювання квантових систем, потребуватимуть надійності та масштабованості FTQC.

Отже, перехід до FTQC не означає негайного відкидання NISQ-моделі, а радше знаменує початок співіснування двох типів квантових платформ, кожна з яких займатиме своє місце в інноваційній екосистемі квантових технологій.

Таким чином, квантові обчислення перетворилися з суто академічної дисципліни на сферу з чіткою комерційною стратегією. Сьогодні почали з'являтися перші практичні реалізації квантових алгоритмів, системи стали доступними у хмарі, а промислові гіганти розгор-

нули дорожні карти до FTQC. Цей етап ознаменував кінець епохи "невідомого" у квантових обчисленнях та початок періоду активного інженерного вдосконалення та комерціалізації. Таким чином, попри обмеження, властиві періоду NISQ, наявні досягнення вже відкривають реальні можливості для прикладного використання квантових обчислень у різних галузях, що підкреслює важливість продовження досліджень у сфері квантових алгоритмів, методів зниження шуму та гібридних архітектур, що у сукупності формують базис майбутньої ери повноцінних квантових обчислень.

Постквантова криптографія в еволюційонму процесі квантових обчислень

Із зростанням обчислювальної потужності квантових комп'ютерів під загрозою опиняються традиційні криптографічні протоколи (зокрема, RSA, ECC), вразливі до алгоритму Шора. У відповідь на це зростає інтерес до квантово-безпечної (post-quantum) криптографії, яка включає розробку алгоритмів, стійких до атак квантових комп’ютерів. Паралельно з цим розвиваються квантові протоколи захисту інформації, зокрема квантового розподілу ключів (QKD), що базується на принципах квантової механіки й гарантує виявлення будь-якої спроби прослуховування. На відміну від класичних криптоаналітичних підходів, квантові алгоритми, зокрема алгоритм Шора, здатні ефективно зламувати криптографію з відкритим ключем, засновану на таких математичних задачах, як факторизація цілих чисел, обчислення дискретного логарифма та дискретного логарифма на еліптичній кривій [7]. Хоча сучасні квантові пристрої ще не є криптографічно релевантними (CRQC), прогрес у галузі передбачає необхідність завчасної підготовки. У період NISQ-ери ці системи ще не здатні виконувати обчислення з довгими ланцюгами квантових гейтів, необхідні для реалізації квантових криптоаналітичних атак на практиці. Наприклад, розв’язання задачі факторизації 2048-бітного RSA-ключа вимагатиме тисячі коректованих від помилок кубітів та мільйони логічних гейтів, що виходить далеко за межі сучасних NISQ-систем [8].

Квантові обчислення мають значно сильніший вплив на алгоритми з відкритим ключем, ніж на симетричні криптографічні схеми. Асиметричні алгоритми, такі як RSA, DSA та алгоритми на еліптичних кривих, базуються на складності математичних задач факторизації, дискретного логарифмування та логарифмування на еліптичних кривих. Відповідно, ці методи є уразливими до атак криптографічно релевантних квантових комп’ютерів (CRQC), які передбачають наявність тисяч коректованих від помилок кубітів. Алгоритм Гровера є ще одним прикладом квантової загрози. Він забезпечує квадратичне прискорення для пошуку в невпорядкованих структурах, знижуючи складність з $O\ N\ O\ N\ O\ N$ до $O\ N\ O\ \sqrt{N}\ O\ N$. Хоча така перевага не настільки драматична, як у Шора, вона може мати серйозні наслідки для симетричних криптосистем.

Оскільки атаки квантових алгоритмів уже змодельовано й підтверджено теоретично, світова спільнота вживає заходів щодо заміни вразливих схем. Зокрема, NIST (Національний інститут стандартів і технологій США) завершив відбір стандартів постквантової криптографії. 3 серпня 2024 р. NIST опублікував перші три фіналізовані стандарти, які мають захистити цифрові дані від потенційних атак квантових комп’ютерів: FIPS 203 (ML-KEM), алгоритм для направленого шифрування, заснований на CRYSTALS-Kyber, FIPS 204 (ML-DSA), алгоритм цифрового підпису, заснований на CRYSTALS-Dilithium та FIPS 205 (SLH-DSA), алгоритм цифрового підпису, заснований на SPHINCS+, який використовує хеш-функції для забезпечення безпеки.

Багато квантових алгоритмів для HSP спираються на принципи визначення періоду. Для абелевих груп складність залишається поліноміальною, але для неабелевих груп складність значно зростає (часто стає експоненціальною), оскільки квантове перетворення Фур’є стає важчим для інтерпретації. Хоча алгоритми Шора та Саймона пропонують ефективний пошук періоду для певних типів періодичностей (модульних та XOR відповідно), їхня складність залишається поліноміальною. Однак для неабелевих груп або інших складних структур квантові алгоритми можуть не мати такої переваги [9, 10].

У сучасних умовах розвитку квантових обчислень особливу увагу криптоаналітиків привертає реалізація фундаментальних квантових алгоритмів на NISQ-пристроях. Значну долю дослідженнь становить вивчення впливу цих обчислень на криптографічні методи та перспективи використання симетрії PT (парність-час) для подолання апаратних обмежень. Спочатку вивчена в контексті негерметичних гамільтоніанів, PT-симетрія була обґрунтована в роботах Карла Бендера і Стефана Беттчера наприкінці 1990-х років. Автори продемонстрували, що, незважаючи на неермітову природу, гамільтоніани з непорушеною PT-симетрією можуть мати дійсні власні значення, а за відповідного визначення внутрішнього добутку – унітарну еволюцію, яка є необхідною умовою для фізичної реалізації квантових систем. Останні експерименти на надпровідних квантових процесорах показали можливість моделювання еволюції квантової системи під дією PT-симетричних негерметичних гамільтоніанів із застосуванням допоміжних кубітів. Такі дослідження відкривають нові перспективи для реалізації складних квантових симуляцій у відкритих системах, зокрема періодично керованих квантових фаз, включно з реалізацією дискретних часових кристалів. Таким чином, PT-симетрія розглядається як інноваційний підхід до подолання обмежень сучасних NISQ-пристроїв і розширення арсеналу ефективних методів квантової симуляції.

Узагальнюючи, можна стверджувати, що сучасні дослідження в галузі квантових обчислень, зокрема в рамках NISQ-парадигми, демонструють значний поступ у реалізації теоретичних моделей, водночас висвітлюючи існуючі технічні та фізичні обмеження. Криптографічні виклики, що постають унаслідок розвитку квантових алгоритмів, актуалізують необхідність розгортання постквантових криптографічних протоколів. У свою чергу, розробка нових підходів, таких як впровадження PT-симетрії, відкриває нові горизонти у підвищенні ефективності квантових обчислень і розширенні їх застосувань у фундаментальній фізиці та прикладних інформаційних технологіях.

Аналіз критерієв квантових обчислень в контексті квантового криптоаналізу

Розглянемо ключові математичні моделі, що формалізують процес розвитку NISQ, EFTQC та FTQC обчислювальних систем. Одним з ключових математичних описів переходу між різними епохами квантових обчислень є модель масштабованості, представлена у статті [11]. Перехідний період між епохами NISQ та FTQC характеризується законом зменшення віддачі у квантовій корекції помилок (QEC), де здатність архітектури підтримувати якісні операції при масштабуванні визначає точку зменшення віддачі. Модель масштабованості опишемо наступним чином:

$$f\ \ Z\ = P_{база} \cdot \left(\frac{n_{фіз.куб.}}{n_0} \right)^{1/\alpha}$$

де $P_{база}$ – базовий рівень помилки для одного кубіта, $n_{фіз.куб.}$ – кількість фізичних кубітів, n_0 – нормалізаційний параметр, α – параметр масштабованості (scalability). Параметр масштабованості α є ключовим для класифікації: NISQ: $\alpha < 2$, EFTQC: $2 \le \alpha \le 3.5$, FTQC: $\alpha > 3.5$ (див. табл. 1). Проаналізуємо результати класифікації наступним чином.

При значеннях параметра масштабованості менших за 2, спостерігається стрімке зростання загального рівня помилок із збільшенням кількості кубітів у системі. Даний режим характерний для сучасного етапу розвитку квантових обчислень з використанням NISQ-пристроїв. Основними чинниками, що зумовлюють низьке значення α, є недостатня ізоляція кубітів від навколишнього середовища, наявність перехресних перешкод між сусідніми кубітами (crosstalk), обмежена точність контролюючих сигналів та високий рівень декогеренції. При таких значеннях параметра масштабованості застосування квантової корекції помилок є неефективним, оскільки процедури виявлення та виправлення помилок вносять більшу кількість нових помилок, ніж здатні виправити.

Таблиця 1

Еволюція квантових обчислень

Критерій	NISQ (Noisy Intermediate-Scale Quantum)	EFTQC (Early Fault-Tolerant Quantum Computing)	FTQC (Fault-Tolerant Quantum Computing)
Часові рамки практичних реалізацій	2018 – 2025	2025 – 2030	2030+
Класи складності	Слабший за BQP, сильніший за BPP	Між NISQ і BQP	BQP
Теорема про поріг помилки	Не застосовується (помилки вищі за поріг)	Частково застосовується (близько до порогу)	Повністю застосовується (нижче порогу)
Математична характеристика фізичної помилки	$P_{error} > P_{th}$	$P_{error} \approx P_{th}$	$P_{error} = P_{th}$
Модель масштабованості (scalability)	$\alpha < 2$	$2 \le \alpha \le 3.5$	$\alpha > 3.5$
Принцип корекції помилок	Пом'якшення помилок	Обмежена корекція помилок	Повна корекція помилок

Діапазон значень параметра масштабованості від 2 до 3.5 відповідає перехідному режиму ранніх відмовостійких квантових обчислень (EFTQC). У цьому режимі зростання рівня помилок при збільшенні кількості кубітів є помірним, що дозволяє імплементувати обмежені схеми корекції помилок з позитивним ефектом. Цей режим вимагає суттєвого покращення якості фізичних кубітів та систем контролю, включаючи: підвищену ізоляцію від оточення, зменшення перехресних перешкод, більш точне управління квантовими гейтами та ефективні методи пом'якшення помилок. Оскільки зростання помилок є достатньо повільним, стає можливим застосування часткової квантової корекції помилок, що дозволяє реалізувати обмежені відмовостійкі квантові схеми. Нижня межа α = 2 для цього режиму відповідає мінімальному значенню, при якому квантова корекція помилок починає давати позитивний ефект і є теоретично обґрунтованою точкою, в якій кількість виправлених помилок починає перевищувати кількість нових помилок, внесених схемами корекції.

Значення параметра масштабованості, що перевищують 3.5, характеризують режим повноцінних відмовостійких квантових обчислень (Fault-Tolerant Quantum Computing). У цьому режимі рівень помилок зростає настільки повільно з розширенням системи, що стає можливим ефективне застосування повномасштабних схем квантової корекції помилок. Досягнення таких значень параметра α вимагає надзвичайно високої якості фізичних кубітів з мінімальним рівнем декогеренції, практично відсутніми перехресними перешкодами та прецизійним квантовим контролем. При α > 3.5 рівень помилок зростає достатньо повільно, щоб забезпечити масштабування до систем з тисячами або навіть мільйонами логічних кубітів, що необхідно для вирішення практично значущих задач. Верхня межа α = 3.5 для EFTQC (яка є одночасно нижньою межею для FTQC) визначає значення, при якому ефективність корекції помилок стає достатньою для реалізації великомасштабних відмовостійких квантових обчислень з довільною кількістю логічних кубітів.

Проаналізуємо критерії співвідношення між фізичними та логічними кубітами в реалізації задач криптографічних квантових обчислень (див. табл. 2).

Таблиця 2

Оцінки характеристик кубітів для систем NISQ, EFTQC та FTQC

Характеристика	NISQ	EFTQC	FTQC
Кількість фізичних кубітів	50-1,000	10^3-10^6	$>10^6$
Кількість логічних кубітів	0	10-100	100-10,000+
Формула для кількості фізичних кубітів на логічний кубіт	не існує	$O\ d^2$	$>O\ d^2$
Рівень фізичної помилки	10^{-2}-10^{-3}	10^{-3}-10^{-4}	$<10^{-4}$
Рівень логічної помилки	N/A	: $p_{phys}^{d/2}$	: $p_{phys}^{d/2}$

NISQ-пристрої оперують з обмеженою кількістю фізичних кубітів (50-1,000) без реалізації логічних кубітів, що унеможливлює застосування квантової корекції помилок. Вони характеризуються високими рівнями фізичних помилок (10^{-2} – 10^{-3}), що суттєво обмежує глибину реалізованих квантових схем. Такі системи, як IBM Eagle (127 кубітів) та Atom Computing Phoenix (понад 100 кубітів), є типовими реалізаціями. Перехід до EFTQC-ери передбачає драматичне збільшення кількості фізичних кубітів (10^3 – 10^6) та реалізацію обмеженої кількості логічних кубітів (10 – 100). Це дозволяє імплементувати часткову корекцію помилок та виконувати квантові алгоритми середньої складності. У таких системах кількість фізичних кубітів на один логічний кубіт масштабується як $O\ d^2$, де d – відстань коду, а рівень фізичних помилок знижується до 10^{-3} – 10^{-4} . FTQC-системи характеризуються використанням понад мільйона фізичних кубітів для забезпечення сотень і тисяч логічних кубітів (100 – 10,000+) з повноцінною корекцією помилок. Рівень фізичних помилок у таких системах нижчий за 10^{-4} , що в поєднанні з більшою відстанню коду забезпечує достатньо низький рівень логічних помилок. Для поверхневого коду та аналогічних кодів рівень логічної помилки масштабується приблизно як: $p_{phys}^{d/2}$, де p_{phys} – рівень фізичної помилки. Дані співвідношення ґрунтуються на теоремі про поріг для квантової корекції помилок, яка стверджує, що для фізичних рівнів помилок нижче порогового значення логічний рівень помилки може бути знижений до довільно малого значення шляхом збільшення відстані коду. Ця теоретична база визначає фундаментальні вимоги до масштабування квантових систем та відкриває шлях до практичної реалізації потужних квантових алгоритмів у майбутньому.

Проаналізуємо квантові обчислювальні підходи (див. табл. 3).

Таблиця 3

Порівняння квантових обчислювальних підходів

Підхід	Обчислювальна парадигма	Математична складність схеми	Логічні кубіти	Глибина схеми
VQE та QAOA (NISQ)	Гібридна	$O\ p$ з глибиною p	Фізичні кубіти	Обмежена
RFE (EFTQC)	Робастні квантові алгоритми	$O\ K$ з параметром K	Обмежена кількість	Середня
QPE (FTQC)	Повна квантова корекція помилок	$O\ 1/\varepsilon$ для точності ε	Необмежена	Висока

Табл. 3 демонструє прогресію від більш обмеженого, але практично доступного NISQ-підходу (Noisy Intermediate-Scale Quantum) до теоретично потужнішого, але технологічно вимогливішого FTQC (Fault-Tolerant Quantum Computing). Підходи VQE (Variational Quantum Eigensolver) та QAOA (Quantum Approximate Optimization Algorithm) працюють в гібридній парадигмі, поєднуючи класичні та квантові обчислення, використовуючи доступні сьогодні фізичні кубіти з обмеженою глибиною схеми. Підхід RFE (Randomized Fourier Estimation) у контексті EFTQC (Error-Free Topological Quantum Computing) знаходиться посередині, пропонуючи кращу стійкість до помилок при середній глибині схеми. Підхід QPE (Quantum Phase Estimation) представляє повну квантову корекцію помилок, що теоретично дозволяє необмежену кількість логічних кубітів і високу глибину схеми, але має складність, що залежить від бажаної точності ε.

Проаналізуємо показникі якості квантових операцій (див. табл. 4).

Таблиця 4

Порівняння показників якості квантових операцій

Метрика	NISQ	EFTQC	FTQC
Точність двокубітного гейта	99 – 99.9 %	99.9 – 99.999 %	>99.9999 %
Кількісна формула для Quops	KiloQuops $\approx 10^3$	MegaQuops $\approx 10^6$ -GigaQuops $\approx 10^9$	TeraQuops $\approx 10^{12}$
Час когерентності відносно часу операції	$T_2 / T_{gate} \approx 10^2 - 10^3$	$T_2 / T_{gate} \approx 10^3 - 10^5$	$T_2 / T_{gate} > 10^5$

Аналіз показників якості квантових операцій демонструє радикальне зростання продуктивності та надійності квантових систем у процесі переходу від ери шумних проміжних квантових пристроїв (NISQ) до ери повноцінних відмовостійких квантових обчислень (FTQC). Ключовими метриками, що характеризують цю еволюцію, є точність двокубітних гейтів, обчислювальна потужність (Quops) та співвідношення між часом когерентності та часом виконання операції. Точність двокубітних гейтів, що є фундаментальним показником якості квантових операцій, зростає від 99 – 99.9 % у NISQ-пристроях до понад 99.9999 % у FTQC-системах. Це експоненційне підвищення точності є критичним фактором для реалізації складних квантових алгоритмів, оскільки навіть незначне покращення у точності гейтів призводить до суттєвого зменшення накопичених помилок під час виконання глибоких квантових схем. Обчислювальна потужність квантових систем, виражена в кількості квантових операцій за секунду (Quops), демонструє зростання на дев'ять порядків від KiloQuops (10^3) у NISQ-ері до TeraQuops (10^{12}) у FTQC-системах. Цей прогрес відображає не лише збільшення кількості кубітів, але й підвищення частоти операцій та впровадження паралельного виконання квантових гейтів, що в сукупності забезпечує безпрецедентне зростання обчислювальної потужності. Співвідношення між часом когерентності та часом виконання операції (T_2 / T_{gate}) зростає від 10^2 – 10^3 у NISQ-системах до понад 10^5 у FTQC-пристроях. Це відображає принципове покращення як технологій збереження квантової когерентності, так і методів швидкого та точного виконання квантових гейтів. Збільшення цього співвідношення означає, що квантові системи зможуть виконувати суттєво більше послідовних операцій до того, як декогеренція зруйнує квантовий стан, що є критичним для реалізації складних квантових алгоритмів з глибокими схемами.

Ці метрики колективно демонструють траєкторію розвитку квантових обчислень від експериментальних систем з обмеженими можливостями до повноцінних квантових комп'ютерів, здатних реалізувати практичні квантові алгоритми з обчислювальною потужністю, що значно перевищує можливості класичних систем. Проаналізуємо EFTQC та FTQC підходи як перспективні з огляду на рішення криптоаналітичних задач (див. табл. 5).

Таблиця 5

Порівняльний аналіз EFTQC та FTQC у вирішенні задач криптоаналізу

Характеристика	Традиційний FTQC підхід	EFTQC підхід	Математичне співвідношення
Кількість операцій на схему	Висока	Знижена в ≈ 100 разів	$O\ T_{FTQC} / 100$
Кількість запусків схеми	Низька	Збільшена в ≈ 10000 разів	$O\ R_{FTQC} \cdot 10^4$
Загальний час виконання	$T_{total} = T_{FTQC} \cdot R_{FTQC}$	$T_{total} = T_{EFTQC} \cdot R_{EFTQC}$	Збільшення в ≈ 100 разів
Розмір задачі (досяжність)	Обмежений кількістю кубітів	Розширений на $\approx 40 - 50\%$	Від ≈ 90 до ≈ 130 логічних кубітів

Порівняльний аналіз підходів EFTQC та FTQC має особливе значення в контексті криптоаналітичних задач, де квантові алгоритми потенційно демонструють експоненційне прискорення порівняно з класичними методами. Принципові відмінності цих підходів визначають різні траєкторії розвитку криптоаналітичних можливостей у квантову еру.

EFTQC підхід із характерним зниженням кількості операцій на схему $O\ T_{FTQC} / 100$ відкриває можливість для раннього впровадження модифікованих версій алгоритму Шора та алгоритму Гровера з обмеженою глибиною. Критичною особливістю такого підходу для криптоаналізу є компенсація обмеженої глибини схем через інтенсивне статистичне накопичення результатів $O\ R_{FTQC} \cdot 10^4$ запусків. Це дозволяє атакувати криптографічні системи з редукованою складністю, вибірково таргетуючи вразливі компоненти або використовуючи часткове знання про структуру криптографічного ключа.

Збільшення розміру задач на 40 – 50 % (від ~90 до ~130 логічних кубітів) у EFTQC підході є особливо значущим для криптоаналізу, оскільки уможливлює атаки на криптоси-

стеми з більшою довжиною ключа. Це дозволяє, наприклад, застосовувати квантові методи для факторизації RSA-модулів більшого розміру або для обчислення дискретних логарифмів у більших елліптичних кривих, навіть при обмеженій глибині схем. Такий підхід потенційно надає можливість проводити "доказові концепції" атак на криптосистеми, які вважаються безпечними в сучасних умовах.

Фундаментальна зміна парадигми в EFTQC ері для криптоаналізу полягає в переході від повномасштабних атак, які вимагають глибоких квантових схем високої точності, до гібридних класично-квантових атак з інтенсивним статистичним післяопрацюванням. Такі атаки можуть включати квантові підпрограми для вирішення специфічних, обчислювально складних підзадач, інтегровані в класичні криптоаналітичні frameworks. Збільшений загальний час виконання (приблизно в 100 разів) залишається прийнятним для криптоаналітичних застосувань, де час атаки не є критичним фактором порівняно з можливістю принципового зламу криптосистеми.

Пріоритезація кількості запусків схеми над її глибиною є особливо релевантною для таких криптоаналітичних алгоритмів, як квантовий варіант meet-in-the-middle атак та квантові версії диференціального та лінійного криптоаналізу, де статистичне накопичення результатів є невід'ємною частиною атаки. Цей підхід дозволяє розширити спектр криптоаналітичних методів, доступних на ранніх етапах квантових обчислень, стимулюючи розвиток постквантової криптографії та прискорюючи транзицію до криптографічних систем, стійких до квантових атак.

Висновок

Проведений аналіз математичних критеріїв різних епох розвитку квантових обчислень має наслідки для вирішення криптоаналітичних задач, трансформуючи розуміння часових рамок та методологічних підходів до подолання криптографічного захисту класичних криптосистем.

Еволюція параметра масштабованості α від $\alpha < 2$ у NISQ до $\alpha > 3.5$ у FTQC системах визначає фундаментальні обмеження для імплементації алгоритму Шора та інших криптоаналітичних алгоритмів, що вимагають низького рівня помилок. Перехід від рівня характеристики фізичної помилки $P_{error} > P_{th}$, характерної для NISQ, до рівня $P_{error} = P_{th}$ у FTQC є критичною точкою біфуркації для практичної реалізації повномасштабних квантових атак на асиметричні криптосистеми в недалекому майбутньому. Співвідношення між фізичними та логічними кубітами, що описується функцією $O\ d^2$, має вирішальне значення для криптоаналізу, оскільки визначає максимальний розмір криптографічних ключів, які можуть бути атаковані. Збільшення кількості доступних логічних кубітів від 10 – 100 у EFTQC до 100 – 10,000+ у FTQC в недалекому майбутньому відкриває можливість для атак на криптосистеми з ключами від 2048 до 4096 біт та більше, що охоплює значну частину сучасної криптографічної інфраструктури. Показники якості квантових операцій демонструють експоненційне покращення від NISQ до FTQC, що безпосередньо корелює з ефективністю криптоаналітичних алгоритмів. Зростання точності двокубітних гейтів від 99 –99.9 % до >99.9999 % критично важливе для реалізації квантового перебору в алгоритмі Гровера та для точного оцінювання фази в алгоритмі Шора. Збільшення обчислювальної потужності від KiloQuops до TeraQuops та співвідношення T_2 / T_{gate} від 10^2 – 10^3 до $>10^5$ визначає швидкість виконання криптоаналітичних операцій та максимальну глибину квантових схем, достатніх для факторизації чи обчислення дискретних логарифмів. EFTQC-підхід пропонує революційний компроміс для квантового криптоаналізу: зниження кількості операцій на схему в ~100 разів при збільшенні кількості запусків у ~10,000 разів уможливлює реалізацію модифікованих версій алгоритму Шора та Гровера, оптимізованих для роботи з обмеженою глибиною схеми. Це дозволяє атакувати криптосистеми більшого розміру (на 40 – 50 % більше логічних кубітів) значно раніше, ніж передбачалося в традиційних моделях квантового криптоаналізу, хоча й з пропорційно більшими часовими

витратами. Еволюція від VQE та QAOA алгоритмів через робастні EFTQC-алгоритми до повноцінних FTQC-алгоритмів трансформує методологію квантового криптоаналізу. В NISQ-ері можливі лише гібридні атаки з обмеженою квантовою складовою; EFTQC-ера відкриває шлях до робастних квантових атак зі складністю O(K), які, хоча й не є оптимальними, але вже становлять реальну загрозу для окремих криптосистем; і, нарешті, FTQC-ера уможливлює повномасштабні квантові атаки зі складністю $O\ 1/\varepsilon$, що повністю компрометують уразливі криптографічні примітиви.

Запропонована модель переходу від NISQ до FTQC із чіткими математичними критеріями дозволяє більш точно прогнозувати часові рамки виникнення квантової загрози для різних криптографічних систем. Особливо важливим є висновок щодо прискореної досяжності квантових атак в EFTQC-ері, що скорочує очікуваний час до компрометації сучасних асиметричних криптосистем. Ці результати підкреслюють нагальну необхідність активної міграції до постквантових криптографічних рішень, спроможних протистояти як повноцінним FTQC-атакам, так і модифікованим EFTQC-атакам, які можуть стати реальністю значно раніше, ніж передбачалося у традиційних моделях квантової загрози.

Список літератури

1. Arute F., Arya K., Babbush R., Bacon D., Bardin J. C., Barends R., Biswas R., Boixo S., Brandao F. G. S. L., Buell D. A., Burkett B., Chen Y., Chen Z., Chiaro B., Collins R., Courtney W., Dunsworth A., Farhi E., Foxen B., ... Martinis J. M. Quantum supremacy using a programmable superconducting processor // Nature. 2019. Vol. 574(7779). P. 505–510. https://doi.org/10.1038/s41586-019-1666-5
2. Kandala A., Mezzacapo A., Temme K., Takita M., Brink M., Chow J. M., Gambetta J. M. Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets // Nature. 2017. Vol. 549(7671). P. 242–246. https://doi.org/10.1038/nature23879
3. Kotukh E., Severinov O., Vlasov A., Tenytska A., Zarudna E. Some results of development of cryptographic transformation schemes using non-abelian groups // Radiotekhnika. 2021. No 204. P. 66–72. https://doi.org/10.30837/rt.2021.1.204.07
4. Khalimov G., Kotukh Y., Sergiychuk Y., Marukhnenko A. Analysis of the implementation complexity of the cryptosystem on the Suzuki group // Radiotekhnika. 2018. No 193. P. 75–81. https://doi.org/10.30837/rt.2018.2.193.08
5. Kotukh Y., & Khalimov G. Hard problems for non-abelian cryptography // 2021: Fifth International Scientific and Technical Conference "computer and information systems and technologies" https://doi.org/10.30837/csitic52021232176
6. Kotukh Y., Khalimov G. Towards practical cryptoanalysis of systems based on word problems and logarithmic signatures // Information security: problems and prospects. https://shorturl.at/IaByX
7. Shor P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // SIAM Journal on Computing. 1997. No 26(5). P. 1484–1509. https://epubs.siam.org/doi/10.1137/S0097539795293172
8. Gidney C., & Ekerå M. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. Quantum. 2021. No 5. 433 p. https://doi.org/10.22331/q-2021-04-15-433
9. Kotukh Y., Khalimov G. Advantages of logarithmic signatures in the implementation of crypto primitives // Challenges and Issues of Modern Science. https://cims.fti.dp.ua/j/article/download/119/158
10. Kotukh Y. Quantum cryptoanalysis of prospective asymmetric cryptosystems // Proceedings of conference “Cybersecurity in energy sector”. https://shorturl.at/1pbcK
11. Preskill J. Quantum Computing in the NISQ era and beyond // Quantum. 2018. No 2. P. 79. https://doi.org/10.22331/q-2018-08-06-79

Надійшла до редколегії 05.02.2025

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

Коробчинський Максим Володимирович – д-р техн. наук, професор, начальник другої кафедри Другого Навчально-наукового інституту Воєнної Академії імені Євгена Березняка; Київ, Україна; e-mail: maks_kor@ukr.net; ORCID: https://orcid.org/0000-0001-8049-4730

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