УДК 004.056.55:004.27

Мельникова О. А., Грасмік С. В.

КВАНТОВІ АТАКИ НА ХЕШ-ФУНКЦІЇ У СТРАТЕГІЇ ОЦІНКИ ЗАГРОЗ BSI

Розвиток квантових обчислень змушує переоцінювати стійкість сучасних криптографічних механізмів. У доповіді розглянуто криптографічні хеш-функції, які широко використовуються для контролю цілісності даних, автентифікації, цифрового підпису та побудови криптографічних протоколів. У документі Федерального відомства з інформаційної безпеки Німеччини (BSI – Bundesamt für Sicherheit in der Informationstechnik) хеш-функції розглядаються як важливий об'єкт квантового криптоаналізу, через зв'язок із застосуванням алгоритму Ґровера до пошуку прообразу та з теоретичними підходами до пошуку колізій [1].

Розгляд цієї проблеми є важливим у широкому контексті постквантового переходу, бо хеш-функції виступають об'єктом криптоаналітичних досліджень і водночас основою окремих квантово-стійких рішень. Це можна побачити в дослідженнях, присвячених розвитку квантово-стійких технологій у Німеччині, де окрема увага приділяється хеш-орієнтованим схемам цифрового підпису [2].

Метою доповіді є узагальнення сучасних підходів до квантових атак на криптографічні хеш-функції та визначення обмежень їх реалізації в сучасних умовах.

У німецьких дослідженнях хеш-функції розглядали в межах аналізу симетричної криптографії. Основним квантовим алгоритмом визначено алгоритм Ґровера. Його застосування до хеш-функцій пов'язано насамперед із задачею пошуку прообразу. Для хеш-функцій з n-бітовим виходом алгоритм Ґровера зменшує складність пошуку прообразу до порядку $O(2^{n/2})$, тобто забезпечує квадратичне прискорення, якщо порівнювати з класичним повним перебором. Водночас BSI підкреслює, що практичне значення такої атаки залежить від складності реалізації самої хеш-функції як квантової схеми, а не лише від асимптотичної оцінки [1].

Окрему увагу приділяють Secure Hash Algorithm, зокрема SHA-2 та SHA-3. Наголошується, що аналіз квантових загроз для хеш-функцій має ґрунтуватися не тільки на загальній математичній оцінці, а й на характеристиках стандартизованих алгоритмів [1, 3, 4].

Практичне значення квантових атак на хеш-функції можна оцінити через необхідні обчислювальні ресурси. Для SHA-2-256 квантова реалізація потребує приблизно 5,7 тисячі логічних кубітів, понад 690 тисяч CNOT-вентилів (двокубітних квантових вентилів) та глибину схеми близько 12,8 тисячі. Важливо зауважити, що вказана кількість стосується ідеальних логічних кубітів; для реальних систем із корекцією

помилок знадобляться мільйони фізичних кубітів, що на порядки перевищує можливості сучасного обладнання. Для SHA-2-384 і SHA-2-512 число логічних кубітів перевищує 13 тисяч, а кількість вентилів – понад 1,8 мільйона. Для SHA-3 оцінки також є суттєвими: схема вимагає понад 22 тисячі логічних кубітів. Все це свідчить про те, що перешкодою для практичного квантового криптоаналізу хеш-функцій є не лише алгоритмічна складність, а й надзвичайно потужна відмовостійка (fault-tolerant) квантова інфраструктура, яка нині відсутня [1].

Крім задачі пошуку прообразу, BSI вказує на проблему пошуку колізій для хеш-функцій. Теоретично квантові підходи можуть забезпечувати прискорення для цього типу задач, однак практична ефективність цих атак є темою дискусій. Основними перешкодами вказуються висока вартість реалізації оракула Ґровера, потреба у значних обсягах квантової пам’яті та складність квантових схем [1, 5].

Розгляд квантових атак на хеш-функції доцільно пов’язувати і з розвитком схем цифрового підпису на основі хеш-функцій. Адже оцінка стійкості хешів у квантовій моделі безпосередньо впливає на надійність таких механізмів, як XMSS та SPHINCS+. У дослідженнях, присвячених розвитку квантово-стійких криптографічних технологій у Німеччині, зазначені рішення розглядаються як один із практичних напрямів довгострокового захисту. Аналіз атак дозволяє точніше оцінити потенційні ризики та криптографічний запас стійкості рішень, що ґрунтуються на хешуванні [1, 2].

Як результат проведеного аналізу встановлено, що криптографічні хеш-функції є ключовим об’єктом у сучасних дослідженнях квантового криптоаналізу. Квантові атаки ставлять під сумнів теоретичну стійкість багатьох криптосистем, проте їх практична реалізація залишається суттєво обмеженою через високі вимоги до ресурсів.

Також підтверджується, що хеш-функції можуть виступати надійним базисом для постквантових цифрових підписів. Таким чином, дослідження квантових атак на хеші допомагають формувати логіку переходу до довгострокових стійких криптографічних рішень. Впровадження отриманих результатів у вітчизняні системи захисту інформації дозволить забезпечити їх відповідність загальноєвропейським вимогам постквантової безпеки, стратегічні напрями яких було проаналізовано у попередніх дослідженнях [6].

Список використаних джерел

1. Wilhelm F. K., Steinwandt R., Lageyre P., Kirchhoff S. *Entwicklungsstand Quantencomputer = Status of quantum computer development*. Bonn : Bundesamt für Sicherheit in der Informationstechnik, 2025.

2. Мельникова О. А., Грасмік С. В. Становлення та розвиток квантово-стійких криптографічних технологій у Німеччині // *Вісник ХНТУ*. 2025. № 4 (95), ч. 2. С. 119–123. DOI: https://doi.org/10.35546/kntu2078-4481.2025.4.2.15

3. *Secure Hash Standard (SHS) : FIPS PUB 180-4* / National Institute of Standards and Technology. Gaithersburg, MD : NIST, 2015.

4. *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions : FIPS PUB 202* / National Institute of Standards and Technology. Gaithersburg, MD : NIST, 2015.

5. Bernstein D. J. Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete? // *SHARCS’09 : Workshop on Special-Purpose Hardware for Attacking Cryptographic Systems (Lausanne, Switzerland, Sept. 9–10, 2009) : proceedings*. 2009. P. 105–116. URL: https://cr.yp.to/hash/collisioncost-20090517.pdf (дата звернення: 09.03.2026).

6. Мельникова О. А., Грасмік С. В. Вплив BSI на європейську стратегію постквантової криптографії. *Проблеми інформатизації* : зб. матеріалів XIII міжнар. наук.-техн. конф. (Харків – Баку, 2025 р.). Харків : НТУ «ХПІ» [та ін.], 2025. Т. 2 : секції 3, 7. С. 50–51. DOI: https://doi.org/10.32620/PI.25.t2