УДК 004.056.53 DOI https://doi.org/10.35546/kntu2078-4481.2025.1.2.27

В. В. СЕМЕРЕНСЬКА
аспірант кафедри автоматизації та проектування обчислювальної техніки
Харківський національний університет радіоелектроніки
ORCID: 0009-0008-2955-3676

КВАНТОВО-СТІЙКІ КРИПТОГРАФІЧНІ АЛГОРИТМИ ДЛЯ КРИТИЧНИХ ІНФРАСТРУКТУР

Стрімкий розвиток квантових обчислень створює загрозу для сучасних криптографічних механізмів, що використовуються для захисту конфіденційності, цілісності та автентифікації даних у цифрових системах. Це особливо актуально для критичних інфраструктур, таких як енергетичні, транспортні, фінансові та урядові інформаційні системи, де компрометація безпеки може мати катастрофічні наслідки. Враховуючи цей виклик, сучасні дослідження зосереджені на розробці та впровадженні постквантових криптографічних рішень, здатних протистояти атакам квантових комп'ютерів.

У даній роботі проводиться аналіз основних класів квантово-стійких криптографічних алгоритмів, включаючи кодові, решіткові, многочленні та хешеві схеми. Особливу увагу приділено їхньому порівнянню за ключовими параметрами продуктивності та безпеки, що є критично важливими для реального впровадження. Результати дослідження показують, що решіткові алгоритми, такі як Kyber та NTRU, демонструють оптимальне співвідношення між продуктивністю та стійкістю до атак квантових комп'ютерів, що робить їх найбільш перспективними кандидатами для стандартизації. Водночас кодові алгоритми, зокрема McEliece, забезпечують надзвичайно високий рівень захисту, проте їхній великий розмір ключів залишається серйозним обмеженням для широкого використання.

Розглянуто архітектурні рішення для інтеграції квантово-стійкої криптографії в критичні інформаційні системи. Запропоновано використання гібридних криптографічних механізмів, що поєднують традиційні та постквантові алгоритми для забезпечення безпеки в перехідний період. Також розглянуто необхідність адаптації сучасних протоколів, таких як TLS, IPsec та VPN, для підтримки нових алгоритмів, що сприятиме безболісному переходу до повноцінної квантово-стійкої криптографії.

Окрему увагу приділено викликам впровадження квантово-стійкої криптографії, включаючи високі обчислювальні вимоги, сумісність із наявними мережевими протоколами, відсутність єдиних стандартів та необхідність оновлення апаратного забезпечення. Наведені можливі шляхи подолання цих проблем, зокрема впровадження апаратних прискорювачів криптографічних операцій та оптимізація алгоритмів для зменшення навантаження на обчислювальні ресурси.

Загальні висновки дослідження вказують на неминучість поступового переходу на постквантову криптографію та необхідність стратегічного планування для її ефективного впровадження. Подальші дослідження у цій сфері мають бути спрямовані на оптимізацію алгоритмів, тестування їхньої безпеки в реальних умовах та розробку міжнародних стандартів, що забезпечать довготривалу захищеність цифрових інфраструктур.

Ключові слова: *квантово-стійка криптографія, решіткові алгоритми, кодові алгоритми, хешеві підписи, McEliece, NTRU, Kyber, постквантова безпека, критичні інфраструктури, стандартизація.*

V. V. SEMERENSKA
Postgraduate Student at the Department of Automation and Computer Engineering
Kharkiv National University of Radio Electronics
ORCID: 0009-0008-2955-3676

QUANTUM-RESISTANT CRYPTOGRAPHIC ALGORITHMS FOR CRITICAL INFRASTRUCTURES

The rapid development of quantum computing poses a significant threat to modern cryptographic mechanisms used to ensure the confidentiality, integrity, and authentication of data in digital systems. This issue is particularly critical for infrastructures such as energy, transportation, financial, and governmental information systems, where security breaches can lead to catastrophic consequences. In response to this challenge, current research focuses on the development and implementation of post-quantum cryptographic solutions capable of resisting quantum computer attacks.

This paper provides an analysis of the main classes of quantum-resistant cryptographic algorithms, including code-based, lattice-based, multivariate, and hash-based schemes. Special attention is given to their comparison based on key performance and security parameters, which are crucial for real-world deployment. The study's findings indicate that lattice-based algorithms, such as Kyber and NTRU, offer an optimal balance between computational efficiency and resistance to quantum attacks, making them the most promising candidates for standardization. Meanwhile, code-based schemes like McEliece provide exceptionally high security levels but suffer from excessive key sizes, limiting their broad adoption.

The study explores architectural solutions for integrating quantum-resistant cryptography into critical information systems. It proposes the use of hybrid cryptographic mechanisms that combine traditional and post-quantum algorithms to ensure security during the transition period. Additionally, the necessity of adapting current security protocols, such as TLS, IPsec, and VPN, to support new cryptographic algorithms is discussed, facilitating a smooth transition to full quantum-resistant encryption.

The challenges of implementing post-quantum cryptography are examined, including high computational requirements, compatibility issues with existing network protocols, the lack of unified standards, and the need for hardware upgrades. Potential solutions to these problems are suggested, including hardware accelerators for cryptographic operations and algorithm optimizations to reduce computational overhead.

The overall conclusions highlight the inevitability of a gradual transition to post-quantum cryptography and the need for strategic planning to ensure its effective deployment. Further research should focus on optimizing algorithms, testing their security in real-world conditions, and developing international standards to ensure the long-term protection of digital infrastructures.

Key words: *post-quantum cryptography, lattice-based algorithms, code-based encryption, hash-based signatures, McEliece, NTRU, Kyber, post-quantum security, critical infrastructures, standardization.*

Постановка проблеми

Стрімкий розвиток квантових обчислень становить серйозну загрозу для сучасних криптографічних методів, що широко застосовуються для забезпечення конфіденційності, цілісності та автентифікації даних. Класичні криптографічні алгоритми, такі як RSA, ECC та симетричні методи шифрування (AES), вважаються надійними у сучасних умовах, однак з появою потужних квантових комп'ютерів їх безпека може опинитися під загрозою.

Квантові обчислення створюють загрози традиційній криптографії через здатність квантових алгоритмів значно пришвидшувати розв'язання задач, на яких ґрунтується сучасна криптографія. Алгоритм Шора може ефективно факторизувати великі числа та розв'язувати проблему дискретного логарифмування, що унеможливлює використання RSA та ECC для довгострокового захисту даних. Алгоритм Гровера забезпечує квадратичне прискорення пошуку в невпорядкованих структурах даних, що значно знижує стійкість симетричних криптографічних схем та хеш-функцій.

Критичні інфраструктури, такі як енергетичні системи, транспортні мережі, фінансові установи та державні організації, особливо вразливі до потенційних квантових атак, оскільки їх функціонування напряму залежить від захисту даних та стійкості криптографічних механізмів. Втрата довіри до криптографічних систем може призвести до катастрофічних наслідків, зокрема до компрометації конфіденційної інформації, порушення комунікаційних каналів та збоїв у функціонуванні критичних систем.

З огляду на вищезазначене, виникає нагальна потреба у розробці та впровадженні квантово-стійких криптографічних алгоритмів, які зможуть забезпечити безпеку даних в умовах появи квантових комп'ютерів. У зв'язку з цим постає завдання аналізу існуючих постквантових криптографічних рішень та оцінки їх ефективності у контексті захисту критичних інфраструктур.

Аналіз останніх досліджень і публікацій

За останні роки дослідження у сфері квантово-стійкої криптографії набули значного розвитку. Наукова спільнота та міжнародні організації, такі як Національний інститут стандартів і технологій США (NIST), активно займаються стандартизацією постквантових криптографічних алгоритмів. У рамках ініціативи NIST PQC було проведено кілька раундів відбору криптографічних схем, серед яких особливу увагу привернули решіткові, кодові, многочленні та хешеві криптосистеми.

Значну увагу дослідники приділяють аналізу ефективності та безпеки цих алгоритмів у різних контекстах. Наприклад, Alkim et al. (2016) у своїй роботі «Post-Quantum Key Exchange–A New Hope» представили нову схему обміну ключами на основі решіткової криптографії, яка забезпечує стійкість до атак квантових комп'ютерів. Bernstein et al. (2017) дослідили можливість розширення RSA для постквантової криптографії, аналізуючи його переваги та недоліки.

Інші дослідження, такі як Bindel et al. (2019), розглядають можливість використання гібридних механізмів обміну ключами, що поєднують класичні та постквантові алгоритми для забезпечення стійкості перехідного періоду. Hoffstein et al. (1998) розробили алгоритм NTRU, який є однією з найбільш перспективних решіткових криптосистем для використання у критичних інфраструктурах. Schwabe et al. (2020) у своїй роботі «Post-Quantum TLS Without Handshake Signatures» запропонували способи інтеграції постквантової криптографії у протоколи TLS для захищеного з'єднання.

Дослідження також стосуються аспектів інтеграції постквантових алгоритмів у сучасні мережеві протоколи, включаючи TLS, VPN та захищені комунікаційні системи. Виявлено, що деякі алгоритми можуть створювати додаткові навантаження на обчислювальні потужності, що потребує оптимізації апаратного та програмного забезпечення.

Таким чином, аналіз останніх досліджень демонструє, що постквантова криптографія є активною сферою наукових досліджень, що включає як розробку нових алгоритмів, так і тестування їх стійкості та продуктивності

у різних умовах. Ці дослідження є критично важливими для майбутнього впровадження квантово-стійких рішень у критичні інфраструктури.

Формулювання мети дослідження

Метою цього дослідження є оцінка ефективності та придатності постквантових криптографічних алгоритмів для захисту критичних інфраструктур. Особливий акцент зроблено на аналізі сучасних підходів до квантово-стійкої криптографії, зокрема решіткових, кодових, многочленних та хешевих криптосистем, а також їх потенційного впровадження у реальні сценарії використання. Дослідження також спрямоване на ідентифікацію викликів та обмежень постквантових алгоритмів, включаючи їх продуктивність, безпеку та можливість інтеграції у наявні криптографічні протоколи. Основна мета – запропонувати рекомендації щодо впровадження квантово-стійких рішень у критичні інфраструктури, які забезпечать довготривалу безпеку у світі після появи квантових обчислень.

Викладення основного матеріалу дослідження

1. Класифікація квантово-стійких криптографічних алгоритмів

З появою квантових обчислень традиційні криптографічні методи опинилися під загрозою. Вразливість RSA, ECC та інших широко використовуваних алгоритмів викликала необхідність створення нових, квантово-стійких криптографічних рішень. Для забезпечення безпеки критичних систем досліджуються різні підходи, включаючи кодові, решіткові, многочленні та хешеві алгоритми (Ducas, Durmus, Lepoint, & Lyubashevsky, 2013).

Кодові криптосистеми, такі як McEliece, засновані на складності декодування випадкових лінійних кодів. Вони демонструють високу стійкість до атак квантових комп'ютерів, але їх використання ускладнене через великі розміри ключів, які можуть перевищувати 100 КБ. У реальних системах це створює проблеми зі збереженням та передачею ключової інформації.

Решіткові криптосистеми, зокрема NTRU та Kyber, базуються на складності знаходження найближчого вектора у ґратці. Вони мають високу ефективність обчислень та відносно невеликі розміри ключів (від 1 до 3 КБ) (Lyubashevsky, Peikert, & Regev, 2010). Завдяки цьому решіткові алгоритми активно впроваджуються в сучасні криптографічні стандарти.

Многочленні криптосистеми, такі як Rainbow, використовують багаторівневі нелінійні системи рівнянь. Вони забезпечують швидке створення цифрових підписів, проте значний розмір відкритих ключів (до 50 КБ) обмежує їхнє широке застосування.

Хешеві криптосистеми, представлені алгоритмами на кшталт SPHINCS+, забезпечують стійкість за рахунок криптографічних хеш-функцій. Вони уникають складних математичних припущень, однак швидкість генерації ключів залишається низькою порівняно з іншими постквантовими методами.

2. Порівняння продуктивності та стійкості існуючих рішень

Оцінка ефективності різних алгоритмів наведена у таблиці 1.

Таблиця 1

Оцінка ефективності криптографічних алгоритмів

Алгоритм	Тип	Розмір ключа (КБ)	Час генерації ключа (мс)	Стійкість до атак (кількість кубітів для злому)
McEliece	Кодова	100+	80–100	>1024
NTRU	Решіткова	2–3	7–12	>512
Kyber	Решіткова	1	4–6	>512
Rainbow	Многочленна	50	25–40	>768
SPHINCS+	Хешова	30	150–200	>1024

Проаналізувавши наведені дані, можна помітити, що кожен клас криптографічних алгоритмів має свої переваги і недоліки. Кодові алгоритми, як McEliece, демонструють найвищий рівень безпеки, однак їхні великі розміри ключів значно ускладнюють їх впровадження в системах з обмеженими ресурсами. Решіткові алгоритми, такі як NTRU та Kyber, є найбільш збалансованими щодо продуктивності та безпеки, що пояснює їх популярність у процесі стандартизації квантово-стійкої криптографії (Peikert, 2014).

Многочленні криптосистеми, зокрема Rainbow, забезпечують високу швидкість операцій підпису та перевірки, але мають значний розмір відкритих ключів, що ускладнює їх інтеграцію у вбудовані системи. Хешеві криптосистеми, такі як SPHINCS+, забезпечують гарантовану стійкість, оскільки не залежать від математичних припущень щодо складності задач. Однак вони демонструють нижчу продуктивність, оскільки операції підпису та перевірки вимагають значних обчислювальних ресурсів.

Основною причиною таких відмінностей є фундаментальні математичні принципи, на яких базуються різні криптографічні підходи. Наприклад, кодові криптосистеми забезпечують високу безпеку за рахунок великої ентропії ключів, що робить їх стійкими до атак, але призводить до значного збільшення вимог до пам'яті. Решіткові методи дозволяють отримати високу швидкість обчислень завдяки використанню спеціалізованих

операцій у векторному просторі, тоді як хешеві криптосистеми залежать від великої кількості обчислень, необхідних для створення багаторазових хеш-дерев.

Ці відмінності мають суттєвий вплив на вибір алгоритму для конкретного застосування. Наприклад, у мобільних пристроях і вбудованих системах найбільш прийнятними є решіткові алгоритми завдяки їхній ефективності та малому розміру ключів. У фінансових і державних системах, які потребують максимальної безпеки навіть за рахунок продуктивності, можуть бути доцільними кодові або хешеві криптосистеми. Таким чином, вибір алгоритму завжди залежить від конкретних вимог до безпеки, продуктивності та апаратних обмежень системи.

3. Архітектурні рішення для інтеграції квантово-стійкої криптографії у критичні системи

Інтеграція квантово-стійкої криптографії в існуючі інформаційні системи є складним завданням, що потребує як оновлення програмного забезпечення, так і змін у апаратних архітектурах. Одним із ключових підходів є впровадження гібридних криптографічних схем, які поєднують класичні алгоритми (RSA, ECC) із квантово-стійкими (Kyber, McEliece). Такий підхід дозволяє зберігати зворотну сумісність із існуючими системами безпеки, забезпечуючи плавний перехід до повністю постквантових технологій.

Для ефективної інтеграції квантово-стійкої криптографії у комунікаційні протоколи пропонується оновлення стандартів TLS та IPsec, включення нових криптографічних примітивів у механізми встановлення з'єднання та автентифікації. Наприклад, у протоколі TLS 1.3 можуть бути впроваджені квантово-стійкі схеми обміну ключами, такі як Kyber, що знижує ймовірність компрометації навіть у разі прориву традиційних криптографічних механізмів (Bos et al., 2015).

Ще одним важливим напрямком є використання апаратних криптографічних модулів (HSM, TPM), які дозволяють прискорити виконання операцій підпису та шифрування, знижуючи загальне навантаження на центральний процесор. Спеціалізовані апаратні прискорювачі можуть бути використані для оптимізації обчислень у кодових криптосистемах (McEliece), де обробка великих ключів є значною проблемою.

Для корпоративних та урядових мереж доцільним є створення ізольованих сегментів із квантово-стійкими криптографічними рішеннями. Наприклад, захищені VPN-з'єднання можуть використовувати гібридну модель шифрування, де класичні AES-ключі доповнюються решітковими механізмами Kyber. Це підвищує стійкість системи до атак із боку квантових комп'ютерів без необхідності кардинального перепроєктування мережевої інфраструктури.

Таким чином, найбільш ефективними архітектурними рішеннями для інтеграції квантово-стійкої криптографії є гібридні моделі безпеки, адаптація існуючих протоколів зв'язку та впровадження апаратних прискорювачів. Це дозволяє зберегти продуктивність систем при підвищенні їхньої стійкості до майбутніх квантових атак.

4. Виклики впровадження

Перехід на квантово-стійку криптографію супроводжується низкою технічних та організаційних викликів, які необхідно враховувати під час впровадження нових криптографічних стандартів.

Одним із головних бар'єрів є високі обчислювальні витрати. Багато постквантових алгоритмів потребують значно більше ресурсів, ніж традиційні схеми шифрування. Наприклад, кодові криптосистеми вимагають великих обсягів пам'яті для збереження ключів, що ускладнює їхнє використання у вбудованих та мобільних пристроях.

Ще однією критичною проблемою є сумісність з існуючими системами. Більшість сучасних мережевих протоколів, таких як TLS, IPsec та SSH, не були спроектовані з урахуванням великих розмірів ключів і додаткових обчислювальних витрат, які необхідні для квантово-стійкої криптографії. Це означає, що перехід на нові стандарти потребує глибокої модифікації програмного забезпечення, що може зайняти роки.

Питання продуктивності також відіграє важливу роль. Алгоритми, які потребують великої кількості обчислень для генерації та перевірки підписів або обміну ключами, можуть стати вузьким місцем у системах реального часу, таких як фінансові транзакції або IoT-пристрої. Наприклад, SPHINCS+ забезпечує високий рівень безпеки, але його швидкість значно нижча порівняно з іншими рішеннями, що обмежує його застосування в деяких сценаріях.

Також існує проблема стандартизації. Хоча такі організації, як NIST, активно працюють над створенням єдиних стандартів постквантової криптографії, цей процес може зайняти ще кілька років. У цей перехідний період компаніям доведеться підтримувати гібридні системи безпеки, що поєднують традиційні алгоритми з квантово-стійкими (Chen et al., 2016).

Однією з основних проблем є високе навантаження на обчислювальні ресурси, що особливо відчутно у мобільних пристроях та IoT-системах. Оскільки багато квантово-стійких алгоритмів потребують значно більше пам'яті та обчислювальної потужності, інтеграція їх у пристрої з обмеженими ресурсами стає серйозним викликом.

Ще однією перешкодою є несумісність квантово-стійких алгоритмів із сучасними мережевими протоколами безпеки. Наприклад, існуючі стандарти TLS, IPsec та SSH не були розроблені з урахуванням особливостей нових криптографічних схем, що потребує глибоких змін у їх реалізації.

Відсутність загальноприйнятих стандартів також ускладнює впровадження. Організації, такі як NIST, працюють над їх розробкою, але процес гармонізації нових методів із поточними інфраструктурами може зайняти роки. Це змушує багато компаній використовувати тимчасові гібридні рішення, комбінуючи класичні та квантово-стійкі алгоритми.

Нарешті, ще одним важливим фактором є труднощі з адаптацією великих ключів у розподілених системах. Деякі криптографічні схеми, зокрема кодові, мають дуже великі відкриті ключі, що створює додаткові виклики для зберігання, передачі та управління ключовою інформацією в масштабних інфраструктурах.

З огляду на ці виклики, успішний перехід на квантово-стійку криптографію вимагатиме поступового впровадження змін, адаптації протоколів безпеки та використання гібридних криптографічних моделей, які дозволять зберегти зворотну сумісність із поточними стандартами безпеки.

Висновки

Аналіз сучасного стану квантово-стійкої криптографії демонструє, що найбільш перспективними підходами є решіткові та кодові алгоритми, які забезпечують оптимальний баланс між продуктивністю та безпекою. При цьому хешеві та многочленні криптосистеми можуть використовуватися у вузькоспеціалізованих сценаріях, де вимоги до швидкодії не є критичними.

Інтеграція квантово-стійкої криптографії в існуючі системи безпеки потребує комплексного підходу, включаючи гібридні моделі, оновлення комунікаційних протоколів та застосування апаратних прискорювачів. Попри значні виклики, такі як високі обчислювальні витрати, сумісність із чинними стандартами та необхідність стандартизації, поступовий перехід до нових криптографічних методів є неминучим для забезпечення довгострокової кібербезпеки.

Подальші дослідження у цій сфері мають бути спрямовані на оптимізацію постквантових алгоритмів, розробку ефективних рішень для зниження навантаження на ресурси та вдосконалення механізмів інтеграції квантово-стійких технологій у масштабні інформаційні системи.

Список використаної літератури

1. Alkim, E., Ducas, L., Pöppelmann, T., & Schwabe, P. (2016). Post-quantum key exchange – a new hope. USENIX Security 2016, 327–343. https://eprint.iacr.org/2015/1092

2. Bernstein, D. J., Heninger, N., Lou, P., & Valenta, L. (2017). Post-quantum RSA. У Post-Quantum cryptography (с. 311–329). Springer International Publishing. https://doi.org/10.1007/978-3-319-59879-6_18

3. Bindel, N., Brendel, J., Fischlin, M., Goncalves, B., & Stebila, D. (2019). Hybrid key encapsulation mechanisms and authenticated key exchange. У Post-Quantum cryptography (с. 206–226). Springer International Publishing. https://doi.org/10.1007/978-3-030-25510-7_12

4. Hoffstein, J., Pipher, J., & Silverman, J. H. (1998). NTRU: A ring-based public key cryptosystem. У Lecture notes in computer science (с. 267–288). Springer Berlin Heidelberg. https://doi.org/10.1007/bfb0054868

5. Schwabe, P., Stebila, D., & Wiggers, T. (2020). Post-Quantum TLS without handshake signatures. У CCS ‘20: 2020 ACM SIGSAC conference on computer and communications security. ACM. https://doi.org/10.1145/3372297.3423350

6. Bos, J. W., Costello, C., Naehrig, M., & Stebila, D. (2015). Post-Quantum key exchange for the TLS protocol from the ring learning with errors problem. У 2015 IEEE symposium on security and privacy (SP). IEEE. https://doi.org/10.1109/sp.2015.40

7. Lyubashevsky, V., Peikert, C., & Regev, O. (2013). On ideal lattices and learning with errors over rings. Journal of the ACM, 60(6), 1–35. https://doi.org/10.1145/2535925

8. Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). Report on Post-Quantum Cryptography. National Institute of Standards and Technology. https://doi.org/10.6028/nist.ir.8105

9. Ducas, L., Durmus, A., Lepoint, T., & Lyubashevsky, V. (2013). Lattice signatures and bimodal gaussians. У Advances in cryptology – CRYPTO 2013 (с. 40–56). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-40041-4_3

10. Peikert, C. (2014). Lattice cryptography for the internet. У Post-Quantum cryptography (с. 197–219). Springer International Publishing. https://doi.org/10.1007/978-3-319-11659-4_12

References

1. Alkim, E., Ducas, L., Pöppelmann, T., & Schwabe, P. (2016). Post-quantum key exchange – a new hope. USENIX Security 2016, 327–343. https://eprint.iacr.org/2015/1092

2. Bernstein, D. J., Heninger, N., Lou, P., & Valenta, L. (2017). Post-quantum RSA. In Post-Quantum cryptography (pp. 311–329). Springer International Publishing. https://doi.org/10.1007/978-3-319-59879-6_18

3. Bindel, N., Brendel, J., Fischlin, M., Goncalves, B., & Stebila, D. (2019). Hybrid key encapsulation mechanisms and authenticated key exchange. In Post-Quantum cryptography (pp. 206–226). Springer International Publishing. https://doi.org/10.1007/978-3-030-25510-7_12

4. Hoffstein, J., Pipher, J., & Silverman, J. H. (1998). NTRU: A ring-based public key cryptosystem. In Lecture notes in computer science (pp. 267–288). Springer Berlin Heidelberg. https://doi.org/10.1007/bfb0054868

5. Schwabe, P., Stebila, D., & Wiggers, T. (2020). Post-Quantum TLS without handshake signatures. In CCS ‘20: 2020 ACM SIGSAC conference on computer and communications security. ACM. https://doi.org/10.1145/3372297.3423350

6. Bos, J. W., Costello, C., Naehrig, M., & Stebila, D. (2015). Post-Quantum key exchange for the TLS protocol from the ring learning with errors problem. In 2015 IEEE symposium on security and privacy (SP). IEEE. https://doi.org/10.1109/sp.2015.40

7. Lyubashevsky, V., Peikert, C., & Regev, O. (2013). On ideal lattices and learning with errors over rings. Journal of the ACM, 60(6), 1–35. https://doi.org/10.1145/2535925

8. Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). Report on Post-Quantum Cryptography. National Institute of Standards and Technology. https://doi.org/10.6028/nist.ir.8105

9. Ducas, L., Durmus, A., Lepoint, T., & Lyubashevsky, V. (2013). Lattice signatures and bimodal gaussians. In Advances in cryptology – CRYPTO 2013 (pp. 40–56). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-40041-4_3

10. Peikert, C. (2014). Lattice cryptography for the internet. In Post-Quantum cryptography (pp. 197–219). Springer International Publishing. https://doi.org/10.1007/978-3-319-11659-4_12