ОСОБЛИВОСТІ ЗАСТОСУВАННЯ КРИПТОСИСТЕМ NTRU В IOT-СИСТЕМАХ

Товма О.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Розвиток технологій Інтернету речей (IoT) супроводжується збільшенням кількості пристроїв, що автоматично обмінюються даними в мережі. Оскільки більшість таких пристроїв має обмежені ресурси пам'яті, енергоспоживання та обчислювальної потужності, використання традиційних криптографічних алгоритмів є ускладненим. Одночасно зростає потреба в надійному захисті даних через підвищену вразливість IoT-систем до кіберзагроз. Розвиток квантових обчислень додатково посилює цю проблему, оскільки традиційні алгоритми, зокрема RSA, можуть втратити стійкість. У зв'язку з цим NTRU розглядається як перспективне постквантове рішення для IoT завдяки високій швидкодії та придатності до роботи на обмежених пристроях

Метою доповіді є визначення особливостей використання криптосистем NTRU в IoT-середовищі, аналіз їхньої ефективності при роботі на ресурсно обмежених пристроях, а також оцінювання практичної доцільності впровадження в сучасних мережевих архітектурах. Криптосистема NTRU базується на операціях у поліноміальному кільці, де шифрування і дешифрування виконуються через відносно прості арифметичні перетворення [1].Саме ця математична конструкція забезпечує нижчі обчислювальні витрати порівняно з багатьма іншими постквантовими алгоритмами. Для IoT-пристроїв така особливість є принципово важливою, оскільки навіть незначне збільшення криптографічного навантаження може впливати на час автономної роботи, стабільність передачі даних і швидкість реакції системи. Практичні дослідження показують, що NTRU демонструє високу швидкість генерації ключів та виконання операцій дешифрування навіть на мікроконтролерах із невеликою частотою процесора. У порівнянні з класичними алгоритмами відкритого ключа час виконання криптографічних процедур скорочується, що дозволяє використовувати захищений обмін ключами без суттєвого впливу на продуктивність сенсорних вузлів. Додатковою перевагою є можливість інтеграції NTRU у гібридні криптографічні схеми, де постквантовий алгоритм використовується паралельно з класичними механізмами захисту. Такий підхід дозволяє забезпечити сумісність із чинними протоколами безпеки та поступово адаптувати IoT-інфраструктуру до нових криптографічних стандартів. [1, 2]. Окремою перевагою NTRU є передбачуваність обчислювальних витрат. У багатьох IoT-сценаріях система повинна гарантувати стабільний час відповіді незалежно від навантаження. Решіткові алгоритми добре адаптуються до таких вимог, оскільки більшість операцій виконуються в межах фіксованої арифметичної структури. Це спрощує планування навантаження в реальному часі та підвищує стабільність роботи критичних пристроїв. Важливим фактором є також криптографічна стійкість NTRU у довгостроковій перспективі. Безпека алгоритму базується на

складності задач пошуку коротких векторів у структурованих решітках, для яких сьогодні не існує ефективного квантового алгоритму поліноміального часу. На відміну від традиційних схем, де квантові методи можуть суттєво скоротити складність зламу, у випадку NTRU навіть часткове квантове прискорення не призводить до практичного компрометування правильно вибраних параметрів [3].

Для IoT це означає можливість побудови захищених систем із тривалим життєвим циклом, де пристрої можуть працювати багато років без повної заміни криптографічної архітектури. Такий аспект особливо важливий для промислових сенсорних мереж, інфраструктурних контролерів та медичних пристроїв, де оновлення програмного забезпечення часто є складним або дорогим. Разом із перевагами існують і практичні обмеження. Одним із них є відносно більший розмір відкритих ключів порівняно з окремими класичними схемами.

Для мереж із дуже низькою пропускною здатністю це може створювати додаткове навантаження на канали передачі. Проте для більшості сучасних IoT-сценаріїв цей недолік компенсується швидкістю обробки та зниженням обчислювального навантаження на вузол, що особливо важливо в системах реального часу [2, 3].

Сучасні тенденції розвитку постквантової криптографії показують, що NTRU розглядається як перспективний компонент гібридних схем захисту, де традиційні алгоритми тимчасово поєднуються з постквантовими механізмами. Такий підхід дозволяє поступово адаптувати IoT-інфраструктуру до нових стандартів без радикальної перебудови всієї системи безпеки. У практичному сенсі впровадження NTRU в IoT-середовищі є доцільним насамперед там, де потрібне поєднання швидкодії, енергетичної ефективності та довгострокового криптографічного захисту. Саме ці властивості роблять алгоритм особливо перспективним для мереж розумних сенсорів, систем автоматизації та захищених комунікацій між вбудованими пристроями. Отже, криптосистеми на основі NTRU демонструють високий рівень придатності до використання в IoT-системах завдяки здатності забезпечувати постквантову стійкість без суттєвого перевантаження обмежених апаратних ресурсів. Їхнє практичне значення визначається поєднанням математичної надійності та технічної ефективності, що дозволяє розглядати NTRU як один із реальних інструментів формування безпечної інфраструктури майбутніх мережевих технологій.

Список літератури

1. Семеренська, В. (2025). Квантово-стійкі криптографічні алгоритми для критичних інфраструктур. Вісник ХНТУ, 2(1 (92)), 204-209.

2. Kotukh, Y., Severinov, E., Vlasov, O., Tenytska, A., & Zarudna, E. (2021). Some results of development of cryptographic transformations schemes using non-abelian groups. Radiotekhnika, 1(204), 66-72..

3. Petrenko O., Petrenko O., Sievierinov O., Fiediushyn O., Zubrych A., & Shcherbina, D. (2021). Analysis of ways to increase stability of cryptographic algorithms on algebraic lattices against time attacks. *Radiotekhnika*, *4*(207), 59–65.