УДК 004.056.5:512.643

Товма О. М., Балагура Д. С.

КРИПТОСИСТЕМИ НА ОСНОВІ NTRU

Сучасний розвиток інформаційних технологій супроводжується зростанням вимог до криптографічного захисту даних, особливо в умовах розвитку постквантових обчислень. Поява квантових комп'ютерів створює ризики для традиційних асиметричних алгоритмів, заснованих на факторизації великих чисел і задачі дискретного логарифмування. У зв'язку з цим особливого значення набувають алгоритми, математична основа яких залишається стійкою до квантових атак, зокрема NTRU як один із найвідоміших представників решіткових криптосистем відкритого ключа [1].

NTRU була запропонована як практична альтернатива класичним алгоритмам ще наприкінці XX століття і з того часу зберігає високу актуальність завдяки поєднанню швидкодії, компактності ключів і стійкості до відомих квантових атак. На відміну від традиційних криптографічних схем, її безпека ґрунтується на складності задач у структурованих алгебраїчних решітках, що сьогодні розглядається як один із найбільш перспективних напрямів побудови постквантових криптографічних систем.

Метою дослідження є аналіз архітектури криптосистем на основі NTRU, визначення їхніх криптографічних переваг, оцінювання практичної стійкості в умовах сучасного криптоаналізу та дослідження можливостей інтеграції в реальні інформаційні системи.

NTRU – це криптосистема відкритого ключа, назва якої походить від скорочення Nth Degree Truncated Polynomial Ring, що в перекладі означає усічене поліноміальне кільце n-го степеня. Назва відображає математичну основу алгоритму, оскільки всі криптографічні операції виконуються в спеціальному поліноміальному кільці з модульною арифметикою. NTRU визначають як решітково-орієнтовану постквантову криптосистему, криптографічна стійкість якої базується на складності задач пошуку коротких векторів у структурованих алгебраїчних решітках. Саме така математична конструкція забезпечує її стійкість до відомих класичних і більшості квантових методів криптоаналізу [2, 3].

Криптосистеми на основі NTRU належать до класу lattice-based cryptography, тобто криптографії, що використовує властивості багатовимірних решіток. Їхня особливість полягає в тому, що всі криптографічні операції виконуються в алгебраїчній структурі

поліномів із модульною арифметикою. Такий підхід дозволяє реалізувати дуже швидкі операції шифрування й дешифрування порівняно з багатьма іншими постквантовими схемами.

Основною перевагою NTRU є те, що навіть при високому рівні стійкості система зберігає низькі обчислювальні витрати. Саме ця характеристика стала ключовою причиною її активного вивчення для застосування в мобільних платформах, мережевих протоколах і вбудованих пристроях. Важливо, що криптографічна стійкість NTRU базується не на одній окремій складній задачі, а на поєднанні кількох складних обчислювальних властивостей, пов'язаних із відновленням коротких векторів у спеціально побудованих решітках. Така структура значно ускладнює застосування відомих ефективних алгоритмів криптоаналізу.

У сучасних дослідженнях NTRU розглядається як одна з найбільш стабільних постквантових схем щодо впливу квантових алгоритмів. На відміну від класичних криптосистем, де Shor's algorithm здатний кардинально знизити рівень безпеки, для NTRU подібного прямого квантового алгоритму поліноміального часу наразі не існує.

Основні методи криптоаналізу спрямовані на застосування алгоритмів редукції решіток, які дозволяють поступово наближатися до секретної структури ключа. Проте навіть сучасні модифікації таких методів залишаються обчислювально складними при правильно підібраних параметрах системи.

Окрему увагу приділяють впливу квантового прискорення окремих частин lattice-атак. Навіть із використанням Grover's algorithm зниження складності не є достатнім для практичного руйнування сучасних параметрів NTRU. Практичні дослідження підтверджують, що сучасні профілі безпеки NTRU забезпечують достатній запас стійкості навіть у довгостроковій перспективі.

Однією з головних причин зростання інтересу до NTRU є її практична придатність до реального впровадження. На відміну від багатьох інших постквантових схем, NTRU демонструє дуже швидку генерацію ключів, високу швидкість дешифрування та стабільну роботу навіть у середовищах із обмеженими ресурсами. Зазначене робить систему особливо перспективною для використання в протоколах захищеного зв'язку, де важлива мінімальна затримка криптографічних операцій. Серед таких напрямів найбільший інтерес становлять сучасні реалізації у TLS, VPN і системах захищеної автентифікації.

У вбудованих пристроях NTRU також демонструє високу ефективність завдяки невеликому навантаженню на процесор і відносно помірним вимогам до пам'яті. Це особливо важливо для IoT-архітектур, де криптографічні ресурси часто є обмеженими. Крім того, сучасні гібридні криптографічні архітектури дедалі частіше поєднують NTRU з іншими постквантовими алгоритмами для підвищення загальної стійкості.

Криптосистеми на основі NTRU сьогодні займають важливе місце серед постквантових криптографічних рішень завдяки вдалому поєднанню математичної стійкості та високої практичної продуктивності. NTRU зберігає конкурентні переваги в умовах сучасного криптоаналізу, оскільки її математична основа залишається стійкою до відомих квантових загроз. Водночас система демонструє високу швидкодію, що робить її придатною для масштабного впровадження в сучасних мережевих і вбудованих інформаційних системах [4].

Перспективність NTRU визначається тим, що ця криптосистема вже стала фундаментом для низки сучасних постквантових стандартів і продовжує активно розвиватися в напрямі оптимізації параметрів безпеки та підвищення захисту від практичних атак. Отже, NTRU можна розглядати як одну з базових криптографічних платформ для формування майбутньої квантово-стійкої цифрової інфраструктури.

Список використаних джерел

1. Matiyko, A., & Alekseychuk, A. (2022). Method for design secure symmetric NTRU-

like encryption schemes. *Collection "Information Technology and Security"*, *10*(2), 165–176. https://doi.org/10.20535/2411-1031.2022.10.2.270406

2. Gorbenko, I., Kachko, O., & Yesina, M. (2017). Analysis of the end-to-end encryption algorithm NTRU PRIME IIT UKRAINE taking into account known attacks. *Radiotekhnika*, *4*(191), 11–23. https://doi.org/10.30837/rt.2017.4.191.023

3. Горбенко, І., Качко, О., та Єсіна, М. (2017). Аналіз алгоритму наскрізного шифрування NTRU PRIME IIT UKRAINE з урахуванням відомих атак. *Радіотехніка* , *4* (191), 11–23. https://doi.org/10.30837/rt.2017.4.191.02

4. Черняк, О. С., & Осташко, І. О. ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ ПОСТКВАНТОВИХ АЛГОРИТМІВ ШИФРУВАННЯ. *КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ ТА ОПТИМІЗАЦІЯ СКЛАДНИХ СИСТЕМ*, 221.