# МЕТОДИКА ОЦІНЮВАННЯ СТІЙКОСТІ NTRU-КРИПТОСИСТЕМ ДО АТАК НА АЛГЕБРАЇЧНИХ РЕШІТКАХ

Товма О.М., Балагура Д.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Розвиток постквантової криптографії потребує не лише створення алгоритмів, стійких до відомих квантових загроз, а й обґрунтованого вибору їх параметрів. Криптосистеми родини NTRU використовують арифметику поліноміальних кілець і пов'язані з нею структуровані решітки. Їхні переваги щодо швидкодії та можливості застосування в обмежених обчислювальних середовищах розглянуто в попередніх дослідженнях [1]. Проте сама висока продуктивність не визначає фактичний запас криптографічної стійкості, який залежить від параметрів, розподілу секретів і складності конкретних атак.

**Метою доповіді є** обґрунтування методики порівняльного оцінювання стійкості криптосистем на основі NTRU-перетворень до решіткових атак з урахуванням параметрів алгебраїчної структури та обчислювальних витрат атакувальника.

На відміну від загального аналізу властивостей NTRU, запропонований напрям дослідження передбачає оцінювання не лише номінального рівня безпеки, а й залежності прогнозованої складності криптоаналізу від зміни параметрів. Для цього доцільно розмежовувати атаку відновлення секретного ключа та атаку відновлення повідомлення, оскільки для них застосовують різні цільові решітки, початкові припущення й критерії успішності [2, 3].

Основу методики становить побудова решіткового представлення досліджуваного екземпляра NTRU та визначення характеристик, що впливають на ефективність редукції базису. До складу вхідних даних включають степінь поліноміального кільця, модуль обчислень, спосіб вибору малих поліномів, параметри ключів і допустиму ймовірність успіху атаки. У разі порівняння різних варіантів NTRU необхідно окремо фіксувати структуру кільця та правила кодування, щоб уникнути некоректного зіставлення схем із різними математичними припущеннями.

Для оцінювання обчислювальної складності пропонується застосовувати параметризовану модель атак із редукцією базису за допомогою алгоритму BKZ. У межах такої моделі для набору параметрів визначають очікуваний розмір блока редукції, орієнтовну вартість його оброблення та умови, за яких редукований базис може містити вектор, придатний для реалізації криптоаналітичної атаки. Вартість слід визначати за явно обраною моделлю обчислень, оскільки кількість елементарних операцій і реальний час виконання не є тотожними показниками [4].

Запропонована процедура аналізу складається з формування наборів параметрів NTRU, побудови відповідних решіток, вибору моделей атак, оцінювання складності редукції та порівняння отриманих оцінок із цільовим рівнем безпеки. Додатково доцільно виконувати аналіз чутливості: змінювати

по одному параметру за незмінності решти та встановлювати, які зміни найбільш суттєво впливають на прогнозовані витрати криптоаналізу. Такий підхід дозволяє відокремити вплив розмірності решітки від впливу розподілу секретних коефіцієнтів.

Особливу увагу потрібно приділити межам застосовності обраної моделі. Оцінка, отримана для BKZ та евристичної моделі пошуку коротких векторів, не є доведенням стійкості до всіх класичних або квантових атак. Для квантового сценарію необхідно окремо обґрунтовувати можливі прискорення окремих підпроцедур, переносити оцінки алгоритму Шора, що стосуються факторизації та дискретного логарифмування, безпосередньо на NTRU некоректно.

Практичну перевірку методики доцільно проводити на експериментальних конфігураціях зі зменшеними параметрами, де можна порівняти прогнозовану складність атаки з фактичними результатами редукції базису. Для відтворюваності слід фіксувати версії програмних засобів, випадкові початкові дані, обрані параметри BKZ і характеристики обчислювальної платформи. Результати таких експериментів мають використовуватися для перевірки адекватності моделі, а не для безпосередньої екстраполяції часу атаки на повномасштабні криптосистеми.

Отже, запропоновано методичний підхід до оцінювання стійкості NTRU-криптосистем, який поєднує параметричний аналіз алгебраїчної структури, моделювання решіткових атак та перевірку адекватності оцінок на контрольних конфігураціях.

Наукове значення підходу полягає в систематизації зв’язку між параметрами NTRU та складністю криптоаналітичних процедур. Подальші дослідження передбачають програмну реалізацію методики, експериментальне порівняння моделей редукції та формування обґрунтованих рекомендацій щодо вибору параметрів NTRU для ресурсно обмежених інформаційних систем.

**Список літератури**

1. Matiyko A., Alekseychuk A. Method for design secure symmetric NTRU-like encryption schemes. Information Technology and Security. 2022. Vol. 10, No. 2. P. 165–176. DOI: 10.20535/2411-1031.2022.10.2.270406.

2. Горбенко І. Д., Качко О. Г., Єсіна М. В. Аналіз алгоритму наскрізного шифрування NTRU Prime IIT Ukraine з урахуванням відомих атак. Радіотехніка. 2017. Вип. 191. С. 11–23.

3. Петренко, О.С., Петренко, О.Є., Сєвєрінов, О.В., Фєдюшин, О.І., Зубрич, А.В., & Щербина, Д.В. (2021). Аналіз шляхів підвищення стійкості криптоалгоритмів на алгебраїчних решітках щодо часових атак. Радіотехніка, 4(207), 59–65. https://doi.org/10.30837/rt.2021.4.207.05

4. Albrecht M. R., Player R., Scott S. On the Concrete Hardness of Learning with Errors. Journal of Mathematical Cryptology. 2015. Vol. 9, No. 3. P. 169–203. DOI: 10.1515/jmc-2015-0016.