An algebraic algorithm for breaking NTRU with multiple keys

Hansraj Jangir

Florida Atlantic University, USA

We present a heuristic polynomial-time algorithm for solving the NTRU problem with multiple keys, given a sufficient number of ring samples. Our approach follows the linearization technique of the Arora-Ge algorithm (ICALP '11), leveraging public keys to construct a system of linear equations. The key contribution of our work is a kernel reduction technique that extracts the secret vector from a linear space of rank nnn, where nnn is the degree of the ring in which NTRU is defined. In contrast to the algorithm proposed by Kim and Lee (Designs, Codes and Cryptography, '23), our method does not require prior knowledge of the Hamming weight of the secret keys. Our algorithm relies on plausible heuristics, and we provide experimental results demonstrating its effectiveness in practice, achieving performance close to cryptographic parameter ranges.

In Special Session 55 on Post-Quantum Cryptography at the Mathematical Congress of the Americas 2025.

MCA 2025 internal code: SS55-T14