MS05

A Study on Multivariate Polynomial Solving in the Construction of Lattice-Based Cryptographic Signature: A Case of Signature Forgery

Amir Hamzah Abd Ghafar[1,2,*], and **Nor Siti Khadijah Arunah**[2]

[1]Department of Mathematics, Faculty of Science, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia
[2]Institute of Mathematical Research, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia

Correspondence
Email: amir_hamzah@upm.edu.my

Abstract

Lattice-based and multivariate-based cryptography have been selected and listed as candidates for post-quantum cryptography. Both of them have an advantage in their relatively efficient encryption, decryption and signing. Learning with error (LWE) is the hard problem for the lattice-based signature scheme. It depends on solving high-degree univariate polynomial in the LWE system of equation $As + e = t$ of ring $R_q = Z_q[X]/(X^n + 1)$. To solve the LWE equation means to find the secret key s or error e. For the multivariate signature schemes, the security depends on the multivariate quadratic problem (MQP) equation of $P = S \circ F \circ T$. Solving MQP means solving m multivariate quadratic polynomial equations with n variables. This paper will show a few past successful attacks on a multivariate signature scheme. It succeeds in forging the signature using a rogue certificate attack by solving the polynomial of the multivariate cryptosystem's public key. We modified these attacks to attack lattice-based signature schemes. Moreover, we showed that, unlike multivariate signature schemes, solving the public key polynomial equation in a lattice-based signature scheme may require additional work before we retrieve its private keys.

Keywords: *Lattice-based signature scheme, Learning with error, Post-quantum cryptography, Multivariate signature scheme, Multivariate quadratic problem*