ICRAMCS 2026

THE EIGHTH EDITION OF THE INTERNATIONAL CONFERENCE ON RESEARCH IN APPLIED MATHEMATICS AND COMPUTER SCIENCE
April 23-24-25, 2026 | Marrakech, Morocco

PQ-LWE: A Novel Post-Quantum Cryptosystem Based on p-Adic Quadratic Forms

Communication Info

Authors:
Najat RAFI[1]
Khalid KHALLOUKI [1]
Khadija BOUZKOURA [1]
Abdelhakim CHILLALI [2]

[1] faculty of science Ben M'sick, Casablanca, Morocco
[2] Polydisciplinary Faculty of Taza, Taza, Morocco

Keywords:
(1) Cryptography
(2) p-adic Quadratic LWE
(3) post quantum cryptography

Abstract

We introduce a lattice-inspired algebraic construction over truncated p-adic rings. The scheme relies on a quadratic masking mechanism obtained by conjugating a diagonal form with an invertible matrix over $\mathbb{Z}_{p^p}$, ensuring efficient coordinate-wise decryption while providing algebraic obfuscation.

We define the associated computational problem, termed p-adic Quadratic LWE (PQ-LWE), and present explicit matrix formulations together with a correctness analysis under bounded noise assumptions. The construction admits polynomial-time key generation and encryption procedures.

This preliminary work highlights structural links between quadratic forms, p-adic lifting, and conjugation invariants, and suggests new directions for integrating p-adic algebraic techniques into lattice-based cryptographic design.

References

[1] V. Lyubashevsky, C. Peikert, and O. Regev,``On ideal lattices and learning with errors over rings,'' in Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2013, pp. 1-23.

[2] J. Ding, X. Xie, and X. Lin, ``A simple provably secure key exchange scheme based on the learning with errors problem", Proceedings of the 2012 International Workshop on Post-Quantum Cryptography, 2012, pp. 1-16.