A Digital Signature Scheme based on Finite Frobenius Rings

Henry Chimal-Dzul

University of Texas at San Antonio

Based on the code-equivalence problem, the digital signature LESS has been proposed as a candidate in the NIST Post-Quantum Standardization Process. In this work, the code equivalence problem is studied in the setting of Finite Frobenius Rings and a natural generalization of LESS in this setting is proposed.

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

MCA 2025 internal code: SS55-T20