

Development of a quantum-resistant digital signature scheme based on the hidden discrete logarithm problem and solving systems of multivariate quadratic equations

Duong Thu May

Abstract: This study constructs a quantum-resistant digital signature scheme to counter the threat posed by quantum computers to cryptographic systems. The approach combines the Hidden Discrete Logarithm Problem (HDLP) and the Multivariate Quadratic (MQ) problem—two problems with high computational complexity for quantum algorithms. Specifically, the study proposes embedding the hidden problem into a multivariate system to optimize key size and signing speed, while enhancing security against Shor's and Grover's attacks. The result is an efficient scheme that ensures data integrity and authentication in the post-quantum era, contributing to cybersecurity.

Keywords: quantum-resistant digital signature, hidden discrete logarithm problem, multivariate quadratic equation system, post-quantum cryptography, information security