Research on building a digital signature scheme based on the integer factorization problem

Cao Hung Phuong

Abstract: This thesis presents a novel approach to constructing a digital signature scheme based on the computational hardness of the integer factorization problem. While traditional factorization-based signatures, such as RSA, rely on the difficulty of factoring large composite numbers, they often require significant computational overhead. This research proposes a new signature scheme that leverages the mathematical structure of the factorization problem to achieve a more efficient balance between security and performance. The proposed scheme is formally defined, and its security is rigorously analyzed under the standard assumption that factoring large integers is computationally infeasible. The construction details, including key generation, signing, and verification algorithms, are provided. A comparative performance analysis against existing factorization-based signatures demonstrates that the new scheme offers reduced signature size and faster verification times while maintaining a provable security level. The findings contribute to the field of post-quantum cryptography by offering an alternative signature primitive that remains secure against classical adversaries and can be efficiently implemented in resource-constrained environments.

Keywords: digital signature scheme, integer factorization problem, cryptographic construction, security analysis