Research on building attack algorithms for the RSA cryptosystem

Vo Ta Hoang

Abstract: This thesis investigates the development of novel algorithms for attacking the RSA cryptosystem, focusing on vulnerabilities arising from specific key generation weaknesses and implementation flaws. While RSA remains a cornerstone of modern public-key cryptography, its security is contingent upon the practical difficulty of integer factorization and the robust selection of parameters. This research systematically analyzes classical attack vectors, including low private exponent attacks (e.g., Wiener's and Boneh-Durfee attacks) and common modulus attacks, before proposing a refined algorithmic framework that integrates lattice reduction techniques with heuristic search methods. The proposed algorithm optimizes the construction of the lattice basis and employs a modified enumeration strategy to reduce the computational complexity of finding small roots for modular polynomial equations. Experimental results demonstrate that the new algorithm significantly improves the success rate and efficiency of recovering private keys under specific weak parameter conditions compared to existing methods. The findings underscore critical security thresholds for RSA parameter selection and provide a practical tool for evaluating cryptographic robustness, contributing to the ongoing discourse on post-quantum cryptographic transitions.

Keywords: RSA, attack, algorithm, cryptosystem