## ABSTRACT


| | |
|---|---|
| Author: | Hansraj Jangir |
| Title: | New Studies in Lattice-Based Cryptography, Quantum Algorithms, and Privacy-Preserving Computation |
| Institution: | Florida Atlantic University |
| Dissertation Co-Advisors: | Dr. Lun-Ching Chang<br>Dr. Dipayan Das |
| Degree: | Doctor of Philosophy |
| Year: | 2026 |



Classical public-key cryptographic schemes primarily rely on the presumed hardness of the integer factorization and discrete logarithm problems. However, Shor's algorithm demonstrates that both problems can be solved efficiently on a sufficiently powerful quantum computer. This breakthrough motivated the search for quantum-resistant hard assumptions. The assumptions based on lattices are one of the primary candidates in post-quantum cryptography due to their strong theoretical foundations and well-established hardness against both classical and quantum attacks. In this thesis, we explore several directions of lattice based cryptology and quantum algorithms.

On the construction side, we propose two compact encryption schemes based on the Module-NTRU problem. These schemes provide flexibility in parameter selection while achieving competitive ciphertext and public key sizes. On the cryptanalytic side, we study three different problems: the multiple-key NTRU problem, the Extrapolated Dihedral Coset Problem (EDCP), and the integer factorization problem. First, we investigate the hardness of the multiple-key NTRU problem and present

a heuristic polynomial-time algebraic attack that recovers a shared secret. Second, we analyze the Extrapolated Dihedral Coset Problem (EDCP), a quantum problem to which the well-known Learning With Errors (LWE) problem reduces. We present a quasi-polynomial-time quantum algorithm for EDCP over power-of-two moduli. Third, we revisit the integer factorization problem under limited quantum resources. We develop classical–quantum hybrid algorithms based on Coppersmith's factorization factory, leveraging Grover's search algorithm to reduce both runtime and logical qubit requirements.

Finally, we explore practical applications of homomorphic encryption in privacy-preserving biomedical data analysis. We develop techniques to improve the efficiency and usability of encrypted linear regression, including adaptive gradient methods, hybrid regression strategies, and optimized arithmetic operations.