ABSTRACT OF THE DISCLOSURE

Title: Automated Vulnerability Discovery and Security Validation System for Post-Quantum Cryptographic Implementations Using GPU-Accelerated Quantum Attack Simulation

Docket Number: RUTHERFORD-012-PROV

A comprehensive defensive cybersecurity testing and validation system designed to discover vulnerabilities in post-quantum cryptographic (PQC) implementations through GPU-accelerated quantum attack simulation. Unlike existing GPU-accelerated implementations that optimize cryptographic operations for performance, this system specifically targets vulnerability discovery and security validation of PQC implementations created by libraries such as NVIDIA cuPQC, LibOQS, and other frameworks.

The system comprises seven integrated components: (1) a GPU-accelerated quantum attack simulation library optimized for adversarial testing using parallel processing and tensor cores; (2) an automated vulnerability discovery engine that identifies implementation weaknesses undetectable by classical cryptanalysis; (3) a parameterized security assessment system evaluating algorithms at NIST-defined security levels; (4) a quantum-enhanced side-channel vulnerability analyzer employing superposition principles for sub-classical threshold detection; (5) a multi-standard compliance report generator supporting NIST FIPS 203/204/205, ETSI TR 103 619, and ISO/IEC 18033-2; (6) a quantum-safe certification scoring mechanism; and (7) an automated migration recommendation engine implementing Mosca's theorem algorithmically.

The invention enables organizations to validate PQC deployments before production, achieving 100-1000x performance improvements over CPU-based testing through novel GPU

optimizations including early termination logic, tensor core cryptanalysis, and parallel attack vector exploration. The system addresses critical security needs for government agencies, financial institutions, and critical infrastructure preparing for quantum computing threats, providing automated compliance documentation and risk assessment essential for regulatory requirements.

Word Count: 236 words (within 250-word limit)