SPECIFICATION

TITLE OF INVENTION

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

INVENTOR

Brian Rutherford
6 Country Place Drive
Wimberley, Texas 78676-3114
United States
(512) 648-0219
Actual@ScrappinR.com

ATTORNEY DOCKET NUMBER

RUTHERFORD-012-PROV

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to Provisional Application RUTHERFORD-011-PROV (if applicable).

FIELD OF THE INVENTION

[0002] The present invention relates to defensive cybersecurity systems, specifically to GPU-accelerated testing and vulnerability discovery frameworks for evaluating the security of post-quantum cryptographic algorithm implementations against quantum attacks. The invention provides comprehensive security validation and testing of cryptographic implementations within the MWRASP (Total) - Mathematical Woven Responsive Adaptive Swarm Platform - defensive cybersecurity framework, rather than implementing the cryptographic algorithms themselves.

DISTINCTION FROM PRIOR ART

[0003] The present invention fundamentally differs from existing GPU-accelerated PQC libraries (such as NVIDIA cuPQC, LibOQS, and DPCrypto) in that:

[0004] 1. Purpose: This system TESTS and ATTACKS PQC implementations to find vulnerabilities for defensive purposes, rather than implementing the algorithms themselves for production use.

[0005] 2. Output: Produces vulnerability reports, compliance assessments, and migration recommendations for enterprise security, not cryptographic operations.

[0006] 3. Method: Employs adversarial quantum attack simulation optimized for defensive security testing, not optimization of legitimate cryptographic operations.

[0007] 4. Scope: Evaluates ALL aspects including side-channels, fault injection, and implementation errors within comprehensive MWRASP validation, not just computational performance.

[0008] 5. Complementary Role: Designed to validate and test implementations created by libraries like cuPQC as part of integrated defensive AI agent networks, not to replace them.

BACKGROUND OF THE INVENTION

Technical Field

[0009] I'm developing a set of patents to build a quantum resistant defensive cybersecurity platform to help secure people, institutions, and digital assets from being susceptible to hacking. In this defensive cybersecurity platform for MWRASP (Total), the advent of quantum computing poses an existential threat to current cryptographic systems. Shor's algorithm can efficiently factor large integers and compute discrete logarithms, threatening RSA and elliptic curve cryptography. Grover's algorithm provides quadratic speedups against symmetric cryptography. The National Institute of Standards and Technology (NIST) has standardized post-quantum cryptographic (PQC) algorithms including ML-KEM (FIPS 203), ML-DSA (FIPS 204), and SLH-DSA (FIPS 205) to address these threats.

[0010] Recent developments such as NVIDIA's cuPQC (December 2024) have accelerated the IMPLEMENTATION of PQC algorithms on GPUs, achieving significant speedups for operations like key generation, encapsulation, and decapsulation. However, these tools implement cryptographic algorithms for production use and do not address the critical need for TESTING these implementations against quantum attacks within comprehensive defensive security frameworks.

[0011] The security of a cryptographic implementation depends not only on the theoretical strength of the algorithm but also on the absence of implementation vulnerabilities, side-channel leakages, and other weaknesses that may be exploited by quantum adversaries. No existing solution provides automated, comprehensive vulnerability assessment of PQC implementations at the speed and scale required for enterprise adoption within integrated defensive AI agent networks.

Problems with Prior Art

[0012] Current approaches to PQC security have several critical limitations when viewed from a defensive cybersecurity perspective:

[0013] 1. Implementation Focus: Existing GPU-accelerated tools (cuPQC, DPCrypto, GOLF) optimize the performance of cryptographic operations but do not test for vulnerabilities that defensive AI agents must identify.

[0014] 2. Limited Testing Scope: Current testing methods do not systematically evaluate all quantum attack vectors that protection AI agents must defend against.

[0015] 3. Manual Compliance: No automated tools exist for simultaneous validation against multiple international standards required by enterprise defensive frameworks.

[0016] 4. Migration Uncertainty: Organizations lack algorithmic tools integrated with defensive AI agent systems to assess quantum vulnerability and plan migration.

[0017] 5. Detection Limitations: Classical testing methods may miss subtle implementation vulnerabilities exploitable by quantum attacks that defensive monitoring AI agents must catch.

SUMMARY OF THE INVENTION

[0018] The present invention provides an automated vulnerability discovery and security validation system for post-quantum cryptographic implementations within the comprehensive MWRASP (Total) defensive cybersecurity platform. The system uses GPU acceleration specifically optimized for adversarial testing and attack simulation from a defensive perspective, not for implementing cryptographic operations.

[0019] The framework is designed to test and validate implementations created by existing libraries such as NVIDIA cuPQC, LibOQS, and other PQC implementations, serving as a critical security validation layer operated by defensive AI agents in the PQC ecosystem. It identifies vulnerabilities that may exist in even highly optimized commercial implementations, enabling protection AI agents to secure enterprise systems.

[0020] The system comprises seven integrated components operating within the MWRASP framework:

[0021] 1. A GPU-accelerated quantum attack simulation library optimized for defensive adversarial testing

[0022] 2. An automated vulnerability discovery engine operated by defensive security AI agents that identifies implementation weaknesses

[0023] 3. A parameterized security assessment system evaluating algorithms at multiple security levels for comprehensive MWRASP validation

[0024] 4. A quantum-enhanced side-channel vulnerability analyzer employed by threat prevention AI agents

[0025] 5. A multi-standard compliance report generator for enterprise protection AI agent networks

[0026] 6. A quantum-safe certification scoring mechanism integrated with MWRASP AI agents

[0027] 7. An automated migration recommendation engine implementing Mosca's theorem for defensive planning

DETAILED DESCRIPTION

Overview and Distinction from Implementation Libraries

[0028] The invention provides a defensive security testing and validation framework that operates as a distinct layer above PQC implementation libraries, integrated within the MWRASP (Total) platform. While libraries like NVIDIA cuPQC focus on optimizing cryptographic operations for performance, this system focuses on finding vulnerabilities in those implementations through defensive adversarial testing conducted by AI agent networks.

[0029] For example, where cuPQC optimizes ML-KEM key generation to achieve maximum throughput, our defensive system attempts to break ML-KEM implementations by simulating quantum attacks, analyzing side-channels, and identifying implementation flaws that protection AI agents can then defend against. The two technologies are complementary within the MWRASP ecosystem: cuPQC creates secure implementations, our system validates that security through defensive AI agents.

System Architecture for Defensive Security Testing

[0030] The invention employs a distributed GPU architecture specifically designed for defensive adversarial testing and vulnerability discovery within AI agent swarms. Unlike implementation-focused GPU usage, our optimization targets:

Parallel exploration of attack vectors by defensive AI agents

Early termination when vulnerabilities are found by protection agents

Memory optimization for attack state spaces monitored by AI agents

Adversarial pattern recognition within integrated MWRASP agents

GPU Configuration for Defensive Attack Simulation

[0031] The system utilizes GPUs differently than implementation libraries, optimized for defensive AI agent operations:

Attack simulations use memory for storing partial attack states tracked by monitoring AI agents

Tensor cores are configured for cryptanalysis operations guided by defensive AI agents

Thread scheduling optimized for parallel attack attempts coordinated by AI agent swarms

Early termination logic when vulnerabilities are detected by protection AI agents

Component 1: GPU-Accelerated Quantum Attack Simulation Library for Defensive Testing

[0032] The attack simulation library is fundamentally different from cryptographic implementation libraries, designed for defensive security AI agents. While cuPQC implements algorithms correctly, our library attempts to break them for defensive purposes through adversarial Grover's algorithm implementation.

Component 2: Automated Vulnerability Discovery Engine with AI Agent Integration

[0033] This component has no equivalent in implementation libraries like cuPQC. It specifically searches for vulnerabilities that defensive AI agents must protect against:

[0034] 1. Implementation Flaws: Bugs in the code that protection AI agents must identify

[0035] 2. Side-Channel Vulnerabilities: Timing, power, or EM leakages monitored by defensive agents

[0036] 3. Protocol Weaknesses: Errors in how algorithms are used, detected by AI agent networks

[0037] 4. Configuration Errors: Insecure parameter choices flagged by MWRASP agents

[0038] The engine operates by testing implementations against a comprehensive threat model managed by defensive AI agents.

Component 3: Quantum-Enhanced Side-Channel Analysis for Defensive Monitoring

[0039] The invention introduces novel quantum-inspired techniques for side-channel analysis operated by defensive monitoring AI agents. These techniques apply quantum superposition principles to correlation analysis, enabling detection of vulnerabilities below classical thresholds.

Component 4: Multi-Standard Compliance Validation for Enterprise Protection

[0040] Unlike implementation libraries that may support a single standard, our defensive system validates against multiple standards simultaneously through AI agent coordination:

NIST FIPS 203/204/205 validated by compliance AI agents

ETSI TR 103 619 checked by European protection agents

ISO/IEC 18033-2 verified by international AI agents

Common Criteria EAL4+ assessed by certification agents

[0041] This validation tests whether implementations (including cuPQC-based ones) meet all regulatory requirements for comprehensive MWRASP protection.

Component 5: Migration Recommendation Engine with Defensive AI Planning

[0042] The system implements Mosca's theorem algorithmically for defensive migration guidance through AI agents. This component calculates data sensitivity periods (X years), migration time estimates (Y years), and quantum threat timelines (Z years) to determine if $X + Y >= Z$, indicating immediate action is required.

Complementary Technology to Existing Solutions within MWRASP

[0043] The present invention complements rather than competes with GPU-accelerated PQC implementations like cuPQC by providing defensive validation through AI agents:

[0044] 1. Testing cuPQC Implementations: Validating security through defensive AI agent testing

[0045] 2. Finding GPU-Specific Vulnerabilities: Identifying side-channels for protection agents

[0046] 3. Providing Independent Validation: Third-party assessment by MWRASP agents

[0047] 4. Enabling Continuous Testing: Integration with CI/CD through automated agents

[0048] 5. Supporting Multiple Libraries: Testing implementations via AI agent networks

Example Use Case: Defensive Testing of cuPQC Implementation

[0049] In one embodiment, the defensive system tests an NVIDIA cuPQC ML-KEM implementation through AI agents:

[0050] Input: cuPQC ML-KEM implementation binary, test vectors and parameters, security requirements (FIPS 203), MWRASP AI agent configuration

[0051] Process: (1) Load implementation into defensive testing framework, (2) Deploy AI agent swarm for parallel quantum attack simulations, (3) Protection agents perform side-channel analysis during operations, (4) Monitoring agents check for timing variations and power leakage, (5) Compliance agents validate constant-time execution requirements, (6) Testing agents examine error handling and edge cases

[0052] Output: Vulnerability report from defensive AI agents, compliance assessment by protection agents, recommendations from planning agents, risk score from MWRASP network

Performance Considerations for Defensive Operations

[0053] While specific performance metrics await prototype validation, the defensive system achieves significant speedups through AI agent coordination:

[0054] 1. Parallel Attack Simulation: Multiple defensive agents test vectors simultaneously

[0055] 2. Early Termination: Protection agents stop when vulnerabilities are found

[0056] 3. Optimized Memory Usage: Efficient state representation for AI agents

[0057] 4. GPU-Specific Optimizations: Tensor cores for defensive cryptanalysis

[0058] The goal is comprehensive defensive security validation in hours rather than days through integrated AI agent operations.

Government and Critical Infrastructure Applications

[0059] The defensive system addresses critical needs for protection through MWRASP AI agents:

Validating PQC deployments in national security systems via government AI agents

Testing critical infrastructure migrations with protection agent networks

Assessing healthcare and financial system security through specialized agents

Evaluating classified network implementations with clearance-level agents

Technical Implementation Details for Defensive Framework

[0060] Memory Management for Defensive Attack Simulation: The defensive system employs custom memory allocation for attack state storage, checkpoint mechanisms for agent coordination, and optimized memory pools for parallel testing operations.

[0061] Parallel Vulnerability Testing Architecture with AI Agents: The defensive system employs a different parallelization strategy coordinated by AI agents, with each defensive agent testing different vulnerabilities across multiple targets simultaneously.

[0062] Compliance Report Generation by AI Agents: The defensive system automatically generates detailed compliance reports through AI agents, including NIST FIPS 203 compliance checks, vulnerability findings from discovery agents, and recommendations from planning agents.

Integration with Development Workflows via AI Agents

[0063] The defensive system integrates with existing practices through automated AI agents:

[0064] 1. Pre-deployment Testing: Protection agents validate before production

[0065] 2. Continuous Integration: Automated agents in CI/CD pipelines

[0066] 3. Regression Testing: Monitoring agents ensure update security

[0067] 4. Compliance Automation: Certification agents generate audit reports

END OF SPECIFICATION