PROVISIONAL PATENT APPLICATION 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

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

Field of Invention

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

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

1. **Purpose**: This system TESTS and ATTACKS PQC implementations to find vulnerabilities for defensive purposes, rather than implementing the algorithms themselves for production use
2. **Output**: Produces vulnerability reports, compliance assessments, and migration recommendations for enterprise security, not cryptographic operations

3. **Method**: Employs adversarial quantum attack simulation optimized for defensive security testing, not optimization of legitimate cryptographic operations
4. **Scope**: Evaluates ALL aspects including side-channels, fault injection, and implementation errors within comprehensive MWRASP validation, not just computational performance
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 Invention

Technical Field

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.

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.

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

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

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

2. **Limited Testing Scope**: Current testing methods do not systematically evaluate all quantum attack vectors that protection AI agents must defend against
3. **Manual Compliance**: No automated tools exist for simultaneous validation against multiple international standards required by enterprise defensive frameworks
4. **Migration Uncertainty**: Organizations lack algorithmic tools integrated with defensive AI agent systems to assess quantum vulnerability and plan migration
5. **Detection Limitations**: Classical testing methods may miss subtle implementation vulnerabilities exploitable by quantum attacks that defensive monitoring AI agents must catch

Summary of Invention

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.

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.

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

1. A GPU-accelerated quantum attack simulation library optimized for defensive adversarial testing
2. An automated vulnerability discovery engine operated by defensive security AI agents that identifies implementation weaknesses
3. A parameterized security assessment system evaluating algorithms at multiple security levels for comprehensive MWRASP validation
4. A quantum-enhanced side-channel vulnerability analyzer employed by threat prevention AI agents
5. A multi-standard compliance report generator for enterprise protection AI agent networks
6. A quantum-safe certification scoring mechanism integrated with MWRASP AI agents
7. An automated migration recommendation engine implementing Mosca's theorem for defensive planning

Detailed Description

Overview and Distinction from Implementation Libraries

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.

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

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

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

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:

Defensive Adversarial Grover's Algorithm Implementation

```cuda
__global__ void defensive_adversarial_grover_kernel(
    uint8_t* target_implementation,
    AttackVector* attack_params,
    VulnerabilityReport* findings,
    DefensiveAIAgent* agent
) {
    // This kernel attempts to break the implementation
    // for defensive security validation by AI agents

    // Search for weak keys or implementation flaws
    if(agent->detect_weak_key_pattern(target_implementation)) {
        findings->vulnerability_found = true;
        findings->type = WEAK_KEY_GENERATION;
        agent->report_to_mwrasp_network(findings);
        return; // Early termination on vulnerability
    }

    // Continue with quantum attack simulation for defense...
}
```

Component 2: Automated Vulnerability Discovery Engine with AI Agent Integration

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

1. **Implementation Flaws**: Bugs in the code that protection AI agents must identify
2. **Side-Channel Vulnerabilities**: Timing, power, or EM leakages monitored by defensive agents
3. **Protocol Weaknesses**: Errors in how algorithms are used, detected by AI agent networks
4. **Configuration Errors**: Insecure parameter choices flagged by MWRASP agents

The engine operates by testing implementations against a comprehensive threat model managed by defensive AI agents:

```cuda
```

```
__global__ void defensive_vulnerability_discovery_kernel(
    ImplementationUnderTest* target,
    ThreatModel* threats,
    SecurityReport* report,
    MWRASPAgentNetwork* agent_network
) {
    // Test each threat vector against the implementation
    // Coordinated by defensive AI agent swarm
    for(int threat_id = 0; threat_id < threats->count; threat_id++) {
        TestResult result = agent_network->simulate_attack(
            target, threats->vector[threat_id]
        );

        if(result.vulnerability_detected) {
            report->add_finding(result);
            agent_network->deploy_protection(result);
            // Continue testing to find all vulnerabilities
        }
    }
}
```

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

The invention introduces novel quantum-inspired techniques for side-channel analysis operated by defensive monitoring AI agents:

```
cuda
```

```
__device__ void quantum_correlation_analysis_defensive(
    float* power_traces,
    uint8_t* hypothesis,
    float* correlation_output,
    DefensiveMonitorAgent* monitor
) {
    // Apply quantum superposition principles to correlation analysis
    // This is a defensive testing technique by AI agents

    // Create superposition of correlation hypotheses
    // Use quantum-inspired amplitude amplification
    // Detect correlations below classical thresholds
    // Report to MWRASP agent network for protection
    monitor->analyze_and_protect(correlation_output);
}
```

Component 4: Multi-Standard Compliance Validation for Enterprise Protection

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

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

The system implements Mosca's theorem algorithmically for defensive migration guidance through AI agents:

```
cuda
```

```
struct DefensiveMoscaAssessment {
    int x_years;  // Data sensitivity period
    int y_years;  // Migration time estimate
    int z_years;  // Quantum threat timeline
    MWRASPPlanningAgent* planning_agent;

    __device__ bool requires_immediate_action() {
        return planning_agent->assess_risk(x_years, y_years, z_years);
    }

    __device__ float calculate_defensive_risk_score() {
        // Algorithmic implementation for defensive planning
        return planning_agent->risk_calculation(x_years, y_years, z_years);
    }
};
```

Complementary Technology to Existing Solutions within MWRASP

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

1. **Testing cuPQC Implementations**: Validating security through defensive AI agent testing
2. **Finding GPU-Specific Vulnerabilities**: Identifying side-channels for protection agents
3. **Providing Independent Validation**: Third-party assessment by MWRASP agents
4. **Enabling Continuous Testing**: Integration with CI/CD through automated agents
5. **Supporting Multiple Libraries**: Testing implementations via AI agent networks

Example Use Case: Defensive Testing of cuPQC Implementation

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

Input:
- cuPQC ML-KEM implementation binary
- Test vectors and parameters
- Security requirements (FIPS 203)
- MWRASP AI agent configuration

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

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

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

1. **Parallel Attack Simulation**: Multiple defensive agents test vectors simultaneously
2. **Early Termination**: Protection agents stop when vulnerabilities are found
3. **Optimized Memory Usage**: Efficient state representation for AI agents
4. **GPU-Specific Optimizations**: Tensor cores for defensive cryptanalysis

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

Government and Critical Infrastructure Applications

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

Memory Management for Defensive Attack Simulation

```cuda
class DefensiveAttackMemoryManager {
    MWRASPMemoryAgent* memory_agent;

    __device__ void* allocate_defensive_attack_state(size_t size) {
        // Custom allocation for defensive testing by AI agents
        return memory_agent->allocate_from_pool(size);
    }

    __device__ void checkpoint_defensive_progress() {
        // Save intermediate states for agent coordination
        memory_agent->checkpoint_to_mwrasp();
    }
};
```

Parallel Vulnerability Testing Architecture with AI Agents

The defensive system employs a different parallelization strategy coordinated by AI agents:

```cuda
```

```
__global__ void parallel_defensive_vulnerability_test(
    TestTarget* targets,
    int num_targets,
    VulnerabilityDatabase* vuln_db,
    MWRASPAgentSwarm* swarm
) {
    int tid = blockIdx.x * blockDim.x + threadIdx.x;
    DefensiveAgent* agent = swarm->get_agent(tid);

    // Each defensive agent tests different vulnerabilities
    if(tid < vuln_db->count) {
        Vulnerability vuln = vuln_db->get(tid);

        // Test all targets for protection
        for(int i = 0; i < num_targets; i++) {
            agent->test_vulnerability_defensive(targets[i], vuln);
        }
    }
}
```

Compliance Report Generation by AI Agents

The defensive system automatically generates detailed compliance reports through AI agents:

```
DEFENSIVE COMPLIANCE VALIDATION REPORT - MWRASP
================================================
Implementation: [Name and Version]
Test Date: [Date]
AI Agent Network: MWRASP-Compliance-v2.0

NIST FIPS 203 Compliance (US Protection Agent):
- Parameter Sets: [PASS/FAIL]
- Constant Time: [PASS/FAIL]
- Error Handling: [PASS/FAIL]
- Overall: [COMPLIANT/NON-COMPLIANT]

Vulnerabilities Found by Defensive Agents:
1. [Description from discovery agent]
2. [Risk level from assessment agent]

Recommendations from Planning Agents:
1. [Remediation from protection agent]
2. [Priority from coordination agent]
```

Integration with Development Workflows via AI Agents

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

1. **Pre-deployment Testing**: Protection agents validate before production
2. **Continuous Integration**: Automated agents in CI/CD pipelines
3. **Regression Testing**: Monitoring agents ensure update security
4. **Compliance Automation**: Certification agents generate audit reports

Claims

Independent Claims

Claim 1. A computer-implemented defensive cybersecurity system for discovering vulnerabilities in post-quantum cryptographic implementations within the MWRASP (Total) framework, comprising:

- a vulnerability discovery engine operated by defensive AI agents that identifies implementation weaknesses undetectable by classical cryptanalysis;
- a GPU-accelerated quantum attack simulator executing parallel simulations through AI agent swarms against target cryptographic implementations for defensive purposes;

- a side-channel analysis module employing quantum-enhanced correlation techniques guided by monitoring AI agents;
- a compliance validation engine with AI agents automatically generating reports for multiple international standards;
- a migration recommendation system with planning AI agents implementing algorithmic risk assessment based on Mosca's theorem; and
- an integrated MWRASP AI agent network coordinating all defensive operations.

Claim 2. A method for automated defensive security validation of post-quantum cryptographic implementations through AI agents comprising:

- deploying defensive AI agent swarms to load cryptographic implementations;
- executing parallel adversarial quantum attack simulations via protection agents on GPU hardware;
- performing quantum-enhanced side-channel analysis by monitoring agents;
- identifying vulnerabilities through AI agent pattern recognition;
- validating compliance via specialized certification agents;
- generating risk assessments through planning AI agents;
- producing comprehensive security reports from the MWRASP network; and
- coordinating all operations through integrated defensive AI agent systems.

Claim 3. A computer-readable medium storing instructions for defensive vulnerability discovery through AI agents, that when executed cause a computing system to:

- configure GPU resources for defensive AI agent testing operations;
- simulate quantum attacks via protection agent networks;
- detect vulnerabilities through discovery AI agents;
- assess compliance via certification AI agents;
- calculate risk scores through planning AI agents;
- generate recommendations from the MWRASP agent network; and
- coordinate all defensive operations through integrated AI agent swarms.

Dependent Claims

Claim 4. The system of claim 1, wherein the defensive AI agents test but do not implement cryptographic algorithms for production use.

Claim 5. The system of claim 1, wherein GPU acceleration is optimized for defensive AI agent adversarial testing operations.

Claim 6. The system of claim 1, designed to validate implementations through defensive AI agent networks testing libraries including NVIDIA cuPQC, LibOQS, and other frameworks.

Claim 7. The system of claim 1, wherein defensive quantum attack simulators operated by AI agents implement Grover's algorithm, Shor's algorithm, quantum collision finding, and amplitude amplification for protection purposes.

Claim 8. The system of claim 1, wherein discovery AI agents employ early termination upon finding vulnerabilities to optimize defensive testing throughput.

Claim 9. The system of claim 1, wherein monitoring AI agents use quantum superposition principles to enhance correlation sensitivity for protection.

Claim 10. The system of claim 1, wherein compliance AI agents simultaneously evaluate NIST FIPS 203, FIPS 204, FIPS 205, ETSI TR 103 619, and ISO/IEC 18033-2 requirements.

Claim 11. The system of claim 1, wherein planning AI agents implement Mosca's theorem through algorithmic calculation of data sensitivity periods, migration time estimates, and quantum threat timelines for defensive purposes.

Claim 12. The method of claim 2, wherein defensive AI agents utilize tensor cores for cryptanalytic operations in protection scenarios.

Claim 13. The method of claim 2, wherein vulnerability identification by AI agents includes detection of timing variations, power consumption patterns, electromagnetic emanations, and error handling flaws for comprehensive protection.

Claim 14. The method of claim 2, further comprising defensive AI agents testing GPU-specific implementation vulnerabilities unique to hardware-accelerated cryptographic libraries.

Claim 15. The computer-readable medium of claim 3, wherein instructions cause defensive AI agent systems to operate as a validation layer above existing PQC implementation libraries within the MWRASP framework.

Claim 16. The system of claim 1, wherein the MWRASP AI agent network comprises specialized agents for discovery, monitoring, protection, planning, and compliance operating in coordinated swarms.

Claim 17. The system of claim 1, wherein defensive AI agents communicate through encrypted channels within the MWRASP platform to coordinate vulnerability discovery and protection deployment.

Claim 18. The system of claim 1, wherein the AI agent architecture supports dynamic scaling across multiple GPU nodes for enterprise-wide defensive testing.

Claim 19. The method of claim 2, wherein AI agents employ machine learning models trained on known vulnerabilities to predict novel attack vectors for defensive purposes.

Claim 20. The system of claim 1, wherein the MWRASP framework provides real-time threat intelligence sharing between defensive AI agents across multiple organizations while preserving data privacy.

Abstract

A comprehensive defensive cybersecurity testing and validation system within the MWRASP (Total) framework designed to discover vulnerabilities in post-quantum cryptographic implementations through GPU-accelerated quantum attack simulation operated by integrated AI agent networks. Unlike existing GPU-accelerated implementations that focus on performance optimization of cryptographic operations, this defensive system specifically targets vulnerability discovery and security validation through coordinated AI agent swarms. The system tests implementations created by libraries such as NVIDIA cuPQC and LibOQS, serving as a critical defensive security validation layer operated by protection AI agents in the PQC ecosystem, identifying weaknesses undetectable by classical cryptanalysis for comprehensive enterprise protection through the Mathematical Woven Responsive Adaptive Swarm Platform.

NOTICE

This invention provides defensive security TESTING and VALIDATION of post-quantum cryptographic implementations through integrated AI agent networks within the MWRASP (Total) framework. It does not implement cryptographic algorithms for production use. The system is designed to identify vulnerabilities through defensive AI agents in existing PQC implementations including but not limited to those created using NVIDIA cuPQC, LibOQS, and other libraries. All performance claims are theoretical design targets pending prototype validation. The MWRASP platform enables comprehensive enterprise protection through coordinated defensive AI agent operations.

End of Specification
Total Pages: 45
Docket Number: RUTHERFORD-012-PROV