INFORMATION DISCLOSURE STATEMENT (IDS)

For Future Non-Provisional Filing

Provisional Application: RUTHERFORD-012-PROV
Title: Automated Vulnerability Discovery and Security Validation System for Post-Quantum Cryptographic Implementations Using GPU-Accelerated Quantum Attack Simulation
Inventor: Brian Rutherford

NOTE

This IDS is prepared for use when filing the non-provisional application. It is NOT required for the provisional filing but documents the prior art discovered during patentability analysis.

U.S. PATENT DOCUMENTS

Cite No.	Patent Number	Date	Patentee	Relevant to Claims	Notes
1	US11218300B1	2022-01-04	Wells Fargo & Co	1-3	Post-quantum cryptography communication channels - Defensive adaptation, not testing
2	US10897344B2	2021-01-19	ARM Limited	9, 13	Side-channel resistance - General crypto, not PQC-specific
3	US7600131B1	2009-10-06	Broadcom	5	Cryptography acceleration chip - Classical crypto, pre-quantum

FOREIGN PATENT DOCUMENTS

Cite No.	Document Number	Country	Date	Applicant	Relevant to Claims
None identified specifically relevant to GPU-accelerated PQC testing					

NON-PATENT LITERATURE (NPL)

Academic Publications

Cite No.	Citation	Date	Relevant to Claims	Notes
A1	"Side-Channel Analysis of Lattice-Based Post-Quantum Cryptography: Exploiting Polynomial Multiplication", IACR ePrint 2022/474	2022	9, 13	CPU-based analysis only
A2	"Non-Profiled Higher-Order Side-Channel Attacks against Lattice-Based Post-Quantum Cryptography", IACR ePrint 2025/1257	2025	9, 13	No GPU acceleration
A3	"DPCrypto: Acceleration of Post-quantum Cryptographic Algorithms using Dot-Product Instruction on GPUs", IACR ePrint 2021/1389	2021	1, 5	Implementation, not testing
A4	"HI-Kyber: A novel high-performance implementation scheme of Kyber based on GPU", IACR ePrint 2023/1194	2023	1, 5	Performance optimization only

Technical Standards

Cite No.	Document	Organization	Date	Relevant to Claims
S1	FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard	NIST	2024-08	10
S2	FIPS 204: Module-Lattice-Based Digital Signature Standard	NIST	2024-08	10
S3	FIPS 205: Stateless Hash-Based Digital Signature Standard	NIST	2024-08	10
S4	TR 103 619: Migration strategies and recommendations for Quantum Safe schemes	ETSI	2020-08	10, 11

Commercial Software/Tools

Cite No.	Product/Tool	Company	Release Date	Relevant to Claims	Notes
C1	NVIDIA cuPQC SDK	NVIDIA	2024-11	1, 6, 14	Implementation library, not testing framework
C2	LibOQS	Open Quantum Safe	2016-present	1, 6	Implementation library
C3	PQClean	PQClean Project	2019-present	1, 6	Reference implementations
C4	cuQuantum SDK	NVIDIA	2021	7	Quantum simulation, not PQC testing

---

STATEMENT OF RELEVANCE

Distinguishing Features Not Found in Prior Art:

1. **GPU-accelerated adversarial testing** specifically targeting PQC implementations for defensive vulnerability discovery (Claims 1, 2)
2. **Quantum-enhanced correlation analysis** using superposition principles for side-channel detection below classical thresholds (Claim 9)
3. **Integrated AI agent networks** within MWRASP framework coordinating defensive testing operations (Claims 1, 16-20)
4. **Tensor core optimization** for cryptanalytic operations rather than cryptographic implementation (Claims 5, 12)
5. **Algorithmic implementation of Mosca's theorem** for automated migration recommendations (Claim 11)
6. **Multi-standard simultaneous compliance validation** (NIST, ETSI, ISO) in single framework (Claim 10)
7. **Early termination logic** upon vulnerability detection for optimized testing throughput (Claim 8)

EXAMINER NOTE

The cited references are the closest prior art identified through comprehensive searching. However, none disclose the specific combination of:

- GPU acceleration + vulnerability testing (not implementation) + PQC focus + AI agent integration + defensive framework

The invention addresses a critical gap between PQC implementation tools (cuPQC, LibOQS) and the need for comprehensive security validation within enterprise defensive frameworks.

DUTY TO DISCLOSE

The applicant acknowledges the duty to disclose all information known to be material to patentability under 37 CFR 1.56. This IDS will be updated if additional relevant prior art is discovered.

SIGNATURE

/s/ Brian Rutherford/
Brian Rutherford
Inventor/Applicant (Pro Se)
Date: [To be dated when filing non-provisional]

IDS Template for RUTHERFORD-012-PROV
Page 1 of 3