COMPLETE USPTO PROVISIONAL PATENT FILING PACKAGE

QUANTUM BENCHMARK-DRIVEN TEMPORAL CORRELATION SYSTEM FOR HARVEST-NOW-DECRYPT-LATER ATTACK DETECTION

DOCUMENT 1: APPLICATION DATA SHEET (ADS)

Form PTO/ADS/14

APPLICANT INFORMATION

Applicant 1:

- Legal Name: Rutherford, Brian James
- Given Name: Brian James
- Family Name: Rutherford
- City of Residence: Wimberley
- State/Country of Residence: Texas, United States
- Country of Citizenship: United States
- Applicant Authority: Inventor
- Applicant is assignee of entire interest: Yes

APPLICATION INFORMATION

Application Type: Provisional Application for Patent **Subject Matter:** Utility **Title of Invention:** QUANTUM BENCHMARK-DRIVEN TEMPORAL CORRELATION SYSTEM FOR HARVEST-NOW-DECRYPT-LATER ATTACK DETECTION THROUGH MATHEMATICAL WOVEN RESPONSIVE ADAPTIVE SWARM PLATFORM WITH HIERARCHICAL AI AGENT COMMUNICATION PROTOCOLS

Attorney Docket Number: BJR-MWRASP-003-PROV **Entity Status:** Micro Entity

CORRESPONDENCE INFORMATION

Correspondence Address:

- Customer Number: [To be assigned]
- Name: Brian James Rutherford
- Address:
  - Street: [Your Street Address]

- City: Wimberley
- State: Texas
- ZIP: 78676
- Country: United States

- Telephone: [Your Phone Number]
- Email: [Your Email]

DOCUMENT 2: SPECIFICATION

QUANTUM BENCHMARK-DRIVEN TEMPORAL CORRELATION SYSTEM FOR HARVEST-NOW-DECRYPT-LATER ATTACK DETECTION THROUGH MATHEMATICAL WOVEN RESPONSIVE ADAPTIVE SWARM PLATFORM WITH HIERARCHICAL AI AGENT COMMUNICATION PROTOCOLS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] Not Applicable.

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH

[0002] Not Applicable.

FIELD OF THE INVENTION

[0003] The present invention relates to defensive cybersecurity platforms utilizing quantum computing benchmark correlation for threat detection, specifically systems that translate real-time quantum performance metrics (qubit counts, coherence times, error rates) into network traffic risk scores through a Mathematical Woven Responsive Adaptive Swarm Platform (MWRASP Total) employing hierarchical AI agent communication protocols for enterprise security.

BACKGROUND OF THE INVENTION

[0004] Current quantum security approaches fail to correlate specific quantum computing benchmarks with network traffic patterns. While post-quantum cryptography standards address future encryption, no existing systems translate quantum performance metrics (qubits, coherence times, error rates) into actionable risk scores for current network traffic. This creates a critical gap where organizations cannot assess which encrypted data faces imminent decryption risk based on actual quantum computing progress.

[0005] Existing multi-tier security architectures, including Samsung's six-tier BDI system (US20200234166), lack quantum-specific communication protocols and fail to dynamically adjust consensus mechanisms based on quantum advancement indicators. Traditional Byzantine fault-tolerant systems operate with static thresholds that cannot adapt to the exponentially changing quantum threat landscape.

[0006] Current swarm-based security platforms employ simple aggregation mechanisms without mathematical weaving of AI agent responses. They lack the sophisticated data fusion required to correlate quantum benchmarks with network patterns, resulting in inability to detect harvest-now-decrypt-later (HNDL) attacks before quantum computers achieve cryptographic relevance.

BRIEF SUMMARY OF THE INVENTION

[0007] The present invention provides a quantum benchmark-driven temporal correlation system within the MWRASP (Total) framework that uniquely translates specific quantum computing metrics (qubit counts, coherence times, gate fidelities, error rates) into network traffic risk scores through a novel mathematical mapping mechanism. The system employs hierarchical AI agent communication protocols with quantum-influenced decision fusion, fundamentally differentiating from static multi-tier architectures.

[0008] The invention's mathematical weaving architecture synchronizes AI agent responses through tensor product operations, eigenvalue decomposition, and quantum-inspired entanglement measures, creating a responsive adaptive swarm that evolves with quantum computing advancement.

DETAILED DESCRIPTION OF THE INVENTION

Core System Architecture [0009] The invention comprises three fundamental innovations operating within the defensive MWRASP (Total) cybersecurity platform:

1. Quantum Benchmark Temporal Correlation Engine (QBTCE)
2. Hierarchical AI Agent Communication Protocol System (HACPS)
3. Mathematical Woven Response Architecture (MWRA)

QUANTUM BENCHMARK TEMPORAL CORRELATION ENGINE (QBTCE) [0010] The QBTCE implements a novel mapping mechanism that translates specific quantum computing benchmarks into network traffic risk scores through multi-dimensional correlation using the formula:

risk = Q_factor × C_factor × T_overlap × exp(-years_to_threat/10)

Where:

- Q_factor represents qubit sufficiency (logical qubit ratio to Shor's requirements)
- C_factor represents coherence sufficiency (T1/T2 harmonic mean adequacy)

- T_overlap represents temporal alignment between data lifetime and quantum capability

HIERARCHICAL AI AGENT COMMUNICATION PROTOCOL SYSTEM (HACPS) [0011] The HACPS implements quantum-specific communication protocols with four quantum-optimized tiers:

1. **Sentinel AI Agents:** Edge detection with quantum benchmark integration
2. **Analyst AI Agents:** Pattern correlation with quantum timeline integration
3. **Strategist AI Agents:** Strategic planning with quantum projection
4. **Commander AI Agents:** Executive coordination with quantum awareness

Dynamic Consensus Adjustment: [0012] Consensus thresholds dynamically adjust according to: adjusted_threshold = base_threshold × (1 - proximity_factor × 0.3) × (1 + qubit_factor × 0.1) × error_factor × (1 + coherence_factor × 0.05)

MATHEMATICAL WOVEN RESPONSE ARCHITECTURE (MWRA) [0013] The MWRA implements sophisticated mathematical operations for AI agent response synchronization through:

- Tensor product operations computing woven responses via Kronecker products
- Entanglement entropy calculation using Von Neumann entropy
- Eigenvalue decomposition for optimal response strategy selection
- Phase-locked synchronization using Kuramoto dynamics with quantum coupling

CLAIMS

What is claimed is:

1. A quantum benchmark-driven temporal correlation system for detecting harvest-now-decrypt-later attacks, comprising: a quantum benchmark temporal correlation engine that translates specific quantum computing metrics including logical qubit counts, coherence times (T1/T2), gate fidelities, and error rates into network traffic risk scores through a mathematical mapping mechanism incorporating Shor's algorithm requirements; a hierarchical AI agent communication protocol system with four quantum-optimized tiers implementing dynamic consensus thresholds that adjust based on quantum advancement metrics; a mathematical woven response architecture employing tensor product operations, eigenvalue decomposition, and phase-locked synchronization mechanisms to weave AI agent responses into coordinated defensive actions; and integration within a Mathematical Woven Responsive Adaptive Swarm Platform (MWRASP Total) for enterprise-wide quantum threat detection.
2. The system of claim 1, wherein said quantum benchmark temporal correlation engine implements a risk transformation formula: risk = Q_factor × C_factor × T_overlap × exp(-years_to_threat/10), where

Q_factor represents qubit sufficiency, C_factor represents coherence sufficiency, and T_overlap represents temporal alignment.

3. The system of claim 1, wherein said hierarchical AI agent communication protocol system comprises Sentinel AI agents, Analyst AI agents, Strategist AI agents, and Commander AI agents, each implementing quantum-specific processing protocols.
4. The system of claim 1, wherein consensus thresholds dynamically adjust according to: adjusted_threshold = base_threshold × (1 - proximity_factor × 0.3) × (1 + qubit_factor × 0.1) × error_factor × (1 + coherence_factor × 0.05).
5. The system of claim 1, wherein said mathematical woven response architecture implements tensor product operations computing woven responses through iterative Kronecker products of AI agent response tensors.

ABSTRACT

A quantum benchmark-driven temporal correlation system for detecting harvest-now-decrypt-later (HNDL) attacks that uniquely translates specific quantum computing metrics (qubit counts, coherence times T1/T2, gate fidelities, error rates) into network traffic risk scores through novel mathematical mapping. The system implements hierarchical AI agent communication protocols with four quantum-optimized tiers using dynamic consensus thresholds adjusted by quantum advancement metrics. The Mathematical Woven Responsive Adaptive Swarm Platform (MWRASP Total) employs tensor product operations, eigenvalue decomposition, and phase-locked synchronization to weave AI agent responses into coordinated defensive actions, enabling proactive enterprise defense against quantum decryption threats through mathematically rigorous response coordination.

DOCUMENT 3: FEE TRANSMITTAL FORM

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

TO: Commissioner for Patents P.O. Box 1450 Alexandria, VA 22313-1450

Inventor(s): Brian James Rutherford

Title: QUANTUM BENCHMARK-DRIVEN TEMPORAL CORRELATION SYSTEM FOR HARVEST-NOW-DECRYPT-LATER ATTACK DETECTION THROUGH MATHEMATICAL WOVEN RESPONSIVE ADAPTIVE SWARM PLATFORM WITH HIERARCHICAL AI AGENT COMMUNICATION PROTOCOLS

FEES CALCULATION:

Fee Description	Fee Code	Quantity	Fee Amount
Provisional Filing Fee (Micro Entity)	1031	1	$65.00
TOTAL FEES DUE:			**$65.00**

Entity Status: Micro Entity **Payment Method:** Credit Card / Electronic Funds Transfer

---

DOCUMENT 4: MICRO ENTITY STATUS CERTIFICATION

CERTIFICATION OF MICRO ENTITY STATUS

I hereby certify that I qualify for micro entity status under 37 CFR 1.29 and that:

1. I qualify as a small entity under 37 CFR 1.27
2. Neither I, nor any individual or entity to whom I am obligated to assign the invention, nor any individual or entity who has a proprietary interest in the application has been named as an inventor on more than four previously filed patent applications
3. Neither I, nor any individual or entity to whom I am obligated to assign the invention, nor any individual or entity who has a proprietary interest in the application had gross income in the previous calendar year exceeding three times the median household income as reported by the Bureau of the Census
4. Neither I, nor any individual or entity to whom I am obligated to assign the invention, nor any individual or entity who has a proprietary interest in the application has assigned, granted, conveyed, or licensed, and is not under an obligation to assign, grant, convey, or license, any rights in the invention to any entity that, in the previous calendar year, had gross income exceeding three times the median household income

Signature: _____ **Date:** _____ Brian James Rutherford, Inventor

---

DOCUMENT 5: FILING INSTRUCTIONS

STEP-BY-STEP FILING PROCESS

BEFORE FILING:

1. **Verify Micro Entity Status:** Ensure you meet all requirements under 37 CFR 1.29
2. **Prepare Electronic Files:** Save all documents as PDF files
3. **Create USPTO Account:** Register at MyUSPTO portal if not already done

FILING THROUGH EFS-WEB:

1. **Login to EFS-Web:** Go to https://efs-web.uspto.gov
2. **Select Application Type:** Choose "Provisional Application for Patent"
3. **Upload Documents in Order:**
   - Application Data Sheet (ADS)
   - Specification Document
   - Fee Transmittal Form
   - Micro Entity Certification
4. **Calculate Fees:** Verify $65.00 total fee
5. **Submit Payment:** Use credit card or bank transfer
6. **Review and Submit:** Check all information before final submission

POST-FILING CHECKLIST:

- [ ] Save filing receipt with application number
- [ ] Calendar 12-month deadline for non-provisional filing
- [ ] Begin prototype development documentation
- [ ] Consider filing related applications for comprehensive protection

IMPORTANT DEADLINES:

- **Priority Date:** Date of this provisional filing
- **Non-Provisional Deadline:** 12 months from filing date
- **PCT Filing Deadline:** 12 months from filing date (if seeking international protection)

NEXT STEPS:

1. **Document Development:** Maintain detailed records of all improvements and developments
2. **Prior Art Monitoring:** Continue searching for relevant prior art
3. **Market Analysis:** Assess commercial potential and licensing opportunities
4. **Non-Provisional Preparation:** Begin preparing comprehensive non-provisional application 8-10 months after filing

---

DOCUMENT 6: REQUIRED SIGNATURES AND CERTIFICATIONS

INVENTOR DECLARATION (For Provisional Applications)

I hereby declare that:

- I am the inventor of the subject matter which is claimed and for which a patent is sought
- I have reviewed and understand the contents of the specification including the claims
- I acknowledge the duty to disclose information which is material to patentability

Inventor Signature: _____
Date: _____
Brian James Rutherford

CORRESPONDENCE AUTHORIZATION

I hereby authorize correspondence regarding this application to be conducted via:

- Email: [Your Email Address]
- Phone: [Your Phone Number]
- Physical Mail: [Your Complete Address]

Signature: _____ **Date:** _____

TOTAL FILING PACKAGE SUMMARY

Documents Included:

1. ✓ Application Data Sheet (ADS)
2. ✓ Complete Specification with Claims and Abstract
3. ✓ Fee Transmittal Form
4. ✓ Micro Entity Certification
5. ✓ Inventor Declaration
6. ✓ Filing Instructions

Total Filing Fee: $65.00 (Micro Entity Rate) **Expected Processing Time:** 2-4 weeks for initial filing receipt
Priority Date Established: Date of electronic filing submission

This complete package provides everything needed for immediate USPTO provisional patent application filing through EFS-Web system.