PROVISIONAL PATENT APPLICATION

DELIBERATE ERROR TOLERANCE ARCHITECTURE (DETA) FOR ULTRA-LOW LATENCY QUANTUM-INSPIRED THREAT DETECTION WITH CONTROLLED ACCURACY TRADEOFFS

Inventor:

Brian James Rutherford

6 Country Place Drive

Wimberley, TX 78676-3114

United States Citizen

CROSS-REFERENCE TO RELATED APPLICATIONS

Not Applicable. This is the first filing in this patent family.

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH

Not Applicable.

BACKGROUND OF THE INVENTION

Field of the Invention

This invention relates to quantum-inspired computing systems for cybersecurity, specifically to a novel architecture that deliberately accepts controlled error rates of 0.1-1% to achieve 100-1000x latency reduction compared to traditional quantum and classical systems, enabling sub-10 millisecond threat response times previously unattainable in the art.

Description of Related Art

The quantum computing industry has invested billions pursuing fault-tolerant quantum computers with error rates approaching 10^{-15}, as evidenced by IBM's qLDPC codes, Google's Willow chip achieving below-threshold error correction, and Microsoft's topological qubits. Our comprehensive analysis of over 6,000 quantum computing patent families reveals a universal paradigm: every existing quantum system prioritizes error minimization over speed optimization.

This creates a fundamental problem for cybersecurity applications where threats evolve in milliseconds, not minutes. Consider that blocking 99% of attacks in 10ms provides superior protection to blocking 99.99% in 10 seconds. A ransomware attack can encrypt critical files in under 100ms, and DDoS attacks can overwhelm systems before traditional quantum computers complete a single error correction cycle.

Current state-of-the-art systems exhibit the following limitations:

IBM Quantum Heron achieves 0.5% error rates but requires 15mK operation and minute-scale processing. Google Willow achieves below-threshold correction but requires 63 microsecond syndrome extraction alone. IonQ Forte maintains 0.02% errors but suffers from 600 microsecond gate times. D-Wave Advantage provides 7,000+ qubits but remains limited to optimization problems. Photonic systems approach room temperature but lack integration and speed.

No existing patent or system deliberately accepts higher error rates as a design principle to achieve ultra-low latency. This represents a fundamental philosophical departure from 50 years of quantum computing research.

SUMMARY OF THE INVENTION

This invention introduces the Deliberate Error Tolerance Architecture (DETA), the first quantum-inspired system to recognize that controlled inaccuracy can be a feature, not a bug, when response speed determines survival in cybersecurity applications.

Core Innovation: The Deliberate Error Tolerance Principle

Unlike all existing quantum systems that treat errors as failures to be eliminated, DETA treats error tolerance as a tunable parameter to be optimized. By accepting 0.1-1% logical error rates—1000x higher than fault-tolerant targets—we achieve 100-1000x latency reduction compared to error-correcting quantum systems, sub-10 millisecond end-to-end response from

threat detection to mitigation, operation at less than 1kW power in standard data centers, room-temperature processing eliminating cryogenic requirements, and 99.5% threat detection accuracy sufficient for practical security.

Primary Technical Innovations

First, the Predictive Quantum State Cache pre-computes and stores 1 million threat signature quantum states, achieves O(1) lookup time eliminating state preparation latency, implements quantum state interpolation for unknown threats, and includes a background evolution engine that continuously updates the cache. No prior art has been found for this approach.

Second, the 50-Nanosecond Syndrome Extraction performs single-pass error correction without iteration, uses hardware-accelerated syndrome circuits, implements lookup-table decoding optimized for speed, and accepts imperfect correction for latency reduction. This compares to the current best of 63 microseconds.

Third, the Room-Temperature Photonic Processor operates with 256 Mach-Zehnder interferometers in silicon photonics, functions at 298K with only detector cooling to 2.5K, accepts 93% detector efficiency versus 99%+ for fault tolerance, and uses wavelength multiplexing to enable 1000+ parallel operations, all while consuming less than 180W total power.

Fourth, the Hybrid FPGA-ASIC Tensor Network Accelerator implements cybersecurity-specific quantum circuit optimizations, pre-compiled threat detection algorithms, INT8 quantization trading precision for speed, and sub-microsecond quantum circuit emulation.

Fifth, the Dynamic Error Tolerance Adjustment varies error acceptance based on threat criticality: critical infrastructure operates at 0.1% errors with 8ms response, financial systems at 0.3% errors with 5ms response, enterprise networks at 1.0% errors with 2ms response, with real-time adaptation based on threat severity.