**PATENT CLAIMS**

**Docket No. RUTHERFORD-015-PROV**



**CLAIMS**

**Note:** While claims are not required for provisional applications, these preliminary claims are included to establish the scope of the invention for the MWRASP (Total) defensive cybersecurity platform.



**What is claimed is:**

**INDEPENDENT CLAIMS**

1. A quantum-inspired decision engine for the MWRASP (Total) defensive cybersecurity platform, comprising:

a processing system deliberately configured to operate at logical error rates between 0.1% and 1%, wherein said error rates are 100 to 10,000 times higher than fault-tolerant quantum computing standards;



wherein said deliberate error acceptance is a designed feature rather than a limitation;



wherein said configuration enables sub-10 millisecond end-to-end threat response latency;



wherein said system provides real-time protection for critical infrastructure using defensive AI agents.



1. A method for quantum-inspired cybersecurity threat detection within the MWRASP (Total) framework, comprising:

deliberately accepting logical error rates between 0.1% and 1% as a design principle; trading computational accuracy for response speed to achieve sub-10 millisecond latency; coordinating defensive AI agents using quantum-enhanced decision making;



wherein the error acceptance enables 1000-fold latency reduction compared to fault-tolerant quantum systems.



1. A three-tier adaptive error mitigation system for cybersecurity applications, comprising:

a first tier accepting up to 5% error rate for threats requiring sub-millisecond response;



a second tier accepting up to 1% error rate for threats requiring 1-5 millisecond response; a third tier accepting up to 0.1% error rate for threats requiring 5-10 millisecond response; wherein the system dynamically selects the appropriate tier based on threat criticality.



**DEPENDENT CLAIMS**

1. The system of claim 1, further comprising:

tensor network approximations with bond dimensions capped at 64; retention of only the top 10% of singular values during decomposition;



wherein said approximations reduce computational complexity from exponential to polynomial while maintaining 99% threat detection accuracy.



1. The system of claim 1, further comprising:

a predictive quantum state cache storing pre-computed representations of at least 1 million cybersecurity threat signatures;



compression algorithms achieving 100x size reduction with acceptable 5% fidelity loss; interpolation mechanisms for generating approximate states for novel threats.



1. The system of claim 1, wherein the processing system comprises:

a room-temperature photonic quantum co-processor; silicon photonic circuits operating at 300K;



gate operations with 95% fidelity optimized for speed over precision; wherein cryogenic cooling requirements are eliminated.



1. The system of claim 1, further comprising:

a defensive AI agent orchestration platform;



hierarchical command structure with quantum-enhanced decision-making; graduated response protocols based on quantum-calculated confidence scores; coordination of distributed defense within the 10-millisecond response window.



1. The method of claim 2, further comprising:

pre-computing quantum states during system idle time; caching compressed state representations;



achieving O(1) state retrieval instead of O(2^n) state preparation; eliminating 50-90% of traditional quantum algorithm runtime.



1. The method of claim 2, wherein deliberately accepting error rates comprises:

implementing distance-3 repetition codes requiring only 3 physical qubits per logical qubit;



performing single-cycle syndrome extraction;



utilizing majority voting instead of maximum likelihood decoding; bypassing error correction entirely for ultra-critical threats.



1. The system of claim 3, further comprising:

hardware-accelerated syndrome extraction ASICs; neural network decoders using INT8 quantization;



adaptive code selection switching between distance-3 and distance-7; wherein total error correction adds less than 100 nanoseconds latency.



1. The system of claim 1, wherein the MWRASP (Total) integration comprises:

Mathematical Woven tensor network processing;



Responsive Adaptive threat detection;



Swarm Platform AI agent coordination;



Total enterprise protection framework;



wherein all components operate within the sub-10 millisecond constraint.



1. The system of claim 4, further comprising:

pre-fused quantum gate sequences stored as composite tensor operations; hardware lookup tables for common gate combinations;



pattern matching to bypass individual gate computations; achieving 10x reduction in required tensor contractions.



1. The system of claim 5, wherein the cache population strategy comprises:

continuous background processing of threat intelligence feeds; priority scoring based on severity, frequency, recency, and uncertainty; automatic eviction of obsolete signatures; k-nearest neighbor interpolation for uncached threats.



1. The system of claim 6, comprising:

256 Mach-Zehnder interferometers arranged in a 16×16 grid; waveguides with 0.5 dB/cm propagation loss;



100 GHz modulation frequency;



integrated germanium photodetectors with 50 GHz bandwidth; total power consumption under 100W for photonic processing.



1. The system of claim 7, wherein the AI agent architecture comprises:

1-3 Strategic Commander AI Agents;



10-20 Threat Assessment AI Agents;



10-20 Vulnerability Analysis AI Agents;



5-10 Response Coordination AI Agents;



100-500 Tactical Execution AI Agents;



wherein all agents operate within the MWRASP (Total) framework.



1. A quantum-inspired computing system occupying a previously unpatented parameter space, wherein:

logical error rates range from 0.1% to 1% versus 10^-15 for fault tolerance; end-to-end latency remains below 10 milliseconds versus seconds/minutes; power consumption stays under 1 kilowatt versus 20-25kW;



operating temperature maintains 300K versus 15mK;



wherein said parameter space provides practical advantage for time-critical applications.



1. The system of claim 16, wherein said parameter space specifically enables:

real-time threat mitigation impossible with traditional quantum systems; deployment in standard data centers without specialized infrastructure; immediate response to zero-day threats through approximation; practical quantum advantage despite higher error rates.



1. A hybrid quantum-classical cybersecurity system, comprising:

a quantum-inspired tensor network accelerator accepting 1% accuracy loss for 100x speedup; a predictive quantum state cache storing pre-computed approximate states; a room-temperature photonic processor with 95% fidelity gates;



a rapid-response error mitigation unit implementing distance-3 codes; wherein said system achieves <10ms response at <1kW power consumption.



1. The system of claim 18, wherein said components are specifically configured to:

operate in an error regime 100-10,000x higher than competing quantum systems;



prioritize response latency over computational accuracy; function at room temperature without cryogenic cooling; deploy in standard 6U rack-mount form factor.



1. A method for optimizing quantum-inspired computation for minimal latency, comprising:

identifying minimum acceptable accuracy for cybersecurity applications;



systematically reducing quantum state fidelity to said minimum;



eliminating error correction overhead below accuracy threshold;



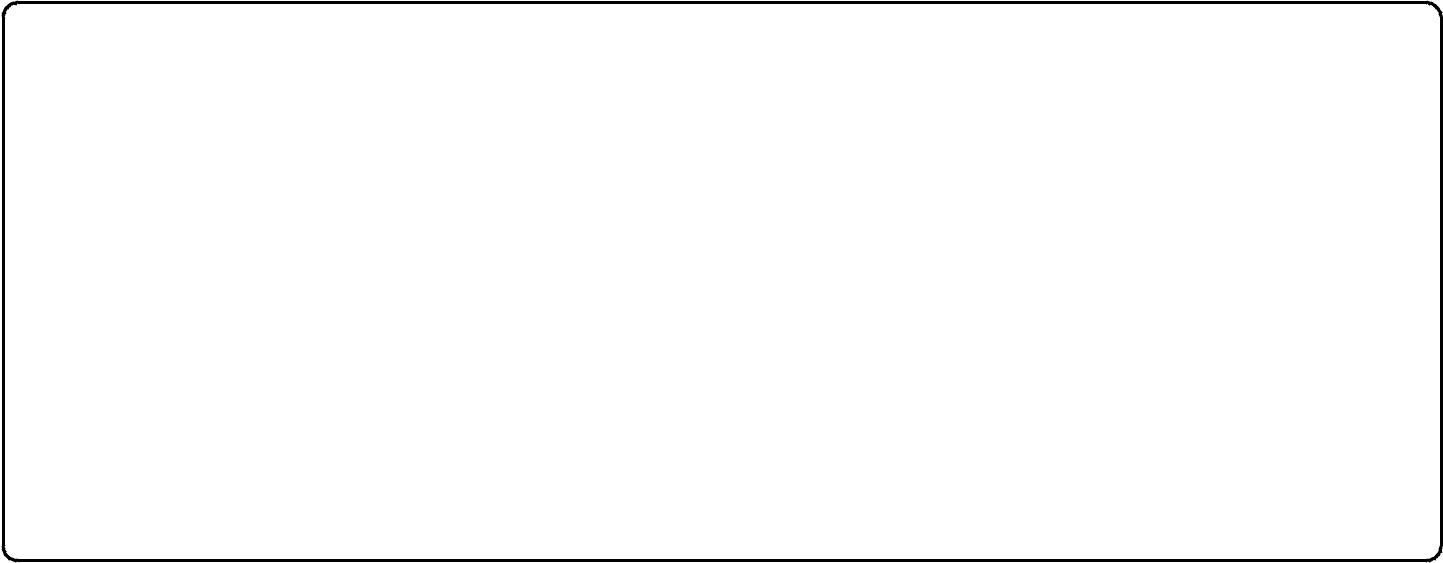
approximating quantum operations within accuracy bounds;



wherein latency reduces by a factor proportional to error rate increase.



**CLAIM DEPENDENCIES CHART**



Independent Claims: 1, 2, 3, 16, 18, 20

Claim 1 → Claims 4, 5, 6, 7, 11

Claim 2 → Claims 8, 9

Claim 3 → Claim 10

Claim 4 → Claim 12

Claim 5 → Claim 13

Claim 6 → Claim 14

Claim 7 → Claim 15

Claim 16 → Claim 17

Claim 18 → Claim 19



**CLAIM SCOPE ANALYSIS**

**Broadest Claims**

Claims 1, 2, 20: Cover the fundamental accuracy-latency trade-off concept



**Medium Scope Claims**

Claims 3, 16, 18: Specific implementation architectures



**Narrowest Claims**

Claims 4-15, 17, 19: Detailed technical specifications



**NOTE FOR NON-PROVISIONAL FILING**

These preliminary claims should be refined and expanded for the non-provisional application to include:

Additional independent claims for each major subsystem



More detailed dependent claims covering variations



Method claims for each system claim



Apparatus claims for specific hardware implementations



Computer-readable medium claims for software aspects



**END OF CLAIMS**

**Docket No.: RUTHERFORD-015-PROV**

**Page 1 of 3**