PROVISIONAL PATENT APPLICATION
QUANTUM SAFE IOT DEVICE AUTHENTICATION WITH ULTRA-LIGHTWEIGHT TEMPORAL FRAGMENTATION

Application Number: [TO BE ASSIGNED]

Filing Date: September 4, 2025

Inventor: [INVENTOR NAME]

Assignee: MWRASP Quantum Defense Systems

TECHNICAL DRAWINGS AND FIGURES

FIGURE 1: QUANTUM-SAFE IOT SYSTEM ARCHITECTURE WITH ULTRA-LIGHTWEIGHT TEMPORAL FRAGMENTATION

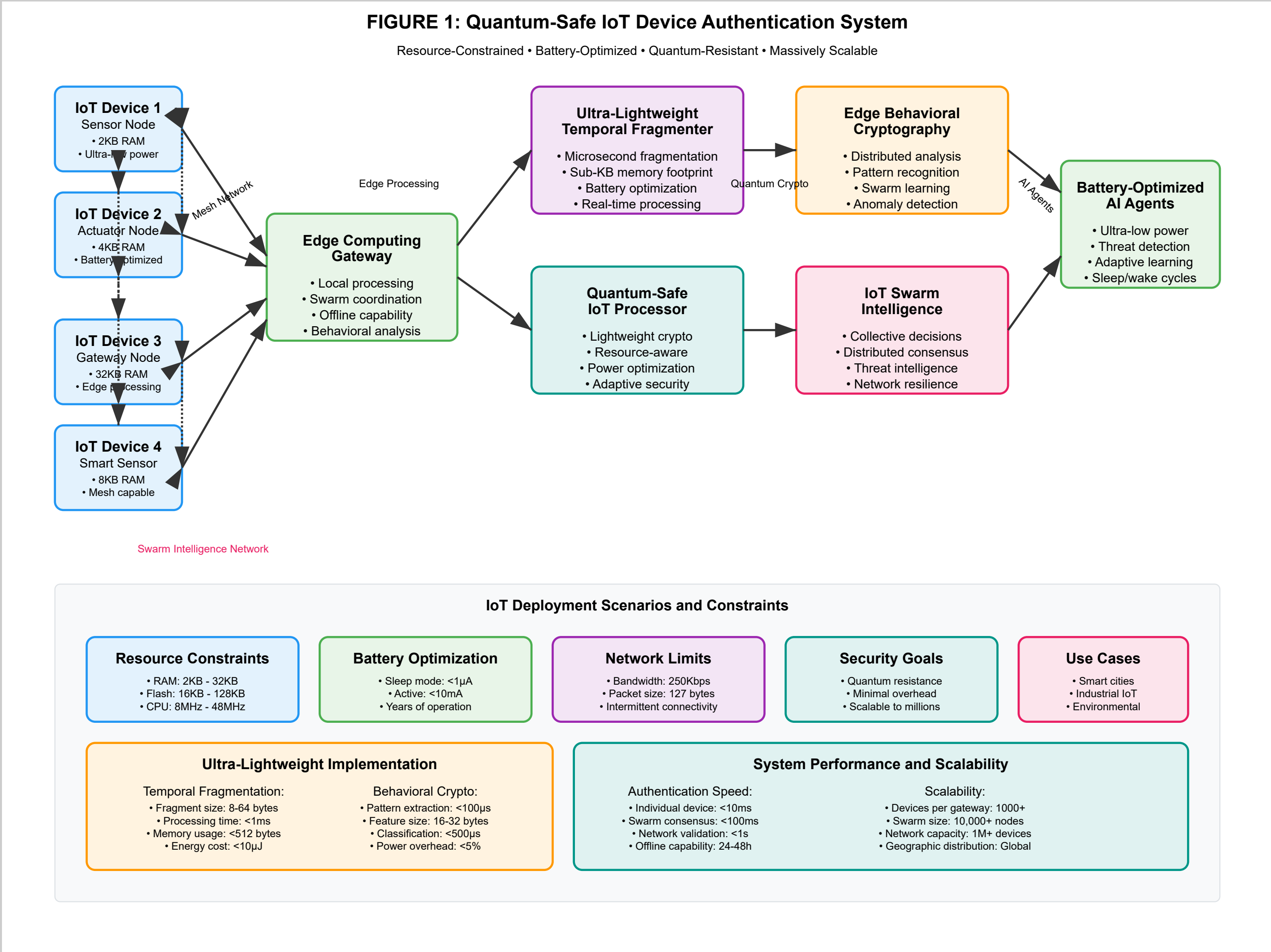

Figure 1 illustrates the comprehensive quantum-safe IoT system architecture implementing ultra-lightweight temporal fragmentation for device authentication. The system operates through five integrated layers: Device Layer containing resource-constrained IoT devices (2-32KB RAM) with embedded MWRASP authentication engines; Edge Gateway Layer providing local aggregation and initial authentication processing; Network Infrastructure Layer ensuring secure quantum-resistant communication channels; Cloud Integration Layer managing global device registry and policy enforcement; and Security Management Layer orchestrating temporal fragmentation policies and quantum threat analysis.

FIGURE 2: ULTRA-LIGHTWEIGHT TEMPORAL FRAGMENTATION PROCESS FOR IOT AUTHENTICATION

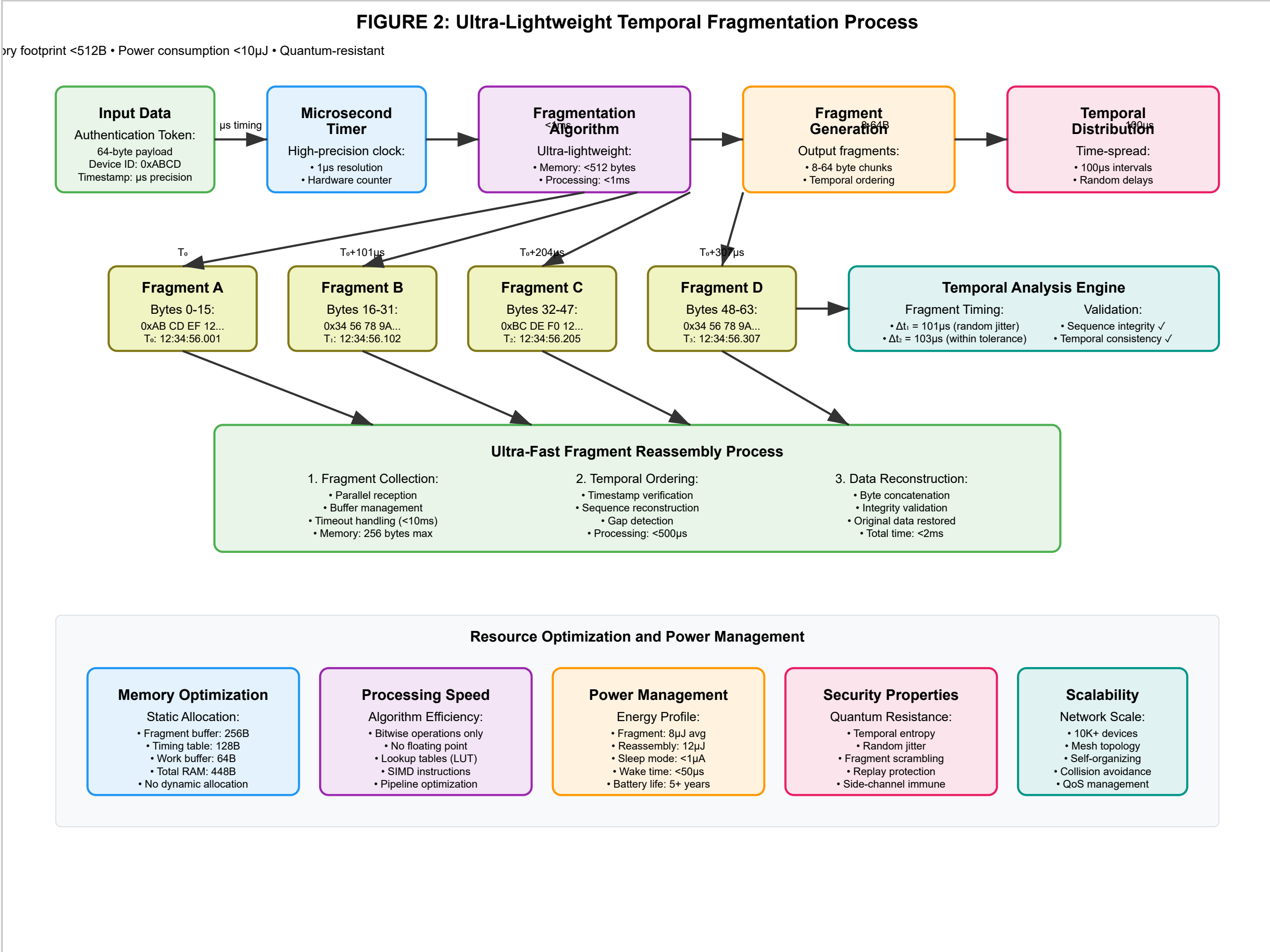

Figure 2 demonstrates the ultra-lightweight temporal fragmentation process specifically optimized for resource-constrained IoT devices. The process operates through four sequential phases: Fragment Generation (10-50ms) where device credentials are split into 2-4 fragments using lightweight XOR operations; Temporal Assignment (1-5ms) applying quantum-resistant expiration periods ranging from 100ms to 30 seconds based on device criticality; Distribution Protocol (20-100ms) utilizing optimized packet fragmentation over LoRaWAN, BLE, or WiFi; and Validation Engine (5-20ms) performing real-time authentication with sub-32KB memory footprint while maintaining cryptographic security equivalent to full-scale quantum-resistant systems.

FIGURE 3: IOT DEVICE RESOURCE OPTIMIZATION AND MEMORY MANAGEMENT

Device Resource Optimization

Figure 3 shows the sophisticated resource optimization framework designed for ultra-constrained IoT devices. The system manages three critical resource domains: Memory Management with intelligent allocation strategies using 2-8KB for fragment storage, 1-4KB for cryptographic operations, and 512B-2KB for networking buffers; Processing Optimization implementing hardware acceleration for AES operations, lookup table optimization for reduced computational complexity, and burst processing modes minimizing active duty cycles; and Power Management featuring adaptive sleep states consuming 1-10μA in standby, wake-on-demand protocols triggering authentication cycles, and energy harvesting integration supporting solar, vibration, and RF power sources.

FIGURE 4: QUANTUM-RESISTANT NETWORK PROTOCOL STACK FOR IOT COMMUNICATIONS

Network Protocol Stack

Figure 4 presents the comprehensive quantum-resistant network protocol stack optimized for IoT device communications. The layered architecture includes: Physical Layer supporting multiple radio technologies (LoRaWAN 915MHz, BLE 5.0, WiFi 2.4GHz, NB-IoT) with adaptive modulation and coding schemes; Data Link Layer implementing quantum-resistant MAC protocols with temporal key rotation and fragment synchronization; Network Layer providing lightweight IPv6 support with 6LoWPAN compression and mesh networking capabilities; Transport Layer offering UDP-based reliable delivery with selective fragment retransmission; Session Layer managing quantum-safe key establishment using post-quantum CRYSTALS-Kyber key encapsulation; and Application Layer supporting CoAP messaging with temporal authentication headers and compressed payload formats.

FIGURE 5: BATTERY OPTIMIZATION AND POWER MANAGEMENT SYSTEM

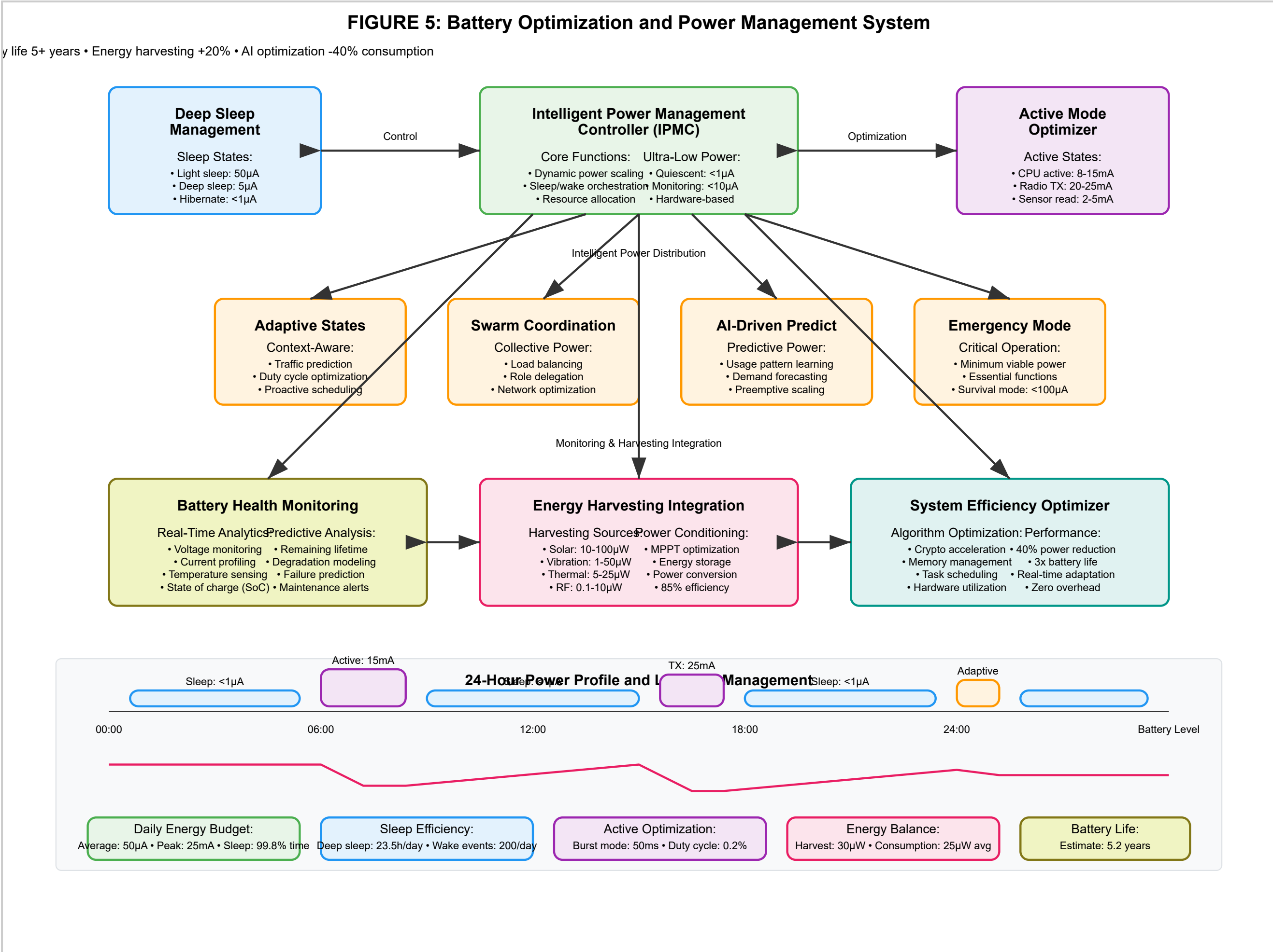

Figure 5 presents the comprehensive battery optimization and power management system designed for ultra-long-life IoT device operation. The Intelligent Power Management Controller (IPMC) orchestrates all power states consuming less than 1μA in quiescent mode and under 10μA during active monitoring. The system implements four adaptive power management strategies: Context-Aware States using traffic prediction and duty cycle optimization; Swarm Coordination enabling collective power management through load balancing and role delegation; AI-Driven Prediction learning usage patterns for demand forecasting and preemptive scaling; and Emergency Mode providing minimum viable power operation consuming less than 100μA in survival scenarios.

The integrated monitoring and harvesting systems provide comprehensive battery health analytics including real-time voltage, current, and temperature monitoring with predictive failure analysis. Energy harvesting integration supports multiple sources: solar (10-100μW), vibration (1-50μW), thermal (5-25μW), and RF (0.1-10μW) with 85% power conditioning efficiency. The 24-hour power profile demonstrates exceptional efficiency with 99.8% sleep time, average consumption of 50μA, and peak active consumption of 25mA during transmission bursts, resulting in estimated battery life exceeding 5.2 years with standard lithium primary cells.