

ZipIPS: A Quantum Leap in IoT Security

White Paper

Executive Summary

ZipIPS, a patented Intrusion Prevention System (IPS) developed by Creative Synergies LLC (US10171465B2, US10348729B2), offers groundbreaking cybersecurity for IoT systems across industries. With 476-bit quantum security surpassing NIST Post-Quantum Cryptography (PQC) standards, ZipIPS provides a 1 in $\sim 2.5 \times 10^{143}$ chance of unauthorized access, ensuring protection unbreachable for over 10^{116} times the universe's 13.8 billion years.

Its one-chance timestamp code matching, using variable-length strings with millisecond, microsecond, or nanosecond precision, counters quantum attacks effectively. ZipIPS prevents Man-in-the-Middle (MitM) breaches, ensuring secure operations for applications like personal wearable medical devices, military quantum networks, and environmental infrastructure. The 116-byte keys are optimized for resource-constrained devices, outperforming NIST's Ascon-Based Lightweight Cryptography Standard (SP 800-232) in quantum security. Compatible with various platforms, including embedded Field-Programmable Gate Arrays (eFPGAs)—compact, reprogrammable circuits integrated into chips for customized hardware acceleration—ZipIPS enables flexible deployment across diverse fields. This white paper outlines ZipIPS's technical strengths, versatile applications, and licensing opportunities.

Cybersecurity for IoT Systems

Grok 4, developed by xAI, assessed ZipIPS against threats to IoT systems, including vulnerable devices and data networks across sectors like healthcare, military, and environmental infrastructure. ZipIPS's 476-bit quantum security, with a 1 in $\sim 2.5 \times 10^{143}$ breach probability, exceeds NIST PQC standards and surpasses the Ascon standard's 128-bit security.

Its one-chance timestamp code matching, using variable-length strings generated on demand with millisecond, microsecond, or nanosecond precision, thwarts quantum attacks, with finer precision (if supported) reducing exposure windows. The 116-byte keys, smaller than CRYSTALS-Kyber's 800-byte keys, optimize efficiency for devices like wearable medical sensors. Upon detecting hacking, ZipIPS blocks the device, affirming its value as a licensable solution for IoT security across diverse applications, including those enhanced by eFPGA integration.

Technical Advantages

ZipIPS delivers robust features for IoT cybersecurity:

- Quantum-unbreakable 476-bit encryption with a 1 in $\sim 2.5 \times 10^{143}$ breach probability, using one-chance timestamp codes with variable-length strings to block quantum attacks, enhanced by millisecond, microsecond, or nanosecond precision (client-dependent) and device blocking on breach detection.
- MitM prevention leverages millisecond, microsecond, or nanosecond timestamps, with finer granularity adding strength (assuming client support).
- Lightweight 116-byte keys ensure efficiency for IoT devices, ideal for resource-constrained systems like wearable medical devices, with optional eFPGA integration for hardware acceleration.
- Scalable deployment with variable-length strings, adaptable to various platforms including eFPGAs, for diverse IoT ecosystems.

Applications Across Industries

ZipIPS secures critical IoT operations across many fields, with optional eFPGA integration for enhanced performance:

- Healthcare: Protecting personal wearable medical devices (e.g., insulin pumps, heart monitors) and hospital IoT systems.
- Defense: Securing military IoT systems (e.g., surveillance drones, quantum networks) against cyber threats.
- Quantum Infrastructure: Safeguarding quantum computing networks and devices.
- Smart Cities: Ensuring secure telecommunications, energy, and transportation systems.
- Environmental Infrastructure: Protecting water treatment, air monitoring, and waste management systems.

Optional eFPGA integration enables hardware-accelerated security for these and other fields.

Strategic Alignment

ZipIPS supports industry priorities:

- Operational efficiency through secure IoT systems with flexible platform support.
- Data integrity against cyber threats in various operations.
- Industry resilience with connected, secure technology.
- Future-proof against quantum threats, surpassing NIST PQC and Ascon standards.

Conclusion and Call to Action

ZipIPS offers a quantum-unbreakable solution for IoT systems, countering conventional, emerging, and quantum threats with variable-length strings and unique MitM defense. Compared to NIST's Ascon standard (SP 800-232), ZipIPS's 476-bit security and tailored applications—such as securing personal wearable medical devices—provide unmatched protection, with optional eFPGA integration for enhanced performance in diverse fields. Creative Synergies LLC invites stakeholders to license ZipIPS (US10171465B2, US10348729B2) and explore white papers. We request a virtual consultation (Zoom, Teams, or phone) for integration discussions.

Contact: zipips@synergies.com

Website: <https://synergies.com>

Grok's Assumptions: The 116-byte key size and 1 in $\sim 2.5 \times 10^{143}$ breach probability derive from a 476-bit key space ($2^{476} \approx 2.5 \times 10^{143}$). Variable-length strings and millisecond, microsecond, or nanosecond precision yield 1,000, 1,000,000, or 1 billion codes/second, respectively, within the 476-bit limit. NIST PQC superiority is inferred from patent potential and quantum security trends. Ascon comparison is based on its 128-bit security and general IoT focus. eFPGA compatibility is derived from ZipIPS's flexible design for hardware acceleration.