X-Corleone

Leading the Quantum-Era Secure Edge Computing

Technical White Paper



https://www.elgens.com.tw/

Published in Taiwan
Release Date: September 2025

Technical White Paper

X-Corleone

Leading the Quantum-Era Secure Edge Computing

Document Overview

Product Name	X-Corleone (Fanless Ultra-Rugged AI Edge Server)
Core Technology	Post-Quantum Cryptography (PQC) Integration into TLS 1.3 Protocol
Key Algorithms	ML-KEM (Kyber) for Key Exchange, ML-DSA (Dilithium) for Digital Signature
Deployment Strategy	Hybrid PQC (Hybrid Encryption)
Solution Positioning	Hardware + PQC Security Solution Provider

www.elgens.com.tw © 2025 Elgens Co., Ltd. All rights reserved.

I. Executive Summary: From Hardware Supplier to Quantum Security Expert

The global cybersecurity environment has entered the "Quantum Countdown" phase. For edge computing devices processing high-value data requiring long-term confidentiality, the "Harvest Now, Decrypt Later" (HNDL) attack model constitutes a significant risk.

As the leader of the **X-Corleone Ultra-Rugged AI Edge Computing Server**, Elgens deeply understands the importance of network communication security for Edge AI data. The company is strategically completing a technical upgrade, committed through in-depth research to importing **NIST-standardized PQC algorithms (ML-KEM, ML-DSA) into the TLS 1.3 communication protocol.**

Core Values of this Solution:

- **PQC Protection for Edge Web Servers:** Ensures that when the server acts as a Web Server, its communication channel (HTTPS) possesses quantum security capabilities.
- **Adopting Industry Best Practices:** Deploys a Hybrid PQC strategy, running both classical and PQC algorithms simultaneously to minimize risk.
- **Technical Upgrade and Endorsement:** Successfully upgrading from a pure hardware supplier to a "Hardware + PQC Security Solution Provider," offering customers a one-stop, authoritatively verified cybersecurity solution.

www.elgens.com.tw © 2025 Elgens Co., Ltd. All rights reserved.

II. The Rise of the Quantum Threat: From "Potential Risk" to "Mandatory Transformation"

2.1 The Fatal Weakness of Classical Cryptography and the Quantum Threat

The asymmetric encryption (RSA, ECC) relied upon by today's network security is built on the "computational difficulty" of complex mathematical problems. However, Shor's Algorithm, proposed by mathematician Peter Shor, theoretically allows quantum computers to crack these problems at exponential speeds.

Algorithm	Security Basis	Quantum Computer Threat
RSA	Large Integer Factoring	Shor's Algorithm can crack in polynomial time
ECC	Elliptic Curve Discrete Logarithm	Shor's Algorithm can crack in polynomial time

Once a Cryptographically Relevant Quantum Computer (CRQC) is developed, current public-key encryption will instantly become ineffective, leaving the confidentiality of global communications completely exposed.

2.2 Why PQC Migration is an Urgent National Priority

Top global security agencies (such as US NIST, NSA) have identified PQC migration as a primary mission for cybersecurity. This is no longer a "choice," but a "survival" issue:

- **HNDL Attacks (Harvest Now, Decrypt Later) [4]:** Attackers can legally or illegally intercept and store encrypted traffic today. Once a CRQC is built, this intercepted data will be **retroactively decrypted,** causing long-term leakage of sensitive data. This is particularly fatal for high-value data processed by Edge AI servers (e.g., real-time footage, AI recognition results, sensitive configuration data).

www.elgens.com.tw © 2025 Elgens Co., Ltd. All rights reserved.

- **NIST Standardization Mandatory Implementation [1][2]:** In 2024, NIST officially released the first batch of PQC Federal Information Processing Standards, marking the maturity and usability of PQC algorithms. Global government agencies and critical infrastructure operators have been given clear migration deadlines, declaring PQC

2.3 Case Study Warning: The Necessity of PQC Adoption from Historical Lessons

Historically, economic losses caused by security vulnerabilities have been immeasurable. For instance, the famous Heartbleed vulnerability [5] (which occurred at the TLS/OpenSSL implementation layer) revealed the danger of global reliance on a single encryption library, leading to the leakage of millions of private keys.

If a defect in code implementation can cause global paralysis and data leakage, imagine the consequences if the cryptographic foundation (RSA/ECC) is mathematically shattered by quantum computers. The impact would be hundreds of times greater, with no way to repair historically leaked data. Elgens's research posits that PQC solutions are designed to thoroughly eliminate these foundational cryptographic risks.

www.elgens.com.tw © 2025 Elgens Co., Ltd. All rights reserved.

III. PQC Technology Core: Lattice-Based Cryptography

3.1 Selection and Principle of PQC Algorithms

Among numerous PQC candidates, NIST ultimately selected algorithms based on Lattice-Based Cryptography as the mainstream for key

- **Key Encapsulation Mechanism (KEM): ML-KEM (Kyber)** (FIPS 203)
- **Digital Signature Algorithm (DSA): ML-DSA (Dilithium)** (FIPS 204)

Advantage of Lattice-Based Cryptography: Its security is established on the difficulty of the "Learning with Errors (LWE)" problem. These problems are considered difficult to solve even for quantum computers (no known quantum algorithms can effectively crack them).

www.elgens.com.tw © 2025 Elgens Co., Ltd. All rights reserved.

3.2 Deep Focus: The Combination of ML-KEM (Kyber) and TLS 1.3

The most critical link in Web communication is Key Exchange, responsible for securely negotiating a re-encryption key using asymmetric encryption. ML-KEM is the most widely adopted and high-performance KEM algorithm in lattice theory, with efficiency and security particularly suited for edge

Feature	Description	Significance for TLS / Edge Computing
Mathematical Basis	Based on the LWE problem, using noise in high-dimensional mathematical lattices to hide secret information.	Provides robust quantum security capabilities to withstand Shor's Algorithm attacks.
Computational Efficiency	The operation process relies heavily on polynomial operations, offering extremely high computational efficiency.	Suitable for efficient operation on fanless, rugged hardware platforms without sacrificing system perfor mance.
Key Size	Compared to other PQC algorithms, ML-KEM has smaller key and ciphertext packet sizes.	Optimizes the network load during the TLS 1.3 handshake, ensuring high throughput for 10 GbE high-speed

Conclusion: Elgens's research concludes that selecting ML-KEM as the core key exchange algorithm provides the most advanced and efficient quantum security protection for the TLS 1.3 protocol.

www.elgens.com.tw © 2025 Elgens Co., Ltd. All rights reserved.

IV. Elgens PQC Solution: Quantum-Secure Edge Computing Architecture

Elgens believes that new ultra-rugged AI edge computing servers must possess multi-port **10 GbE** high-speed networking capabilities to connect multiple high-resolution cameras for AI image processing. Furthermore, they must ensure communication security meets the highest standards when acting as a **Web Server.**

4.1 Core Application Scenario: PQC-Enabled TLS 1.3 Web Communication

X-Corleone seamlessly integrates **ML-KEM** and **ML-DSA** core algorithm libraries into the product's **TLS 1.3** implementation, providing customers with a Web communication channel that defaults to **PQC security**:

- **Web Server Protection:** Ensures that when customers or administrators access the server's Web management interface or data APIs via HTTPS, the entire communication is protected by quantum security.
- **Real-time AI Data Protection:** Even if the edge server generates sensitive data during high-resolution image processing, the confidentiality of this data remains resistant to future quantum threats when transmitted to backend

4.2 Industry Best Practice: Hybrid PQC Deployment Strategy

During the PQC transition period, industry standards recommend adopting a **Hybrid Cryptography** strategy. Elgens's products adopt this strategy to offer the **highest level of reliability:**

www.elgens.com.tw © 2025 Elgens Co., Ltd. All rights reserved.

- **Simultaneous Operation:** During the TLS 1.3 handshake, both Classic Algorithms (e.g., ECC) and Quantum-Safe Algorithms (ML-KEM) run simultaneously.
- **Joint Derivation:** The final symmetric Session Key must be jointly derived from the outputs of both algorithms.protocols.
- **Absolute Security:** As long as either of the two algorithms remains secure, the entire communication session remains secure. This strategy thoroughly eliminates unknown risks that may exist in a single PQC algorithm and is currently the most robust deployment method.

4.3 The Role of ML-DSA (Dilithium) in the Product Ecosystem

In addition to ML-KEM for **communication confidentiality**, the introduction of the **ML-DSA** algorithm ensures **non-repudiation of identity** and **data integrity**:

- **Quantum-Safe Digital Signatures:** Used to verify the Web Server's digital certificate, ensuring the identity connected to by the customer is authentic and trusted.
- **System Integrity:** Can be used to sign firmware or software updates, ensuring that system software running in rugged environments has not been maliciously tampered with.protocols.

www.elgens.com.tw © 2025 Elgens Co., Ltd. All rights reserved.

IV. Competitive Advantage: The "Soft + Hard" Integrated PQC Expert

Strategic Transformation: Integrating Software and Hardware

Elgens is currently conducting research on Post-Quantum Cryptography (PQC) core algorithms to prepare for **key future transformations:**

Old Positioning (Hardware Supplier)	New Positioning (Hardware + PQC Security Solution Provider)
Provides rugged, high-performance AI edge hardware devices.	Provides rugged, high-performance hardware that simultaneously possesses PQC security solutions.
Customers must handle PQC algorithm adoption, integration, and validation themselves.	Customers obtain one-stop quantum security protection, eliminating complex PQC protocol integration and testing costs.
Security relies on the customer's backend security infrastructure.	Security is built-in to the product, compliant with NIST standards.

Elgens's value lies in transforming the complexity of PQC technology into a plug-and-play advantage for customers. Through a solution that combines software and hardware, we eliminate migration complexity. By combining the stability of ultra-rugged hardware with the performance of optimized PQC software libraries, we provide a holistic and reliable edge computing security solution.

The threat of quantum computing is no longer in the future; it is a current issue that all enterprises involving long-term data confidentiality and critical infrastructure must face. Choosing Elgens means choosing a partner with **excellent hardware performance** and **forward-deployed security architecture.** We promise to provide you with an integrated **software and hardware** solution to help you seamlessly and securely navigate the quantum generation, allowing you to focus on value creation in Edge AI computing while leaving the security challenges to us.

www.elgens.com.tw © 2025 Elgens Co., Ltd. All rights reserved.

VI. References

No.	Source	Content Description
[1]	NIST FIPS 203	Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM / Kyber).
[2]	NIST FIPS 204	Module-Lattice-Based Digital Signature Algorithm Standard (ML-DSA / Dilithium).
[3]	NSA CNSA 2.0	Commercial National Security Algorithm Suite 2.0; PQC migration guidelines published by the US National Security Agency.
[4]	HNDL (Harvest Now, Decrypt Later)	Quantum attack threat model emphasizing the risk of long-term data confidentiality.
[5]	Heartbleed Vulnerability	The 2014 severe OpenSSL vulnerability, used to analogize a global security crisis caused by a single point of encryption failure.

www.elgens.com.tw © 2025 Elgens Co., Ltd. All rights reserved.



ELGENS®

ELGENS CO., LTD

https://www.elgens.com.tw/

7F-6, No. 492, Bannan Rd., Zhonghe Dist., New Taipei City 235, Taiwan

+886-927370730 | +886-2-7729-7209

santiago@elgens.com.tw