# CQX WAVE-ON Q-TERA SERIES: KYBER PCIe ACCELERATOR CARD PRODUCT BROCHURE



PRESENTED BY

CeQureX Technology Limited

# CQX Wave-On Q-Tera Series: Kyber PCIe Accelerator Card Product Brochure

**Engineered for the Quantum Era: The Pinnacle of Taiwan's Chip Design**

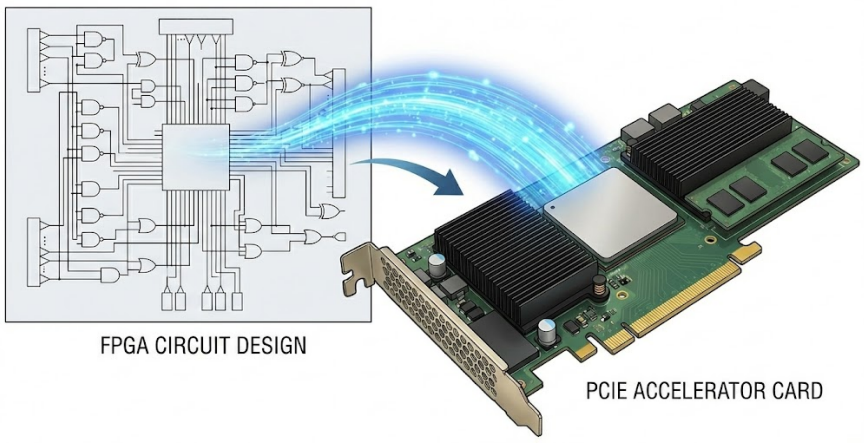
Born from the world-leading semiconductor expertise of Taiwan, this breakthrough PQC accelerator is the definitive answer to the massive computational demands of the post-quantum era. While traditional software struggles under the high-load requirements of quantum-resistant math, our hardware-level solution delivers **unmatched throughput and near-zero latency**. Designed specifically for high-performance servers and hyperscale data centres, this chip provides the specialized architecture needed to secure global infrastructure without compromising on speed or scale.

The core of our solution lies in its **high-performance FPGA-based PQC chipset**, a specialized hardware architecture designed to meet the extreme computational demands of the post-quantum era. Unlike rigid, fixed-function chips, our **FPGA-driven design** offers the perfect synergy of **raw hardware speed** and **unrivaled crypto-agility**. This unique flexibility allows the chipset to be dynamically re-programmed to support evolving NIST standards or custom business-specific use cases, ensuring your infrastructure remains future-proof. By combining the throughput of dedicated silicon with the ability to adapt to changing cryptographic requirements, we provide a high-velocity, low-risk foundation for securing your most critical data assets.

## 1. Product Overview

**Product Positioning:** A mission-critical PQC (Post-Quantum Cryptography) PCIe acceleration card, purpose-built for high-performance servers, cloud infrastructure, and hyperscale data centers.

**Core Value:** As quantum computing threatens to break legacy encryption, the industry is pivoting to NIST-standardized algorithms like **ML-KEM (Kyber)**. However, Kyber's intense computational load can drain up to 90% of traditional CPU resources. Our **dedicated ASIC/FPGA engine** solves this by completely offloading PQC workloads. By moving encryption and decryption to a specialized hardware layer, we restore your server's primary processing power, drastically increasing connection capacity while maintaining **ultra-low, deterministic latency**.



## 2. Application Scenarios

**Strategic Application Scenarios: Securing the Digital Backbone**

- **Next-Gen PQC-WAF Integration:** Functions as the high-velocity hardware engine for Web Application Firewalls, effortlessly managing **millions of concurrent PQC-encrypted sessions**. It provides the backbone for a true, quantum-safe Zero-Trust architecture.
- **Hyperscale Cloud Resource Pools:** Acts as the primary compute heart for **Cloud HSMs** and **PQC-as-a-Service** platforms, providing scalable, multi-tenant cryptographic power for server clusters.
- **Ultra-Low Latency Fintech:** Engineered for High-Frequency Trading (HFT) and financial institutions, delivering robust quantum defense without compromising the **microsecond-level latency** required for global markets.
- **Secure Distributed Storage:** Enables **real-time PQC encryption** for Big Data and distributed file systems, ensuring that "Data at Rest" remains impenetrable against future decryption threats.

## 3. Core Architecture & Technical Features

### 3.1. Dedicated Cryptographic Engine

**Architectural Advantage: Parallelized Number Theoretic Transform (NTT) Acceleration**

Our chip features a proprietary array of **parallelized Arithmetic Logic Units (ALUs)**, custom-engineered for the rigorous mathematical demands of the Kyber algorithm. By deeply optimizing for **Polynomial Multiplication** and **Number Theoretic Transform (NTT)**, the architecture achieves a massive throughput leap. It enables the simultaneous processing of multiple data sets within a **single clock cycle**, effectively eliminating the computational bottlenecks that slow down standard processors.

### 3.2. Zero-Trust Security

**Advanced Hardware Security & Integrity**

- **Side-Channel Resilience:** Engineered with hardware-level defenses to neutralize **timing attacks** and **differential power analysis (DPA)**, ensuring that cryptographic operations remain invisible to external observation.
- **Immutable Secure Boot:** Establishes a hardware root of trust that verifies firmware integrity at startup, effectively blocking malicious code implantation or unauthorized system modifications.
- **Hardware-Isolated Key Storage:** Features a dedicated, **air-gapped storage enclave** that ensures sensitive keys never leave the secure boundary, preventing leakage even during high-load cryptographic computations.

### 3.3. Crypto-Agility

In a rapidly evolving threat landscape, the ability to adapt is just as critical as the ability to encrypt. Our PQC hardware, powered by a specialized **FPGA-based chipset**, is engineered with **Crypto-Agility** at its core. Unlike traditional fixed-function ASICs (Application-Specific Integrated Circuits) that become obsolete when cryptographic standards change, our FPGA architecture allows for **seamless field updates and re-programmability.**

- **Dynamic Standard Alignment:** As NIST continues to refine Post-Quantum standards (transitioning from drafts to final FIPS versions like ML-KEM or ML-DSA), our hardware can be updated via firmware to ensure total compliance without the need for physical replacement.
- **Algorithm Swap Capability:** Should a specific algorithm be found vulnerable or should a superior method emerge, our chipset can be reconfigured to support new mathematical primitives or hybrid schemes instantaneously.
- **Customized Business Logic:** The programmable nature of the FPGA enables us to tailor cryptographic performance to specific business cases—whether optimizing for high-volume transactions, ultra-low latency edge computing, or specialized government signing workflows.

By moving away from static silicon and embracing an agile, hardware-accelerated approach, we ensure that your investment is protected against the "Quantum Apocalypse" and any future shifts in the global cryptographic horizon. This is not just a security upgrade; it is a **sustainable, long-term infrastructure strategy.**

## 3.4. Seamless Integration

**Seamless Ecosystem Integration: Zero-Code PQC Acceleration**

We eliminate the friction of migrating to quantum-safe standards by providing comprehensive drivers and a robust SDK. Our solution supports **direct mounting** into the standard **OpenSSL library**, enabling hardware acceleration for your existing infrastructure instantly. Legacy and modern applications — including **Nginx, Apache, and OpenSSH**—can leverage elite PQC performance **without a single line of code modification**, ensuring a rapid and risk-free transition for your entire software stack.

# THANK YOU

We are a team of dedicated Ph.D.-level cybersecurity experts and passionate pioneers in post-quantum cryptography and quantum-secure networking.

Our mission is to be the region's leading partner in building sovereign, quantum-resilient infrastructure, enables our partners/clients to agilely discover, plan and transform their security systems to quantum-grade protection across multi-cloud environments—including on-premise data centers, AWS, GCP, and Azure.”.


## ADDRESS

8 F.-5, No. 19, Jingye 1st Rd., Zhongshan Dist., Taipei City 104051, Taiwan (R.O.C.)

## E-MAIL

sales@cequrex.com

## WEBSITE

www.CeQureX.com