



CQX WAVE-ON Q-TERA SERIES: KYBER PCIe 加速卡

產品介紹

© 2026 CeQureX Technology Limited. All rights reserved.

No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of CeQureX Technology Limited, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law.

PRESENTED BY
CeQureX Technology Limited

CQX Wave-On Q-Tera Series: Kyber PCIe 加速卡

專為量子時代而生：台灣晶片設計的極致巔峰

誕生自台灣領先全球的半導體專業技術，這款突破性的後量子密碼（PQC）加速處理器，是因應後量子時代龐大運算需求的終極解答。當傳統純軟體解決方案在具備量子安全（抗量子）數學運算的高運算負載要求下陷入效能瓶頸時，我們**基於硬體層級的解決方案能提供無與倫比的吞吐量與近乎零延遲的極致表現**。專為高效能伺服器與超大規模（Hyperscale）資料中心量身打造，本晶片能提供全域基礎設施防護所需的專用架構，且在連線速度與擴充規模上毫無妥協。

我們解決方案的核心，在於其基於**高效能 FPGA 架構的 PQC 晶片組**——這是一套專為應對後量子時代極限運算需求而設計的專用硬體架構。有別於運算邏輯僵化、功能固定的晶片，我們由 FPGA 驅動的設計，完美融合了**原始硬體的極致速度與無可比擬的加密敏捷性（Crypto-Agility）**。這種獨一無二的彈性，允許晶片組進行動態重新編程，以無縫支援持續演進中的 NIST 標準或企業自訂的專屬業務情境，確保您的基礎設施具備面向未來的抗量子準備度。透過將專用矽晶片的極致吞吐量，與適應密碼技術需求變化的彈性融為一體，我們為保護組織最關鍵的密碼技術資產與數據，提供了高速度、低切換風險的堅實底座。

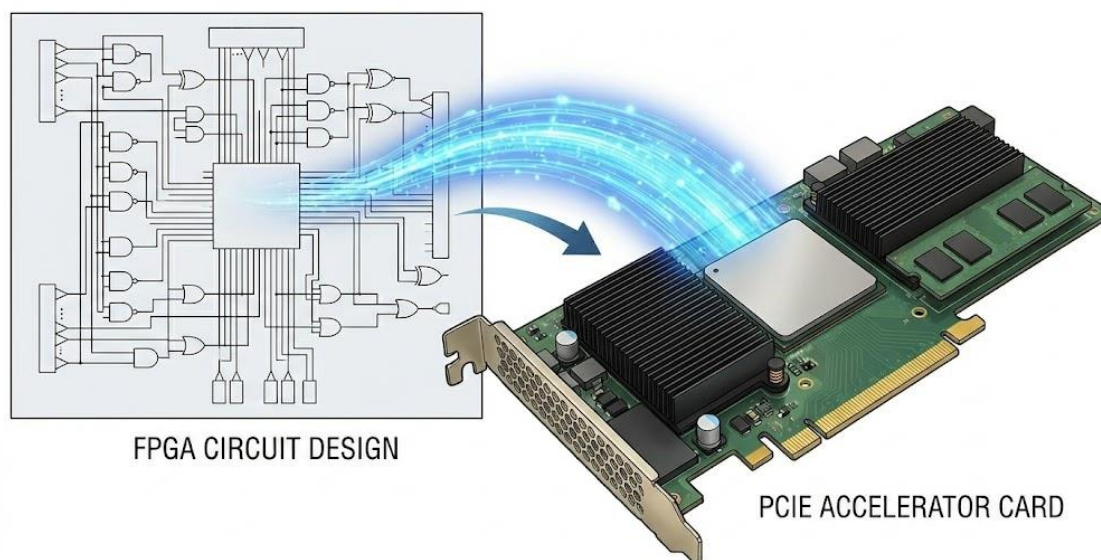
1. 產品總覽

產品定位：

一款專為執行關鍵型任務之業務量身打造的 PQC（後量子密碼）PCIe 加速卡，專為高效能伺服器、雲端基礎設施與超大規模資料中心構建。

核心價值：

隨著量子運算威脅到既有加密技術的安全性，產業正全面轉向標準化的 NIST 演算法，例如 **ML-KEM（Kyber）**。然而，Kyber 高強度的數學運算負載，可能會消耗高達 90% 的傳統 CPU 處理器資源。我們**專用的 ASIC / FPGA 引擎**能透過完全卸載（Offloading）PQC 運算負載來徹底解決此瓶頸。透過將加解密作業移轉至專屬的硬體運算層，我們能全面釋放伺服器的核心處理能量，在維持極低且具備確定性延遲（Deterministic Latency）的同時，大幅提升連線承載容量。



2. 應用場景

戰略應應場景：鞏固數位骨幹防線

- **下一代 PQC-WAF 整合 (Next-Gen PQC-WAF Integration) :**

作為網頁應用防火牆 (WAF) 的高速硬體引擎，能毫不費力地應付並管理數百萬筆並發的 PQC 加密連線階段。為打造真正具備量子安全 (抗量子) 能力的零信任 (Zero-Trust) 架構，提供最堅實的底層骨幹。

- **超大規模雲端資源池 (Hyperscale Cloud Resource Pools) :**

作為雲端硬體安全模組 (Cloud HSM) 與 PQC 即服務 (PQC-as-a-Service) 平台的運算核心，為龐大的伺服器叢集提供具備高擴充性、多租戶 (Multi-tenant) 架構的密碼學運算能量。

- **極低延遲之金融科技 (Ultra-Low Latency Fintech) :**

專為高頻交易 (HFT) 與金融機構量身打造，在毫無妥協全球金融市場極度苛求之微秒級低延遲的前提下，提供強悍且穩固的量子防禦韌性。

- **安全分散式儲存 (Secure Distributed Storage) :**

賦予海量資料 (Big Data) 與分散式檔案系統即時的 PQC 加密能量，確保靜態資料 (Data at Rest) 在面對未來「先攔截、後解密 (HNDL)」的破密威脅時，依然堅不可摧。

3. 核心架構與技術特點

3.1. 專用密碼學運算引擎

架構優勢：平行化數位理論轉換 (NTT) 加速

我們的晶片採用專有的**平行化算術邏輯單元 (ALUs) 陣列**，專為 Kyber 演算法極其嚴苛的數學運算需求進行客製化工程設計。透過針對多項式乘法 (Polynomial Multiplication) 與數位理論轉換/數論轉換 (NTT, Number Theoretic Transform) 進行深度演算法優化，本架構在吞吐量上取得了巨大的躍進。它能在單一時脈週期內同時處理多個資料集，徹底消除了拖慢標準處理器的運算瓶頸。

3.2. 零信任資安架構

進階硬體安全防護與完整性

- **側信道攻擊防禦韌性 (Side-Channel Resilience)**：由硬體層級的防禦工程精心構建，能徹底中和計時攻擊 (Timing Attacks) 與差分電力分析 (DPA, Differential Power Analysis)，確保所有的密碼技術運算過程對外部觀測者而言完全隱形。
- **不可竄改之安全開機 (Immutable Secure Boot)**：建立硬體信任根 (Hardware Root of Trust)，在開機階段即時驗證韌體完整性，有效阻絕惡意程式碼植入或未經授權的系統改作。
- **硬體隔離金鑰儲存 (Hardware-Isolated Key Storage)**：具備專用的實體氣隙隔離 (Air-gapped) 儲存安全區，確保機敏金鑰絕對不會離開安全邊界，即使在極高負載的密碼運算期間，亦能澈底防止金鑰外洩。

3.3. 加密敏捷性

在瞬息萬變的資安威脅中，具備調適與適應能力，與加密防護本身同等重要。我們的 PQC 硬體由專用的 FPGA 晶片組驅動，是以加密敏捷性 (Crypto-Agility) 為核心骨幹進行設計。有別於當密碼學標準改變時便面臨淘汰的傳統固定功能 ASIC (特定應用積體電路)，我們的 FPGA 架構允許無縫的現場部署更新與可重新編程能力。

- **動態標準規範對照與對齊 (Dynamic Standard Alignment)**：隨著 NIST 持續精進與微調後量子標準 (從草案過渡至最終的 FIPS 正式標準版本，如 ML-KEM 或 ML-DSA)，我們的硬體僅需透過韌體更新即可確保 100% 絕對合規，完全無需耗時費力地更換實體晶片或硬體設備。

- **演算法即時抽換能力 (Algorithm Swap Capability)**：若特定演算法未來被證實存在脆弱性，或是有更優異的數學方法問世，我們的晶片組能隨刻重新組態，以即時支援全新的數學原始元件 (Mathematical Primitives) 或 PQC 混合模式 (Hybrid Schemes)。
- **客製化企業業務邏輯 (Customized Business Logic)**：FPGA 的可編程特性，使我們能針對特殊的業務情境量身調校密碼技術運算效能——無論是針對海量金融交易進行優化、極低延遲的邊緣運算，或是政府機關專屬的高規格數位簽章工作流。

透過拋棄靜態僵化的矽晶片，並擁抱敏捷、由硬體加速的策略，我們確保您的資安預算與投資，能抵禦未來的「量子啟示錄/破密危機 (Quantum Apocalypse)」以及全球密碼學領域的任何演進。這不僅僅是一次單純的資安升級，更是一項兼顧永續與長遠營運的基礎設施戰略。

3.4. 無縫生態系整合

無縫生態系整合：零程式碼 PQC 加速

透過提供全方位的驅動程式與強健的軟體開發套件 (SDK)，我們徹底消弭了量子安全標準遷移時的阻力與摩擦成本。我們的解決方案支援直接掛載至標準 OpenSSL 函式庫中，為您既有的基礎設施隨插即用地提供立即的硬體加速能量。

無論是傳統或現代化應用服務 (包含 Nginx、Apache 與 OpenSSH) 皆能在**無須修改任何一行程式碼 (Zero-Code)** 的情況下，運用頂級的 PQC 運算效能，確保您企業全體軟體技術堆疊能達成最為快速、且零切換風險的順暢轉型。



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@cequirex.com

WEBSITE

www.CeQureX.com