PQ Code Package

「最安全的後量子安全函式庫」

規格

- 支援後量子金鑰封裝機制 ML-KEM (FIPS 203)

跨平台支援：

- Windows 10/ server 2019,
- macOS 11-15,
- Ubuntu18.04/20.04/22.04/24.04,
- RHEL 7/8/9"

PQ Code Package

PQ Code Package (PQCP) 是一個開源專案，專注於高安全性的後量子密碼學算法軟體實現。

PQCP 針對後量子密碼技術進行實作，初步階段專注於模組化格子基密鑰封裝機制 (ML-KEM) 的演算法。此專案目標在於提供跨平台支援，並將實現 C 語言、AVX2 優化、Rust 以及 AArch64 優化版本。此外，PQCP 的實作將透過外部審核或形式驗證以確保安全性，增強信賴度。