# PQC-VPN: A Windows VPN Client with NIST Post-Quantum Cryptographic Algorithms

**Ria Lestari**
Pusat Sertifikasi Teknologi Keamanan Siber dan Sandi,
Badan Siber dan Sandi Negara Republik Indonesia
Jakarta, Indonesia
ria.lestari@bssn.go.id

## ABSTRACT

The rapid advancement of quantum computing poses a significant threat to conventional public-key cryptographic systems, including those currently deployed in Virtual Private Network (VPN) protocols. This research presents the design, implementation, and verification of a post-quantum cryptography (PQC) VPN client for Windows that integrates NIST-standardized quantum-resistant algorithms into an OpenVPN-based secure tunnel. The proposed system incorporates ML-KEM-768 (FIPS 203) for key encapsulation and ML-DSA-65 (FIPS 204) for digital signatures, implemented through the Open Quantum Safe (OQS) provider for OpenSSL. A hybrid key exchange scheme, X25519MLKEM768, is employed to maintain backward compatibility while achieving quantum resistance. The TLS 1.3 handshake is used as the transport security layer with AES-256-GCM for symmetric encryption. A graphical user interface (GUI) was developed as a distributable Windows executable using WPF (.NET 9), providing real-time connection monitoring and PQC algorithm visibility. The implementation was verified using Wireshark packet analysis, which confirmed the negotiation of the ML-KEM key exchange during the TLS handshake. Additionally, OpenSSL diagnostic logs confirmed the use of ML-DSA-65 for certificate signing and verification. The results demonstrate that post-quantum cryptographic algorithms can be successfully integrated into an existing VPN infrastructure with minimal latency overhead, offering a practical migration path toward quantum-safe network security.