Note: All abstracts must be submitted using this approved template and must not include pictures, graphs, or tables. The abstract must not exceed 400 words, excluding the abstract title, page numbering, or any ancillary entrant information. Citations or references are not a necessity with the abstract. If your abstract is accepted for consideration, you may include citations or references with your poster.

Abstract Title: Kyber Odyssey: Charting a course for secure innovation in a post-Crowdstrike world

Background: The catastrophic Crowdstrike patch failure of July 19, 2024, exposed critical vulnerabilities in global healthcare systems, stemming from a memory safety issue in C++ code. This null pointer error, a common pitfall in languages without automatic memory management, led to system-wide failures in Microsoft-based environments while Linux/GNU and Apple systems remained unaffected. This event underscores the urgent need for robust, quantum-resistant cryptographic solutions in healthcare IT infrastructure.

Methods: We developed a protocol for building and benchmarking National Institute of Standards and Technology (NIST)-endorsed classical and post-quantum encryption algorithms on-premesis, using consumer grade Linux computers to prioritize viability for underserved regions & underfunded institutions. We compiled OpenSSL with Open Quantum Safe (OQS) C library to enable post-quantum encryption development that allowed the same level of access as Crowdstrike's faulty driver code while allowing for bindings with numerous memory safe programming languages. Our focus on post-quantum Key Encapsulation Mechanism (KEM) encryption reflects the ubiqutious protection that these protocols provide to secure communication and knowledge-work as well as the relative ease of hybridization with classical encryption protocols like Elliptical Curve Diffie-Hellman (ECDH). Following on-device compilation and installation of the encryption binaries, we built and executed an evaluation script with OpenSSL's native toolkit for twenty-four NIST-endorsed KEM protocols consisting of classical, quantum, and hybrid KEM implementations. We evaluated the KEMs on the number and rate of key generations (keygen), key encapsulation (encap) rate, and key decapsulations (decap) and rated their NIST post-quantum security level according to NIST advanced encryption standard (AES) exaustic key search levels.

Results: We successfully benchmarked all 24 KEM protocols, producing an example public/private key pair following the evaluation. The 24 KEM protocols are evenly split across NIST security levels 1, 3, and 5, with 8 protocols at each.We made all relevant code, regulatory information, and the example cryptographic key pairs available on the Qompass AI Github page. We released them under the GNU Affero General Public License (AGPL) to maintain the free availability of these encryption tools to benefit communities.

Conclusion: Out of the evaluated KEMs, we propose hybrid combinations of ECDH and Kyber for most acute adoption of enhanced encryption protocols due to the layered security of nascent post-quantum encryption with established efficient classical protocols. Currently, GoogleChrome implements X25519_Kyber768 hybrid encryption as part of its Transport Layer Security (TLS), offering a familiar and accessible platform to perform institutional assessements.