ABSTRACT

The quick rise of smart homes, which offer comfort, highlights the need to protect users' personal data. This is crucial to keep user trust and stop misuse by harmful individuals, which can cause financial and personal harm. Encryption and digital signatures are key to securing data, making it hard for attackers to misuse it. However, using these methods on smart home devices is tough because these devices lack the necessary computing power, as they are part of the IoT system in homes. The National Institute of Standards and Technology (NIST) is working on Post-Quantum Cryptography (PQC) to protect data from quantum computer attacks. Research is ongoing to apply PQC to IoT devices, especially smart home devices, due to their close connection to personal life. This research examines the use of PQC on smart home devices.

This research assesses the use of Kyber-Dilithium Signcryption in post-quantum cryptography for smart home devices. It is implemented on the Raspberry Pi 4 Model B as a smart home gateway and on web servers. The study compares various combinations of Kyber-Dilithium Signcryption on the Raspberry Pi 4 Model B, including Kyber512-Dilithium2, Kyber512-Dilithium3, Kyber512-Dilithium5, Kyber768-Dilithium2, Kyber768-Dilithium3, Kyber768-Dilithium5, Kyber1024-Dilithium2, Kyber1024-Dilithium3, and Kyber1024-Dilithium5. The analysis focuses on the process time and computational resources used by each combination.

The result is Kyber512-Dilithium2 signcryption, which is fast and uses little memory and CPU, making it ideal for the Raspberry Pi, which has limited resources. Higher parameter configurations overload the Raspberry Pi, causing slow and resource-heavy processes. RSA needs more computing power than ECC, which can be faster and use less memory than Kyber512-Dilithium2 but isn't secure against quantum attacks. Kyber512-Dilithium2 is effective in smart homes for data protection, even against passive attacks like sniffing, and can be used on the Raspberry Pi as an IoT node gateway against quantum threats.
Keywords: Signcryption, IoT, Kyber, Dilithium, Post-Quantum, Data Security