World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:16, No:03, 2022

Identity-Based Encryption: A Comparison of Leading Classical and Post-Quantum Implementations in an Enterprise Setting

Authors : Emily Stamm, Neil Smyth, Elizabeth O'Sullivan

Abstract : In Identity-Based Encryption (IBE), an identity, such as a username, email address, or domain name, acts as the public key. IBE consolidates the PKI by eliminating the repetitive process of requesting public keys for each message encryption. Two of the most popular schemes are Sakai-Kasahara (SAKKE), which is based on elliptic curve pairings, and the Ducas, Lyubashevsky, and Prest lattice scheme (DLP- Lattice), which is based on quantum-secure lattice cryptography. In order to embed the schemes in a standard enterprise setting, both schemes are implemented as shared system libraries and integrated into a REST service that functions at the enterprise level. The performance of both schemes as libraries and services is compared, and the practicalities of implementation and application are discussed. Our performance results indicate that although SAKKE has the smaller key and ciphertext sizes, DLP-Lattice is significantly faster overall and we recommend it for most enterprise use cases.

Keywords : identity-based encryption, post-quantum cryptography, lattice-based cryptography, IBE
Conference Title : ICCNS 2022 : International Conference on Cryptography and Network Security
Conference Location : Miami, United States
Conference Dates : March 11-12, 2022