World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:15, No:05, 2021

Alternative Key Exchange Algorithm Based on Elliptic Curve Digital Signature Algorithm Certificate and Usage in Applications

Authors : A. Andreasyan, C. Connors

Abstract : The Elliptic Curve Digital Signature algorithm-based X509v3 certificates are becoming more popular due to their short public and private key sizes. Moreover, these certificates can be stored in Internet of Things (IoT) devices, with limited resources, using less memory and transmitted in network security protocols, such as Internet Key Exchange (IKE), Transport Layer Security (TLS) and Secure Shell (SSH) with less bandwidth. The proposed method gives another advantage, in that it increases the performance of the above-mentioned protocols in terms of key exchange by saving one scalar multiplication operation.

Keywords : cryptography, elliptic curve digital signature algorithm, key exchange, network security protocol
Conference Title : ICCCIS 2021 : International Conference on Cryptography, Coding and Information Security
Conference Location : Amsterdam, Netherlands
Conference Dates : May 13-14, 2021