World Academy of Science, Engineering and Technology
International Journal of Cognitive and Language Sciences
Vol:17, No:07, 2023

A Lightweight Authentication and Key Exchange Protocol Design for Smart Homes

Authors : Zhifu Li, Lei Li, Wanting Zhou, Yuanhang He

Abstract : This paper proposed a lightweight certificate-less authentication and key exchange protocol (Light-CL-PKC) based on elliptic curve cryptography and the Chinese Remainder Theorem for smart home scenarios. Light-CL-PKC can efficiently reduce the computational cost of both sides of authentication by forgoing time-consuming bilinear pair operations and making full use of point-addition and point-multiplication operations on elliptic curves. The authentication and key exchange processes in this system are also completed in a a single round of communication between the two parties. The analysis result demonstrates that it can significantly minimize the communication overhead of more than 32.14% compared with the referenced protocols, while the runtime for both authentication and key exchange have also been significantly reduced.

Keywords : authentication, key exchange, certificateless public key cryptography, elliptic curve cryptography
Conference Title : ICSLP 2023 : International Conference on Speech and Language Processing
Conference Location : Stockholm, Sweden
Conference Dates : July 06-07, 2023