Abstract

This paper introduces a new scheme “ A Public Verifiability Signcryption Scheme Without Pairings ”, based on elliptic curve discrete logarithm problem (ECDLP) and in addition to achieve the functionality of the Signcryption schemes, unforgeability, confidentiality and nonrepudiation, it achieves forward security and public verifiability directly. Also, it uses a strong encryption key depends on random choose value and the sender’s private key, although the proposed scheme is slower than the Zheng’s signcryption scheme, it achieves saving in communication overhead reach to 50% with respect to the traditional approach signature then encryption. The proposed scheme has been verified using the Mathematica program.

References

1. Y. Zheng, “Digital signcryption or how to achieve cost (signature & encryption)