Abstract

The novel technique titled as "signcryption" announced by Yuliang Zheng, completes both the functionality of signature scheme and encryption scheme in single logical step with a reduced amount of computational cost and communication overhead than Signature-then-encryption scheme. A number of signcryption scheme has previously been announced by many researchers nonetheless each scheme has their own restriction. This paper is grounded on an elliptic curve cryptosystem (ECC) implemented using java technology.
An Efficient Security Protocol based on ECC with Forward Secrecy and Public Verification

with reduced amount of computational cost and communication overhead than the existing techniques. It not only offers the integrity, authenticity, confidentiality, unforgeability, non-repudiation beside that forward secrecy and public verification. By forward secrecy of message confidentiality, unauthorized person cannot be able to mine the original message content even if the long-term private key of the sender is compromised. It doesn’t affect the confidentiality of the previously stored message. By the public verification, Anyone can confirm the sender signature without reading the content of message since the message is in encrypted format. As our proposed scheme takes a comparable amount of computational cost, it can be applied in lower computational power devices like smart card based applications, e-voting etc.

References


Index Terms

Computer Science Security

Keywords

Elliptic Curve Cryptosystem Digital Logarithmic Problem Signcryption Digital Signature Encryption Decryption.