Identity Based Encryption and Signature Schemes with Elliptic Curve Cryptosystem Challenges

Kalyani, D[1]* and Vijay Kumar, P[2]

1. Department of Information Technology, VNR VIGNANA Jyothi Institute of Engineering & Technology, Bachupally, Hyderabad, Telangana, INDIA
2. Department of CSE, DRK Institute of Science And Technology, Bowrampet, Hyderabad - 500043, Telangana, INDIA

KEYWORDS

Cryptography;

Elliptic Curves;

Identity Based Encryption;

Public Key Crypto system;

Abstract: *Cryptography is the study of science assuring the secrecy, authentication and confidentiality of information exchanges. Public key crypto system schemes are secure if only if an authenticity and confidentiality of the public-key is assured in the form of an authorized public key certificate through certificate authority. By using an Identity-Based Encryption, a party can encrypt a message using the recipient's identity as a public key which avoids the necessity of public keys management and distribute public key certificates. An Elliptic curve discrete logarithm hard problem arithmetic is the principle tool to perform key exchange, encryption, digital signature including identity based encryption to avoid key revocation problem of public key infra structure(PKI) . The main key factor of elliptic curve cryptography compared to other asymmetric crypto systems is that it offers equivalent security afford by an RSA based system with large modulus even for a smaller key-size, which reduces the storage and transmission requirements. In this paper we discuss a new identity based encryption and signature algorithms over elliptic curves with finite fields.*