Authenticated Encryption Based on Prime Moduli and Its Applications

Debasis Giri

Maulana Abul Kalam Azad University of Technology, WB, India

Email: debasis_giri@hotmail.com

Abstract: In an authenticated encryption scheme, a signer signs a message for a particular verifier using signer's own private key and the public key of the verifier. The verifier recover the original message from the signcrypted message using the signer's public key and the verifier's own private key. Significant work is done in this direction by the authors Zheng and others. In this paper, we propose an authenticated scheme scheme which is based upon a variant of the ElGamal encryption scheme and a variant of the ElGamal signature scheme over large prime moduli.

Keywords: Encryption; Digital Signature; Authenticated Encryption; Attack; Cryptography.

Categories: E.3; K.6.5; D.4.6; C.2.0