Cryptology ePrint Archive: Report 2013/037

Provably Secure Identity-Based Aggregate Signcryption Scheme in Random Oracles

Jayaprakash Kar

Abstract: This article proposes a provably secure aggregate signcryption scheme in random oracles. Security of the scheme is based on computational infesibility of solving Decisional Bilinear Diffie-Hellman Problem and Discrete Logarithm Problems. Confidentiality and authenticity are two fundamental security requirement of Public key Cryptography. These are achieved by encryption scheme and digital signatures respectively. Signcryption scheme is a cryptographic primitive that performs signature and encryption simultaneously in a single logical steps. An aggregate signcryption scheme can be constructed of the aggregation of individual signcryption. The aggreagtion is done taking n distinct signcryptions on n messages signed by n distinct users.

Category / Keywords: cryptographic protocols /

Date: received 25 Jan 2013

Contact author: jayaprakashkar at yahoo com