Elgamal digital signature scheme with Integrated cfea-technique

ABSTRACT

One of the four security goals is authentication. Authentication is a mechanism to ensure that we are communicating with the intended party. If Alice and Bob want to communicate securely, then the authentication mechanism will be able to ensure that Alice is truly communicating with Bob, and Bob is truly communicating with Alice. This mechanism can be provided by the cryptography. One of the most established cryptography schemes is ElGamal cryptosystem. The original version of this cryptosystem is to provide confidentiality through encryption and decryption procedures. By manipulating these procedures, the authentication mechanism can be carried out. Thus, ElGamal Digital Signature Scheme emerges as one of the most popular authentication mechanisms. In order to provide good level of security, proper parameters must be used in this scheme. This includes the size of the parameters. Larger parameters will provide a better level of security. As a consequence, the performance of the scheme becomes an issue in real life application. In this paper, we proposed the enhancement of the ElGamal Digital Signature Scheme by integrating the Continued-Fraction-Euclidean-Algorithm (CFEA) technique. This technique is able to reduce the number of data to be processed in the signing and verification procedures. By integrating the CFEA-technique into the ElGamal Digital Signature Scheme, any number of documents can be compressed becomes a pair of documents. Therefore, the signing and verification procedures can be done in smaller number of steps.