CFEA-Technique: Smaller size of the compressed plaintext

ABSTRACT

Key distribution problem has been solve by the emergence of asymmetric cryptography. Without exchanging private key, two parties are able to communicate securely via insecure channel. As a tradeoff, the efficiency of asymmetric cryptosystems are much slower since the size of the numbers implemented are large in order to provide a good level of security. Since that, efficiency enhancement become one of the most conducted research in cryptography. We proposed a technique that we named as CFEA-technique which aims to reduce the number of plaintext and ciphertext to be encrypted and decrypted by asymmetric cryptosystems. By applying this technique, we the number of plaintext can be reduced from k plaintext, where k is a positive integer and greater than 2, to only 2 plaintext. Hence, instead of encrypting plaintext, now we need to encrypt only 2 compressed plaintext. Since the number of plaintext to be encrypted have been reduce, the number of ciphertext to be decrypted also become lesser. Unfortunately, even though the number of plaintext have been reduced to only 2 plaintext, the size of these compressed plaintext are become larger for large . This problem will minimize the efficiency enhancement in encryption and decryption procedures. In this paper, we embed a method into the CFEA-technique in order to produce a new pair of plaintext with smaller sizes.