On the Computational Cost of Cocks' Identity Based Encryption

ABSTRACT

Identity Based Encryption is a public key cryptosystem where the user's identity becomes the public key. The first Identity Based Encryption scheme was constructed in 2001 based on elliptic curves and with pairings. Another variant of Identity Based Encryption which is without pairings was the Cocks' Identity Based Encryption. The security of Cocks' Identity Based Encryption lies on integer factorization problem and quadratic residuosity modulo composite N problem. Unfortunately, lack of efficiency becomes a major drawback of the Cocks' Identity Based Encryption. The algorithms in Cocks' Identity Based Encryption consists of four stages: Setup, Extract, Encrypt and Decrypt. Therefore, the aim of this paper is to investigate which algorithm in Cocks' Identity Based Encryption consumes high computational cost and subsequently contributes to its inefficiency. The experiments were conducted by comparing the computational time between Encrypt and Decrypt algorithms. Results from the study showed that decryption in Cocks' Identity Based Encryption has higher computational cost as compared to the encryption. A further improvement can be made on accelerating the decryption process without compromising the security.