Identity-based encryption schemes - a review

ABSTRACT

Identity-based encryption (IBE) allows a user to compute public key from arbitrary string such as name or email address as user's identity explicitly, thus provides a key-certificateless encryption platform while ensuring message confidentiality. In this paper, several identity-based encryption schemes are reviewed, ranging from the first practical well-known Boneh-Franklin IBE scheme based on pairing function to the recent IBE based on lattices. The aim of this review is to provide an extensive view and classification of these IBE schemes based on their setting, including underlying primitives in the parameter setup, fundamental security behind these schemes, comparative computational complexity and efficiency analysis. This review does not consider the variants of IBE such as hierarchical IBE, fuzzy IBE and those from the similar categories. Some current trends in IBE research and its implementation, along with some possible suggestions in designing new IBE schemes in the future are given as a conclusion of this review.

Keyword: Identity-based encryption; Pairing function; Multivariate; Trapdoor subgroup; Lattice; Post-quantum