Identity Based Encryption(IBE)

Subba Rao Y V
University of Hyderabad
Email yvsrcs@uohyd.ac.in

Identity based encryption is a public key encryption scheme in which identity is used as the public key which is used to encrypt the message and to decrypt the message the receiver will get the corresponding private key from PKG. In IBE, identity plays the role of public key, it solves the public key management problem and has no need to issue certificates to authorize the public keys. This idea was proposed by Adi Shamirin 1984. He was however only able to give an instantiation of identity-based signatures. Identity-based encryption remained an open problem for many years.This scheme became practical after Boneh and Franklin proposed an IBE scheme by using pairings. Pairings can be an interesting Math concept for people from Mathematics. This Talk will motivate the need of IBE with brief introduction Public key cryptosystems and key management issues there and then can introduce IBE scheme using pairings.