CERTIFICATELESS IDENTIFICATION: DEFINITIONS AND CONSTRUCTIONS

By: Dr. Chin Ji Jian, Lecturer at the Faculty of Engineering, Multimedia University

Although identity-based cryptography, first proposed by Shamir in 1984, was meant to circumvent certificate management issues faced by traditional public key cryptography, it still maintained private key escrow, as the Trusted Authority generating the user secret keys had full access to every user's private key. In 2003, Al-Riyami and Paterson introduced the notion of certificateless cryptography, and subsequently many certificateless schemes such as encryption, signature, were introduced in literature. However, until this work there has been little work done to define and certificateless identification schemes. This talk will cover the formal definition and security model of certificateless identification schemes, present the cryptanalysis of Dehkordi and Alimoradi's initial attempt at certificateless identification, and show the first provable-secure constructions of certificateless identification schemes, both in the random oracle model and standard model.