Design and Analysis of Certificate-Free Public Key Cryptographic Schemes

Prof. Dr. Swee-Huay Heng[1,2]

[1]Vice President (R&D), Multimedia University

[2]Faculty of Information Science & Technology, Multimedia University

Email: shheng@mmu.edu.my

Abstract:

Public key cryptography without certificates has become a very popular research area within the cryptography community since 2001 due to its implicit certification property. In this talk, we shall cover on the design and analysis of public key cryptographic schemes in certificate-free settings, more specifically, in identity-based and certificateless settings. The concept of identity-based cryptography that deals away with certificates was introduced by Shamir in 1984. Generally, an identity-based scheme is an asymmetric system wherein the public key is effectively replaced by or constructed from a user's publicly available identity information. The main negative consequence of identity-based schemes is the inherent key escrow or key recovery problem. In order to solve this problem while keeping the implicit certification, a new paradigm called certificateless public key cryptography was introduced by Al-Riyami and Paterson in 2003. Over the past 10 years, we have designed, analysed and cryptanalysed many certificate-free public key cryptographic schemes. In this talk, we shall provide some introduction on the certificate-free settings and the underlying frameworks. We shall then introduce and summarise briefly cryptographic schemes with provable security that we have designed and cryptanalysed to date. This covers primitives such as encryption, signature and identification.

Keywords: identity-based, certificateless, encryption, signature, identification, cryptanalysis