ID-based Cryptography: Introduction, Variants & Applications

Prof. Dr. Bok-Min Goi[1], Syh-Yuan Tan[2], Yar-Ling Tan[1]

[1]Faculty of Engineering and Science,
Universiti Tunku Abdul Rahman, Kuala Lumpur, Malaysia

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

Email: goibm@utar.edu.my

Abstract:

Cryptography aims to enable users to communicate with one another securely over an insecure channel by constructing schemes or protocols to ensure users' privacy and authenticity. Public key cryptography (PKC) enables different communication parties to exchange messages securely in an insecure channel. However, issues such as storage and key management arose as a certification authority is needed to generate certificate to authenticate each user's public key. Therefore, ID-based cryptography is potent as it eliminates the issues in PKC. Furthermore, ID-based cryptography has brought forth to the development of fuzzy ID-based and attribute-based cryptography. In this paper, we present the concept of identity-based cryptography and its variants as well as discuss on their applications.

Keywords: ID-based, Fuzzy ID-based, Attribute-based, Cryptography.