Malaysian Journal of Mathematical Sciences

Journal homepage: https://einspem.upm.edu.my/journal

Group Identity-Based Identification: Definitions, Construction and Implementation

Vangujar, A. K. *[1], **Ng, T. S.**[2], **Chia, J.**[1], **Chin, J. J.**[1,3], and **Yip, S. C.**[1]

[1]*Faculty of Engineering, Multimedia University, Malaysia*
[2]*School of Electrical & Electronic Engineering, Yonsei University, Seoul*
[3]*Information Security Lab, MIMOS Berhad, Malaysia*

E-mail: apurva710@gmail.com
**Corresponding author*

Received: 29 October 2020
Accepted: 5 July 2021

Abstract

As an extension of identification schemes in multiparty setting, we propose the first definitions and construction for a Group Identity-Based Identification (Group-IBI) scheme. The Group-IBI involves a group manager ($\mathcal{GM}$) that is in charge of a specific group, which in turn manages several group members. The $\mathcal{GM}$'s role is not only to control the registration and revocation of the members, but also to perform an identification protocol with a verifier as a whole entity, i.e., a group. The Group-IBI scheme that we proposed is potentially suitable for numerous real-world online applications such as e-shopping, e-banking, and e-voting where consensus of all members of a group is required to be derived before proceeding with authentication. In this paper, we propose the first definitions and security models for Group-IBI. We also show the first provable-secure construction that is pairing free by using the Schnorr identity-based identification (IBI) and Schnorr signature.

Keywords: multiparty schemes; identity-based identification scheme; provable security.