*The Second Indonesian-Japanese Conference on Knowledge Creation and Intelligent Computing (KCIC) 2013*

*ISBN : 978-602-9494-68-6*

# A Light-Weight Group Signature Scheme for Wireless Networks Based-on BBS Short Group Signature

Amang Sudarsono and Mike Yuliana
Division of Telecommunication Engineering, Dept. of Electrical Engineering,
Electronic Engineering Polytechnic Institute of Surabaya (EEPIS), Surabaya, Indonesia.
EEPIS Campus, Jalan Raya ITS Sukolilo, Surabaya 60111
Email :amang@eepis-its.edu, mieke@eepis-its.edu

**Abstract**

*In the natural context of wireless network environment, the communications between wireless nodes are more easily observed for the goal of the network traffic analysis. Thus, to enable a secure and anonymous communication system from thwarting of such analysis attacks would be strongly desirable. In this paper, we propose a secure and anonymous communication system using pairing-based group signatures. The achievement of secure and anonymous communication is performed by allowing all valid member wireless nodes of a particular privilege group to authenticate each other without revealing their own identities.*

Keywords: group signature, anonymity, signer, verifier, wireless networks, authentication.

## 1. Introduction

Recently, there are numerous ubiquitous services growing rapidly along with the advancement of personal computer, laptop, smart phone, and other embedded devices. Almost services require an authentication or identification for accessing control and authorization. As the result the accessed services by a user can be linked and tracked, hence the system obtained the user preference access history. One of user-privacy problem solving in the privacy-preserving authentication systems is the use of group signature, since it is very practical and able to provide not only the anonymity, but also unlinkability and untraceability.

Group signature is a kind of digital signature based on public key (one is given to a privilege group, not to one user). The group signature was introduced by Chaum and Heyst [13] for the first time. Currently, group signature also becomes one of the main topics in the cryptographic technology and many researchers actively have been taking in account such topic of interest [2–9]. The group signature scheme allows the users to sign messages without revealing their own privacy information (i.e. identity). In case of misuses or other reasons, there is an authority called group manager (GM) can trace the signer. Many applications of group signature also have been proposed and studied [6, 9]. In this paper, we consider the use of group signature for communication protocol in the wireless mobile networks such that able to provide a secure and anonymous communication.

Again, in the current era of pervasive computing, where ubiquitous services exist as an integrated part of our environment settings. Thus, computers, handhelds, gadgets, and other mobile devices are going to be exchanging messages nodes with each other (e.g., wireless networks, sensor networks, vehicle-2-vehicle communications [6, 9–11]). To satisfy these systems requirement such that they are able to work properly, every message has to deliver the most important information of authentication. However, the system requirements on the authentication are depend on any cryptographic solution. Ideally, such requirements should fulfill the following matters simultaneously:

a. Low bandwidth consumption: that due to the limited spectrum available for wireless communication, sensor network, and vehicular communication. Thus, a mechanism to achieve any shorter than RSA signatures is needed (i.e., shorter signature size, shorter processing time, shorter bit-length, lower power consumption).
b. Fast verification for large numbers of messages from different sources: that due to the suggestion of [12]whereas the safety message re-transmission of vehicles is done every 300ms to all other vehicles within 110 meters of a minimum range. This means that it is much more critical in the authentication phase. Therefore, it is better if the verification process is faster than generation process.
c. Privacy-friendly or anonymity: that due to users-privacy information should be protected from the information involved for every authentication process.

One of applications requiring group signatures in wireless network implementation for IEEE802.1X-based wireless protocol [6] showed the effectiveness of using group signature to achieve a user-privacy enhancing authentication. The modification of verifier-local