International Journal of Innovative Computing, Information and Control
Volume **6**, Number **5**, May **2010**

 ISSN 1349-4198
pp. 2341–2351

NONIDENTIFIABLE RFID PRIVACY PROTECTION WITH OWNERSHIP TRANSFER

Iuon-Chang Lin[1], Ching-Wen Yang[2] and Shyh-Chang Tsaur[2]

[1]Department of Management Information Systems
National Chung Hsing University
Taichung, Taiwan
iclin@nchu.edu.tw

[2]Department of Electronic Engineering
National Chin-Yi University of Technology
Taichung County, Taiwan
{ aawen0505; sctsaur }@gmail.com

Received December 2008; revised May 2009

Abstract. *RFID application brings huge conveniences, but low-cost tags were not designed to have much access control mechanism. The tag's information is easily read by anyone. So far, there are many schemes proposed to protect the user privacy for using RFID. In general, user privacy includes data privacy and location privacy. Most of the proposed schemes just provide the protection for data privacy. Recently, the scheme proposed by Lee can protect both data privacy and location privacy. Our scheme is based on the scheme proposed by Lee, and we improve Lee's weakness and make it can apply on someone sells his RFID system in security, to make our scheme achieves the property of ownership transfer.*
Keywords: RFID, Data privacy, Location privacy, Ownership transfer and dynamic ID

1. **Introduction.** Radio Frequency Identification (RFID) has been promoted in the past few years by Wal-Mart, the biggest retailer in the world, and the DOD (Department Of Defense) of US and also has been the extremely popular technology nowadays. Because the information sending and receiving of RFID is by using the wireless radio waves, therefore, it is an important research issue how to improve the data security and the user privacy. Data privacy means that attackers use illegitimate reader to eavesdrop the information of tag without user's consent. Location privacy means that attackers can collect those messages and trace the user's location when tags send some messages. If we want to protect the data privacy and location privacy at the same time, the ID location of the tag in RFID should not be fixed, otherwise it is easy to be tracked and attackers even steal the information of tag.

The security requirement of authentication is a very important issue in several topics that need to confirm the authorization [6, 8, 10]. The concept is also applied to protect user privacy in RFID systems. RFID authentication mechanism can protect the transmitted message from modification, and can authenticate the authorized reader. However, the transmission between tag and reader would expose tag's information. Therefore, RFID security authentication mechanism still exist legal user privacy issues. For example, using simple and quick one-way hash function, and X-OR operation to encrypt tag ID such as Hash Lock scheme [11] and Randomized Hash Lock scheme [11]. But in those schemes, the encrypted ID for each round is the same, so they can't protect location privacy. Furthermore, some schemes apply symmetric cryptographic algorithm and asymmetric