International Journal of Innovative
Computing, Information and Control
Volume **6**, Number **12**, December **2010**

 ISSN 1349-4198
pp. 5463–5471

EFFICIENT AND SCALABLE KEY AGREEMENT SCHEMES FOR MOBILE RFID READERS AND SERVERS

Hung-Yu Chien[1] and Tzong-Chen Wu[2]

[1]Department of Information Management
National Chi-Nan University
Puli, Nantou County, Taiwan
hychien@ncnu.edu.tw

[2]Department of Information Management
National Taiwan University of Science and Technology
43, Sec.4, Keelung Rd., Taipei, 106, Taiwan
tcwu@mail.ntust.edu.tw

Received August 2009; revised December 2009

Abstract. *Traditionally, researchers have assumed that the channels between Radio Frequency Identification (RFID) readers and backend servers are secure or that RFID readers can afford computationally-expensive cryptographic schemes. However, as RFID is being integrated into legacy systems like Enterprise Resource Planning (ERP) and low-cost RFID readers are becoming more and more popular for their cost-savings, the security between RFID readers and backend servers should be further examined. Lo et al. proposed an efficient reader-server authenticated key agreement scheme to meet the requirement. However, we find several fatal security weaknesses in Lo et al.'s scheme. In this paper, we reveal these weaknesses and propose two new schemes to improve security, computational performance, and communication. We provide two efficient solutions: one is for a single domain without a trusted third party, and the other is for multi-domains where a trusted third party is required. These merits make our solution more suitable and flexible for practical applications.*
Keywords: RFID, Security, Authentication, Elliptic curves, Public key, Key agreement

1. **Introduction.** An RFID system is composed of tags, readers and servers. Communication between tags and readers occurs through a wireless channel; communication between readers and servers can occur through a wired or wireless link. Due to its low cost and the convenience of identifying an object without line-of-sight reading, RFID has found many practical applications in supply chain management, package tracking, and manufacturing.

As RFIDs are becoming more and more popular, the security of RFID systems has drawn extensive attention from both academics and industry. However, most previous studies on RFID security like [1-5] have focused on the wireless channel between readers and tags. Many researchers assume that both backend servers and readers have enough resources to implement conventional computationally-expensive cryptographic protocols like [6-8] in order to secure the channel between them. However, this assumption might not hold, as pervasive and low-cost readers are becoming more popular. Furthermore, RFID is being integrated into legacy systems, and low-cost readers are communicating with distinct servers in specific domains through wireless channels [9]. These emerging scenarios call for new security mechanisms for RFID-based systems.

Lo et al. [10] considered the reader-to-server channel when they designed their RFID authentication scheme. To gain efficiency, Lo et al. utilized elliptic curve cryptography