Chapter 12
Building Scalable, Private RFID Systems

Li Lu
University of Electronic Science and Technology of China, China

ABSTRACT
Due to low cost and easy deployment, RFID has become a promising technology in many applications, such as retailing, medical-patient management, logistics, and supply chain management. Although a number of RFID standards have been issued and widely adopted by many off-the-shelf products, those standards, however, scarcely added privacy concerns because of computing and communication patterns. On the other hand, in RFID systems, RF tags emit their unique serial numbers to RF readers. Without privacy protection, however, any reader can identify a tag ID via the emitted serial number. Indeed, a malicious reader can easily perform bogus authentications with detected tags to retrieve sensitive information within its scanning range. The main obstacle to preserving privacy in RFID systems lies in the capability of tags. Due to the cost consideration, common RFID tags have tight constraints on power, computational capacity, and memory. Therefore, the mature cryptographic tools for bulky PCs are not suitable for RFID devices. In this chapter, the author focuses on the privacy issue to establish scalable and private RFID systems. The chapter first discusses the privacy issue in RFID systems; and then correspondingly introduces privacy preserving techniques including privacy-preserving authentication and secure ownership transfer. Finally, the theoretic formal privacy models for RFID systems are given, in which the author formally defines privacy and the behaviors of adversaries in RFID systems. Based on a formal model, say the weak privacy model, the chapter illustrates the methodology for designing highly efficient privacy-preserving authentication protocols.

12.1 OVERVIEW
Privacy is a basic requirement of human beings. “Privacy is the quality or state of being apart from company or observation; and the freedom from unauthorized intrusion” – (Merriam-Webster (2009)). In the information technology, privacy requires protecting the users’ private information from being exposed to unauthorized individuals or organizations.

In RFID systems, RF tags emit their unique serial numbers to RF readers. Without privacy
Building Scalable, Private RFID Systems

protection, however, any reader can identify a tag ID via the emitted serial number. Indeed, within the scanning range, a malicious reader can easily perform bogus authentications with detected tags to retrieve sensitive information. Today, many companies embed tags in items. Since the tags indicate information of the items, a customer carrying those tags is subject to silent tracking from unauthorized readers. Sensitive personal information might be exposed: the illnesses she suffers from, indicated by the pharmaceutical products; the malls where she shops; the types of items she prefers to buy, and so on. The majority of today’s RFID applications lose sight of privacy, which exacerbates serious threats from emerging attacks.

12.2 PRIVACY-PRESERVATION IN RFID SYSTEMS

The basic type of RF tag identification is a “challenge-response” procedure. That is, a reader sends a request as a challenge to a tag, and then receives the corresponding response from the tag, as plotted in Figure 1.

The basic type of RF tag identification leaks the private information of RF tags. To preserve privacy, many Privacy-Preserving Authentication, PPA, Protocols have been proposed to achieve private authentication in RFID systems. Weis (Weis, Sarma, Rivest & Engels (2003)) proposed a hash function based authentication scheme, HashLock, to avoid tags being tracked, as illustrated in Figure 2. In this approach, each tag shares a secret key $k$ with the reader. The reader sends a random number $r$ as the authentication request. To respond to the reader, the tag uses a hash function $h$ to generate a response $h(k, r)$ on the inputs of $r$ and $k$. The reader then computes $h(k, r)$ of all stored keys until it finds a key to recover $r$, thereby identifying the tag. The search complexity of HashLock is linear in $N$, where $N$ is the number of tags in the system. Subsequent approaches in the literature mostly aimed at improving the efficiency of key search. Juels (Juels (2006)) classifies those approaches into three categories.

Synchronization approaches: Such approaches (Ohkubo, Suzuki & Kinoshita (2004), Juels (2004), Dimitriou (2005), Tsudik (2006)) use an incremental counter to record the state of authentication. When an authentication is successfully performed, the tag increases the counter by one. The reader compares the value of a tag’s counter with the record in the database. If the difference of the two counter values is in a proper window, the tag is viewed as valid and the reader synchronizes the counter record of the tag. Synchronization schemes are subject to the De-synchronization Attack, in which a malicious reader interrogates a tag so many times such the counter of the tag exceeds the range of the window and the reader fails to recognize a valid tag.

Time-space tradeoff approaches: OSK (Ohkubo, Suzuki & Kinoshita (2004)) and AO (Avoine & Oechslin (2005)) employ Hellman tables to

Figure 1. Challenge-response based RFID authentication