A Secure Protocol for Ultralightweight Radio Frequency Identification (RFID) Tags

Aras Eghdamian and Azman Samsudin

School of Computer Sciences, Universiti Sains Malaysia, 11800 Pulau Pinang, Malaysia
ae11_coml09@student.usm.my, azman@cs.usm.my

Abstract. Recently, an ultra light weight protocol for RFID tags has been published. The advantage of this protocol was its low computation cost, but it fails in its security objectives, being vulnerable to several important attacks such as traceability, full disclosure, cloning and desynchronization. In this research, that protocol was enhanced and a new Ultralightweight RFID authentication protocol with mutual authentication was proposed, while keeping the computation cost low. The proposed protocol requires only simple bit-wise operations and can resist various attacks which the previous one could not.

Keywords: RFID, Security, Ultralightweight RFID, Mutual Authentication Protocol.

1 Introduction

RFID as a significant and simultaneously growing technology has revolutionized the automatic identification of objects. RFID is used in many different areas ranging from automobile manufacturing, microchip fabrication industries, credit cards, e-passports, and many more. The advantages in this unique technology are numerous but the most notable is contactless, so that the Tag can be read from a distance.

The challenge that most of the Ultralightweight RFID systems face is the issue of authentication, in which the inadequate secure authentication mechanism, in most of the RFID systems, is currently being debated. Researchers have been directed toward making a mutual authentication in which the security is in its maximum. If security measures are not taken, a Tag or a Reader may lose its information easily. Protecting the privacy is a vital requirement for Tag holders; in which most of the RFID systems are lacking.

Peris et al. in their investigation in 2006 [1,2,3] initiated the design of Ultralightweight RFID protocols which includes only simple bitwise logical or arithmetic operations such as bitwise XOR, OR, AND, and addition. This combination of operations was discovered later to be inadequate for security. In 2007, Chien et al. proposed the SASI protocol [4] in order to offer a better security and they added the bitwise rotation to the set of supported operations. Although certain attacks have been published against the SASI protocol, this scheme reflected as a turning point in the design of Ultralightweight RFID protocols [5,6,7]. In 2008, a new protocol, named...
“Gossamer” [8], was proposed that can be considered as a further development of both the UMAP [1,2,3] family and SASI [4].

Lee et al. in 2009 [9] has published a RFID scheme that resemblance SASI. Although the computation cost of Lee’s protocol in comparison with other existing protocols is low, it fails in its security objectives, being vulnerable to several important attacks like traceability, full disclosure, cloning and desynchronization [10]. This research propose an Ultralightweight RFID authentication protocol with mutual authentication based on Lee’s protocol but without its security short comings, and at the same time, keep the computation cost low.

2 Lee et al.’s Protocol

There are three entities in the Lee et al.’s protocol [9]: Tag, Reader, and Server on the backend. Suppose that the channel between the Reader and the backend Server is secure, but the communication channel between the Reader and the Tag is susceptible to all the possible attacks due to its open nature. Let ID be a static identification for a Tag. Tag shares a dynamic temporary identification (IDT) and secret key (K) with the backend Server. The length of each ID, IDT or K is 128 bits. To resist the possible desynchronization attack, each Tag keeps two entries of (IDT, K): one is for the old values and the other is for the potential next values. The protocol consists of two main stages: authentication phase and key updating phase. In authentication phase, the Reader first inquires the Tag, and then the Reader and the Tag authenticate each other. In the following key updating phase, the Reader and the Tag, respectively, update their temporary identifications and secret keys.

In Lee et al.’s protocol, the random number generator is installed in the Server only, and calculations at the Tags involve only simple bitwise operations such as XOR ($\oplus$), OR ($\lor$), AND ($\land$), and left rotate $\text{Rot}(A, B)$, where $\text{Rot}(A, B)$ denotes left rotate the value of $A$ with $n$ bits, where $n$ is the number of “1” in $B$.

Without loss of generality, suppose that the initial message in the Tag and Server are $(\text{IDT}_0, K_0)$, and $(A \rightarrow B: C)$ denotes A sends message C to B. At the $i$-th session, both the Tag and Server store $(\text{IDT}_i, K_i)$ and $(\text{IDT}_{i-1}, K_{i-1})$ in their memory. The authentication and key updating procedures are then described in the following subsections.

2.1 Authentication Phase

Step 1. ($Tag \rightarrow Reader: \text{IDT}_i$): The Tag first transmits $\text{IDT}_i$ to the Reader after the Tag receives a request message. Note that the temporary identification and secret key are updated on each session of the authentication.

Step 2. ($Reader \rightarrow Tag: A, B$): After receiving $\text{IDT}_i$ in Step 1, The Reader finds the Tag’s corresponding secret key $K_i$. Then the Reader generates a random number $N_i$ and computes $(A, B)$ as follows.