An Unconditionally Secure Lightweight RFID Authentication Protocol with Untraceability

Hung-Yu Chien[1], Jia-Zhen Yen[2]
and Tzong-Chen Wu[2,3]
[1]*Department of Information Management,*
National Chi-Nan University
[2]*Department of Information Management,*
National Taiwan University of Science and Technology
[3]*Taiwan Information Security Center (TWISC) at*
National Taiwan University of Science and Technology
Taiwan

1. Introduction

Radio frequency identification (RFID) is a wireless technology that uses radio signals to identify objects automatically and remotely. The most popular tags are passive devices owing to their low cost. Nowadays, RFID devices are widely deployed in many applications, such as supply chain management, inventory control, contactless credit card and so on, due to the low-cost and convenience in identifying objects with non-line-of sight reading, However, there are many potential security threats around the tiny RFID tags attached to users. The carrying items or privacy information contained in these tags might be compromised. Furthermore, low-cost makes these tags very resource-limited, which makes it very challenging to design secure protocols for these tags.

From the point of end user's side, a secure RFID system should provide the capability of location/content privacy protection, anonymity, untraceability and availability [2]. Several RFID lightweight authentication protocols like [4-10] have been developed, but not all of them satisfy all the security requirements. All the previously proposed protocols are designed to be computationally secure, i.e., the security depends on the hardness of solving mathematical problem. Recently, Alomair *et al*. [1] proposed an unconditionally secure lightweight RFID (UCS-RFID for short) protocol, and claimed that their protocol achieved unconditional secrecy and unconditionally integrity. The security of the UCS-RFID protocol depends on the freshness of the keys. However, the UCS-RFID protocol does not achieve backward untraceability, even though it does achieve forward untractability.

Forward and backward untraceability are important privacy properties for RFID authentication protocol [4]. Forward untraceability requires that even if the adversary reveals the internal state of a tag at time τ, the adversary still cannot know whether a transaction after time $\tau + \delta$ (for some $\delta > 0$) involves the same tag or not, provided that the adversary does not eavesdrop on the tag continuously after time τ. Backward untraceability requires that even if the adversary reveals the internal state of a tag at time *τ*, the adversary is not able to tell whether a transaction before time *τ* involves the same tag or not [3]. These two properties are important for the RFID systems that the equipped tags are low-cost and potentially prone to being captured and compromised.

Notation	Description
R	RFID reader
T_i	i-th RFID tag
S	Back-end database
p	A 2N-bit prime integer, where N is …..
Z_p	The finite integer ring with usual addition and multiplication modulo p
Z_p^*	The multiplicative group modulo p, Z_p^* contains all non-zero elements of Z_p; that is, $Z_p^* = Z_p \setminus \{0\}$
$n^{(m)}$	n denotes a 2N-bit random number which is drawn uniformly from the Z_p^*, m denotes that it is used in the m-th session
$n_l^{(m)}$	The left N most significant bits of $n^{(m)}$
$n_r^{(m)}$	The right N least significant bits of $n^{(m)}$
$K_i^{(m)}$	The secret keys of the RFID tag T_i . They consist of five subkeys, i.e., $K_i^{(m)} = (k_{a\ i}^{(m)}, k_{b\ i}^{(m)}, k_{c\ i}^{(m)}, k_{d\ i}^{(m)}, k_{e\ i}^{(m)})$. The superscript m denotes the m-th run, and the subscript i denote the i–th tag T_i .
$k_{a\ i}^{(0)}$	A subkey which is initially drawn independently and uniformly from Z_{2^N}
$k_{b\ i}^{(0)}$	A subkey which is initially drawn uniformly from Z_p
$k_{c\ i}^{(0)}$	A subkey which is initially drawn independently and uniformly from Z_p^*
$k_{d\ i}^{(0)}$	A subkey which is initially drawn independently and uniformly from Z_{2^N}
$k_{e\ i}^{(0)}$	A subkey which is initially drawn independently and uniformly from Z_p^* that will be used for updating the secret keys to maintain certain properties

Table 1. Notations or Symbols

In this book chapter, we first examine the USC-RFID protocol, and show that the USC-RFID protocol does not achieve backward untraceability. After that, we will extend the USC-RFID protocol to an enforced one with untraceability.

2. The UCS-RFID protocol

The UCS-RFID procotol [1] is a lightweight RFID authentication protocol and is the first RFID protocol providing unconditional security for low-cost tags. The UCS-RFID protocol has the merits that it does not require tags to support random number generation and it requires only one simple multiplication on tags. The security of this protocol mainly relies on the RFID reader's capability to deliver random numbers to RFID tags in an authenticated and secure way.

The UCS-RFID protocol consists of four phases: the tag identification phase, the reader authentication phase, the tag authentication phase, and the key updating phase (see Fig. 1 for more details). For the convenience of describing the UCS-RFID protocol, we first introduce the notations or symbols shown in Table 1. Initially, each tag T_i has a secret key set $K_i^{(0)}$ shared with the back-end database. In the following, we describe the *m*-th run of the protocol.

Tag identification phase

i. The reader *R* sends a *Hello* message to the tag T_i.

ii. T_i sends its message $A^{(m)}$ to *R*, and *R* forwards this message $A_i^{(m)}$ to the back-end database *S*.

iii. *S* looks up the database for the secret key $K_i^{(m)}$ corresponding to the message $A_i^{(m)}$. If the $A_i^{(m)}$ could be identified as a valid identifier, then *S* sends back the tag's secret key $K_i^{(m)}$ to *R*. Otherwise, the tag T_i is rejected.

Reader Authentication Phase

i. *R* generates a random number $n^{(m)}$, computes $B^{(m)} \equiv n^{(m)} + k_{b\ i}^{(m)} \bmod p$ and $C^{(m)} \equiv n^{(m)} \times k_{c\ i}^{(m)} \bmod p$, and then sends these two messages ($B^{(m)}$, $C^{(m)}$) to T_i.

ii. After receiving $B^{(m)}$ and $C^{(m)}$, T_i extracts $n^{(m)} \equiv (B^{(m)} - k_{b\ i}^{(m)}) \bmod p$, and then verifies its integrity via checking whether the equation $(B^{(m)} - k_{b\ i}^{(m)}) \times k_{c\ i}^{(m)} \equiv C^{(m)} \bmod p$ holds. If so, *R* is authenticated; otherwise, the tag aborts the protocol.

Tag Authentication Phase

i. T_i computes $D^{(m)} = n_l^{(m)} \oplus k_{d\ i}^{(m)}$ and returns this value.

ii. After receiving the value, *R* verifies whether the equation $D^{(m)} \overset{?}{=} n_l^{(m)} \oplus k_{d\ i}^{(m)}$ holds. If so, the tag is authenticated; Otherwise, the tag is rejected.

Key Updating Phase: After a successful mutual authentication between the tag and the reader, the secret key and the tag identifier are updated at the back-end database and the tag respectively as specified in Fig. 1. Fig. 1 depicts the protocol for the *m*-th run.

The above protocol cannot deter possible denial-of-service attacks (DOS attacks), and Alomair et al. had extended the above protocol to prevent DOS attacks and possible key exposure problem. Since these extensions are not relevant to our improvements, we will not discuss these parts for easy presentation, and interested readers are referred to [1] for details.

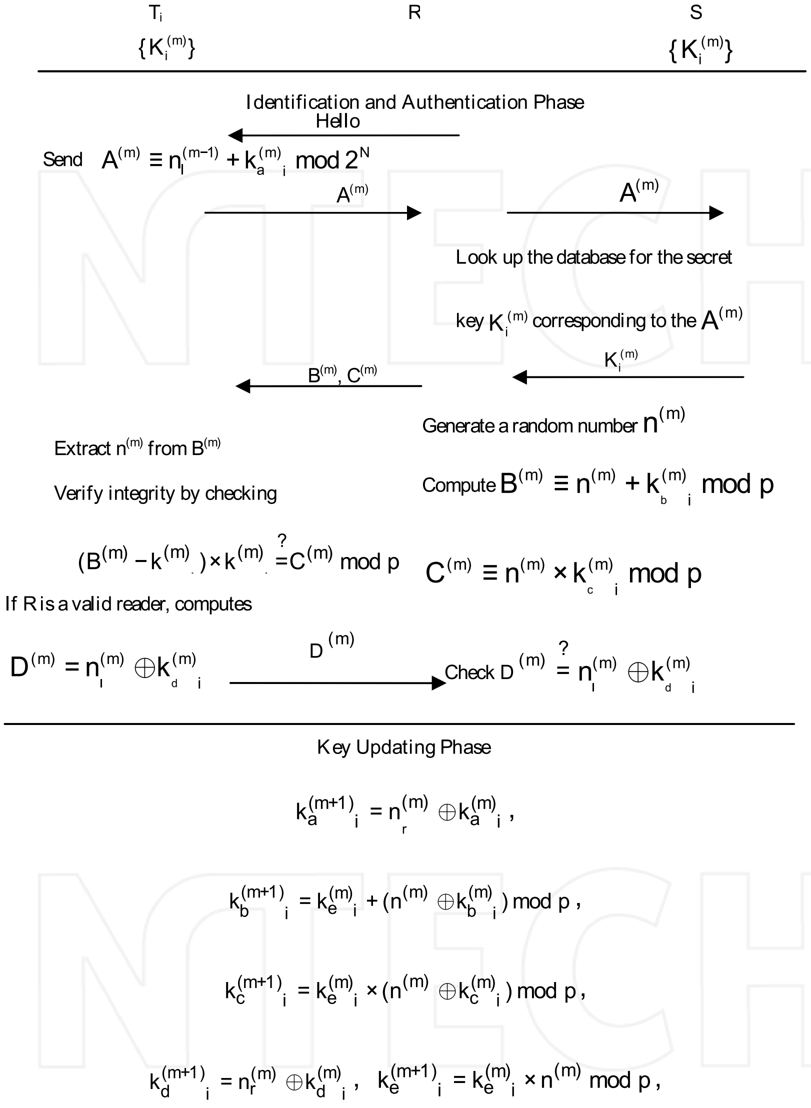
T_i
R
S
$\{K_i^{(m)}\}$
$\{K_i^{(m)}\}$
Identification and Authentication Phase
Hello
Send $A^{(m)} \equiv n_I^{(m-1)} + k_{a\ i}^{(m)} \bmod 2^N$
$A^{(m)}$
$A^{(m)}$
Look up the database for the secret
key $K_i^{(m)}$ corresponding to the $A^{(m)}$
$K_i^{(m)}$
$B^{(m)}, C^{(m)}$
Generate a random number $n^{(m)}$
Extract $n^{(m)}$ from $B^{(m)}$
Verify integrity by checking
Compute $B^{(m)} \equiv n^{(m)} + k_{b\ i}^{(m)} \bmod p$
$(B^{(m)} - k^{(m)}) \times k^{(m)} \overset{?}{=} C^{(m)} \bmod p$
$C^{(m)} \equiv n^{(m)} \times k_{c\ i}^{(m)} \bmod p$
If R is a valid reader, computes
$D^{(m)} = n_I^{(m)} \oplus k_{d\ i}^{(m)}$
$D^{(m)}$
Check $D^{(m)} \overset{?}{=} n_I^{(m)} \oplus k_{d\ i}^{(m)}$
Key Updating Phase
$k_{a\ i}^{(m+1)} = n_r^{(m)} \oplus k_{a\ i}^{(m)}$,
$k_{b\ i}^{(m+1)} = k_{e\ i}^{(m)} + (n^{(m)} \oplus k_{b\ i}^{(m)}) \bmod p$,
$k_{c\ i}^{(m+1)} = k_{e\ i}^{(m)} \times (n^{(m)} \oplus k_{c\ i}^{(m)}) \bmod p$,
$k_{d\ i}^{(m+1)} = n_r^{(m)} \oplus k_{d\ i}^{(m)}$, $k_{e\ i}^{(m+1)} = k_{e\ i}^{(m)} \times n^{(m)} \bmod p$,

Fig. 1. The UCS-RFID protocol.

3. Extending the USC-RFID to untraceability

In Section 3.1, we examine the untraceability of the USC-RFID protocol, and then provide an improved scheme to enhance its untraceability.

3.1 Untraceability of the UCS-RFID protocol

Here we show that the UCS-RFID protocol does not provide backward untraceability as follows.

Suppose the tag T_i has been compromised and the internal secrets $A^{(m)} \equiv n_l^{(m-1)} + k_{a\ i}^{(m)} \bmod 2^N$ and $K_i^{(m)}$ =($k_{a\ i}^{(m)}$, $k_{b\ i}^{(m)}$, $k_{c\ i}^{(m)}$, $k_{d\ i}^{(m)}$, $k_{e\ i}^{(m)}$) are revealed at time *τ*. Let (*A*, *B*, *C*, *D*) be one eavesdropped message. Then we can tell whether the message (*A*, *B*, *C*, *D*) comes from the same tag or not as follows.

1. Derive $n_l^{(m-1)} = A^{(m)} - k_{a\ i}^{(m)} \bmod 2^N$.
2. Derive $k_{d\ i}^{(m-1)} = D \oplus n_l^{(m-1)}$, $n_r^{(m-1)} = k_{d\ i}^{(m)} \oplus k_{d\ i}^{(m-1)}$ and $n^{(m-1)} = n_l^{(m-1)} \,||\, n_r^{(m-1)}$.
3. Now we can derive the previous internal state $k_{a\ i}^{(m-1)} = n_r^{(m-1)} \oplus k_{a\ i}^{(m)}$, $k_{e\ i}^{(m-1)} = k_{e\ i}^{(m)} \times (n^{(m-1)})^{-1} \bmod p$, $k_{b\ i}^{(m-1)} = (k_{b\ i}^{(m)} - k_{e\ i}^{(m-1)} \bmod p) \oplus n^{(m-1)}$, $k_{c\ i}^{(m-1)} = (k_{c\ i}^{(m)} \times (k_{e\ i}^{(m-1)})^{-1} \bmod p) \oplus n^{(m-1)}$ and $k_{d\ i}^{(m-1)} = n_r^{(m-1)} \oplus k_{d\ i}^{(m)}$.
4. Now we check whether the two equations $B \overset{?}{=} n^{(m-1)} + k_{b\ i}^{(m-1)} \bmod p$ and $C \overset{?}{=} n^{(m-1)} \times k_{c\ i}^{(m-1)} \bmod p$ hold. It is obvious that if the two equations hold, then the message (*A*, *B*, *C*, *D*) is the $(A^{(m-1)}, B^{(m-1)}, C^{(m-1)}, D^{(m-1)})$ from the compromised tag.

   We can recursively apply the above steps to trace the messages from the same tag for *i*-th run, where $i \le m-1$. That is, the USC-RFID protocol cannot provide backward untraceability.

Even though the USC-RFID protocol does not satisfy backward untraceability, it does provide forward untraceability. This is because, in forward untraceability, if the adversary reveals the internal state of a tag at time *τ*, it is required that the adversary does not eavesdrop on the tag *continuously* after time *τ*. It is this break of eavesdropping that makes the USC-RFID satisfy forward untraceability.

3.2 Enhancing the untraceability

The key to find the link in our backward traceability is that the equation $A^{(m)} = n_l^{(m-1)} + k_{a\ i}^{(m)} \bmod 2^N$ contains only one unknown value $n_l^{(m-1)}$ when the adversary learn the internal state $A^{(m)}$ and $K_i^{(m)}$ =($k_{a\ i}^{(m)}$, $k_{b\ i}^{(m)}$, $k_{c\ i}^{(m)}$, $k_{d\ i}^{(m)}$, $k_{e\ i}^{(m)}$); therefore, the adversary can derive $n_l^{(m-1)} = A^{(m)} - k_{a\ i}^{(m)} \bmod 2^N$ and the other values accordingly. We also notice that each of the other key updating equations in the key updating phase contains at least two unknown values. Therefore, we can amend the protocol by simply modifying this equation $A^{(m)} = n_l^{(m-1)} + k_{a\ i}^{(m)} \bmod 2^N$ to contain two unknowns. One simple suggestion is that $A^{(m)} = n_l^{(m-1)} + k_{a\ i}^{(m-1)} \bmod 2^N$. With this modification, the adversary should solve two unknowns in each equation to derive the secret even assume he has learned the current state ($A^{(m)}, k_{a\ i}^{(m)}$, $k_{b\ i}^{(m)}$, $k_{c\ i}^{(m)}$, $k_{d\ i}^{(m)}$, $k_{e\ i}^{(m)}$). It, therefore, cannot provide adversaries a unique and deterministic link to trace the tag.

4. Conclusion

In this book chapter, we have shown that the UCS-RFID protocol which is the first unconditionally secure mutual authentication protocol for RFID systems cannot satisfy backward untraceability, and we have proposed a simple amendment to enhance its backward untraceability. The unconditional secure RFID protocol is very promising approach for RFID security. In this book chapter, we have enhanced the first unconditional secure RFID protocol to satisfy untraceability. Our future work is to further analyze and improve the security of unconditional secure RFID protocols.

5. References

[1] B. Alomair, A. Clark, J. Cuellar, and R. Poovendran, Securing Low-Cost RFID Systems: an Unconditionally Secure Approach, 2010 Workshop on RFID Security – RFIDsec'10 Asia, 2010.

[2] H. -Y. Chien and C. -S. Laih, ECC-Based Lightweight Authentication Protocol with Untraceability for Low-Cost RFID, Journal of Parallel and Distributed Computing. 69 (10) (2009) 848-853.

[3] R. C. -W. Phan, J. Wu and K. Ouafi, Privacy Analysis of Forward and Backward Untraceable RFID Authentication Schemes, 2008. Available from : <http://www.cacr.math.uwaterloo.ca/~dstinson/papers/bfrfid-2.pdf/>.

[4] A. D. Henrici, and P. MÄuller, "Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers," In the Proceedings of PerSec'04 at IEEE PerCom, 2004, pp.149-153.

[5] S. Karthikeyan, M. Nesterenko, "RFID security without extensive cryptography," Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, 2005, pp. 63-67.

[6] D. Molnar and D. Wagner, "Privacy and security in library RFID: Issues, practices, and architectures," Conference on Computer and Communications Security – CCS'04, 2004, pp. 210–219.

[7] M. Ohkubo, K. Suzki and S. Kinoshita, "Cryptographic Approach to 'Privacy-Friendly' Tags," In RFID Privacy Workshop, 2003.

[8] S. A. Weis, "Security and Privacy in Radio-Frequency Identification Devices," Masters Thesis MIT, 2003.

[9] G. Avoine, E. Dysli, and P. Oechslin, "Reducing time complexity in RFID systems," The 12th Annual Workshop on Selected Areas in Cryptography(SAC), 2005.

[10] H. Y. Chien, "SASI: A New Ultra-Lightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity", IEEE Transactions on Dependable and Secure Computing 4(4), pp. 337-340, October, 2007.

Current Trends and Challenges in RFID
Edited by Prof. Cornel Turcu

ISBN 978-953-307-356-9
Hard cover, 502 pages
Publisher InTech
Published online 20, July, 2011
Published in print edition July, 2011

With the increased adoption of RFID (Radio Frequency Identification) across multiple industries, new research opportunities have arisen among many academic and engineering communities who are currently interested in maximizing the practice potential of this technology and in minimizing all its potential risks. Aiming at providing an outstanding survey of recent advances in RFID technology, this book brings together interesting research results and innovative ideas from scholars and researchers worldwide. Current Trends and Challenges in RFID offers important insights into: RF/RFID Background, RFID Tag/Antennas, RFID Readers, RFID Protocols and Algorithms, RFID Applications and Solutions. Comprehensive enough, the present book is invaluable to engineers, scholars, graduate students, industrial and technology insiders, as well as engineering and technology aficionados.

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821