Cryptanalysis of Some Protocols for RFID Systems

Masoumeh Safkhani†, Majid Naderi†, Nasour Bagheri+ and Somitra Kumar Sanadhya*
† Iran University of Science and Technology (IUST), Tehran, Iran.
+ Electrical Engineering Department, Shahid Rajaee University, Tehran, Iran.
* Indraprastha Institute of Information Technology (IIIT) Delhi, New Delhi, India.

***Abstract*— In this paper we analyze the security of the mutual authentication and ownership transfer protocols which have been recently proposed by Kulseng *et al.* Our analysis demonstrates a variety of attacks against these protocols. We present a secret parameters disclosure attack which discloses any secret parameter between the tag and the reader. Our disclosure attack can be easily used as an impersonation attack against the mutual authentication protocol. In addition, we present an attack that retrieves the PIN-value in the ownership transfer protocol, where the PIN-value is a parameter that must be kept secret from any party including the owner of the tag.**

All the attacks presented in this work are passive, have low complexity and have the success probability of 1.

***Index Terms*— RFID, Lightweight Mutual Authentication, Ownership Transfer Protocol, PUF, LFSR.**

I. Introduction

Mutual authentication protocols are employed by readers and tags in RFID systems to authenticate each other. Commonly, a mutual authentication protocol includes a game playing argument between the tag and the reader. One of the principals in the protocol poses some challenge(s) to the other principal and then verifies the response(s) received. In general, RFID authentication protocols need to authenticate both the entities to one another. Such protocols are referred to as mutual authentication protocols. On the other hand, an ownership transfer protocol is a protocol that transfers the ownership right of a tag securely from the old owner to the new owner such that:

- The old owner can not access the new RFID transactions after the occurrence of ownership transfer.
- The new owner can not access the old RFID transactions after the occurrence of ownership transfer.

Common use of an ownership transfer protocol is to reissue a tag attached with one product to another product in a shopping mall.

Several mutual authentication protocols [3], [10], [8], [9], [11] and ownership transfer protocols [5], [4], [12], [15] have been proposed in the literature recently. All the protocols mentioned here are claimed to be "lightweight protocols", i.e. they require low power to operate and require (non-specialized) low cost RFID tags/readers to operate. Some of these protocols, e.g. [13], [14], [7], rely on encryption or cryptographic hash functions for their security. However, Feldhofer and Rechberger [1] have shown that the number of gates required to implement most common hash functions on an RFID chip is very high. Consequently, the use of standard hash functions on RFID chips, and hence in RFID protocols, is ruled out. In fact, in order to promote the use of RFID technology in authentication, the cost of the RFID tags must be competitive with the available low cost solutions, e.g. bar codes, otherwise there is no incentive for businesses to use the RFID technology. Hence, the available protocols are not applicable in many applications which need low cost tags.

To overcome the above problems, Kulseng *et al.* have recently proposed a lightweight mutual authentication protocol and an ownership transfer protocol for RFID Systems[6]. Both these protocols do not use a block cipher or a hash function in their designs. These protocols rely on Physically Unclonable Functions (PUFs) and Linear Feedback Shift Registers (LFSRs) for their security. The designers' motivation was the efficiency of PUFs and LFSRs in hardware.

The designers have claimed optimal security for both the proposed mutual authentication protocol and ownership transfer protocol. However, in this work, we exhibit a variety of weaknesses in these protocols. We present an efficient attack which discloses any secret parameter, including the tag-identifier ID, which was shared between the tag and the reader prior to running the protocol. As an extension of this attack, we also develop an impersonation attack against the mutual authentication protocol. In addition, we present an attack that retrieves the PIN in the ownership transfer protocol. The PIN is a secret preloaded value in the tag which must be kept secret even from the owner of the tag.

II. Preliminaries

Through the paper, we use the following notations:

- ID: It is the static tag identifier which is always fixed, even through the ownership right transfer.
- IDS: It is the tag pseudonym which is updated after each successful run of the protocol.
- $P(.)$: It is the tag's random permutation function based on Physically Unclonable Function (PUF). Different tag's PUFs will produce different outputs for a certain input value.
- $F(.)$: It is a public random permutation function based on a Linear Feedback Shift Register (LFSR). The LFSR is assumed to be maximal length, which means its period for a non zero seed is $2^L - 1$ when the state of the LFSR is L bits long.
- G_n: It is a greeting number which is produced by the tag, utilizing the tag's $P(.)$-function and shared with the reader. After each successful run of protocol G_n is get updated.

- K_n, K'_n and K''_n: They are parameters which are used through the authentication and ownership transfer processes. These parameters are computed and updated by utilizing a public $F(.)$-function.
- K_t: It is a parameter which is computed as $K_t = LFSR(G_n \oplus G_{n+1})$.
- PIN: It's an identifier of tag which is shared between the Trusted Third Party (TTP) and the tag.
- All parameters in the protocol are of length L-bit.
- The expression $A \rightarrow B$ refers to assigning A to B.

III. Protocols Description

The kulseng *et al.* mutual authentication protocol and ownership transfer protocol are depicted in Fig. 1 and Fig. 2 respectively.

The mutual authentication protocol includes two phase that are the setup phase and the mutual authentication phase. In the setup phase the secret values are preloaded to the tag and the reader. These secret values are IDS, ID and G_n where ID and G_n are updated in each round and the reader also keep G_{n+1}. In addition, they share a permutation function F. This function can be an LFSR which its implementation details are known to all parities includes the adversary [[6], Section III]. Tag also employs a random function P based on PUF.

In the mutual authentication phase, the reader sends Req and the tag responses with its IDS. The reader uses this value to find the shared secret values with this tag and sends $ID \oplus G_n$ to the tag. The tag use this value to authentication the reader. Whenever the tag authenticates the reader it updates G_n and sends $G_{n+1} \oplus F(G_n)$ and $G_{n+2} \oplus F(F(G_n))$ to the reader. The reader knows G_n and F. Hence, it can extract G_{n+1} from $G_{n+1} \oplus F(G_n)$ which can be used as a measure to authenticate the tag. Whenever the reader authenticates the tag it extractG_{n+2} from $G_{n+2} \oplus F(F(G_n))$ and consider it as the new value of G_{n+1} while it use G_{n+1} as the new value of G_n. In addition, the tag and the reader updates IDS to $F(IDS \oplus G_n)$. The details of the mutual authentication protocol is depicted in Fig. 1.

The ownership transfer protocol includes two phase that are the setup phase and the Ownership transfer phase. In the setup phase, the old reader pass the stored $\{IDS, ID, G_{n+1}\}$ to the new reader and the verification pair $\{G_n, G_{n+1}\}$ to TTP. TTP and tag also share the secret value PIN.

The details of ownership transfer phase is depicted in Fig. 2. In this phase the new reader pass a secure request to TTP and use G_{n+1} as a proof for its claim to access the tag. TTP sends $F(PIN) \oplus PIN \oplus G_n$ to the new reader and it pases this value to the tag. The tag extract G_n for the received value and uses it to authenticate TTP. Whenever the tag authenticates TTP it computes a new pair of G'_n and G'_{n+1} to replace the old values such that $G'_n = P(G_{n+2})$ and $G'_{n+1} = P(G'_n)$. The tag pases $G'_n \oplus F(F(G_n))$, $G'_{n+1} \oplus F(F(F(G_n)))$ and $K_t = F(G_n \oplus G_{n+1})$ to the new reader. The new reader pass the received value to TTP. TTP verifies the correctness of K_t and extract G'_n and G'_{n+1} form the received values and sends them through a secret channel to the new reader. Finlay, the tag and TTP update PIN to $F(PIN \oplus G_n)$.

Algorithm 1: Secret parameters disclosure attack against the Kulseng *et al.* mutual authentication protocol.

Online Phase;
Eavesdrop the first run of the mutual authentication protocol and store the $((IDS)_1, (ID \oplus G_n)_1, (G_{n+1} \oplus K_n)_1, (G_{n+2} \oplus K'_n)_1)$ triplet;
Eavesdrop the second run of the mutual authentication protocol and store the $((IDS)_2, (ID \oplus G_n)_2, (G_{n+1} \oplus K_n)_2, (G_{n+2} \oplus K'_n)_2)$ triplet;

Off line Phase;
$F^{-1}((IDS)_2) \rightarrow (IDS)_1 \oplus (G_n)_1$;
$(IDS)_1 \oplus (G_n)_1 \oplus (IDS)_1 \rightarrow (G_n)_1$; // $(G_n)_1$ disclosures;
$(ID \oplus (G_n))_1 \oplus (G_n)_1 \rightarrow ID$; // ID disclosures;
$F(G_n) \rightarrow K_n$;
$F(K_n) \rightarrow K'_n$;
$(G_{n+1} \oplus K_n)_1 \oplus K_n \rightarrow G_{n+1}$; // $(G_{n+1})_1$ disclosures;
$(G_{n+2} \oplus K'_n)_1 \oplus K'_n \rightarrow G_{n+2}$; // $(G_{n+2})_1$ disclosures;
$G_{n+1} \rightarrow G_n$;
$G_{n+2} \rightarrow G_{n+1}$;
$F(IDS \oplus G_n) \rightarrow IDS$; // IDS disclosures;
$F(G_n) \rightarrow K_n$;
$F(K_n) \rightarrow K'_n$;
$(G_{n+1} \oplus K_n)_2 \oplus K_n \rightarrow G_{n+1}$; // $(G_n)_2$ disclosures;
$(G_{n+2} \oplus K'_n)_2 \oplus K'_n \rightarrow G_{n+2}$; // $(G_{n+1})_2$ disclosures;
$G_{n+1} \rightarrow G_n$; // G_n disclosures;
$G_{n+2} \rightarrow G_{n+1}$; // G_{n+1} disclosures;
return (IDS, ID, G_n, G_{n+1});

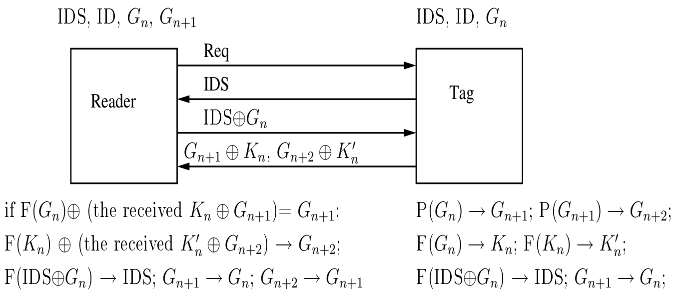

Fig. 1. The mutual authentication protocol of Kulseng *et al.*

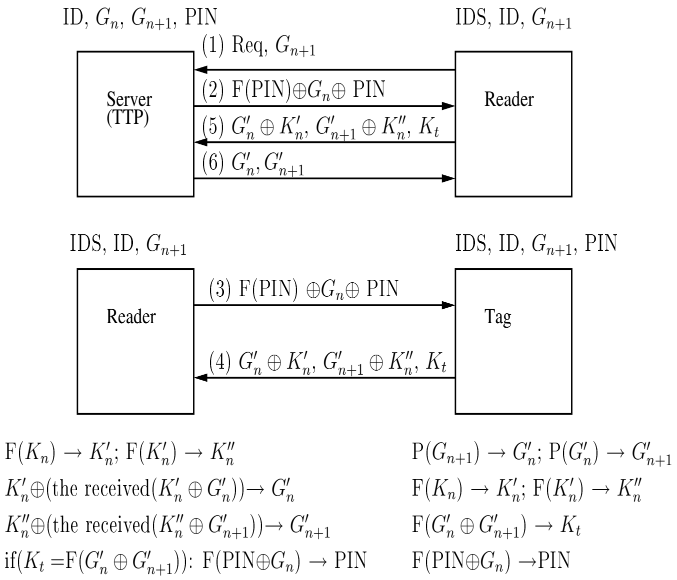

Fig. 2. The ownership transfer protocol of Kulseng *et al.*

IV. Security Analysis of Mutual Authentication Protocol

In this section we analyze the security of the Kulseng *et al.* mutual authentication protocol. Our attacks is based on an observation that for a publicly known LFSR of length L, given any L-bit sequence of its output is enough to determine the internal state of LFSR in any given time by clocking the LFSR in backward or forward manner [2]. Briefly, an LFSR corresponds to a recurrence relation and if the recurrence relation is publicly known then any given LFSR state can be extended in both forward and backward directions to know the state of the LFSR at any given time. On the other hand, the designers of the protocols state that [[6], Section III]:

> *The implementation of F function needs not to be secret, so even adversaries know how to construct this function.*

It means that any one, including the adversary, knows the LFSR length L and its irreducible feedback polynomial over finite field $GF(2)$ of degree L. In addition, any parameter which is exchanged in this protocol is L bits long. Hence, given $F(X)$, where $F(.)$ is an LFSR implementation, it would be easy to clock the LFSR backward and determine X. We denote by $F^{-1}(.)$ a function that implements the inverse of $F(.)$. That is, the output of $F^{-1}(F(X))$ would be the value X. In the rest of this work, we use the observation mentioned above to mount various attacks on the mutual authentication protocol.

A. Secret Parameters Disclosure Attack

We now show how an adversary can disclose any secret parameter stored with either the reader or the tag. Recall that the reader parameters are (IDS, ID, G_n, G_{n+1}) and the tag parameters are (IDS, ID, G_n). Given those parameters any one can deceive the reader to be a legitimate tag and vise versa. The adversary eavesdrops two sequential successive runs of Kulseng *et al.* mutual authentication protocol and outputs (IDS, ID, G_n, G_{n+1}). The details of the attack are presented in Algorithm 1. Any parameter related to the first run (resp. second) of protocol is indexed by 1 (resp. indexed by 2), e.g. IDS_1 (resp. IDS_2). Recall from the description of the protocol that $(G_{n+1})_1 = (G_n)_2$ and $(G_{n+2})_1 = (G_{n+1})_2$.

B. Impersonation Attack

After disclosure attack, the adversary has retrieved IDS, ID, G_n and G_{n+1}. So it can impersonate any legitimate reader for this tag and vise versa.

V. Security Analysis of Ownership Transfer Protocol

Now we analyze the security of the Kulseng *et al.* ownership transfer protocol. Our attack against this protocol is based on the same observation that is mentioned in section IV.

We show how can an adversary retrieve the PIN in Kulseng *et al.* ownership transfer protocol, despite the claims of the protocol designers. The details of attack are presented in Algorithm 2.

In this attack, the attacker eavesdrops the full transactions between the new reader and the tag through the ownership transfer protocol as well the following successive run of Kulseng *et al.* mutual authentication protocol between the new owner and the tag. In addition, we assume that the reader knows the (IDS, ID, G_n, G_{n+1}) triplet that the tag has shared with the old owner. Note that these assumptions are achievable in practice since a passive adversary can listen to all the messages being exchanged between the tag and the reader. Further, as mentioned earlier, the designers of the protocol allow the design of the LFSR to be public and hence also available to the adversary.

The attack is described in Algorithm 2. All parameters related to the ownership transfer protocol in this attack are indexed by OT. At the end of Algorithm 2, the attacker outputs the PIN_{old}-value and PIN_{new}-value.

VI. Conclusions

In this work, we have analyzed the security of recently proposed mutual authentication and ownership transfer protocols by Kulseng *et al.*. Our attacks completely break the protocols. We have shown the following two attacks in this work.

1) An attack on the mutual authentication protocol which discloses any secret parameter which is shared between the tag and the reader, given the information exchanged in two sequential runs of the protocol. The attacker is a passive attacker and the success probability of the attack is “1”.
2) An attack against the ownership transfer protocol which retrieves the PIN value, given the transferred information through the ownership transfer phase and next run of protocol by the new owner. Again, the attacker is a passive attacker and the success probability of the attack is “1”.

We do not see any minor tweak of the protocols of Kulseng *et al.* which would allow them to withstand our attacks.

Algorithm 2: Retrieving the PIN of the tag in the Kulseng *et al.* ownership transfer protocol.

input : IDS, ID, G_n, G_{n+1} which is shared between the tag and old owner(reader);

Online Phase;
Eavesdrop the transactions between the tag and the new owner through the ownership transfer phase and store the $(K_n \oplus G_n \oplus PIN)_{OT}, (G'_n \oplus K'_n)_{OT}, (G'_{n+1} \oplus K''_n)_{OT})$ triplet;
Eavesdrop the first run of mutual authentication protocol by the new owner and store the $((IDS)_1, (ID \oplus G_n)_1, (G_{n+1} \oplus K_n)_1, (G_{n+2} \oplus K'_n)_1)$ triplet; `// Recall that` $(G_n)_1 = (G'_n)_{OT}$ `and` $(G_{n+1})_1 = (G'_{n+1})_{OT}$`;`

Off line Phase;
$F^{-1}((IDS)_2) \rightarrow (IDS)_1 \oplus (G_n)_1$;
$(IDS)_1 \oplus (G_n)_1 \oplus (IDS)_1 \rightarrow (G_n)_1$; `//` $(G_n)_1$ `disclosures;`
$(ID \oplus (G_n))_1 \oplus (G_n)_1 \rightarrow ID$; `//` ID `is not changed when the ownership is transferred;`
$G_n \rightarrow G'_n$; `//` G'_n `disclosures;`
$F(G_n) \rightarrow K_n$;
$(G_{n+1} \oplus K_n)_1 \oplus K_n \rightarrow G_{n+1}$; `//` $(G_{n+1})_1$ `disclosures;`
$G_{n+1} \rightarrow G'_{n+1}$; `//` G'_{n+1} `disclosures;`

$(G'_n \oplus K'_n)_{OT} \oplus G'_n \rightarrow (K'_n)_{OT}$;
$F^{-1}((K'_n)_{OT}) \rightarrow (K_n)_{OT}$;
$F^{-1}((K_n)_{OT}) \rightarrow PIN_{old}$; `//` PIN_{old} `disclosures;`
$F(PIN_{old} \oplus G_n) \rightarrow PIN_{new}$; `//` PIN_{new} `disclosures;`

return (PIN_{old}, PIN_{new});

References

[1] M. Feldhofer and C. Rechberger. A Case Against Currently Used Hash Functions in RFID Protocols. In R. Meersman, Z. Tari, and P. Herrero, editors, *OTM Workshops (1)*, volume 4277 of *Lecture Notes in Computer Science*, pages 372–381. Springer, 2006.

[2] S. Golomb. *Shift register sequences*. Aegean Park Press, 1982.

[3] C. Hung-Yu. SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity. *IEEE Transactions on Dependable and Secure Computing*, 4(4):337–340, December 2007.

[4] K. Y. K. Osaka, T. Takagi and O. Takahashi. An Efficient and Secure RFID Security Method with Ownership Transfer. In *CIS*, volume 4456, pages 778–787. LNCS, 2007.

[5] Konidala and Kim. RFID Tag-Reader Mutual Authentication Scheme Utilizing Tag Access Password. In *Auto-ID Labs White Paper WPHARDWARE- 033*, 2007.

[6] L. Kulseng, Z. Yu, Y. Wei, and Y. Guan. Lightweight Mutual Authentication and Ownership Transfer for RFID systems. In *The proceedings of IEEE INFOCOM 2010*, pages 1–5, March 2010.

[7] K. S. Ohkubo M., Suzuki K. Hash-chain based forward-secure privacy protection scheme for low-cost RFID. In *Proc. of the 2004 Symposium on Cryptography and Information Security (SCI 2004)*, pages 719–724, 2004.

[8] P. Peris-Lopez, J. C. H. Castro, J. M. Estévez-Tapiador, and A. Ribagorda. LMAP:A Real Lightweight Mutual Authentication Protocol for Low cost RFID tags. In *RFIDSec*, 2006.

[9] P. Peris-Lopez, J. C. H. Castro, J. M. Estévez-Tapiador, and A. Ribagorda. Advances in Ultralightweight Cryptography for Low-Cost RFID Tags: Gossamer Protocol. In K.-I. Chung, K. Sohn, and M. Yung, editors, *WISA*, volume 5379 of *Lecture Notes in Computer Science*, pages 56–68. Springer, 2008.

[10] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, and A. Ribagorda. EMAP: An Efficient Mutual Authentication Protocol for Low-Cost RFID Tags. In *OTM Federated Conferences and Workshop: IS Workshop – IS'06*, volume 4277 of *Lecture Notes in Computer Science*, pages 352–361, Montpellier, France, November 2006. Springer-Verlag.

[11] A. Sadighian and R. Jalili. AFMAP: Anonymous Forward-Secure Mutual Authentication Protocols for RFID systems. In R. Falk, W. Goudalo, E. Y. Chen, R. Savola, and M. Popescu, editors, *The Third IEEE International Conference on Emerging Security Information, Systems and Technologies(SECURWARE 2009)*, pages 31–36, Athens, Greece, 2009. IEEE Computer Society.

[12] J. Saito, K. Imamoto, and K. Sakurai. Reassignment Scheme of an RFID Tag Key for Owner Transfer. In *IFIP EUC*, volume LNCS 3823, pages 1303–1312, 2005.

[13] S. Weis. *Security and Privacy in Radio Frequency Identification Devices*. Masters Thesis, Massachusetts Institute of Technology (MIT), 2003.

[14] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In *International Conference on Security in Pervasive Computing-SPC 2003*, volume 2802 of *Lecture Notes in Computer Science*, pages 201–212, 2004.

[15] H. L. Y. Seo, T. Asano and K. Kim. A Lightweight Protocol Enabling Ownership Transfer and Granular Data Access of RFID Tags. In *SCIS*, 2007.