Grouping Proof for RFID tags

Saito, Junichiro
Graduate School of Information Science and Electrical Engineering, Kyushu University

Sakurai, Kouichi
Faculty of Information Science and Electrical Engineering, Kyushu University

http://hdl.handle.net/2324/6216

出版情報：SLRC 論文データベース，2005-03
バージョン：accepted
権利関係：
Grouping proof for RFID tags

Junichiro SAITO
Graduate School of Information Science and
Electrical Engineering, Kyushu University
saito@itslab.csce.kyushu-u.ac.jp

Kouichi SAKURAI
Faculty of Information Science and
Electrical Engineering, Kyushu University
sakurai@csce.kyushu-u.ac.jp
http://itslab.csce.kyushu-u.ac.jp/index.html

Abstract

An RFID tag is a small and cheap device which is combined in IC chip and an antenna for radio communications. The tag is used for management of goods and its distribution. Moreover it reduces the cost of managements of goods. However, an RFID system has some security problems. Juels proposed a “yoking-proof” which guarantees the existence of two tags [2]. But we point out that this scheme is not secure against a replay attack. In this paper, we propose a scheme which deals with the problem by using time stamp. Moreover, we propose a scheme which guarantees the existence of a group of RFID tags.

1 Introduction

A Radio-Frequency-Identification (RFID) tag is a small and cheap device which is combined in IC chip and an antenna for radio communications. The tag emits its ID in response to a query from a reader. By using RFID tags as a substitute of a bar code, it is expected to reduce a cost of managements of goods and its distribution. Moreover, we can realize supply chain management by managing its ID in database and guarantee the safety of foods by using a traceability of RFID tags. We show a common RFID system in Fig. 1.

However, there are some problems of using RFID tags. Privacy problem is the most serious [3, 4, 5, 6]. Since RFID tags emit an ID by radio, you can find an object attached an RFID tag. Moreover, a location of a tag’s owner can be leaked by using strong traceability of RFID tags. The privacy of owner’s location is called as location privacy. Juels proposed another security problem [2]. This security problem is called as “yoking-proof” which proves an existence of two tags. This proof uses a MAC (Message Authentication Code) made by RFID tags. For example, such proofs might be useful when a product and its safety cap must leave its factories together and when a medicine must be dispensed with a leaflet. In these examples, we can prove by attaching RFID tags to two objects. Moreover, RFID tags will be used for preventing shrinkages in America. Shrinkages mean that products are decreased while the distribution [1]. You can prevent it by tracing products with RFID tags.

However, an attacker who has a reader can enable a replay attack by using a MAC because it is made by a random number produced by an RFID tag. So you can get a “yoking-proof” even if you have only one RFID tag.

In this paper, we improve the “yoking-proof” by using a time stamp and prevent from the replay attack. In our scheme, an RFID tag computes a MAC by using the time stamp from a reader. By using the time stamp, we can verify the time of producing a MAC. Moreover, we propose an existence proof of plural RFID tags. In the scheme, we use a product tag which is attached to a product and a pallet tag which is attached to a pallet. The pallet is a large metal plate or flat wooden frame on which some products can be lifted or moved. The product tag produces a MAC by using a query from a reader. The reader emits some MACs from plural product tags to the pallet tag. Then the pallet tag encrypts MACs by using symmetric key encryption and emits the ciphertext to the reader. In our scheme, the pallet tag needs more calculation power than the product tag. But since the pallet tag can be reused, we can hold down the cost of using RFID tags.
2 Yoking-proof

Juels proposed a new security notion which is called “yoking-proof” [2]. This notion proves a simultaneous existence of two RFID tags.

Since RFID tags are cheap and small devices, they cannot communicate with each other. Therefore in “yoking-proof”, RFID tags communicate with each other by using a reader as a communication medium. Moreover Juels’s scheme relies on timeout assumption [2]. RFID tags always terminate a session within a certain interval of time \( t \).

Now we introduce a “yoking-proof” for RFID tags.

2.1 Notations

- \( T \) : an RFID tag.
- \( V \) : verifier. It verifies a MAC.
- \( r \) : a random number.
- \( x \) : a secret key of symmetric key cryptosystem.
- \( MAC \) : a message authentication code using a standard cryptosystem.
- \( MAC_x[m] \) : a MAC computed by applying secret key \( x \) to message \( m \).
- \( SK_x[m] \) : a ciphertext by using secret key \( x \) to message \( m \).

2.2 Protocol

In Juels’s protocol, RFID tags, \( T_A \) and \( T_B \), share secret key \( x_A \) and \( x_B \) with a verifier \( V \) and select random numbers \( r_A \) and \( r_B \), respectively every session.

1. \( T_A \) submits the random number \( r_A \) in response to query from a reader.
2. The reader sends \( r_A \) to \( T_B \).

3. \( T_B \) computes a MAC by applying the secret key \( x_B \) to \( r_A \). Moreover \( T_B \) submits \( m_B = MAC_{x_B}[r_A] \) and \( r_B \).
4. The reader sends \( r_B \) to \( T_A \).
5. \( T_A \) computes a MAC \( m_A \) by applying the secret key \( x_A \) to \( r_B \) and submits it.
6. The reader submits \( m_A \) and \( m_B \) to the verifier. The verifier can verify that \( T_A \) and \( T_B \) were scanned simultaneously.

The “yoking-proof” for RFID tags is shown in Fig. 2.

3 Attack against a “yoking-proof”

In Juels’s scheme, since RFID tags compute a MAC by using a random number, we can enable a replay attack by keeping a previous random number. We describe the replay attack for “yoking-proof” for RFID tags below.

1. An attacker \( A \) emits a query to \( T_A \) and gets \( r_A \).
2. The attacker \( A \) submits \( r \) created by \( A \) to \( T_A \) and gets \( m_A = MAC_{x_A}[r] \).
3. The attacker can get \( m_B = MAC_{x_B}[r_A] \) from \( T_B \) by using \( r_A \) and submit \( m_A \) and \( m_B \) to a verifier \( V \). Then the attacker can prove a “yoking-proof” even if there is only \( T_B \).

Since the attacker \( A \) submits an input to two RFID tags separately, we cannot prevent this attack by using timeout assumption. Replay attack against a “yoking-proof” is shown in Fig. 3.
4 “yoking-proof” using time stamp

We propose a “yoking-proof” using time stamp for addressing the replay attack. In our proposal, RFID tags compute a MAC by applying a secret key to a time stamp from a database. Therefore a verifier can verify a time of making the MAC. Since a RFID tag computes the MAC using the time stamp, we can prevent the replay attack by reusing the MAC. Moreover our scheme relies on timeout assumption, too.

In our scheme, RFID tags $T_A$ and $T_B$ share secret key $x_A$ and $x_B$ with a verifier $V$, respectively in advance.

1. A reader gets a time stamp $TS$ from a database and queries to $T_A$ and $T_B$ by using $TS$.
2. $T_A$ computes $m_A = MAC_{x_A}[TS]$ and submits it to the reader.
3. The reader submits $m_A$ to $T_B$.
4. $T_B$ computes $m_B = MAC_{x_B}[TS, m_A]$ and submits it to the reader.
5. The reader submits $m_B$ to a verifier $V$. The verifier $V$ verifies it by using $x_A$ and $x_B$.

Our proposal is shown in Fig. 4.

5 Grouping proof

In this section, we extend our proposal to a scheme which can prove an existence of plural RFID tags.

5.1 Our model

In our scheme, secret keys are assumed to be securely shared in advance.

- Product tag $T_i$: This tag is attached to each product. A verifier $V$ has its secret key $x_i$.
- Pallet tag $PT$: This tag is attacked to a pallet which is a large metal plate or flat wooden frame on which some products can be lifted or moved. The verifier $V$ has its secret key $x$. It can compute symmetric key encryption and has larger memory than a product tag. It terminates protocol within a certain interval of time $t$.
- Reader: It derives a time stamp $TS$ from a database and submits it to an RFID tag.
- Database: It submits a time stamp $TS$ to a reader.
- Verifier $V$: It shares secret keys with a product tag and a pallet tag. It can verify a MAC by using the secret key.

5.2 Protocol

We introduce our proposal.

- A reader derives a time stamp $TS$ from a database and submits it to $n$ of product tags and a pallet tag $PT$.
- The product tag $T_i (1 \leq i \leq n)$ computes a MAC $m_i$ by using $TS$ and submits it to the reader.
- The reader gathers $n$ of MACs and submits them to $PT$.
- $PT$ encrypts $n$ of MACs and submits this ciphertext $C_P$ to the reader.
The reader submits $C_P$ to a verifier $V$. $V$ decrypts $C_P$ by using $x$ and derives the MAC $m_i$. Then $V$ verifies $m_i$ by using $x_i$. Therefore we can prove an existence of $n$ of product tags.

Our proposal is shown in Fig. 5.

5.3 Discussion

In our scheme, we can prevent a replay attack by using a time stamp from a database. Moreover since a pallet tag has timeout assumption, we can guarantee that a session is finished within a certain interval of time $t$.

In a distribution using RFID tags, we cannot reuse RFID tags because RFID tags attached to products are distributed to consumers. Therefore, RFID tags are disposable and it is important to hold down a cost of RFID tags. In our proposal, product tags attached to products compute only a MAC. Pallet tags process timeout and compute symmetric key encryption. However, since pallet tags are attached to pallets, we can reuse pallets after finishing distribution. Therefore, we can hold down the cost of pallet tags by reusing it.

An application is preventing shrinkages by tracing RFID tags. In our proposal, we can easily trace and watch plural products because we can verify when RFID tags are read.

6 Conclusion

In this paper, we proposed a replay attack against "yoking-proof" and "yoking-proof" using time stamp for addressing the replay attack. Moreover, we proposed a grouping proof extended "yoking-proof". By using our proposal, we can realize management of goods and its distribution using RFID tags.

In future works, we should evaluate a cost of our scheme. If RFID tags are used for goods management, industrial espionage is an important problem. Therefore, we should discuss a problem of privacy.

7 Acknowledgements

Thanks to Wonil Lee and Dong-Guk Han for their comments on this work.

References


