A Provably Secure Offline RFID Yoking-Proof Protocol with Anonymity

Daisuke Moriyama
NICT
Cryptographic Protocols Target on RFID tag

- RFID authentication protocol

There are many results...

- RFID ownership transfer protocol

I proposed a provably secure protocol at LightSec 2013

- RFID yoking/grouping proof protocol

This talk
- During a session, a reader communicates with two RFID tags
- Tags generate a “proof”, which a (specific) verifier can check these tags were communicated with the reader in one session.
- During a session, a reader communicates with multiple RFID tags.
- Tags generate a “proof”, which a (specific) verifier can check these tags were communicated with the reader in one session.
Summary of the existing proposals and **attack reports**

<table>
<thead>
<tr>
<th>Existing Proposal</th>
<th>Attack Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Juels (PerSec2004)</td>
<td>Saito, Sakurai (AINA 2005)</td>
</tr>
<tr>
<td>Bolotnyy, Robins (Mobiquitous2006)</td>
<td>I could Attack</td>
</tr>
<tr>
<td>Saito, Sakurai (AINA2005)</td>
<td>Pamamithu (SecPerU2006)</td>
</tr>
<tr>
<td>Pamamithu (SecPerU2006)</td>
<td>Peris et al. (SecPerU2007)</td>
</tr>
<tr>
<td>Burmester et al. (CARDIS2008)</td>
<td>Peris et al. (JNCA2011)</td>
</tr>
<tr>
<td>Chien, Liu (NSWCTC2009)</td>
<td>Peris et al. (JNCA2011)</td>
</tr>
<tr>
<td>Huang, Ku (JoMS2009)</td>
<td>Peris et al. (JNCA2011)</td>
</tr>
<tr>
<td>Duc, Kim (ePrint2009)</td>
<td>I could attack</td>
</tr>
<tr>
<td>Peris et al. (JNCA2011)</td>
<td>Bagheri, Safkhani (ePrint2013/453)</td>
</tr>
<tr>
<td>Batina et al. (JoPUC2012)</td>
<td>Hermans, Peeters (RFIDSec2012)</td>
</tr>
<tr>
<td>Hermans, Peeters (RFIDSec2012)</td>
<td>I could attack</td>
</tr>
</tbody>
</table>

Unfortunately, the existing protocols can be attacked!!!

**Reason 1:** No provable security

**Reason 2:** No definition for sufficient “security”

Propose a security model to achieve strong security is the first task.
Security Model against Yoking-proof Protocols
Execution model

Setup Phase:

Verifier $\mathcal{V}$

RFID tags $\mathcal{T} := \{t_0, \ldots, t_n\}$

Yoking-Proof Generation Phase:

Reader $\mathcal{R}$

Two tags do not have direct communication but interaction via a reader

Verification Phase:

Verifier $\mathcal{V}$

$\text{Ver}(sk, \mathcal{T}, \sigma) \neq 1$

Verifier does not participate in the above phase and checks the validity of yoking-proof later in the offline case
Security against man-in-the-middle attack

Adv wins the security game if the verifier accepts $\sigma^*$ on the condition that:

$\sigma^*$ is not derived from a matching session between $(t_0^*, t_1^*)$

All communication messages between tags in a session is honestly transferred

This is still honest communication!
Privacy (optional in yoking-proof)

**Adv**

\[ \mathcal{R}, \mathcal{T} \]

Launch, SendReader, SendTag, Result

\[ \leftarrow \rightarrow \]

\[ \mathcal{T}_0^*, \mathcal{T}_1^* \]

\[ (\mathcal{T}_0^* \neq \mathcal{T}_1^*) \]

Launch, SendReader, SendTag, Result

\[ \leftarrow \rightarrow \]

\[ b \overset{\mathcal{U}}{\leftarrow} \{0, 1\} \]

\[ \mathcal{T}' := \mathcal{T} \setminus \{\mathcal{T}_0^*, \mathcal{T}_1^*\} \]

**Cha**

Setup reader \( \mathcal{R} \), tags \( \mathcal{T} \) and verifier

Interact with \( \mathcal{R}, \mathcal{T}' \)

Interact with members of \( \mathcal{T}_b^* \) anonymously

Adv wins the privacy game if \( b' = b \)
The Proposed Protocol
Anonymous RFID yoking-proof protocol

Setup Phase:

Verifier

\[ k_X, k_1, k_2 \leftarrow \{0, 1\}^* \]

Hierarchical structure of the RFID tag:
- Consider groups of the tags
- One secret key is shared among the group, another key is unique for each tag
Anonymous RFID yoking-proof protocol

Setup Phase:

Verifier

\[ k_X, k_1, k_2 \leftarrow \{0, 1\}^* \]

Yoking-proof generation Phase:

\[ r_1 \leftarrow \{0, 1\}^k \]
\[ u_1 := \text{PRF}(k_X, (ts, r, r_1)) \]
\[ r, r_1, u_1 \leftarrow \text{ts, r} \]

\( ts : \text{time stamp} \)

\[ r \leftarrow \{0, 1\}^k \]
Anonymous RFID yoking-proof protocol

Setup Phase:

Verifier

\[ k_X, k_1, k_2 \leftarrow \{0, 1\}^* \]

Generation Phase:

Check whether the message is came from a group member

\[ r_1 \leftarrow \{0, 1\}^k \]
\[ u_1 := \text{PRF}(k_X, (ts, r, r_1)) \]
\[ r, r_1, u_1 \]
\[ ts, r, r_1, u_1 \]
\[ r_2 \leftarrow \{0, 1\}^k \]
\[ u_2 := \text{PRF}(k_X, (ts, r, r_1, r_2)) \]
\[ v_2 := \text{PRF}(k_2, (ts, r, r_1, r_2)) \]
\[ r, r_2, u_2, v_2 \]
\[ \leftarrow \{0, 1\}^{3k} \]
Anonymous RFID yoking-proof protocol

Setup Phase:

Verifier

\[ k_X, k_1, k_2 \triangleleft \{0, 1\}^* \]

Generation Phase:

\[ r_1 \triangleleft \{0, 1\}^k \]
\[ u_1 := \text{PRF}(k_X, (ts, r, r_1)) \]

\[ u_2 \overset{?}{=} \text{PRF}(k_X, (ts, r, r_1, r_2)) \]
\[ v_1 := \text{PRF}(k_1, (ts, r, r_1, r_2)) \]

Else, \[ v_1 \triangleleft \{0, 1\}^k \]

Check whether the message is came from a group member and the peer responds against \( r_1 \)
Anonymous RFID yoking-proof protocol

Setup Phase:

Verifier

\[ k_X, k_1, k_2 \leftarrow \{0, 1\}^* \]

\[ t_1, t_2 \]

Generation Phase:

\[ r_1 \leftarrow \{0, 1\}^k \]
\[ u_1 := \text{PRF}(k_X, (ts, r, r_1)) \]

\[ r, r_1, u_1 \]

\[ r_1, r_2, u_2 \]

\[ v_1 := \text{PRF}(k_1, (ts, r, r_1, r_2)) \]

Else, \( v_1 \leftarrow \{0, 1\}^k \)

\[ r, v_1 \]

\[ \sigma := (ts, r, r_1, r_2, u_2, v_1, v_2) \]

\[ u_1 \leftarrow \text{PRF}(k_X, (ts, r, r_1)) \]
\[ r_2 \leftarrow \{0, 1\}^k \]
\[ u_2 := \text{PRF}(k_X, (ts, r, r_1, r_2)) \]
\[ v_2 := \text{PRF}(k_2, (ts, r, r_1, r_2)) \]

Else, \( r_2, u_2, v_2 \leftarrow \{0, 1\}^{3k} \)

All outputs from PRFs are bound by same input
Anonymous RFID yoking-proof protocol

Setup Phase:

Verifier needs to execute an exhaustive search for privacy (similar to the canonical RFID authentication protocol)

But the hierarchy of the tag enables faster verification

1. Find a valid group secret key \( k_X \) which satisfies \( u_2 \equiv \text{PRF}(k_X, (ts, r, r_1, r_2)) \)
2. Find two tags by checking \((v_1, v_2)\)
Security Proof: security against man-in-the-middle attack

Assume $\sigma^* := (ts^*, r^*, r_1^*, r_2^*, u_2^*, v_1^*, v_2^*)$ is the final output of the adversary.

1. $v_1^*$ is accepted on the condition that $t_1$ does not output it
   - The security of $\text{PRF}(k_1, \cdot)$ can be broken

2. $v_2^*$ is accepted on the condition that $t_2$ does not output it
   - The security of $\text{PRF}(k_2, \cdot)$ can be broken

$(v_1^*, v_2^*)$ is reused from a session
   - $\text{PRF}$ is deterministic and the verifier accepts only if the remained tuple is also generated by $t_1$ and $t_2$

   $\Rightarrow$ Man-in-the-middle attack is impossible

\[
\begin{align*}
    u_2 & \triangleq \text{PRF}(k_X, (ts, r, r_1, r_2)) \\
    r_1, r_2, u_2 & \xrightarrow{} r, r_2, u_2, v_2 \\
    v_1 & \triangleq \text{PRF}(k_1, (ts, r, r_1, r_2)) \\
    \text{ Else, } v_1 & \triangleq \{0, 1\}^k \\
    r, v_1 & \xrightarrow{} r, u_2 := \text{PRF}(k_2, (ts, r, r_1, r_2)) \\
    \{0, 1\}^k & \xrightarrow{} u_2, v_1, v_2 \\
\end{align*}
\]
Security proof: privacy (Game 0)

Generation Phase:

\[
\begin{align*}
    r_1 &\overset{\$}{\leftarrow} \{0, 1\}^k \\
    u_1 &:= \text{PRF}(k_X, (ts, r, r_1)) \\
    \text{Else, } v_1 &\overset{\$}{\leftarrow} \{0, 1\}^k \\
    u_2 &\overset{?}{\leftarrow} \text{PRF}(k_X, (ts, r, r_1, r_2)) \\
    v_1 &:= \text{PRF}(k_1, (ts, r, r_1, r_2)) \\
    \sigma &:= (ts, r, r_1, r_2, u_2, v_1, v_2) \\
\end{align*}
\]
Security proof: privacy (Game 1-j)

- Replace \( \text{PRF}(k_X, \cdot) \) (PRF using a j-th group secret key) to a truly random function.

Generation Phase:

\[
\begin{align*}
  r_1 & \overset{\$}{\leftarrow} \{0, 1\}^k \\
  u_1 & \overset{\$}{\leftarrow} \{0, 1\}^k \\
  \text{check } u_2 \\
  v_1 & := \text{PRF}(k_1, (ts, r, r_1, r_2)) \\
\end{align*}
\]

Else, \( v_1 \overset{\$}{\leftarrow} \{0, 1\}^k \)

\[
\begin{align*}
  \sigma & := (ts, r, r_1, r_2, u_2, v_1, v_2) \\
  \text{check } u_1 \\
  r_2 & \overset{\$}{\leftarrow} \{0, 1\}^k \\
  u_2 & \overset{\$}{\leftarrow} \{0, 1\}^k \\
  v_2 & := \text{PRF}(k_2, (ts, r, r_1, r_2)) \\
\end{align*}
\]

Else, \( r_2, u_2, v_2 \overset{\$}{\leftarrow} \{0, 1\}^{3k} \)

\[
\begin{align*}
  \text{check } u_2 \\
  v_1 & \overset{?}{=} \text{PRF}(k_1, (ts, r, r_1, r_2)) \\
  v_2 & \overset{?}{=} \text{PRF}(k_2, (ts, r, r_1, r_2)) \\
\end{align*}
\]
Security proof: privacy (Game 2-j)

- Replace $\text{PRF}(k_X, \cdot)$ (PRF using a j-th group secret key) to a truly random function
- Replace $\text{PRF}(k_j, \cdot)$ (PRF using a j-th individual secret key) to a truly random function

**Generation Phase:**

$$r_1 \overset{\$}{\leftarrow} \{0, 1\}^k$$

$$u_1 \overset{\$}{\leftarrow} \{0, 1\}^k$$

check $u_2$

$$v_1 \overset{\$}{\leftarrow} \{0, 1\}^k$$

$$(ts, r)$$

$$r, r_1, u_1$$

$$ts, r, r_1, u_1$$

$$r_1, r_2, u_2$$

$$r, r_2, u_2, v_2$$

check $u_1$

$$r_2 \overset{\$}{\leftarrow} \{0, 1\}^k$$

$$u_2 \overset{\$}{\leftarrow} \{0, 1\}^k$$

$$v_2 := \text{PRF}(k_2, (ts, r, r_1, r_2))$$

Else, $r_2, u_2, v_2 \overset{\$}{\leftarrow} \{0, 1\}^{3k}$

$$r, v_1$$

$$\sigma := (ts, r, r_1, r_2, u_2, v_1, v_2)$$

check $u_2$

check $v_1$

$$v_2 \overset{?}{=} \text{PRF}(k_2, (ts, r, r_1, r_2))$$
Security proof: privacy (Game 2-\(j\))

After the game transformation is finished, communication messages include no information about the identity of the RFID tag. 

There is no opportunity for the adversary to violate privacy game.

Generation Phase:

\[
\begin{align*}
  r_1 &\leftarrow \{0,1\}^k \\
  u_1 &\leftarrow \{0,1\}^k \\
  r, r_1, u_1 &\rightarrow ts, r_1, u_1 \\
  r_1, r_2, u_2 &\rightarrow r, r_2, u_2, v_2 \\
  r, v_1 &\rightarrow \\
  \sigma := (ts, r, r_1, r_2, u_2, v_1, v_2) &
\end{align*}
\]

check \(u_1\)

\[
\begin{align*}
  r_2 &\leftarrow \{0,1\}^k \\
  u_2 &\leftarrow \{0,1\}^k \\
  v_2 &\leftarrow \{0,1\}^k \\
  \text{Else, } r_2, u_2, v_2 &\leftarrow \{0,1\}^{3k} \\
  \text{check } u_2 \\
  \text{check } v_1 \\
  \text{check } v_2
\end{align*}
\]
Open problems

1. Extend to the grouping-proof protocol
   • Who checks whether all group members are interacted?

2. Privacy against tag corruption
   • Shared key mechanism in the same group is useless

3. Evaluation with implementation
   • No implementation result
Conclusion

- There is no secure RFID yoking/grouping-proof protocol
- We formalize a strong security model for RFID yoking-proof
- We propose the first RFID yoking-proof protocol provably secure against man-in-the-middle attack
- Our protocol also satisfies anonymity such that no party except the verifier can learn the identity of the RFID tag