RFID Tag Ownership Transfer

Boyeon Song

Information Security Group
Royal Holloway, University of London
b.song@rhul.ac.uk

July 11, 2008

RFID protocols

General Requirements for RFID protocols

RFID protocols

General Requirements for RFID protocols

- To resist privacy and security threats
- To consider limited tag resources in performance

RFID Protocols

General Requirements: Privacy and Security

RFID protocols should resist the following threats.

RFID Protocols

General Requirements: Privacy and Security

RFID protocols should resist the following threats.

Privacy Threats

- Tag information leakage
- Tag location tracking

RFID Protocols

General Requirements: Privacy and Security

RFID protocols should resist the following threats.

Privacy Threats

- Tag information leakage
- Tag location tracking

Security Threats

- Eavesdropping
- Tag impersonation
- Replay attacks
- Man-in-the-middle attacks
- Denial-of-service attacks
- Backward traceability
- Forward traceability
- Server impersonation

RFID Protocols

General Requirements: Performance

RFID protocols should have the following performance characteristics.

RFID Protocols

General Requirements: Performance

RFID protocols should have the following performance characteristics.

- Capacity minimisation ($\because$ constrained tag memory)
- Computation minimisation ($\because$ limited tag processing capability)
- Communication compression: the number and size of exchanged messages should be minimised.

RFID Protocols

Additional Requirement: Tag Ownership Transfer

Secure **Tag Ownership Transfer** should be considered.

Why?

In some applications, an RFID tag may change its owner a number of times during its lifetime.

RFID Protocols

Additional Requirement: Tag Ownership Transfer

Secure **Tag Ownership Transfer** should be considered.

Why?

In some applications, an RFID tag may change its owner a number of times during its lifetime.

What does RFID Tag Ownership mean?

The server of an RFID tag's owner has authorisation over the tag to interact with and identify/authenticate the tag.

RFID Protocols

Additional Requirement: Tag Ownership Transfer

Secure **Tag Ownership Transfer** should be considered.

Why?

In some applications, an RFID tag may change its owner a number of times during its lifetime.

What does RFID Tag Ownership mean?

The server of an RFID tag's owner has authorisation over the tag to interact with and identify/authenticate the tag.

What does Tag Ownership Transfer mean?

The server of a tag's owner transfers such authorisation over the tag to the server of the new owner.

RFID Protocols

Additional Requirement: Tag Ownership Transfer

To transfer ownership of a tag, all information associated with the tag should be passed from the old to the new owner's server.

Possible Privacy Threats

At the moment of tag ownership transfer, both the old and new owners have the information necessary to authenticate a tag, and this fact may cause an infringement of tag owner privacy.

Tag Ownership Transfer

Privacy Requirements

Once ownership of a tag has been transferred to a new owner,

1) New Owner Privacy

Only the new owner should be able to identify and control the tag. The previous owner of the tag should no longer be able to identify or trace the tag.

Tag Ownership Transfer

Privacy Requirements

Once ownership of a tag has been transferred to a new owner,

1) New Owner Privacy

Only the new owner should be able to identify and control the tag. The previous owner of the tag should no longer be able to identify or trace the tag.

2) Old Owner Privacy

The new owner of a tag should not be able to trace past interactions between the tag and its previous owner.

Tag Ownership Transfer

Additional Requirement

In some special cases, such as after-sales service for an RFID tagged object, the previous owner of a tag might need to interact with it again.

3) Authorisation Recovery

If the previous owner of a tag needs to temporarily recover the means to identify it, the present owner should be able to transfer its authorisation rights over the tag to the previous owner.

Novel RFID Authentication Protocols

For Secure Tag Ownership Transfer

Goal

Designing RFID protocols that meet the three requirements identified for secure tag ownership transfer

Novel RFID Authentication Protocols

For Secure Tag Ownership Transfer

Goal

Designing RFID protocols that meet the three requirements identified for secure tag ownership transfer

Features

- Operating in conjunction with the Song-Mitchell Protocol [ACM WiSec 08]
- Consists of three protocols

Novel RFID Authentication Protocols

For Secure Tag Ownership Transfer

Goal

Designing RFID protocols that meet the three requirements identified for secure tag ownership transfer

Features

- Operating in conjunction with the Song-Mitchell Protocol [ACM WiSec 08]
- Consists of three protocols
  - P1: Ownership Transfer Protocol
  - P2: Secret Update Protocol
  - P3: Authorisation Recovery Protocol

Song-Mitchell Protocol

Initialisation

Server

Database

T_1	(t_1, s_1)	$(\hat{t}_1, \hat{s}_1)$	Info_1
$\vdots$		$\vdots$	
T_i	(t_i, s_i)	$(\hat{t}_i, \hat{s}_i)$	Info_i
$\vdots$		$\vdots$	
T_N	(t_N, s_N)	$(\hat{t}_N, \hat{s}_N)$	Info_N

Tag

Memory

t

s	A string of l bits assigned to T
t	Tag T's identifier of l bits, which equals $h(s)$
$\hat{s}$	The most recent value of s
$\hat{t}$	The most recent value of t
Info	The other necessary information for T

Song-Mitchell Protocol

Authentication Process

Server

Database

$\cdots$	$\cdots$		
T_i	(t_i, s_i)	$(\hat{t}_i, \hat{s}_i)$	Info_i
$\cdots$	$\cdots$		

- Tag Authentication
  Search (t, s) in the DB for which
  $M_2 = f_t(r_1 \oplus M_1 \oplus t)$
- Response
  $r_2 = M_1 \oplus t$
  $M_3 = s \oplus (r_2 \gg l/2)$
- Secrets Update
  $\hat{s} \leftarrow s$, $\hat{t} \leftarrow t$
  $s \leftarrow (s \ll l/4) \oplus (t \gg l/4) \oplus r_1 \oplus r_2$
  $t \leftarrow h(s)$

$\xrightarrow{r_1}$

$\xleftarrow{M_1, M_2}$

$\xrightarrow{M_3}$

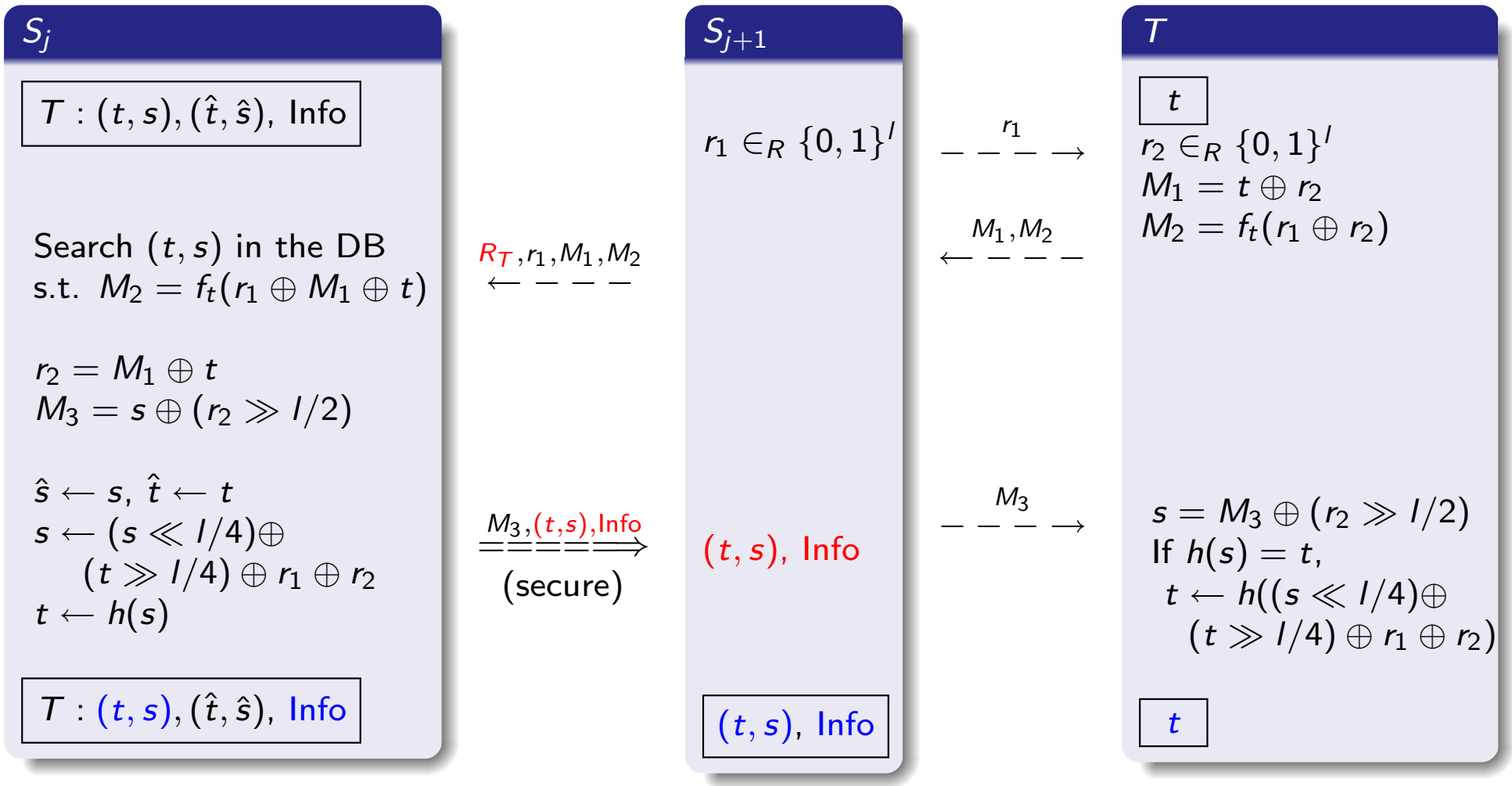
Tag

Memory

t

- Reply
  $r_2 \in_R \{0,1\}^l$
  $M_1 = t \oplus r_2$
  $M_2 = f_t(r_1 \oplus r_2)$
- Server Authentication
  $s = M_3 \oplus (r_2 \gg l/2)$
- Secret Update
  If $h(s) = t$,
  $t \leftarrow h((s \ll l/4) \oplus (t \gg l/4) \oplus r_1 \oplus r_2)$

P1: Ownership Transfer Protocol



P1

- **P1 satisfies Old Owner Privacy.**
  The new owner of a tag cannot trace past interactions between the tag and its previous owner.

P1

- **P1 satisfies Old Owner Privacy.**
  The new owner of a tag cannot trace past interactions between the tag and its previous owner.
- **However, New Owner Privacy?**
  Can the previous owner of the tag no longer identify or trace the tag?

P2: Secret Update Protocol

Goals

- Providing New Owner Privacy
- Improving performance

P2: Secret Update Protocol

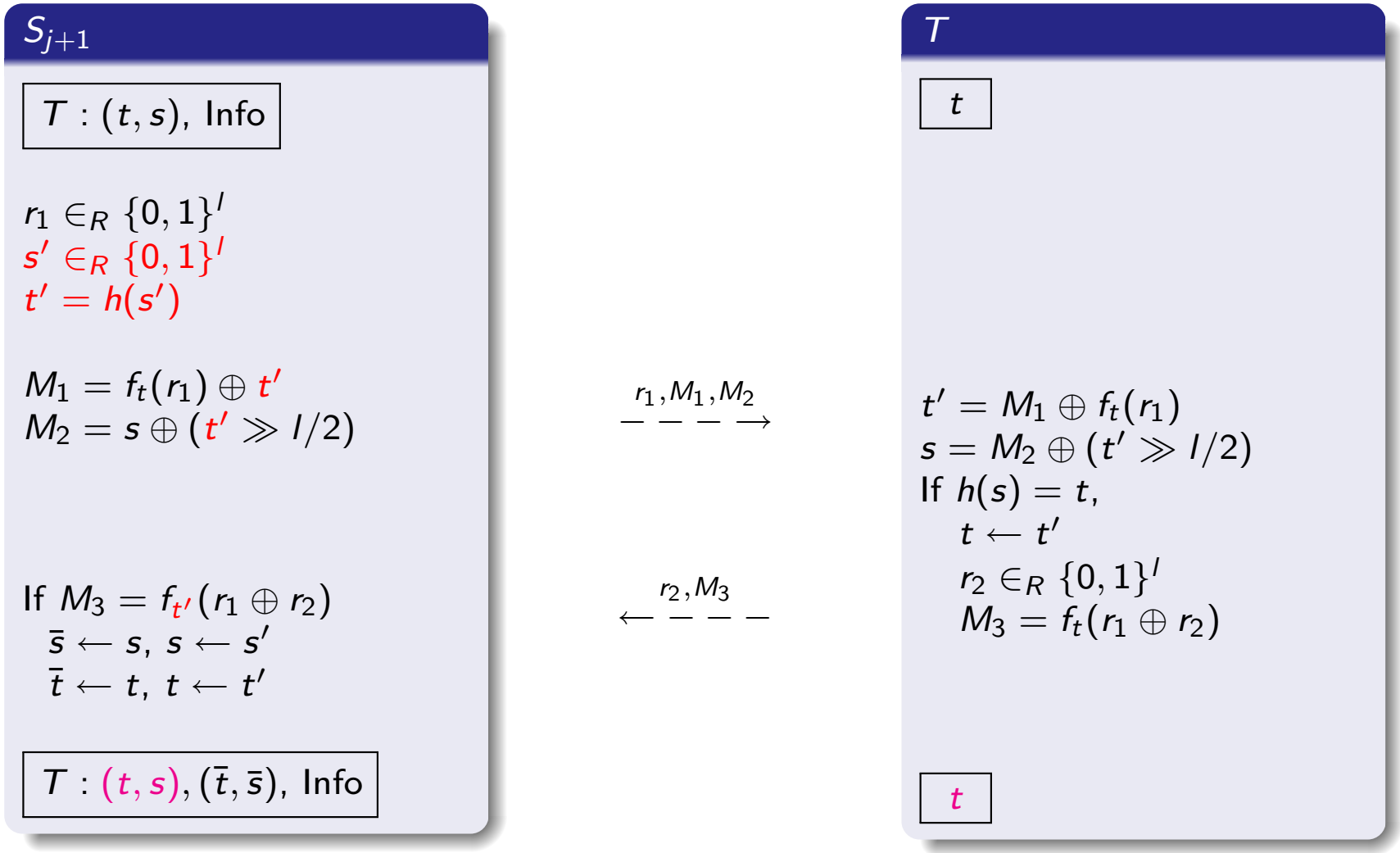
Goals

- Providing New Owner Privacy
- Improving performance

Features

- Updating shared secrets to new ones created by the server
- Requires only two message flows

P2: Secret Update Protocol



P1 & P2

- **P1 & P2 satisfy New Owner Privacy and Old Owner Privacy**

P1 & P2

- **P1 & P2 satisfy New Owner Privacy and Old Owner Privacy**
- **How about Authorisation Recovery?**
  Is the present owner able to transfer its authorisation over the tag to the previous owner temporarily?

P3: Authorisation Recovery Protocol

Goals

- Providing Authorisation Recovery

P3: Authorisation Recovery Protocol

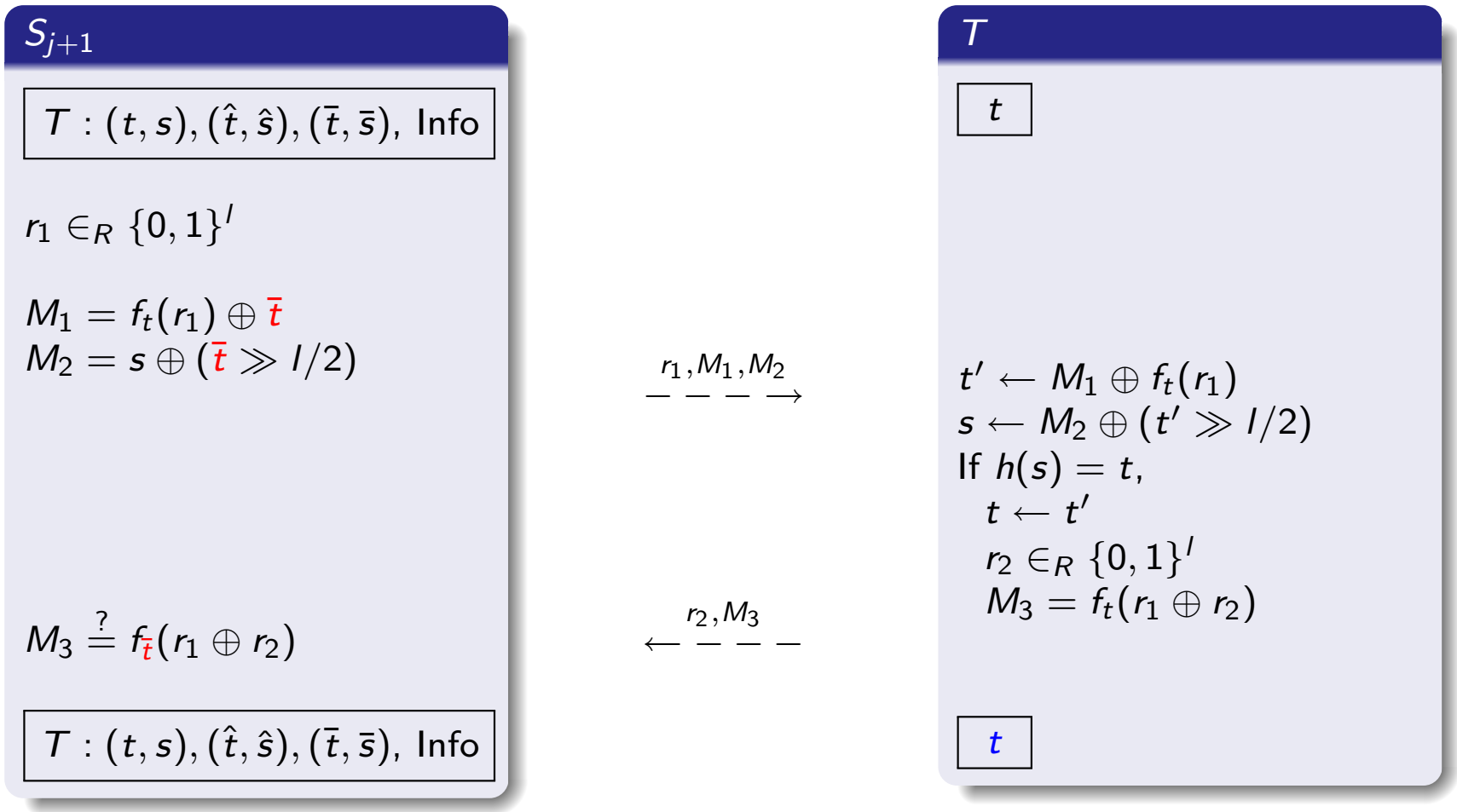
Goals

- Providing Authorisation Recovery

Features

- Resetting a tag secret to the old value shared with the previous owner's server
- Is similar to P2

P3: Authorisation Recovery Protocol



Related Work

- MSW scheme [Molnar, et al. SAC 2005]
- SIS scheme [Saito, et al. EUC 2005]
- LK scheme [Lim and Kwon, ICICS 2006]
- OTYT scheme [Osaka, et al. CIS 2006]
- FA scheme [Fouladgar and Afifi, EURASIP 2007/JCM 2007]

Properties for Tag Ownership Transfer

	MSW	SIS-1	SIS-2	LK	OTYT	FA-1	FA-2	**P1,P2,P3**
NOP	×	○	○	○	○	×	○	○
OOP	×	×	×	×	○	×	○	○
AR	×	×	×	×	×	×	×	○

NOP : New Owner Privacy
OOP : Old Owner Privacy
AR : Authorisation Recovery
○ : provided
× : not provided

Privacy and Security Properties

	LK	OTYT	FA-1	FA-2	**P1(SM)**	**P2/3**
Tag information leakage	√	√	√	√	√	√
Tag location tracking	√	·	√	√	√	√
Eavesdropping	√	√	√	√	√	√
Tag impersonation	√	√	√	√	√	√
Replay attack	√	√	·	√	√	√
Man-in-the-middle attack	√	·	√	√	√	√
Denial-of-service attack	√	·	√	√	√	√
Backward traceability	√	·	√	·	√	√
Forward traceability	∗	·	·	·	∗	∗
Server impersonation	∗	·	·	·	∗	∗

√ : resists such an attack
∗ : resists attack under an assumption
· : does not protect against such an attack

Performance Characteristics

P2(/P3) is compared with the secret update process for other proposed schemes.

	LK	OTYT	FA-1	FA-2	**P2/3**
Tag's cryptographic functions	4 PF	1 HF	5 HF	2 SE	3 HF
Tag's non-volatile memory	k_s, k_w, c	k_e	k_u, k_p, c	k_u, k_p, c	t
Message flows	3	3	3	3	2

PF : Pseudorandom function
HF : Hash function
SE : Symmetric encryption
s : a tag identifier in the LK scheme
w : a server validator in the LK scheme
c : a counter
e : a tag identifier $e = E_k(ID)$ in the OTYT scheme
k_p : a key used to compute pseudonyms in the FA scheme
k_u : a key used to update keys in the FA scheme
t : a tag identifier in **P2** and **P3**

Conclusion

- Have identified three requirements for secure and privacy-preserving tag ownership transfer.

Conclusion

- Have identified three requirements for secure and privacy-preserving tag ownership transfer.
  - New owner privacy
  - Old owner privacy
  - Authorisation recovery

Conclusion

- Have identified three requirements for secure and privacy-preserving tag ownership transfer.
  - New owner privacy
  - Old owner privacy
  - Authorisation recovery
- Have proposed novel RFID authentication protocols - P1, P2 & P3

Conclusion

- Have identified three requirements for secure and privacy-preserving tag ownership transfer.
  - New owner privacy
  - Old owner privacy
  - Authorisation recovery
- Have proposed novel RFID authentication protocols - P1, P2 & P3
  - Satisfy the identified privacy and security requirements
  - Have desirable performance characteristics
  - Provide all the identified requirements for tag ownership transfer

Thank you

Any Questions and Comments?