SCIS 2006 The 2006 Symposium on Cryptography and Information Security
Hiroshima, Japan, Jan. 17-20, 2006
The Institute of Electronics, Information and Communication Engineers

RFID Mutual Authentication Scheme based on Synchronized Secret Information

Sangshin Lee[1] Tomoyuki Asano[2] Kwangjo Kim[1]

[1]CAIS Lab, Information and Communications University (ICU), Korea
Auto-ID Lab, ICU, Korea

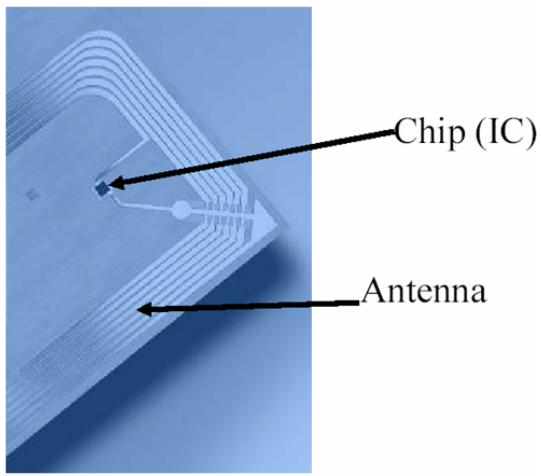
[2]Sony Corporation, Japan

21st January 2006

Contents

RFID Technology

- **RFID technology**
  - An automatic identification system, relying on storing and remotely retrieving data about objects
  - By using a device called “RFID tag”
- **Effects of RFID**
  - Automation of industry
  - Convenience to individuals
- **User privacy problems inherently**
  - No access-control and tamper-resistance



Notations

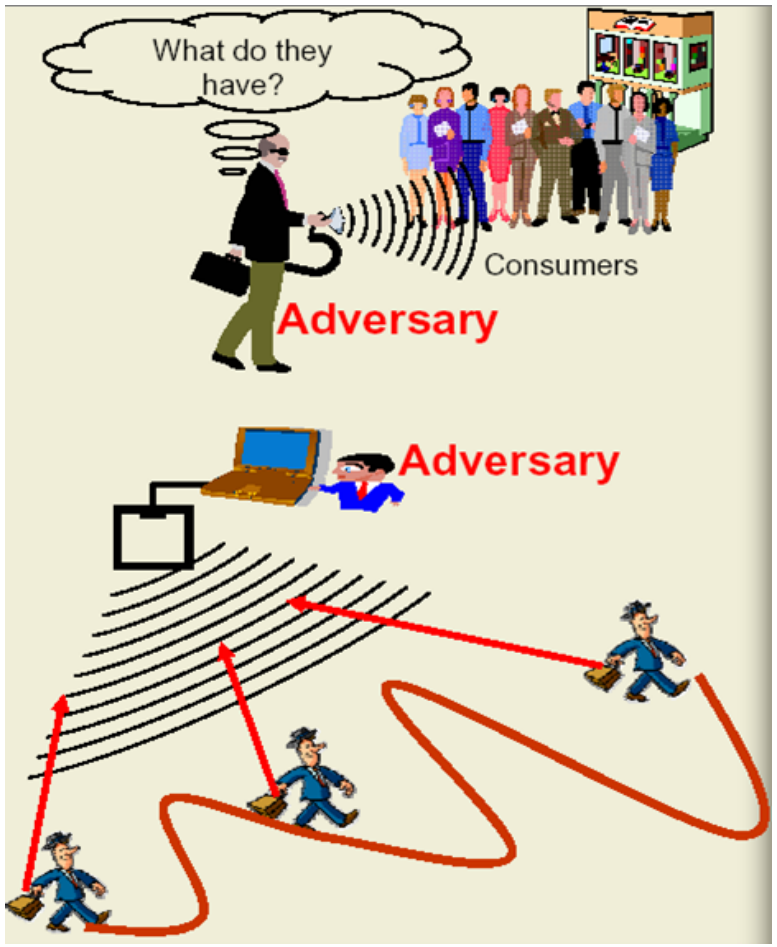
- $\mathcal{T}$ RF tag.
- $\mathcal{R}$ RF tag reader.
- $\mathcal{B}$ Back-end server, which has a database.
- $\mathcal{A}$ Adversary.
- $h()$ One-way hash function.
- $PRNG$ PseudoRandom Number Generator.
- $\oplus$ Exclusive-or (XOR) function.
- r_r Pseudorandom number generated by $PRNG$ of $\mathcal{R}$.
- r_t Pseudorandom number generated by $PRNG$ of $\mathcal{T}$.
- $\stackrel{?}{=}$ Verification operator to check whether the left hand side is valid for the right hand side or not.
- $\leftarrow$ Update operator from the right hand side to the left hand side.

Components and Channels

- **Channel btw $\mathcal{B}$ and $\mathcal{R}$**
  - Secure channel
    - Enough computational power of $\mathcal{B}$ and $\mathcal{R}$.
- **Channel btw $\mathcal{R}$ and $\mathcal{T}$**
  - Insecure channel
    - Limited computation power of $\mathcal{T}$
    - RF interface

Privacy Problems

- **Information leakage of user belongings**
  - Some are quite personal
  - ex) medicine, books, money, or expensive products
- **Behavioral tracking**
  - If a user carries traceable $\mathcal{T}$, the identity and movements of the user can be traced by tracking $\mathcal{T}$.



@ picture is credited to Ohkubo *et. al.*

Attacking Model

- **Eavesdropping**
  - $\mathcal{A}$ can easily eavesdrop communications btw $\mathcal{T}$ and $\mathcal{R}$ without user's recognition.
- **Active Query**
  - $\mathcal{A}$ can actively query to $\mathcal{T}$ to get responses.
- **DB Desynchronization**
  - $\mathcal{A}$ can try to desynchronize identification information btw $\mathcal{B}$ and $\mathcal{T}$.
- **Tampering**
  - $\mathcal{A}$ can tamper with $\mathcal{T}$ because a low-cost $\mathcal{T}$ offers no tamper-resistance mechanism.

Security Requirements

Indistinguishability

- Values emitted by $\mathcal{T}$ must not be discriminated from the other $\mathcal{T}$.

Security Requirements

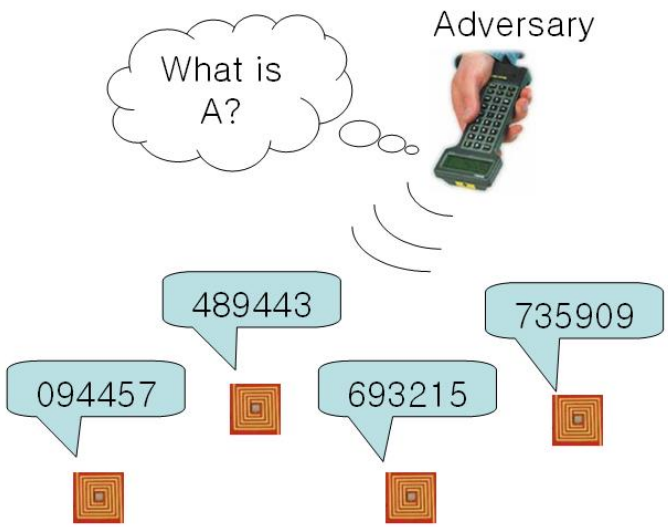
Indistinguishability

- Values emitted by $\mathcal{T}$ must not be discriminated from the other $\mathcal{T}$.

Security Requirements

Indistinguishability

- Values emitted by $\mathcal{T}$ must not be discriminated from the other $\mathcal{T}$.



Security Requirements

Indistinguishability

- Values emitted by $\mathcal{T}$ must not be discriminated from the other $\mathcal{T}$.

Forward Security

- Contents of memory in $\mathcal{T}$ does not give any hint to detect past outputs

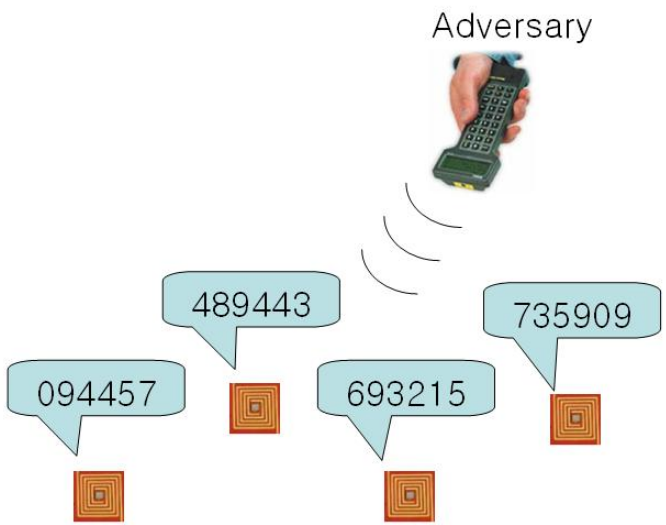
Security Requirements

Indistinguishability

- Values emitted by $\mathcal{T}$ must not be discriminated from the other $\mathcal{T}$.

Forward Security

- Contents of memory in $\mathcal{T}$ does not give any hint to detect past outputs



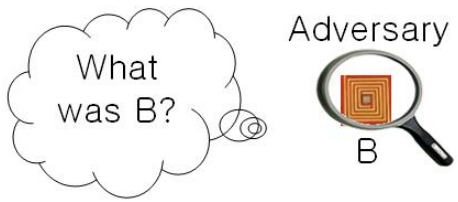
Security Requirements

Indistinguishability

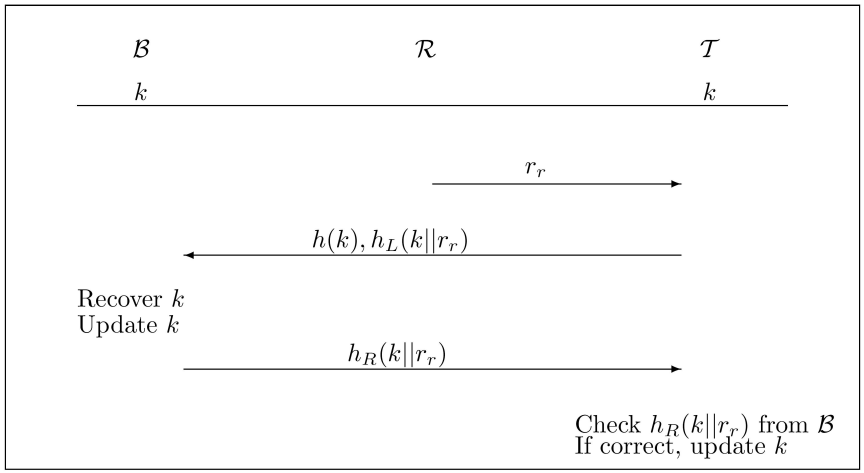
- Values emitted by $\mathcal{T}$ must not be discriminated from the other $\mathcal{T}$.

Forward Security

- Contents of memory in $\mathcal{T}$ does not give any hint to detect past outputs

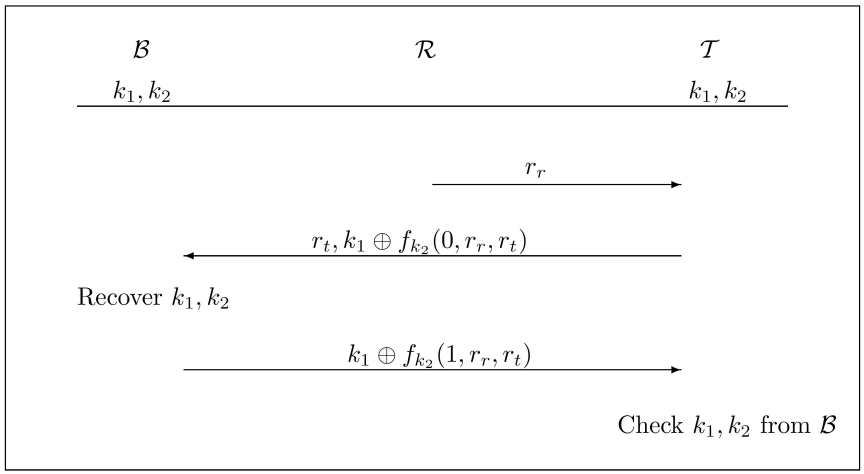


Lee *et al.*'s Scheme [ICCSA 2005]



- **Scheme**
  - Update: $k \leftarrow k \oplus r_r$
- **Security analysis**
  - Partially indistinguishable: $h(k)$ doesn't vary within successive mutual authentications.
  - Not forward secure: r_r can be eavesdropped.

Molnar *et al.*'s Scheme [ACM CCS 2004]

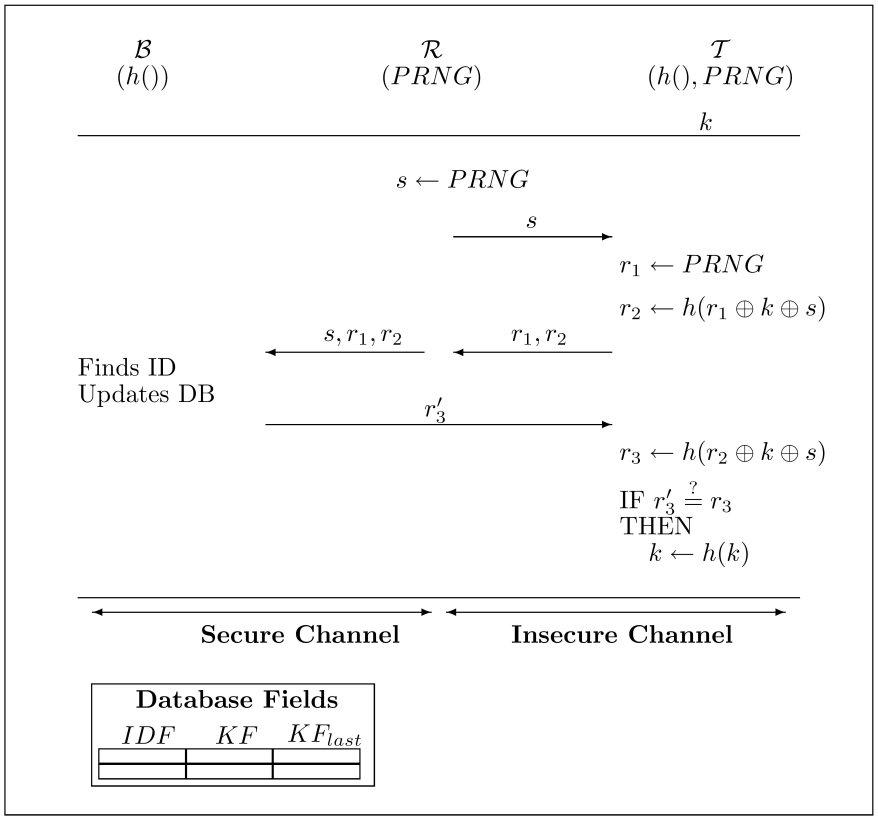


- **Scheme**
  - Do not update k_1, k_2
- **Security analysis**
  - Indistinguishable
  - Not forward secure: $\mathcal{A}$ can test responses of $\mathcal{T}$ by using fixed k_1, k_2.

Our Scheme (1/5) - Main Idea

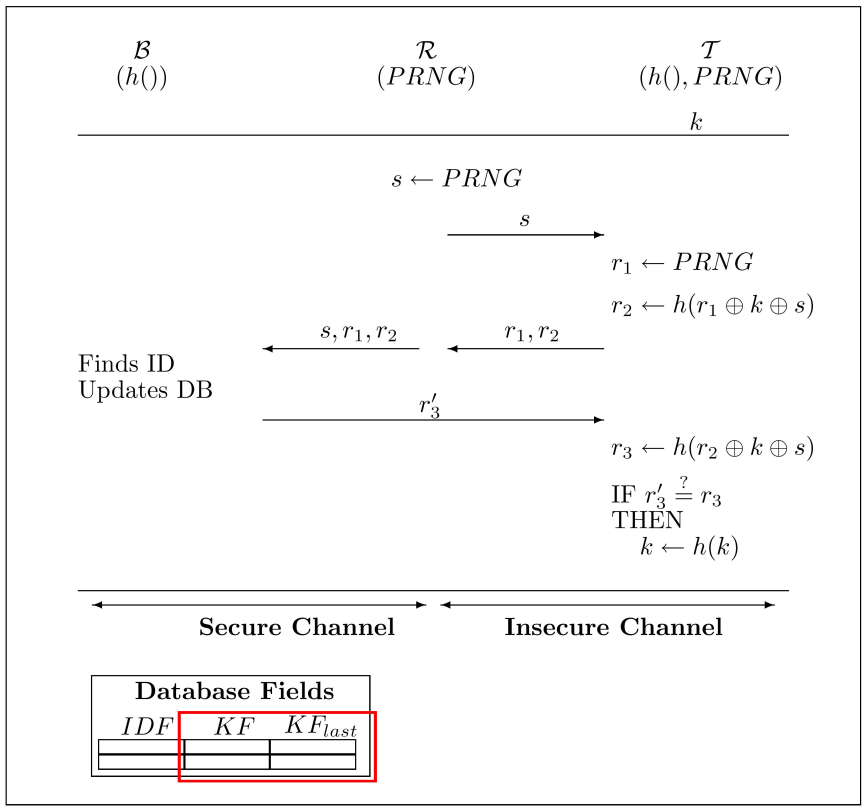
- Share a key between $\mathcal{B}$ and $\mathcal{T}$
- Mutual authentication between $\mathcal{B}$ and $\mathcal{T}$
  - Essential for key update
- To prevent desynchronization
  - Save a preceding key in DB
- For indistinguishability
  - Random numbers are participated in all emitted values
- For forward security
  - Update a key by hashing it

Our Scheme (2/5) - Mutual Authentication



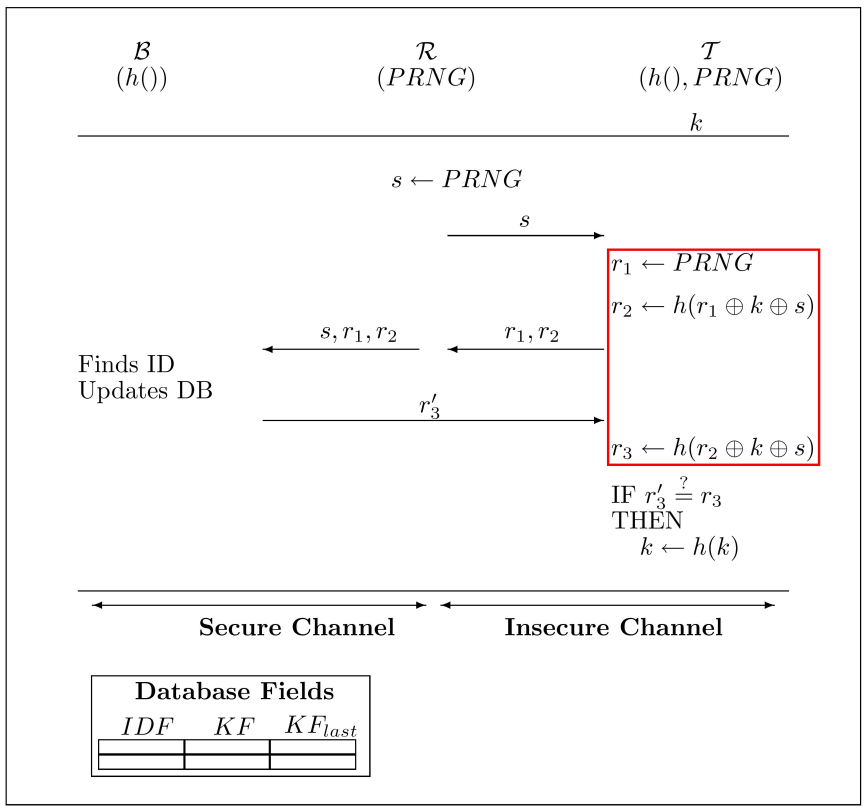
- At $\mathcal{B}$
  - Authentication of $\mathcal{T}$: Find $k' \in KF \cup KF_{last}$, $h(r_1 \oplus k' \oplus s) \stackrel{?}{=} r_2$
  - $r'_3 \leftarrow h(r_2 \oplus k' \oplus s)$
- Update
  - $k \leftarrow h(k)$

Our Scheme (3/5) - Update k



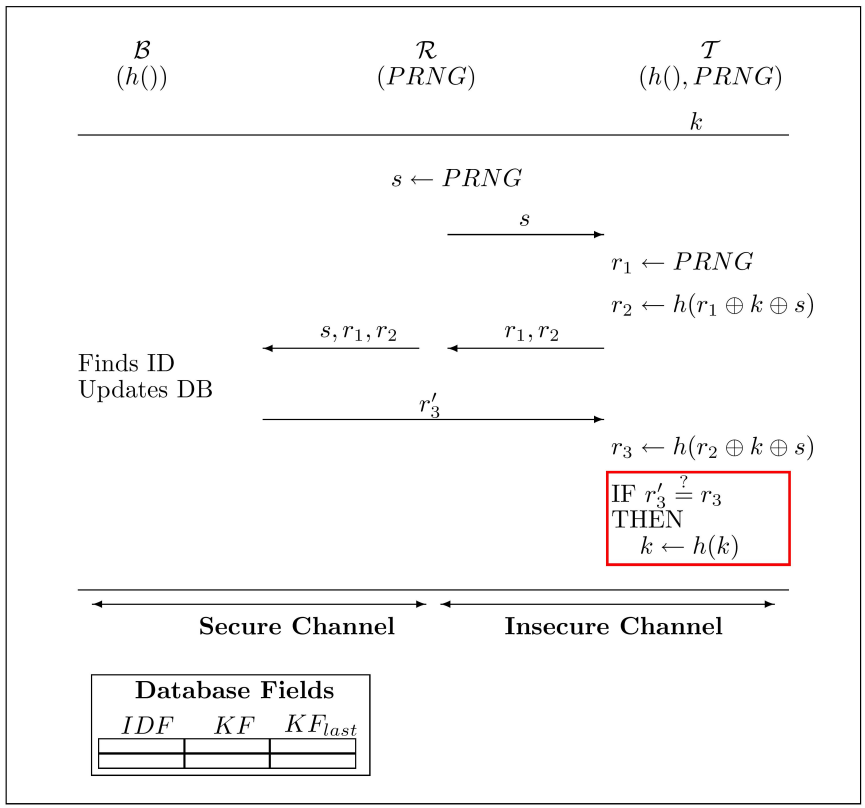
- Attack
  - Man-in-the-middle attack to desynchronize k
- KF: Current k
- KF_{last}: Preceding k
- Update at $\mathcal{B}$
  - When $\mathcal{T}$ is authenticated by using k in KF
    - $k_{last} \leftarrow k, k \leftarrow h(k)$
  - When $\mathcal{T}$ is authenticated by using k in KF_{last}
    - Do not update DB

Our Scheme (4/5) - Indistinguishability



- Attack
  - Eavesdropping or query
- r_1
  - Random number
- r_2 and r_3
  - $\mathcal{A}$ who doesn't know k cannot distinguish r_2 and r_3 from a random number.

Our Scheme (5/5) - Forward Security



- Attack
  - Collect responses from many $\mathcal{T}$
  - Tamper with a given $\mathcal{T}$
- k is updated by $h()$
  - $h()$ is a one-way function.
  - $\mathcal{A}$ cannot know previous k
- Partially forward traceable
  - The forward trace is limited to a short period.

Security Comparison

Scheme	Lee	Molnar	Our scheme
Computation at $\mathcal{B}$	$O(1)$	$O(m)$	$O(m)$
Indistinguishability	$\triangle$	O	O
Forward Security	X	X	$\triangle$

m : The number of $\mathcal{T}$ in a system

O : Satisfy

$\triangle$: Partially satisfy (Traceable within key update)

X : Do not satisfy

Comparison of Efficiency in $\mathcal{T}$

Scheme	Lee	Molnar	Our scheme
Hash operations	2	2	3
Communication complexity	$3l$	$4l$	$4l$
Non-volatile memory	l	$2l$	l

l : The length of an output of $h()$ and $PRNG$

Conclusion

- Proposed mutual authentication scheme
  - Utilize a hash function and synchronized secret information
  - Indistinguishable and almost forward secure
  - One more hash operation in comparison with Molnar *et al.*'s scheme
- Further work
  - Analyze security of our scheme in provable security setting
  - Study a mutual authentication scheme which is totally indistinguishable and forward secure