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

Enhancing Security of EPCglobal Gen-2 RFID Tag against Traceability and Cloning

Dang Nguyen Duc, Jaemin Park, Hyunrok Lee and Kwangjo Kim*

CAIS Lab, Information and Communications University (ICU), Korea

Auto-ID Lab, ICU, Korea

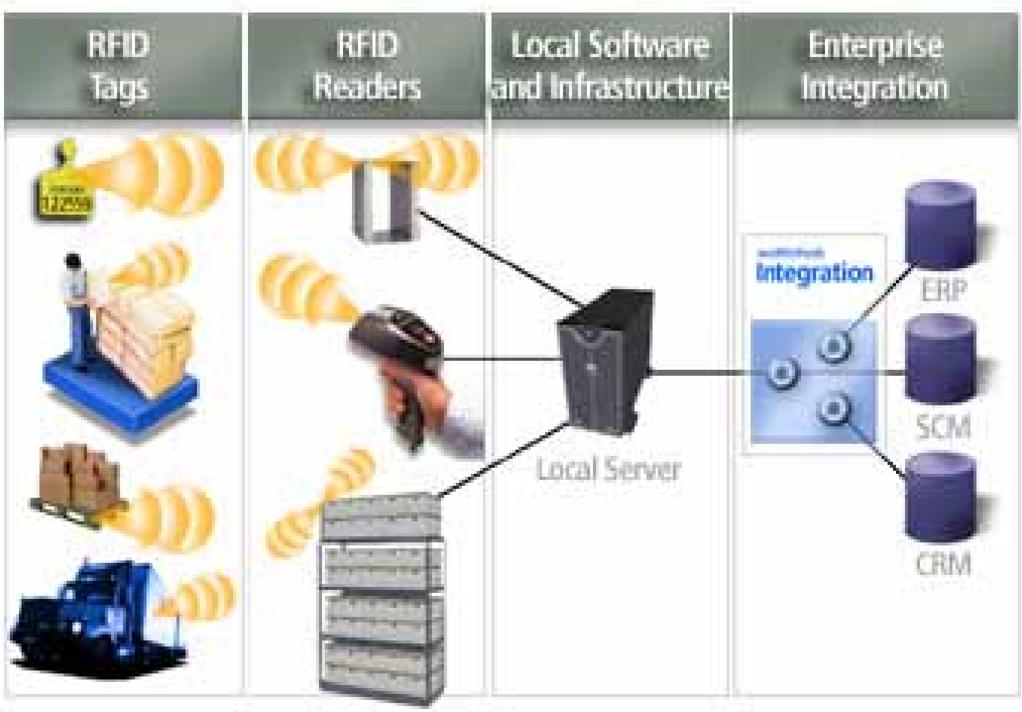
This work was partially supported by a grant No.R12-2003-004-01004-0 from Ministry of Commerce, Industry and Energy

Content

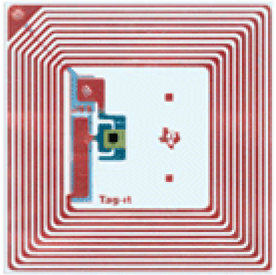
- RFID Overview
- Security and Privacy Issues in RFID System
- Previous Protocols
- New Protocol
- Analysis and Comparison
- Conclusion and Future Work

RFID Overview

- Wirelessly and Automatically identify objects nearby:



A multi-tier system: RFID tag, reader and backend server



A typical RFID tag

@ Pictures are adapted from Internet

RFID Applications

Supply chain management

Smart appliance

Payment system

Library management

Smart labels

Security Lock

@ Pictures are adapted from Internet

Distinguished Properties of RFID

- Properties of RFID tag that matter:
  - Short range wireless communication.
  - Extremely low cost (expected to be 5 cents by 2007).
  - Minimal computational functionalities.
  - Limited memory.
  - No power source (receive power from reader).

RFID Organization

- **Auto-ID Lab**
  - Established at MIT. Later expand to Keio, Fudan, St. Gallen, Cambridge, Adelaide and ICU Universities..
  - Research on RFID technology and develop open standards.
  - Our work in Auto-ID Lab in Korea focuses on Mobile RFID and RFID security.
- **EPCglobal Inc.**
  - Joint venture of EAN International (Europe) and UCC (USA).
  - Develop industry RFID standards.
  - Class-1 Gen-2 RFID standard: air interface protocol for RFID devices – latest version 1.09

This work aims at suggesting possible security enhancements for Gen-2 standard !

EPCGlobal Class-1 Gen-2 Tag

- Passive RFID Tag
  - Receive power from Tag reader.
  - Communicate in UHF Band (800 – 960 MHz) and communication range up to 10m.
- Privacy Protection
  - Self-destruct when received kill command (with valid 32-bit kill PIN).
- Other security features
  - Memory access possible only when Tag in “secure mode”.

Security and Privacy Issues in RFID

- Lack of authentication:
  - Malicious reading (skimming)
  - Captured information aids duplicating genuine tags.
  - Denial-of-Service due to deployment of cloned tags.

- Privacy invasion:
  - Static ID is subject to tracking.

@ picture is credited to Juels et. al.

Previous Protocols for Secure RFID

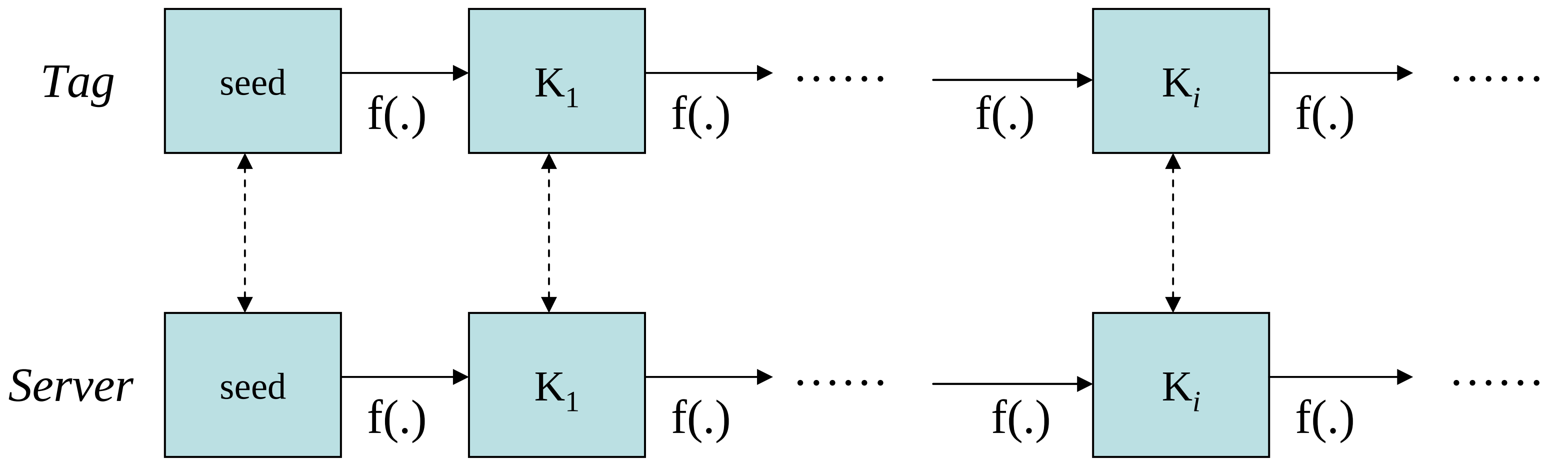
- Hash-based protocols:
  - By Ohkubo *et. al*. and other researchers.
  - Cons: cryptographic hash is still beyond current capability of RFID tag.
- Juels' protocol for Gen-2 Tag:
  - Provide authentication but not eavesdropping and privacy protection.
  - Cons: Tag and reader need to repeat q rounds of PIN-test to get $1/2^q$ security margin.

New protocol - Design Considerations

- RFID Tag is extremely computational limited:
  - Employ only PRNG, logical operations, CRC $\Rightarrow$ ratified by Gen-2 standard.
    - **Note:** We will not make use of “weak” one-way property of CRC. We use only its *compression* and *integrity-checking* properties.
- Secure
  - Provide reasonable protection against cloning and privacy invasion.
- Easy to adapt to current RFID standards:
  - Need not to rework entire standard.

Main Idea

- Using seeded PRNG to share session key



- Reader is a proxy between Tag and Server:
  - Reader always asks Server to decode EPC for every Tag query ⇒ easy access control and accountability.
  - Reader has to authenticate to Server first ⇒ no need to Reader-to-Tag authentication (except when Reader "access" Tag's memory).

- Some Notations

- f(.) – pseudo-random number generator
- CRC(.) – cyclic redundancy check function (produce checksum)
- K_i – secret key at the *i*-th session
- EPC – Electronic Product Code
- *r* – random nonce.
- PIN – “access” command password
- T – Tag
- R – Reader
- S- Backend Server

- Protocol

- Deployment time:
  - For each RFID tag, choose a unique seed's number *seed* and compute.

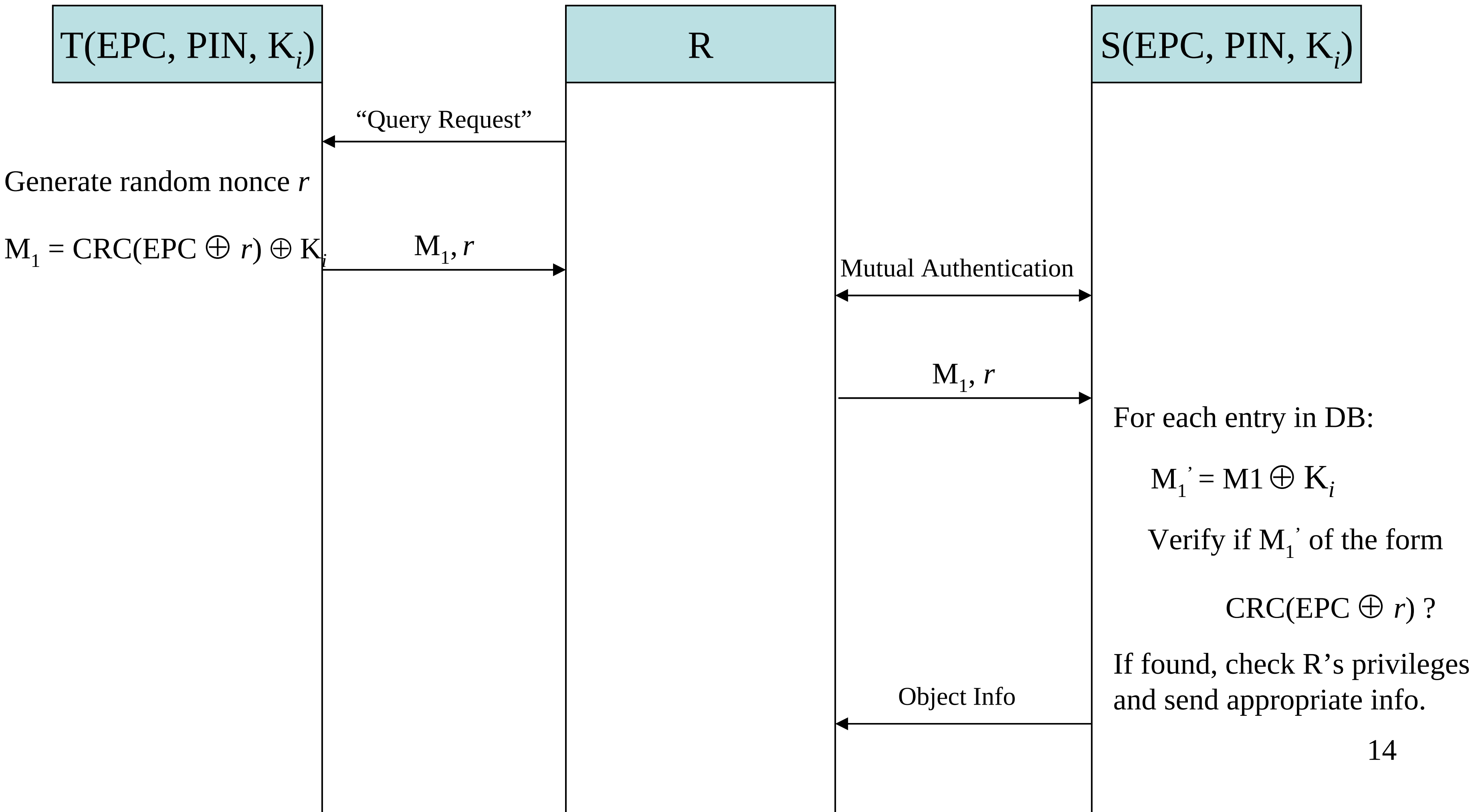
$$K_1 = f(\textit{seed})$$

  - Choose PIN for each tag.
  - Store EPC, PIN, K_1 on each tag and in EPC, PIN, K_1in backend server's database.

id	**pin**	$\mathbf{K_i}$
EPC	PIN	K_1

- Protocol (cont.)

- Tag Query Protocol:



- Protocol (cont.)

- Tag Access Protocol:
  - S $\rightarrow$ R: $M_2 = CRC(EPC \parallel PIN \parallel r) \oplus K_i$
  - R $\rightarrow$ T: forward authentication token M_2 to T.
  - T: Verify $M_2 \oplus K_i = CRC(EPC \parallel PIN \parallel r)$?
- Key Updating Protocol
  - R $\rightarrow$ T, S: ‘End Session’
  - T: $K_{i+1} = f(K_i)$
  - S: $K_{i+1} = f(K_i)$

Database-desynchronization protection: R announces ‘End Session’ with a token CRC($r' \oplus$ PIN’) where r' is a random nonce broadcasted to Tag with ‘Query Req’ and PIN’ is a secret shared between T and legitimate R.

Security Analysis

- Tag authentication:
  - CRC(EPC $\oplus$ r) is blinded by K_i to avoid direct attack on weak one-wayness of CRC.
  - Tag's EPC must satisfy integrity-checking property of CRC to be recognized by server.
- Reader authentication:
  - Reader must authenticate himself to server get object information.
  - A valid access PIN and K_i are required to "access" Tag's memory.
- Privacy protection
  - Tag does not directly emit EPC and session key is kept changing, then malicious readers cannot perform tracking.

Comparison with Juels' Protocol

	Juels' Protocol	Our Protocol
Server's complexity	O(N)	O(N)O(CRC)
Reader's complexity	O(q)	O(1)
Tag's complexity	O(q)	1CRC+1PRNG
Tag authentication	YES	YES
Reader authentication	YES	YES
Eavesdropping protection	NO	YES
Privacy protection	NO	YES

Note: N – # of tags; O(CRC) – complexity of CRC; q – number of PIN-test round; Reader-to-Server authentication complexity not counted

Conclusion & Future Work

- Propose a new communication protocol for Gen-2 RFID:
  - Light-weight
  - Implicit authentication of Reader and Tag.
  - Eavesdropping protection.
  - Privacy protection.
- Future work:
  - Rigorous analysis.
  - Multiple reading.
  - Backend server’s complexity should be improved.
  - Transfer of tag’s ownership.