

# Information confinement, privacy, and security in RFID systems

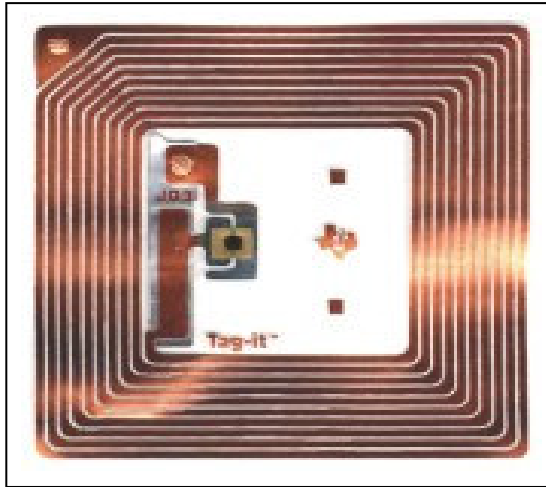
(To appear at ESORICS '07)

Roberto Di Pietro  
Università di Roma Tre  
dipietro@mat.uniroma3.it

\*Joint work with Prof. Refik Molva, Eurecom Institute, Sophia Antipolis, France

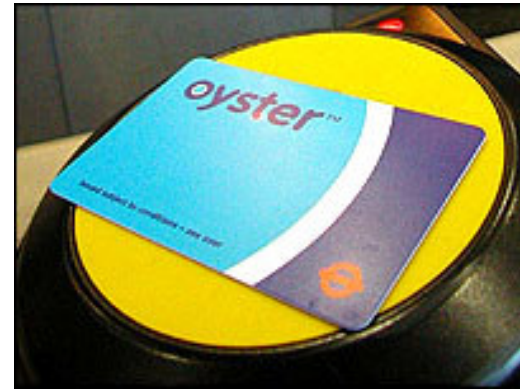
# Outline

- (brief) Introduction to RFID
- Contributions highlight
- Information Confinement (in case of Reader compromise)
- Identification Protocol
- Mutual Authentication Protocol
- Analysis
- Conclusions



- Silicon chips and antenna
- 64 bit identifying sequence
- No internal power source
- Very small:  $.15 \text{ mm}^2$
- Cheap: 50 cents, possibly 5 cents in future

RFID tags are (and will be) pervasive



The dawn of 1984....



## Assumptions:

Tags can:

- run a PRNG;
- run a hash function (H)

Tags cannot:

- grab any power but the power provided by an external source -e.g. the reader- (are passive);
- unable to run public key crypto.

Readers:

- have enough power and memory;
- store the symmetric keys shared with the tags;
- there are... multiple readers (think of a Wall Mart warehouse).

## Contributions highlight

We have designed a protocol that provides:

- information confinement in case of reader compromise;
- efficient, lightweight tag identification protocol;
- mutual authentication between tag and reader;
- privacy and resilience to reply and (some) DoS attacks

# Information confinement

**Center** set-up activities for:

Tags:

- generates  $n$  keys  $k_1, \dots, k_n$  ;
- assign key  $k_i$  to tag  $ID_i$

Readers:

- computes the  $n$  keys to be assigned to the  $m$  readers;

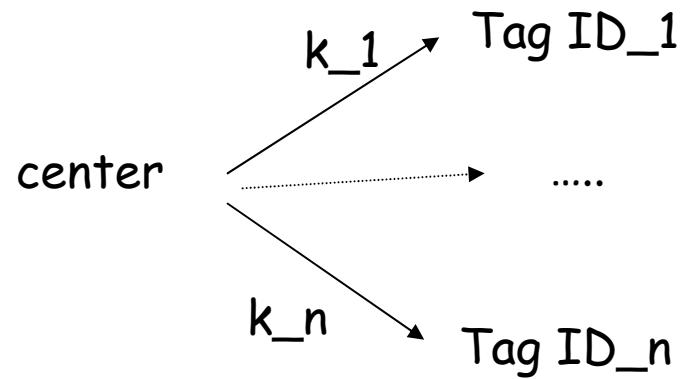
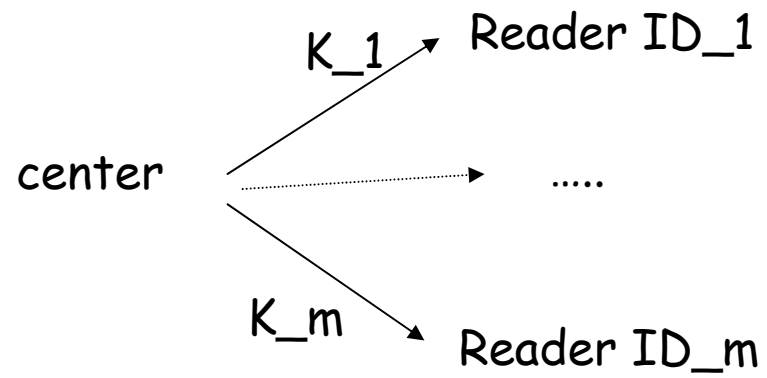
For instance, for reader  $ID_j$ :

For  $i=1$  to  $n$ :

$$k_{(i,j)} = H(k_i \parallel ID_j \parallel k_i)$$

- Let  $K_j = \langle k_{(1,j)}, \dots, k_{(n,j)} \rangle$ , assign  $K_j$  to reader  $ID_j$

## Information confinement



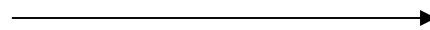
# Information confinement

Reader ID\_ j

Stores  $K_j$ , that is:

$$K_j = \left\{ \begin{array}{l} k_{(1,j)} \\ k_{(2,j)} \\ \dots \\ \boxed{k_{(i,j)}} \\ \dots \\ k_{(n,j)} \end{array} \right.$$

ID\_ j

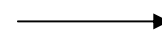


Tag ID\_ i

Stores just  $k_i$

Computes:

$$H(k_i \parallel ID_j \parallel k_i)$$



$$\boxed{k_{(i,j)}}$$

## Information confinement

- Tag ID<sub>i</sub> has been compromised: sorry, the adversary **IS** the tag.
- Reader ID<sub>j</sub> has been compromised !

Reader ID<sub>j</sub> cannot pretend to be the reader ID<sub>t</sub>, for  $t \neq j$ .

Indeed, once Reader ID<sub>j</sub> sends ID<sub>t</sub> to the tag, the tag will compute:

$$k_{(i,t)} = H(k_i \parallel ID_t \parallel k_i)$$

But  $k_{(i,t)}$  **will not belong** to  $K_j$

# Tag Identification

Preliminaries:

- Given:

- $r_p \in_{\mathcal{R}} \{0,1\}^L$  for  $p= 1, \dots, q$
- $\alpha_p = k_{(i,j)} \text{ XOR } r_p$

- Define the function DPM as:

DPM:  $\{0,1\}^L \rightarrow \{0,1\}$ , where  $\text{DPM}(r_p) = P(M(r_p))$  where:

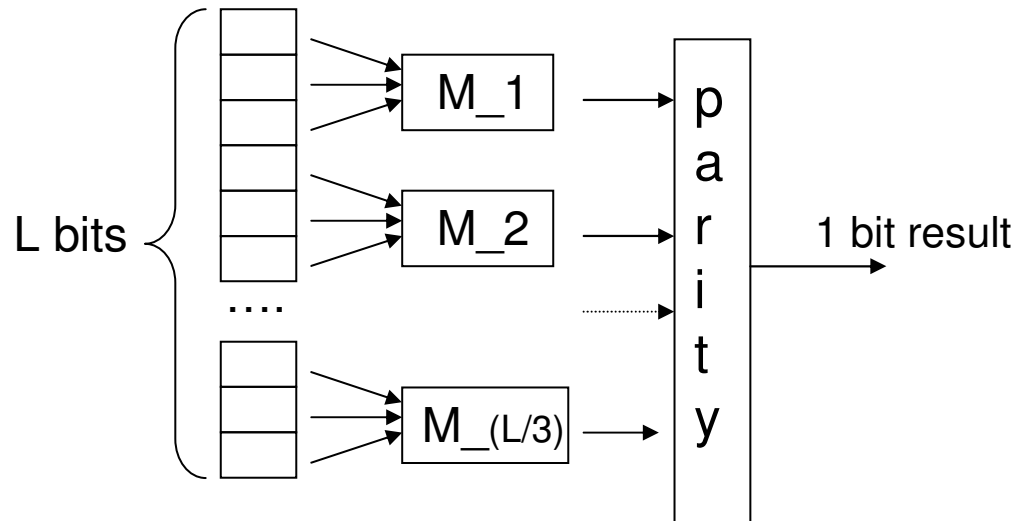
$M: \{0,1\}^L \rightarrow \{0,1\}^{L/3}$  and  $P: \{0,1\}^{L/3} \rightarrow \{0,1\}$

- Let  $V \in \{0,1\}^q$  a vector of  $q$  bits.

Populate vector  $V$  as:  $V[p] = \text{DPM}(r_p)$

# Tag Identification

The function DPM:



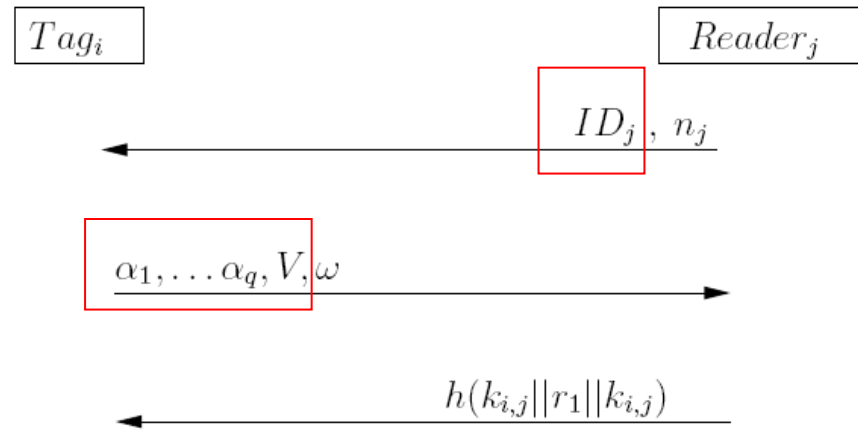
$M_i$ : **majority** function, defined as:

$$M_1 = b_1 \text{ AND } b_2 \text{ OR } (b_1 \text{ AND } b_3) \text{ OR } (b_2 \text{ AND } b_3)$$

**parity** function, defined as:

$$P = M_1 \text{ xor } M_2 \text{ xor } \dots \text{ xor } M_{(L/3)}$$

# Tag Identification



**Fig. 1.** The proposed protocol

Where:

- $r_p \in_{\mathcal{R}} \{0,1\}^L$  for  $p= 1, \dots, q$
- $\alpha_p = k_{(i,j)} \text{ XOR } r_p$
- $V[p]=\text{DPM}(r_p)$


# Tag Identification

**Global variables:**  $n ; q ; KDB$

**Input** :  $\langle \alpha_1, \dots, \alpha_q, V, w \rangle$

**Output** : The active entries of the KDB.

```
1.1 for  $i=1$  to  $n$  do
1.2 |    $Active[u] = True$ 
1.3 end
1.4  $count = 0 ; a = 0$ 
1.5 while  $a < q$  do
1.6 |    $u = 0$ 
1.7 |   while  $u < n$  do
1.8 |     if  $Active[u]$  then
1.9 |        $r' = \alpha_a \oplus KDB[u]$ 
1.10 |      if  $DPM(r') \neq V[a]$  then
1.11 |         $Active[u] = False$ 
1.12 |         $count ++$ 
1.13 |      end
1.14 |    end
1.15 |     $u ++$ 
1.16 |  end
1.17 |   $a ++$ 
1.18 end
1.19 if  $count = n$  then
1.20 |   fail
1.21 else
1.22 |   return  $KDB[j]$  s.t.  $Active[j] = True$ 
1.23 end
```

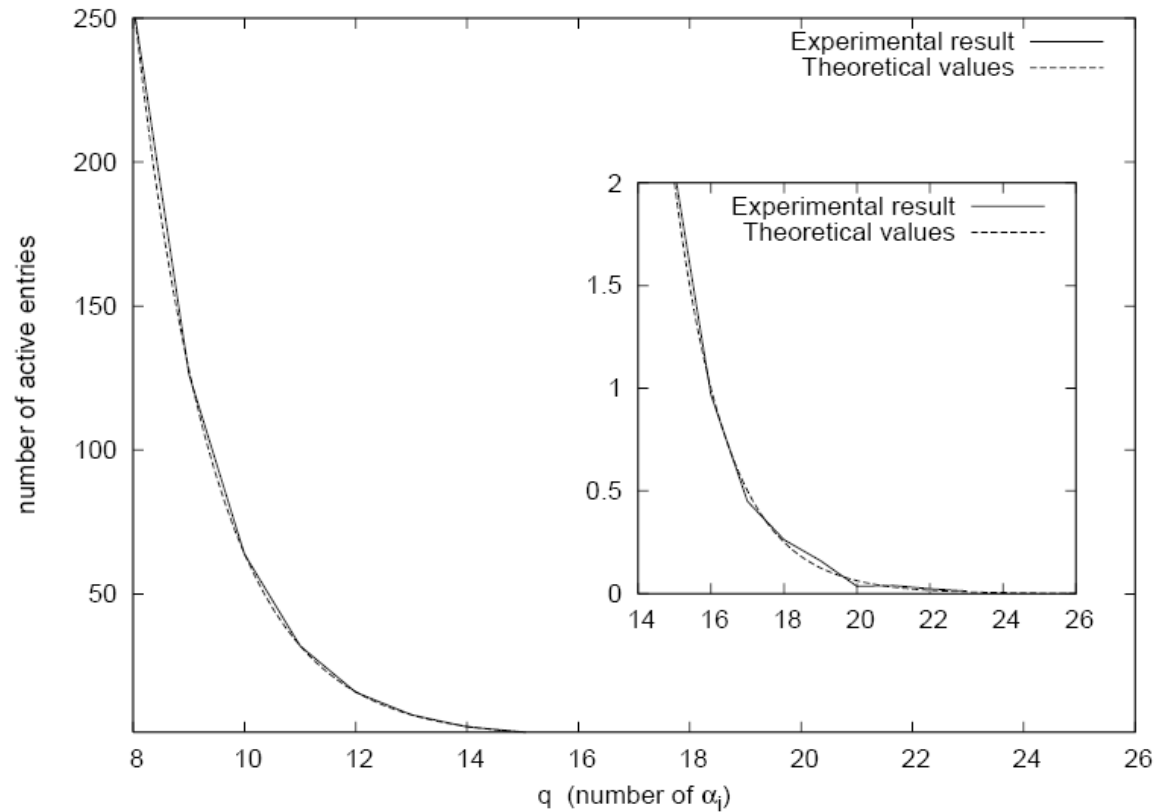


## Tag Identification

Outcome of the identification procedure:

- no active entries are left in the KDB (id failed);
- one active entry is returned;
- more than one entry is returned.

# Tag Identification



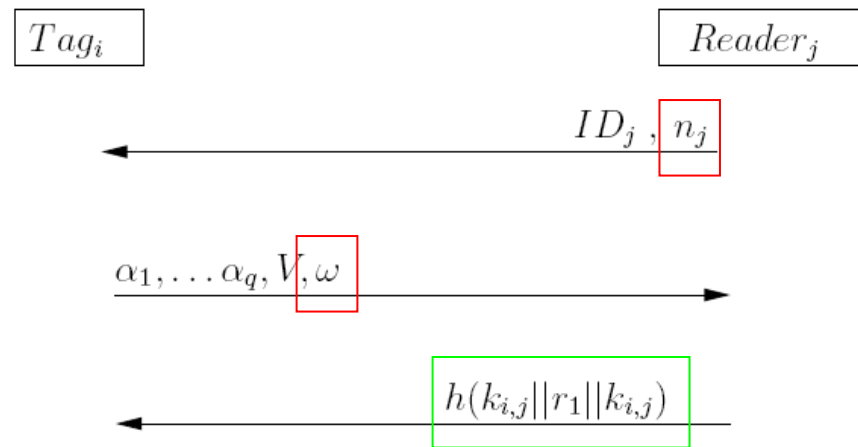
Simulation: protocol execution where the KDB ( $K_j$ ) has 65,536 entries.

## Mutual authentication

Assume the Identification protocol succeeded:  
just one entry has been returned

We now want to achieve mutual authentication.

# Tag authentication

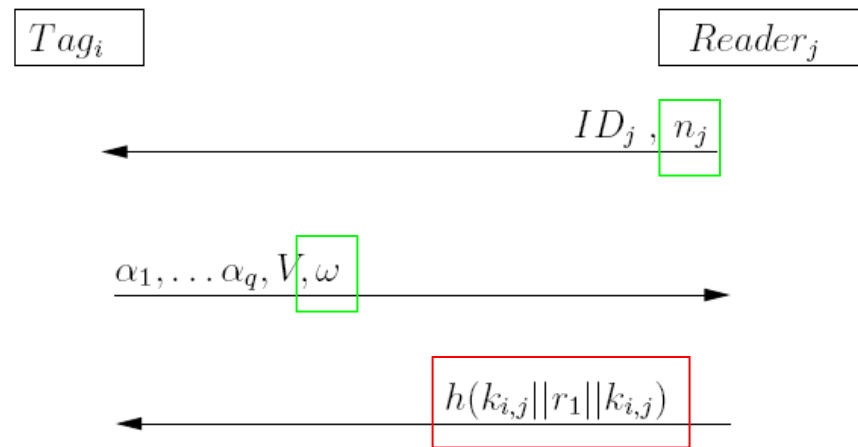


**Fig. 1.** The proposed protocol

Where:

$$\omega = H(k_{(i,j)} || n_j || r_1 || k_{(i,j)})$$

## Reader authentication



**Fig. 1.** The proposed protocol

Where:

$$\omega = H(k_{(i,j)} || n_j || r_1 || k_{(i,j)})$$

## Features:

### Overhead analysis

|                      | Reader ID_ j              | Tag ID_i   |
|----------------------|---------------------------|--|
| <b>Memory</b>        | $K_j$ , that is: $n$ keys | just one key: $k_i$  |
| <b>Computations*</b> | $nq$ XOR, $nq$ comparison | $q$ invocations of PRNG<br>$qL$ AND + $qL$ OR + $qL/3$ XOR |
|                      | 2 invocations of H        | 2 invocations of H   |

\*note that, on the average,  $q = \log n$ .

## Features:

### Protocols comparison

**Table 1.** Comparison of our proposal with some protocols

| Protocol         | Properties |                 |                   |                      |
|------------------|------------|-----------------|-------------------|----------------------|
|                  | Privacy    | Mutual<br>auth. | DoS<br>resilience | reply<br>attack res. |
| Our [this paper] | Yes        | Yes             | Yes               | Yes                  |
| OSK/OA [5]       | Yes        | Yes             | No                | Yes                  |
| CR/MW [3]        | weak       | Yes             | Yes               | Yes                  |
| Ya-Trap[2]       | Yes        | No              | No                | Yes                  |

## Conclusions

- Relaxed the assumption that readers cannot be compromised
- Provided a confinement technique: the secret database of each reader is made reader-dependent
- Proposed a **lightweight**, probabilistic tag identification mechanism that:
  - is privacy preserving;
  - is leveraged to achieve mutual authentication between the reader and the tag;
  - is resilient to DoS and replay attacks.

Questions ?



# References

1. Juels, A.: Rfid security and privacy: A research survey. *IEEE Journal on Selected Areas in Communications* 24(2) (2006) 381-394
2. Tsudik, G.: Ya-trap: Yet another trivial rfid authentication protocol. In: *IEEE PerComWorkshops*. (2006) 640-643
3. Molnar, D., Wagner, D.: Privacy and security in library rfid: issues, practices, and architectures. In: *CCS '04: Proceedings of the 11th ACM conference on Computer and communications security*, New York, NY, USA, ACM Press (2004) 210-219
4. Rhee, K., Kwak, J., Kim, S., Won, D.: Challenge-response based RFID authentication protocol for distributed database environment. In Hutter, D., Ullmann, M., eds.: *International Conference on Security in Pervasive Computing - SPC 2005*. Volume 3450 of LNCS., Boppard, Germany, Springer-Verlag (April 2005) 70-84
5. Avoine, G., Dysli, E., Oechslin, P.: Reducing time complexity in RFID systems. In Preneel, B., Tavares, S., eds.: *Selected Areas in Cryptography - SAC 2005*. Volume 3897 of LNCS., Kingston, Canada, Springer-Verlag (August 2005) 291-306
6. Avoine, G., Oechslin, P.: A scalable and provably secure hash based RFID protocol. In: *International Workshop on Pervasive Computing and Communication Security - PerSec 2005*, Kauai Island, Hawaii, USA, IEEE, IEEE Computer Society Press (March 2005) 110-114
7. Hellman, M.: A cryptanalytic time-memory tradeoff. *IEEE Transactions on Information Theory* 26 (1980) 401-406

# References

8. Conti, M., Di Pietro, R., Mancini, L.V., Spognardi, A.: RIPP-FS: an rfid identification, privacy preserving protocol with forward secrecy. In: Proceedings of the 3rd IEEE International Workshop on Pervasive Computing and Communication Security, IEEE Press, to appear (2007)
9. Juels, A., Weis, S.: Authenticating pervasive devices with human protocols. In Shoup, V., ed.: Advances in Cryptology - CRYPTO'05. Volume 3126 of LNCS., Santa Barbara, California, USA, IACR, Springer-Verlag (August 2005) 293-308
10. Hopper, N.J., Blum, M.: Secure human identification protocols. In: ASIACRYPT. (2001) 52-66
11. Gilbert, H., Robshaw, M., Sibert, H.: An active attack against HB+ - a provably secure lightweight authentication protocol. Cryptology ePrint Archive, Report 2005/237 (2005)
12. Bringer, J., Chabanne, H., Emmanuelle, D.: HB++: a lightweight authentication protocol secure against some attacks. In: IEEE International Conference on Pervasive Services, Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing - SecPerU 2006, Lyon, France, IEEE, IEEE Computer Society Press (June 2006)
13. Piramuthu, S.: HB and related lightweight authentication protocols for secure RFID tag/reader authentication. In: Collaborative Electronic Commerce Technology and Research - COLLECTeR 2006, Basel, Switzerland (June 2006)
14. Menezes, A.J., van Oorschot, P.C., Vanstone, S.A.: Chapter 9 - Hash Functions and Data Integrity. In: Handbook of applied cryptography. CRC Press (1996)

# References

15. Feldhofer, M., Wolkerstorfer, J., Rijmen, V.: Aes implementation on a grain of sand. IEE Proceedings - Information Security 152(1) (October 2005) 13-20
16. Pramstaller, N., Rechberger, C., Rijmen, V.: A compact fpga implementation of the hash function whirlpool. In: FPGA '06: Proceedings of the 2006 ACM/SIGDA 14th international symposium on Field programmable gate arrays, New York, NY, USA, ACM Press (2006) 159-166
17. Matsui, M.: Linear cryptanalysis method for des cipher. In Springer, ed.: Advances in Cryptology-Eurocrypt '93, Lecture Notes in Computer Science n. 765 (1993) 386-397