

# Open Questions in Radio Frequency Identification

**Gildas Avoine**

EPFL, Lausanne, Switzerland



What is the RFID?

What is the Purpose of the RFID?

What are the Security Issues?

How to Design an RFID Protocol?

What is the RFID?

What is the Purpose of the RFID?

What are the Security Issues?

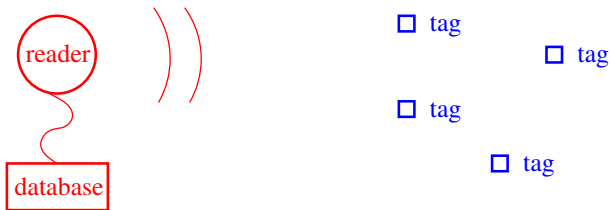
How to Design an RFID Protocol?

**W**hat is the RFID?

## Definition

Radio Frequency IDentification (**RFID**) is a method of storing and remotely retrieving data using devices called RFID **tags**.

An RFID tag is a **small object** that can be **attached to or incorporated** into a product, animal, or person.



The boom which RFID technology is enjoying today relies essentially on the willingness to develop **small** and **cheap** RFID tags.

- Passive (power supplied by the reader)
- Communication distance (up to a few meters)
- Memory (identifier + possibly additional EEPROM)
- Tamper-resistance (**usually not**)
- Computation capabilities (**Memory, Symmetric, Asymmetric**)

- Management of stocks
- Libraries
- Anti-counterfeiting
- Access control
- Localization of people
- Electronic documents
- Counting cattle

What is the RFID?

**What is the Purpose of the RFID?**

What are the Security Issues?

How to Design an RFID Protocol?

**W**

**hat is the Purpose of the RFID?**

- Management of stocks
- Libraries
- Anti-counterfeiting
- Access control
- Localization of people
- Electronic documents
- Counting cattle

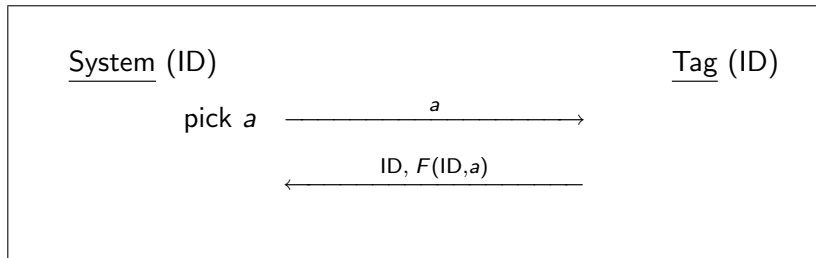
Do we need **security** or just **functionality**?

### Definition (Tag Authentication)

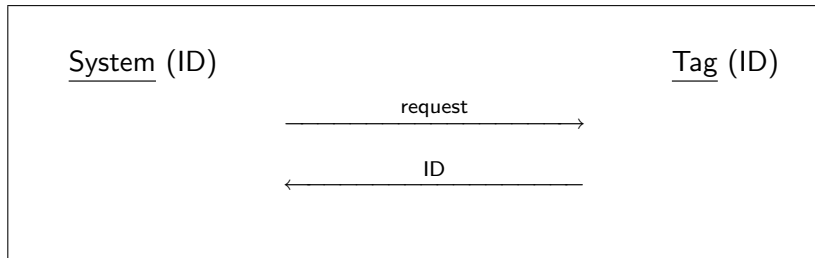
The authentication of a tag consists for the reader in obtaining the identity of the tag and a **proof** that the claimed identity is correct.

### Definition (Tag Identification)

The identification of a tag consists for the reader in obtaining the identity of the tag, but **no proof is required**.



Basic challenge-response authentication scheme



Basic identification scheme

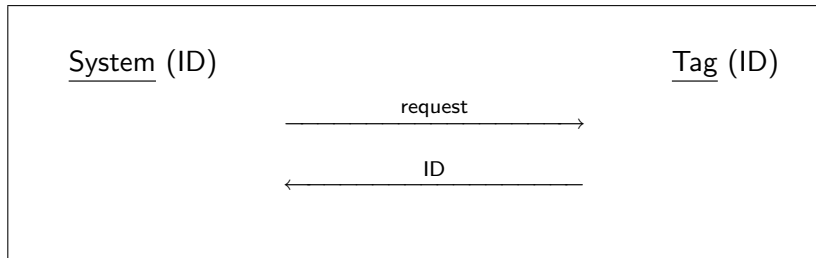
# W hat are the Security Issues?

- Denial of service
- Impersonation (only with authentication protocols)
- Leakage of information
- Traceability

## Definition (Untraceability)

Given a set of readings between tags and readers, an adversary must not be able to find any relation between any readings of a same tag or set of tags.

The (**malicious**) traceability issue must be addressed if we want a large scale diffusion of the RFID technology



Basic identification scheme

# H

## ow to Design an RFID Protocol?

How to design an RFID protocol such that only an authorized party is able to **identify** a tag while an adversary is neither able to **identify** it nor to **trace** it?

The adversary should not be able to **distinguish** the information sent by the tag from a **random value**.

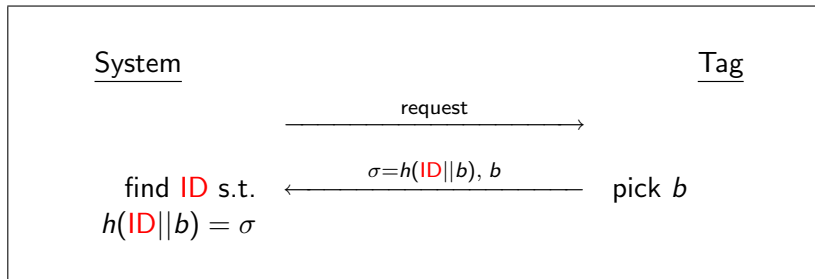
Protocols where the **reader is involved** in the refreshment of the information sent by the tag.

These protocols are only secure within a **weak adversary model**.

Protocol	Weaknesses pointed out by
[GolleJJS04]	[SaitoRS04], [Avoine05]
[SaitoRS04]	[Avoine05]
[HenriciM04]	[AvoineO05]
[Juels04]	[Juels04]
[JuelsP03]	[Avoine04], [ZhangK05]
[VadjaB03]	[VadjaB03]

Protocols where the reader is not involved, which are based on a challenge-response.

Protocol	Weaknesses pointed out by
[JuelsW05]	[GilbertRS05]
[WeisSRE02]	
[MolnarW04]	
[FeldhoferDW04]	
[RheeKKW05]	
[OhkuboSK03]	



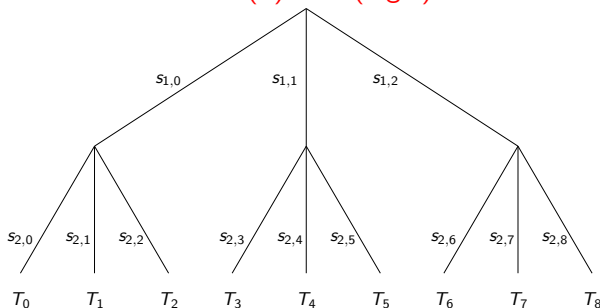
Protocol of Weis, Sarma, Rivest, and Engels  
(CHES 2002)

Challenge-response protocols are **secure** (in term of untraceability) if we deal with a pseudo-random function but suffer from a high **complexity**.

Contrary to the approach we usually take in cryptography, here the verifier **does not know the identity** of the prover before the protocol starts.

Is it possible to design an RFID protocol with a complexity **better than linear**?

[MW04] reduces the complexity of the identification of one tag  
from  $O(n)$  to  $O(\log n)$ .



$n$ : number of tags,  $\delta$ : branching factor  $\ell$  :, depth =  $\log_{\delta}(n)$

Identifying one tag requires  $\delta \log_{\delta}(n)$  operations instead of  $n$ .

**Tradeoff** between complexity and traceability.

## Conclusion

Can we design a secure RFID protocol (relying on symmetric crypto only) whose complexity to identify **one tag** is **better than linear**?

Can we design a secure RFID protocol (relying on symmetric crypto only) whose complexity to identify **the whole system** is **better than quadratic**?

More information available at

<http://lasecwww.avoine.epfl.ch/~gavoine/rfid/>