ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Radio Frequency Identification Systems in our Daily Lives

Gildas AVOINE

Mobile Information and Communication Systems, Annual Workshop

July 6-7, 2004, Zurich, Switzerland

Outline

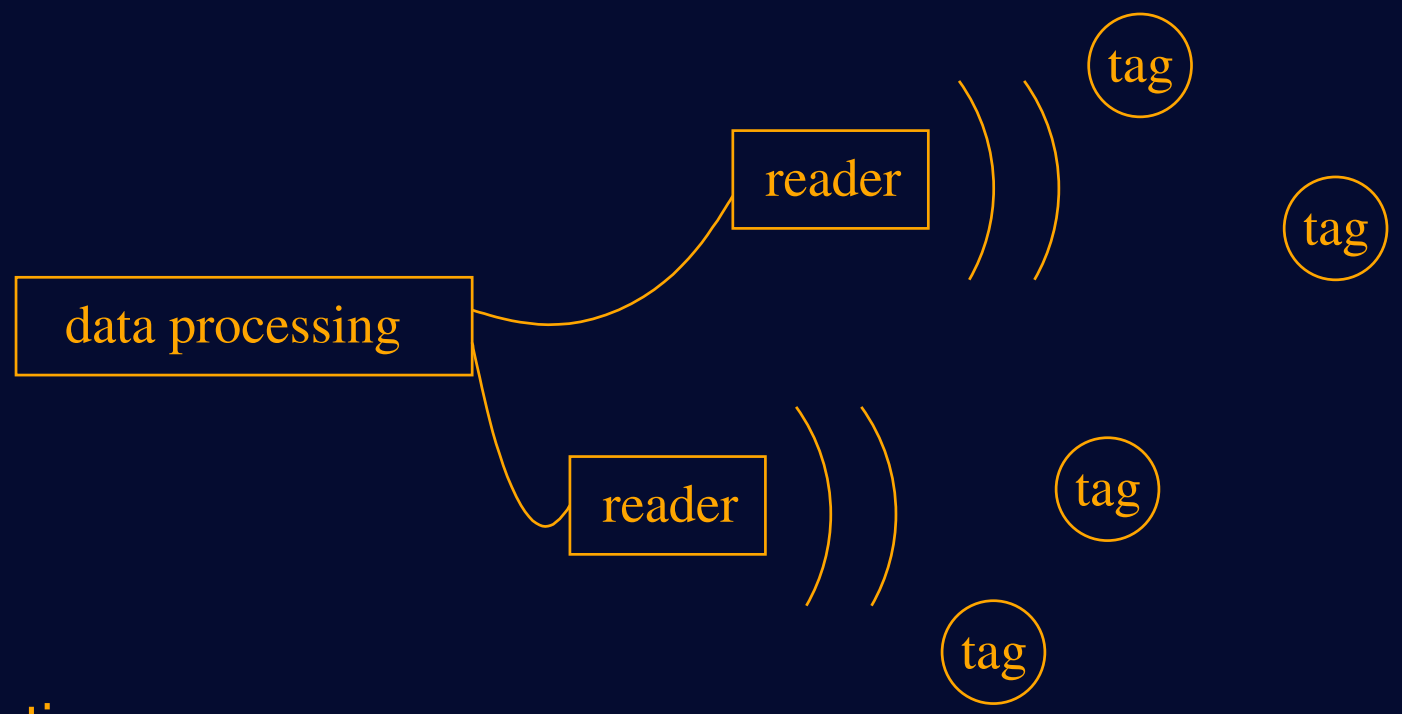
RFID Technology

Security Issues

A Practical Example of Identification Protocol

RFID Technology

RFID Systems



Interaction:

-1- The reader broadcasts a request in its communication zone.

-2- The tags send back their answers.

-3- The answers are sent to the data processing subsystem.

The Explosion of the RFID Technology

Is the RFID technology new?

The Explosion of the RFID Technology

Is the RFID technology new?

No ! i.e., contactless smartcards were already RFID devices.

The Explosion of the RFID Technology

Is the RFID technology new?

No ! i.e., contactless smartcards were already RFID devices.

What is new?

The Explosion of the RFID Technology

Is the RFID technology new?

No ! i.e., contactless smartcards were already RFID devices.

What is new?

The Auto-ID center has been created in 1999 at the MIT in order to promote and establish standards on the small and cheap RFID technology.

RFID Characteristics

RFID Characteristics

- Very low cost

RFID Characteristics

- Very low cost
- Small size

RFID Characteristics

- Very low cost
- Small size

Hitachi's μ-tag
(0.4mm$\times$ 0.4mm$\times$ 60 microns)

RFID Characteristics

- Very low cost
- Small size

RFID Characteristics

- Very low cost
- Small size
- Storage and computation capabilities are extremely limited

RFID Characteristics

- Very low cost
- Small size
- Storage and computation capabilities are extremely limited

No processor

Memory: A few hundred bits (ROM or EEPROM)
Typically between 64 and 128 bits in ROM

RFID Characteristics

- Very low cost
- Small size
- Storage and computation capabilities are extremely limited
- Not tamper-resistant

RFID Characteristics

- Very low cost
- Small size
- Storage and computation capabilities are extremely limited
- Not tamper-resistant
- No battery

RFID Characteristics

- Very low cost
- Small size
- Storage and computation capabilities are extremely limited
- Not tamper-resistant
- No battery

Energy is brought to the tag by the electric or magnetic field of the reader

RFID Characteristics

- Very low cost
- Small size
- Storage and computation capabilities are extremely limited
- Not tamper-resistant
- No battery
- Reader-to-Tag channel: up to 100 meters

RFID Characteristics

- Very low cost
- Small size
- Storage and computation capabilities are extremely limited
- Not tamper-resistant
- No battery
- Reader-to-Tag channel: up to 100 meters
- Tag-to-Reader channel: up to a few meters

RFID Characteristics

- Very low cost
- Small size
- Storage and computation capabilities are extremely limited
- Not tamper-resistant
- No battery
- Reader-to-Tag channel: up to 100 meters
- Tag-to-Reader channel: up to a few meters
- Channel between readers and tags is not secure

RFID Systems vs Bar-Code Systems

The goal of the RFID tags is to identify objects in open environments, as done by the bar-codes. They should replace the latter in the near future.

RFID tags and bar-codes differ from several points:

- A tag can be remotely read without optical access to the item holder.
- Several tags can be read at the same time.
- While a bar-code represents a lot of items, a RFID tag has its own identifier (therefore an item has a unique identifier).

Targeted Applications

- Speed up the checkouts in the shops
- Management of stocks and stocktakings
- Renting (e.g. libraries)
- Recycling
- Pets identification
- Carriage of small amount of data
- Anti-counterfeiting
- Sensor networks

Every-Day Life Examples

Every-Day Life Examples

- Wal-Mart announced that it wants their suppliers to embed RFID tags in products at the pallet/carton level.

Every-Day Life Examples

- Wal-Mart announced that it wants their suppliers to embed RFID tags in products at the pallet/carton level.

- Michelin has decided to implant RFID tags inside the rubber sidewall of its tires. These tags aim at pinpointing tires belonging to a defective batch. The ultimate goal is to join some pressure sensors to the tags.

Every-Day Life Examples

- Wal-Mart announced that it wants their suppliers to embed RFID tags in products at the pallet/carton level.

- Michelin has decided to implant RFID tags inside the rubber sidewall of its tires. These tags aim at pinpointing tires belonging to a defective batch. The ultimate goal is to join some pressure sensors to the tags.

- Gillette razors are one of the most shoplifted items in the world.

Every-Day Life Examples

- Wal-Mart announced that it wants their suppliers to embed RFID tags in products at the pallet/carton level.
- Michelin has decided to implant RFID tags inside the rubber sidewall of its tires. These tags aim at pinpointing tires belonging to a defective batch. The ultimate goal is to join some pressure sensors to the tags.
- Gillette razors are one of the most shoplifted items in the world.
- Benetton planned to fit clothing with RFID tags, but it gives up this project.

Security Issues

Threats

Threats

Threats on the tag's bearers

(privacy)

Threats

Threats on the tag's bearers
(privacy)

Threats on the system
(denial of service attacks, tag forgery, ...)

Threats

Threats on the tag's bearers
(privacy)

Threats on the system
(denial of service attacks, tag forgery, ...)

Privacy

Privacy

Information leakage

Traceability

Information leakage: The tag gives some information related to the object holder.

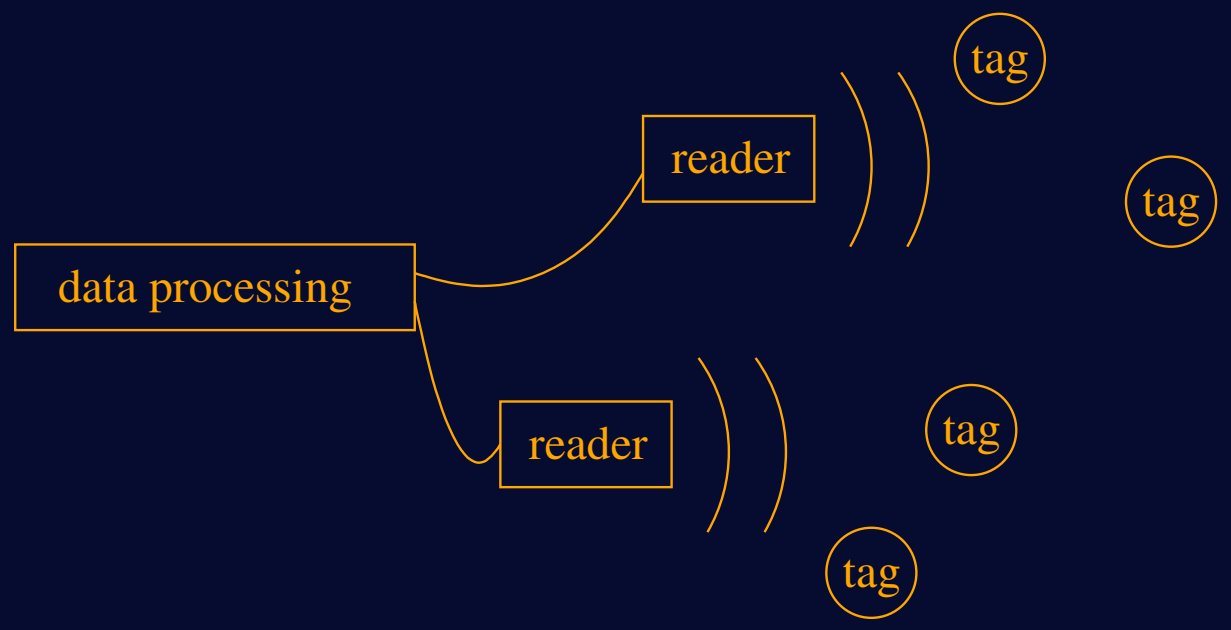
Traceability: Thanks to the tag's identifier, an adversary is able to track the tag, and therefore its bearer.

Information Leakage (Solution)

A solution consists in using identifiers chosen randomly: the tag's identifier contains no useful data for an adversary; only the data processing manager can match the identifier with the corresponding item.

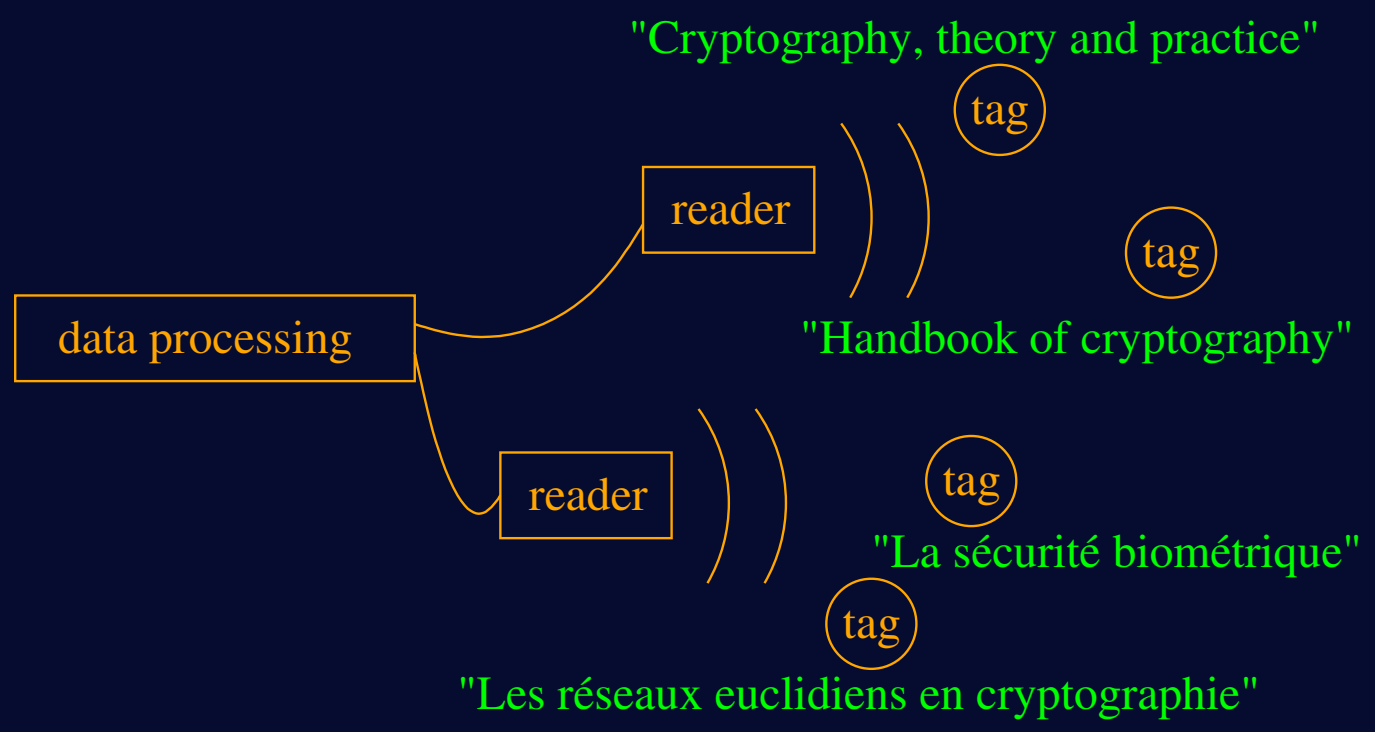
Information Leakage (Solution)

A solution consists in using identifiers chosen randomly: the tag's identifier contains no useful data for an adversary; only the data processing manager can match the identifier with the corresponding item.



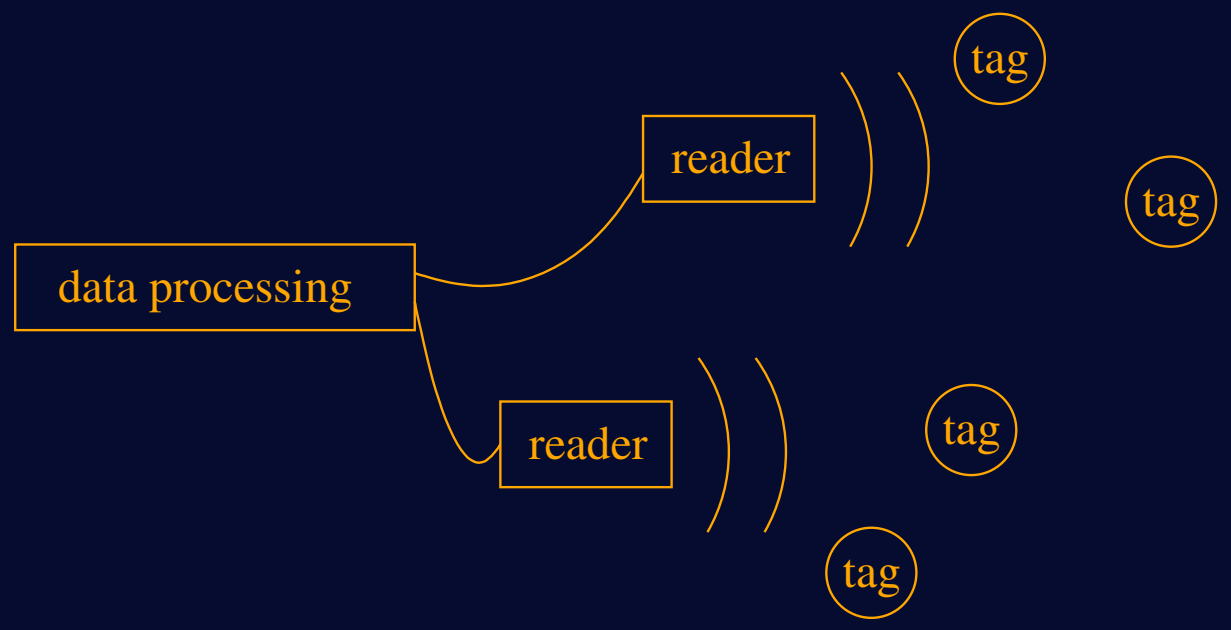
Information Leakage (Solution)

A solution consists in using identifiers chosen randomly: the tag's identifier contains no useful data for an adversary; only the data processing manager can match the identifier with the corresponding item.



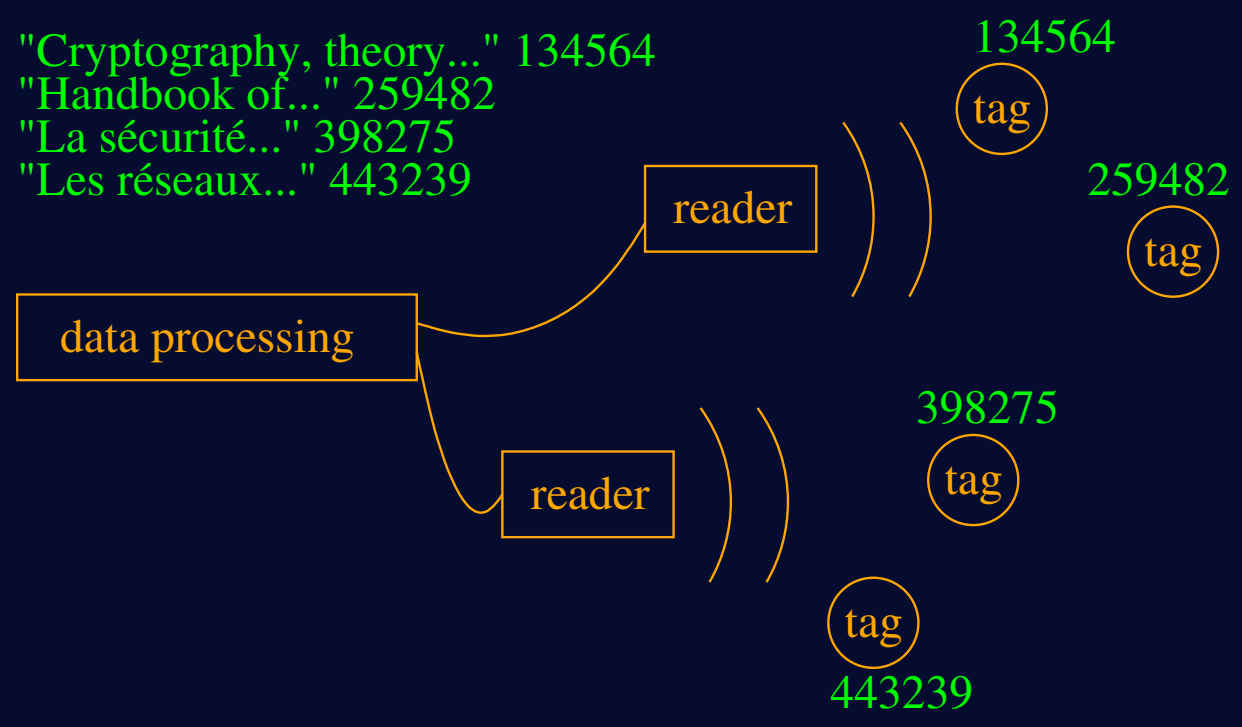
Information Leakage (Solution)

A solution consists in using identifiers chosen randomly: the tag's identifier contains no useful data for an adversary; only the data processing manager can match the identifier with the corresponding item.



Information Leakage (Solution)

A solution consists in using identifiers chosen randomly: the tag's identifier contains no useful data for an adversary; only the data processing manager can match the identifier with the corresponding item.



Traceability (Solutions)

Traceability (Solutions)

- Killing the Tags

Traceability (Solutions)

- Killing the Tags : The tag is deactivated (or physically destroyed) when the customer pays for an item. Efficient and straightforward, but:

1. Suitable for some specific applications only
2. Loss of functionalities (the tag is not usable anymore)
3. Doubt kept in mind (Are tags really invalid?)
4. DoS attacks (the kill key is usually too short)

Traceability (Solutions)

- Killing the Tags

Traceability (Solutions)

- Killing the Tags

- Interfering the request/answer

Traceability (Solutions)

- Killing the Tags

- Interfering the request/answer : This can use physical phenomena (e.g. Faraday cage) or electronic devices (e.g. blocker tag), but:

  1. Not always possible
  2. The tag has to stay in the device electronic field
  3. Electronic pollution

Traceability (Solutions)

- Killing the Tags

- Interfering the request/answer

Traceability (Solutions)

- Killing the Tags
- Interfering the request/answer
- Answering to authorized readers Only

Traceability (Solutions)

- Killing the Tags

- Interfering the request/answer

- Answering to authorized readers Only : No such a (secure) protocol exists yet.

Traceability (Solutions)

- Killing the Tags
- Interfering the request/answer
- Answering to authorized readers Only

Traceability (Solutions)

- Killing the Tags
- Interfering the request/answer
- Answering to authorized readers Only
- Refreshing the tag's identifier

Traceability (Solutions)

- Killing the Tags

- Interfering the request/answer

- Answering to authorized readers Only

- Refreshing the tag's identifier : The tag's identifier is modified each time the tag is queried by a reader. Several schemes exist: Juels/Pappu, Ohkubo/Suzuki/Kinoshita, Henrici/Müller, ...

Traceability (Solutions)

- Killing the Tags

- Interfering the request/answer

- Answering to authorized readers Only

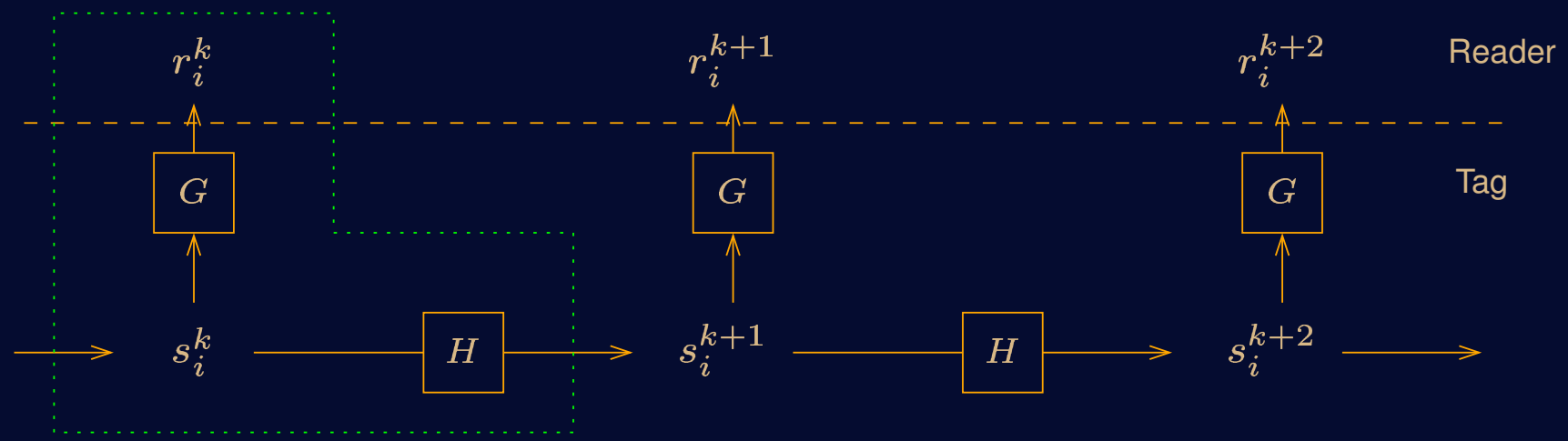
- Refreshing the tag's identifier : The tag's identifier is modified each time the tag is queried by a reader. Several schemes exist: Juels/Pappu, Ohkubo/Suzuki/Kinoshita, Henrici/Müller, ...

A Practical Example of Identification Protocol

Ohkubo, Suzuki, and Kinoshita

Initially, the tag T_i has the identity s_i^1, also known by the database.

The tag refreshes itself its current identifier using a hash function.



Ohkubo, Suzuki, and Kinoshita (Cont.)

Receiving r_i^k, the database has to identify the corresponding tag. For that, it constructs the hash chains from the initial values it stores, until it finds (i', k') such that $\boxed{r_i^k = G(s_{i'}^{k'})}$.

$$\begin{array}{ccccc} s_1^1 & s_1^2 & s_1^3 & \dots & s_1^m \\ s_2^1 & \dots & & \dots & s_2^m \\ \vdots & & & & \vdots \\ s_n^1 & \dots & & \dots & s_n^m \end{array}$$

where

$$s_i^k = H^{k-1}(s_i^1)$$

Ohkubo, Suzuki, and Kinoshita (Cont.)

This scheme suffers from several drawbacks:

- Putting a hash function into the tags is not possible yet (but could become possible in the near future)
- The protocol implies a high complexity on the data processing hand.
- The singulation protocol is supposed to be atomic.

Singulation protocol

The singulation protocol is used to identify several tags at the same time in order to avoid collisions.

The most used singulation protocol is a tree-walking-based algorithm, but such an algorithm, which is based on the identifier of the tag, needs several requests to identify the tags.

Conclusion

Work carried out and future work

- Three existing protocols have been studied until now (Juels/Pappu, Ohkubo/Suzuki/Kinoshita, Henrici/Müller). Each of them suffers from some flows.
- Developing a "theory of the privacy" in the RFID model. Generalization to ad hoc networks.
- Designing an identification protocol preserving the privacy of the tags's bearer. This cannot be done without considering the singulation subproblem.