Soutenance Publique de Thèse de Doctorat

Cryptography in Radio Frequency Identification and Fair Exchange Protocols

Gildas Avoine

EPFL, Lausanne, Switzerland

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Summary of my Work

- Fair Exchange

  AV03a, AV03b, AV04, AGGV05, Avo03.

- Radio Frequency Identification

  Avo04, ADO05, AO05a, AO05b, CA06, AB06.

- Odds and Ends

  Avo05, AMP04, AJO05, AJ03, VAJ03, AJO05.

Outline of the Presentation

RFID PRIMER

IMPERSONATION OF TAGS

INFORMATION LEAKAGE

MALICIOUS TRACEABILITY

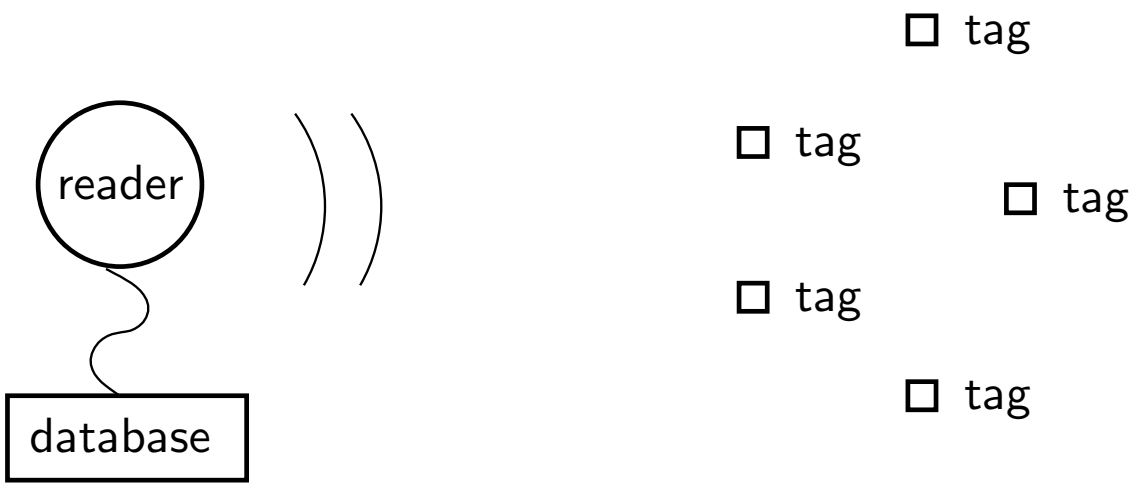
TRACEABILITY THROUGHT THE COMMUNICATION LAYERS

RFID PRIMER

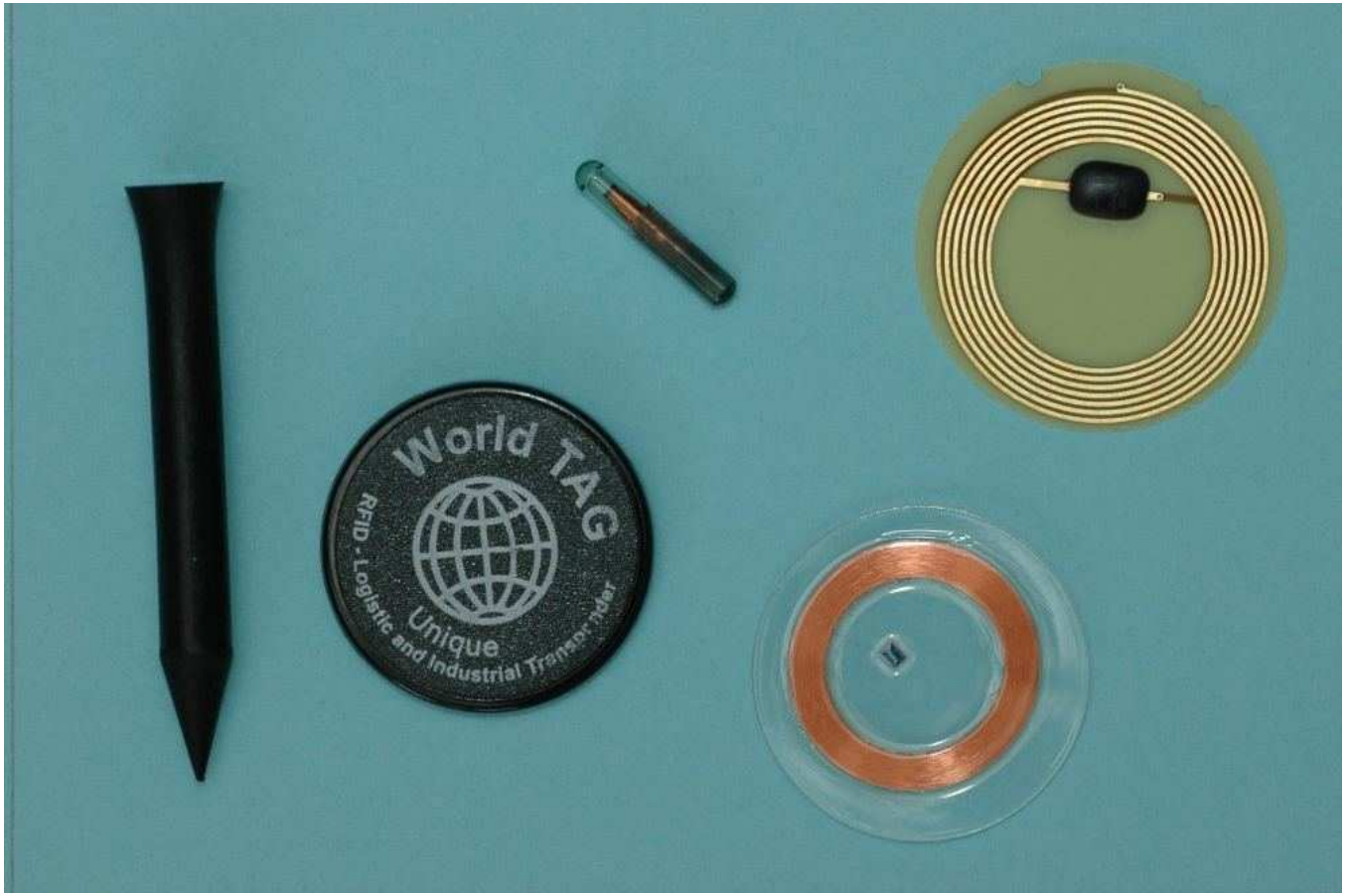
RFID Definition and Architecture

Definition RFID

Radio Frequency IDentification (RFID) is a method of remotely identifying objects or subjects using transponders (tags) queried through a radio frequency channel.

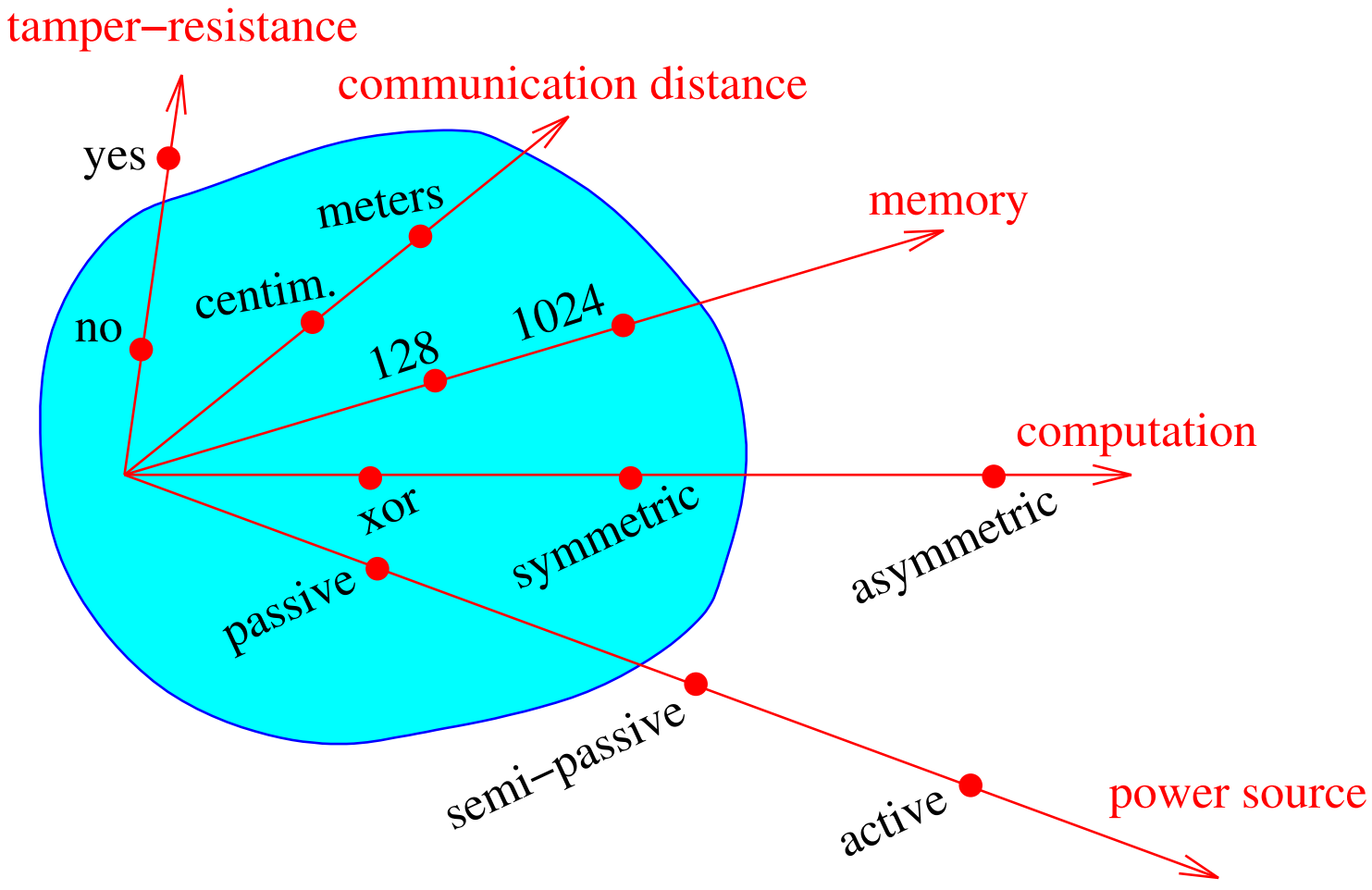


RFID Tags


World TAG
Unique
RFID - Logistic and Industrial Transponder

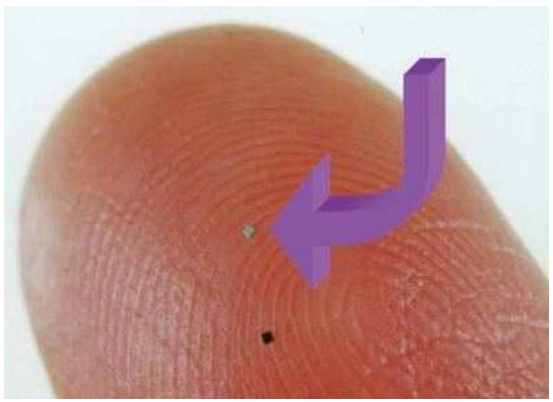
RFID Readers

Tag Characteristics



Tag Specificities

- Tags cannot be switched-off
- Tags answer without the agreement of their bearers
- Increasing of the communication range
- Tags can be almost invisible



Daily Life Examples

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

Security Threat Classification

- Denial of service
- Impersonation
- Information Leakage
- Malicious traceability

IMPERSONATION OF TAGS

Problem and Adversary Means

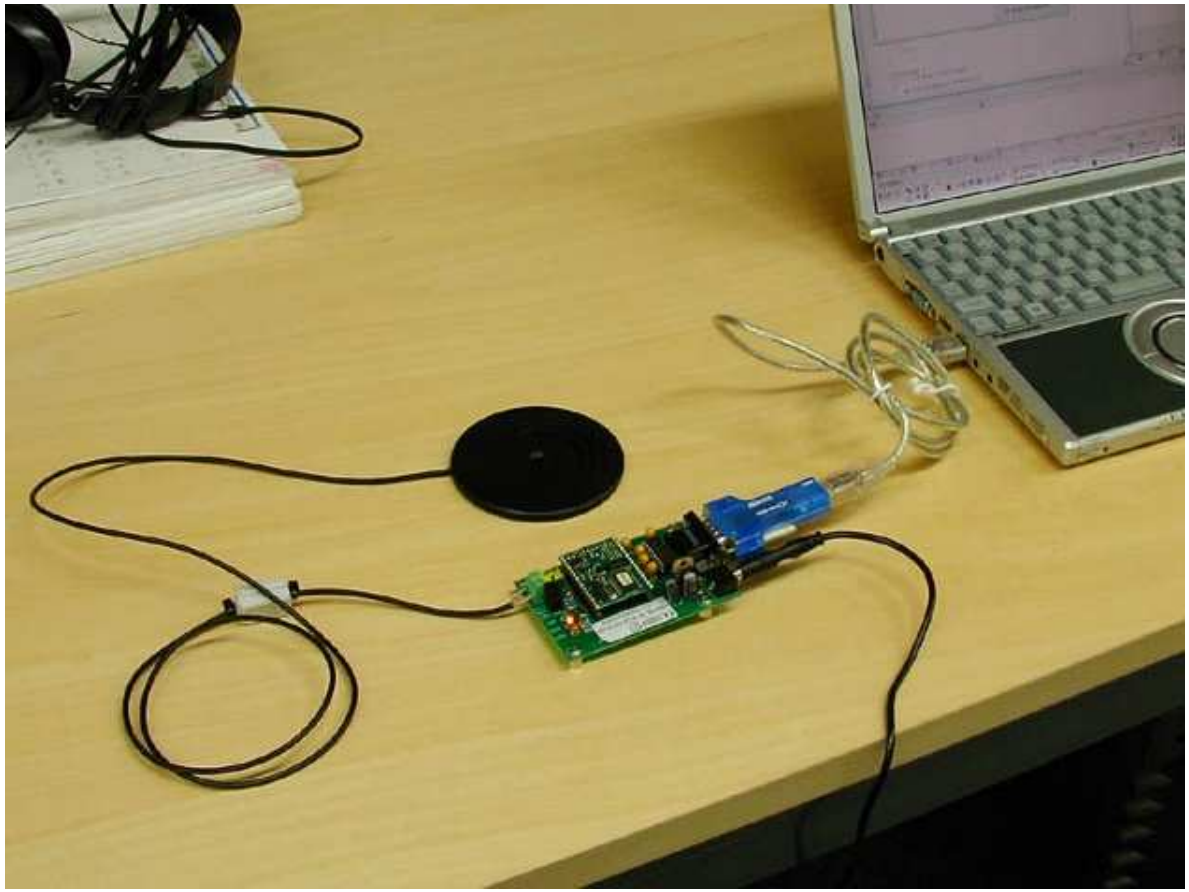
Problem

An adversary should not be able to impersonate a tag.

Adversary Means

The adversary can query the targetted tag or eavesdrop (RFID) communications between the tag and readers. Then the adversary tries to simulate the tag in front of a legitimate reader.

Tag Simulator



Identification vs Authentication

Primal goal of RFID is to provide security.

Definition — **Authentication**

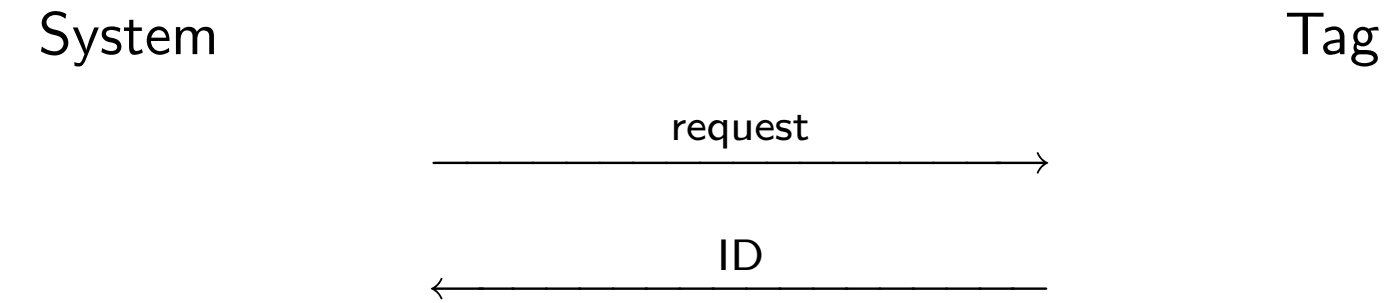
The authentication consists for the reader in obtaining the identity of the tag and a proof that the claimed identity is correct.

Primal goal of RFID is to provide functionality.

Definition — **Identification**

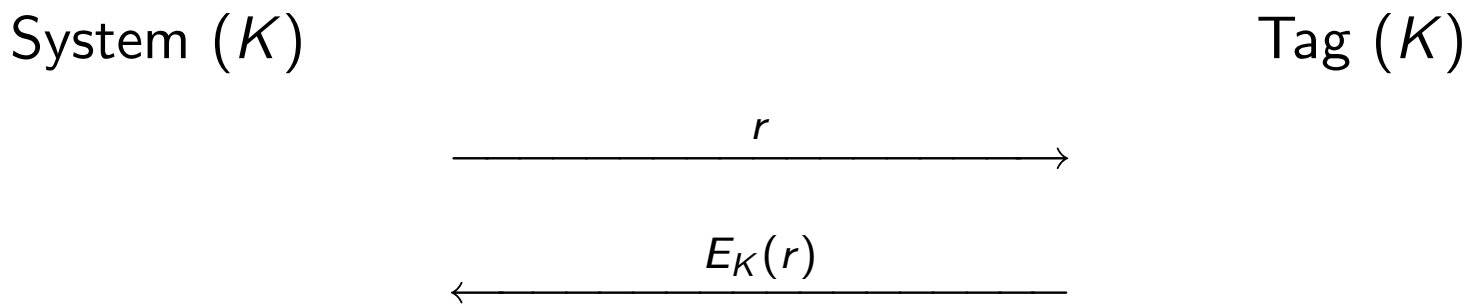
The identification consists for the reader in obtaining the identity of the tag, but no proof is required.

Identification Protocol



Examples: Counting cattle, localization, stock management.

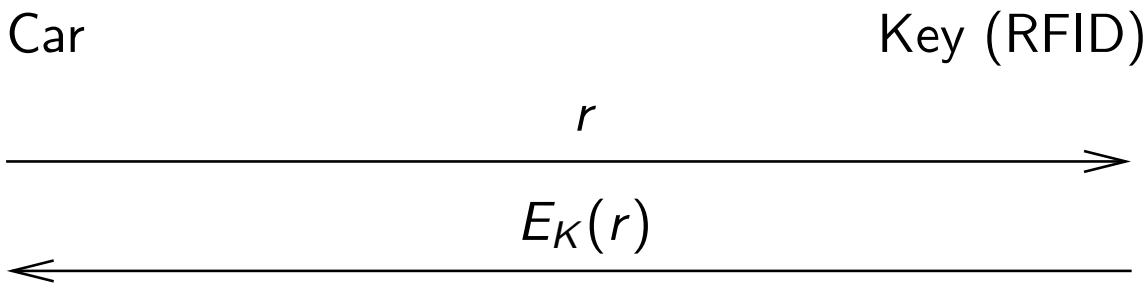
Authentication Protocol



Examples: Access control, e-documents, anti-counterfeiting.

Impersonation (Example: Texas Instrument DST Module)

- Attack of Bono *et al.* on the Digital Signature Transponder manufactured by TI, used in automobile ignition key.

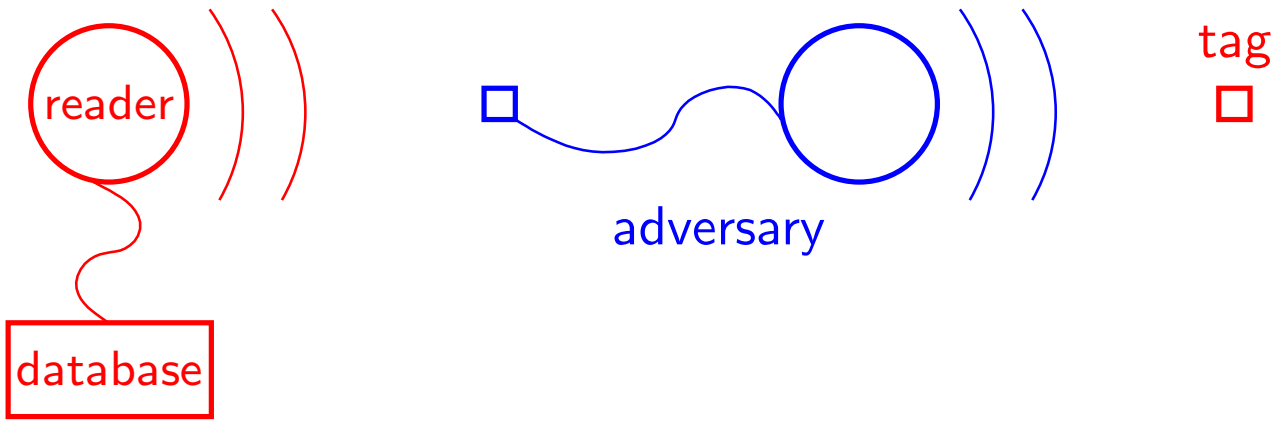


- Recovering the 40-bit key requires less than 1 minute using a time-memory trade-off.

Recovering the cryptographic key / Impersonating the ignition key / Impersonating the SpeedPass card

Impersonation (Example: Relay Attack)

- The reader believes the tag is within its electromagnetic field.
- The attacker behaves as an extension cord.



- The solution consists in using a distance bounding protocol.

INFORMATION LEAKAGE

Problem and Adversary Means

Problem

An adversary should not be able to obtain useful information about the tagged object.

Adversary Means

The adversary can query the targetted tag or eavesdrop (RFID) communications between the tag and readers.

Information Leakage Problem

- Tagged books in libraries
- Tagged pharmaceutical products
- Electronic documents like passports, ID cards, etc.

MALICIOUS TRACEABILITY

Problem and Adversary means

Problem

An adversary should not be able to track people thanks to the RFID tags they carry.

Adversary Means

The adversary can query the targetted tag and eavesdrop (RFID) communications between his target and readers.

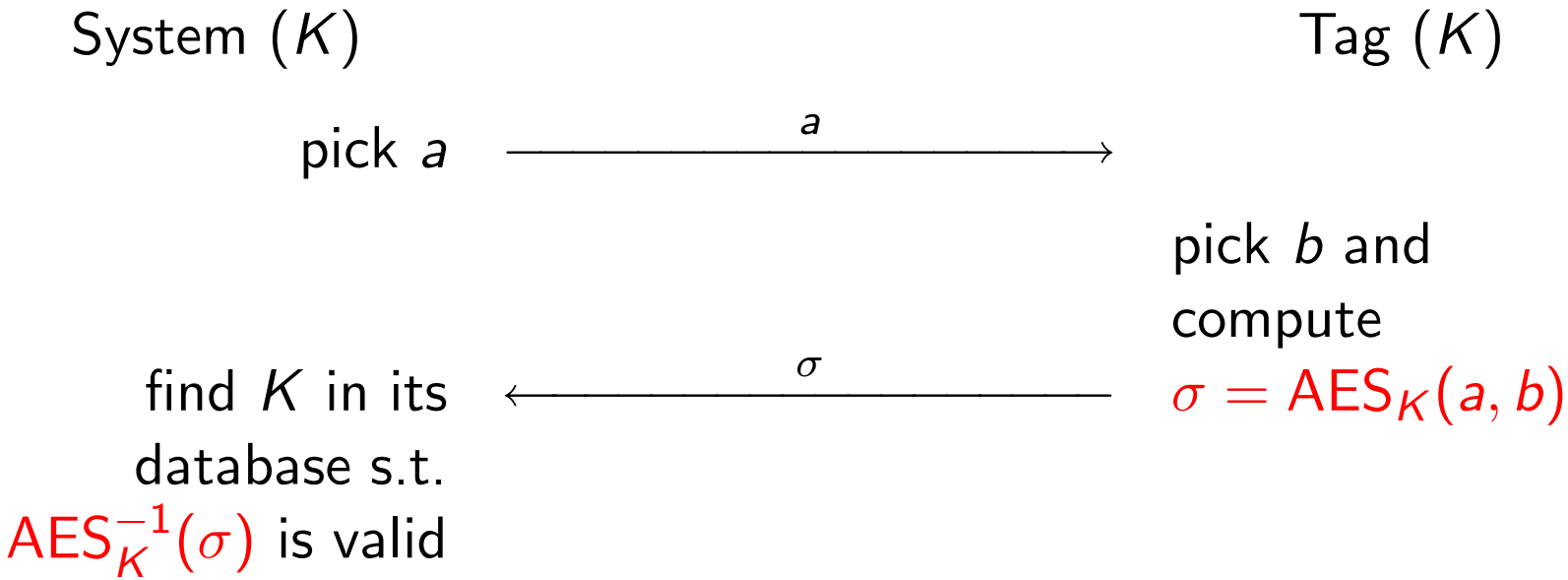
Avoiding Malicious Traceability

- The information sent back by the tag must be indistinguishable (by an adversary) from a random value.
- The information must be refreshed at each new identification.

Protocols

Protocol	Weaknesses pointed out by
[JuelsP03]	[Avoine04], [ZhangK05]
[VadjaB03]	[VadjaB03]
[GolleJJS04]	[Avoine05], [SaitoRS04]
[Juels04]	[Juels04]
[HenriciM04]	[AvoineO05]
[SaitoRS04]	[Avoine05]
[JuelsW05]	[GilbertRS05]
[WeisSRE02]	
[OhkuboSK03]	
[FeldhoferDW04]	
[MolnarW04]	
[RheeKKW05]	

Feldhofer, Dominikus, and Wolkerstorfer's Protocol

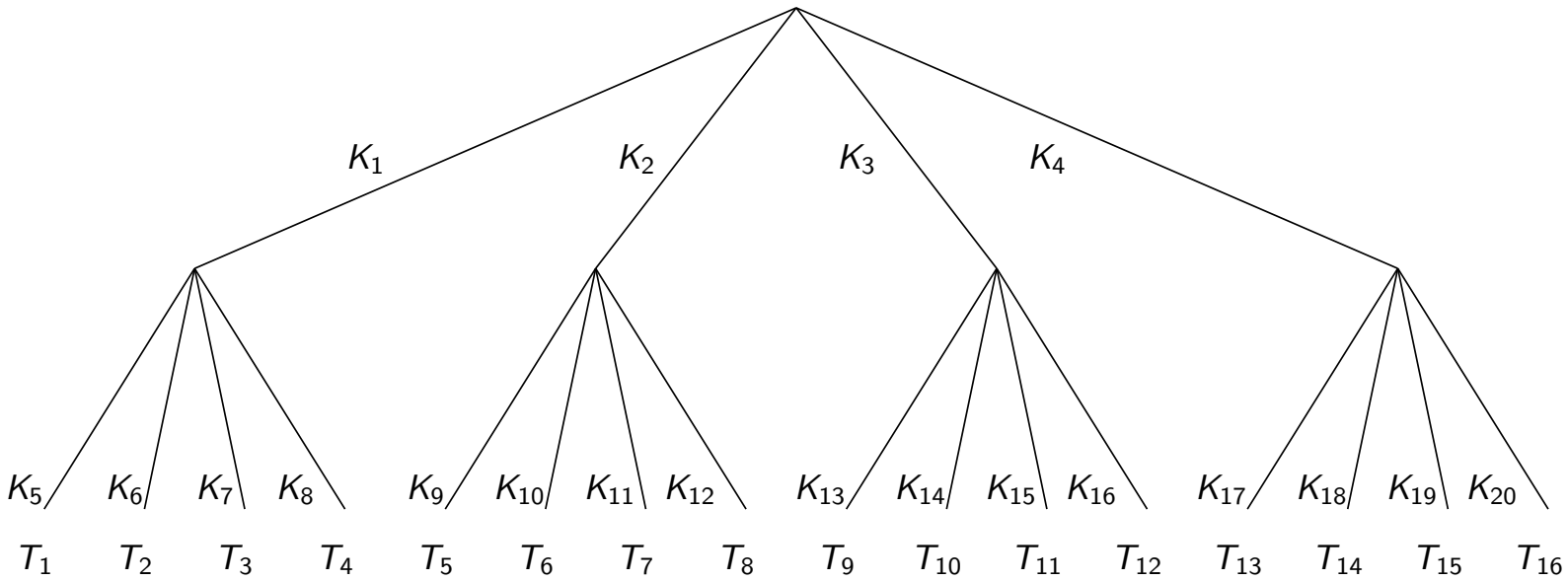


Computation Complexity of Challenge-Response Protocols

- An exhaustive search in the system's database is required to identify one tag.
- Complexity too high in particular in case of inventory.
- Is it possible to design an RFID protocol with a complexity better than linear?
- Molnar and Wagner proposed a solution that reduces the complexity of any challenge-response from $O(n)$ to $O(\log n)$.

Molnar and Wagner's Tree-Based Technique

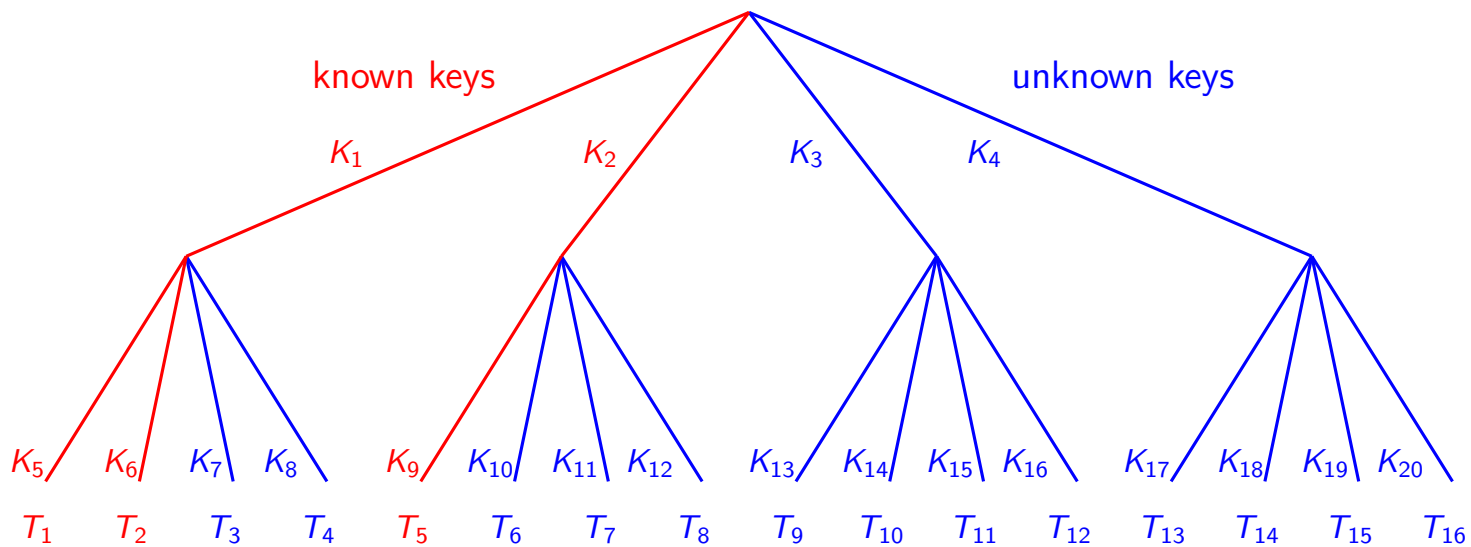
- Each tag stores $\log_\delta(n)$ keys.



- A challenge-response is applied at each level of the tree.
- Instead of carrying out 1 exhaustive search in a set of size n, $\log_\delta(n)$ exhaustive searches are performed in sets of size δ.

Drawbacks

- Tags share some keys.
- Tampering with tags gives information about the other tags.

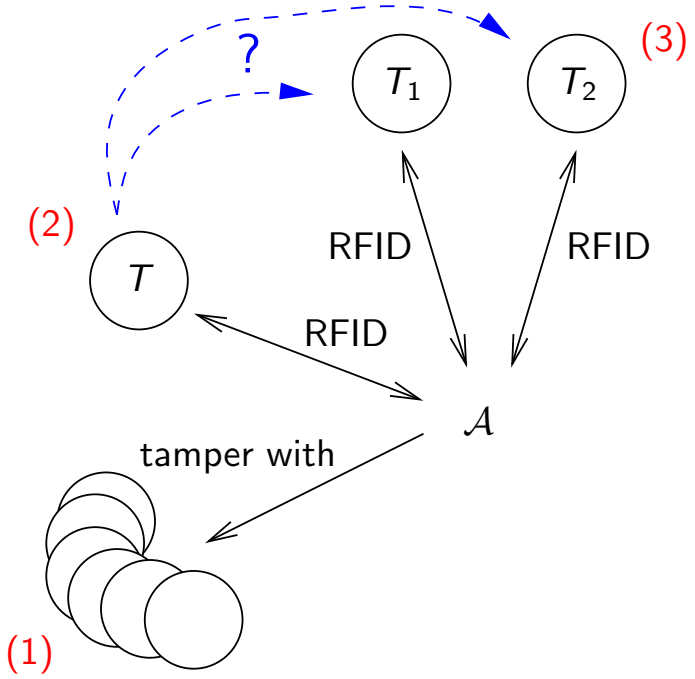


How to Trace a Tag

(1) Tamper with k tags.

(2) Choose any target T and query it at will.

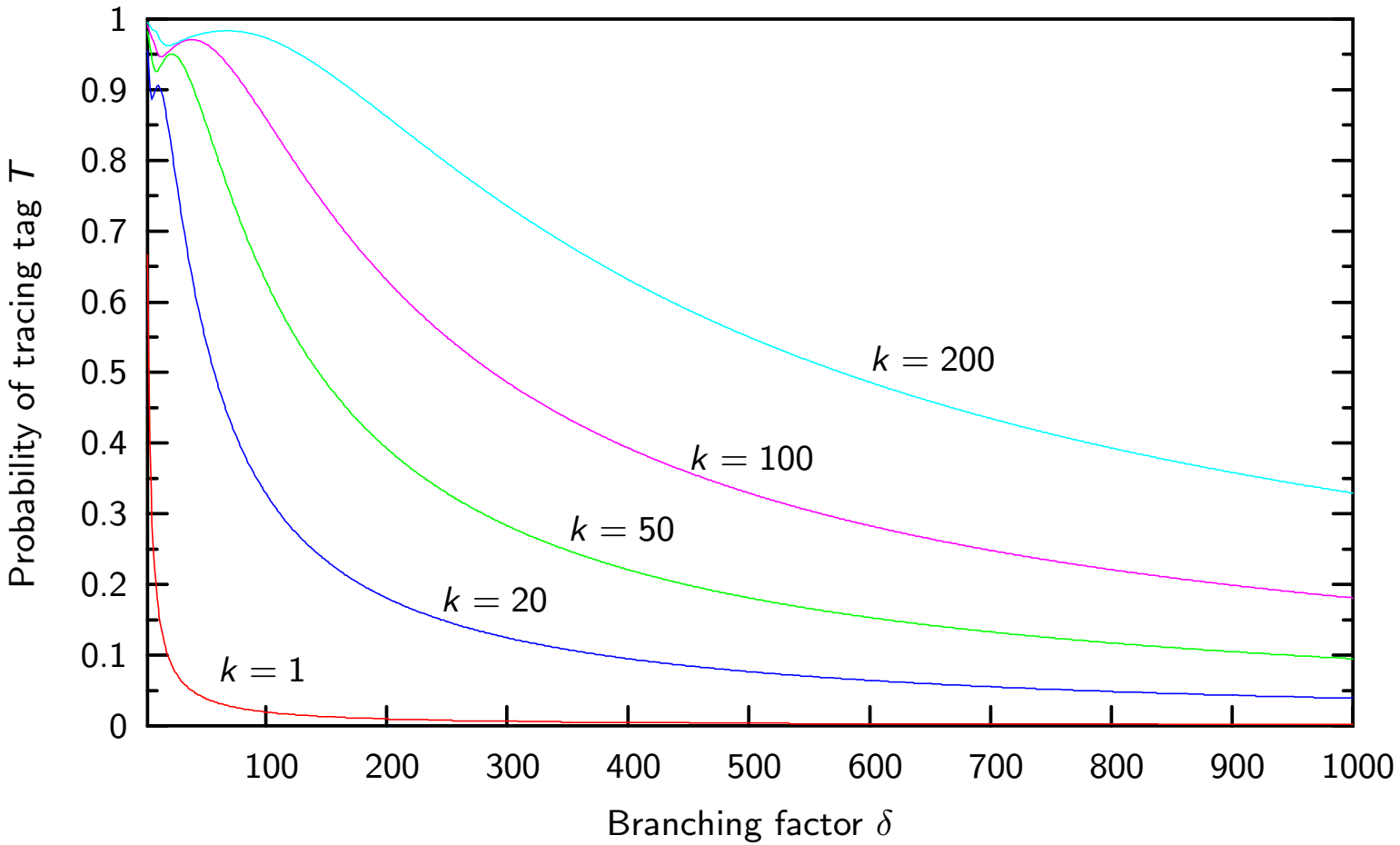
(3) Query T_1 and T_2 to determine which of the two is T.



Five Cases to Analyze

- T_1 on known branch and T_2 on unknown branch: success.
- T_2 on known branch and T_1 on unknown branch: success.
- T_1 and T_2 both on known but different branches: success.
- T_1 and T_2 both on unknown: failure.
- T_1 and T_2 both the same known branch: failure at level i but the attack moves on to level $i + 1$.

Probability of Success



Using a Time-Memory Trade-Off

- Time complexity can be reduced against a memory cost.
- [AO05] as efficient as [MW04].
- [AO05] does not degrade security.

TRACEABILITY THROUGHT THE COMMUNICATION LAYERS

Problem and Adversary Means

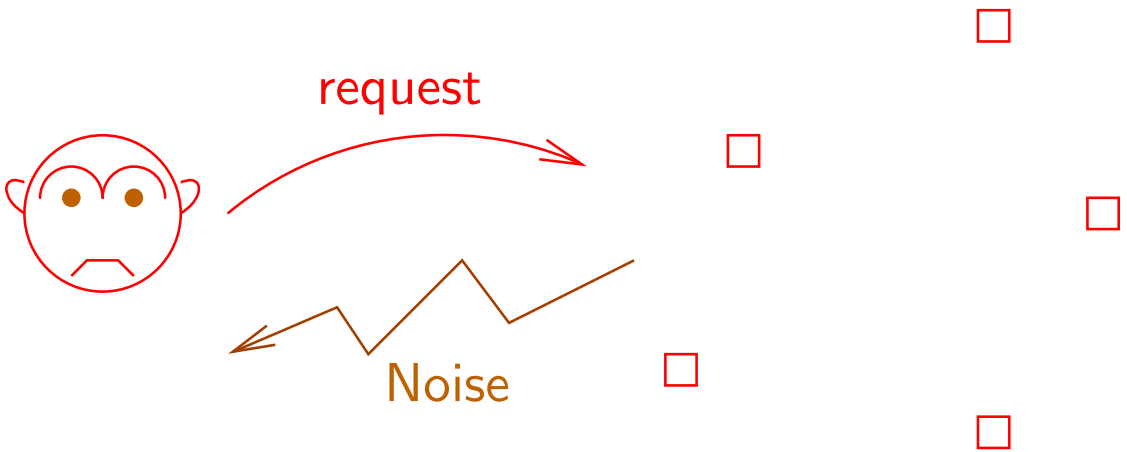
Problem

An adversary should not be able to track people thanks to the RFID tags they carry.

Adversary Means

The adversary takes benefit of a side channel instead of using the RFID protocol. This side channel can be in any layer of the communication model.

Malicious Traceability in the Communication Layer



Collision-Avoidance Protocols (Example: Slotted Aloha)

- The access to the communication channel is split into time slots.
- The number of slots is chosen by the reader which informs the tags they will have n slots to answer.
- Each tag randomly chooses one slot among the n and replies to the reader when its slot arrives.
- If n is not sufficiently large, then some collisions occur.
- Example: Philips ICode1 Label.

CONCLUSION

Conclusion

- Will low cost RFID become an ubiquitous technology?
- Is malicious traceability a problem?
- Is it too late to deal with this problem?
- Are there existing solutions?
- Shall we have a drink after the presentation?