RFID and ticketing application

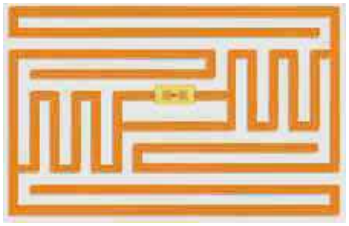
Who? Cédric Lauradoux
EPL/INGI/GSI

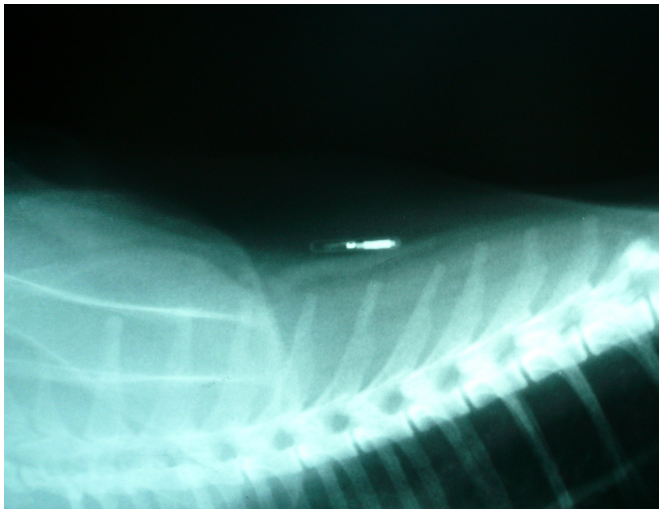
When? January 22, 2009

Outline

- RFID primer
  - Technology
  - Information leakage
  - Malicious tracability
  - Denial of service
  - Relay attacks
- Ticketing primer
  - Problem
  - Attacks
- when RFID meet ticketing...

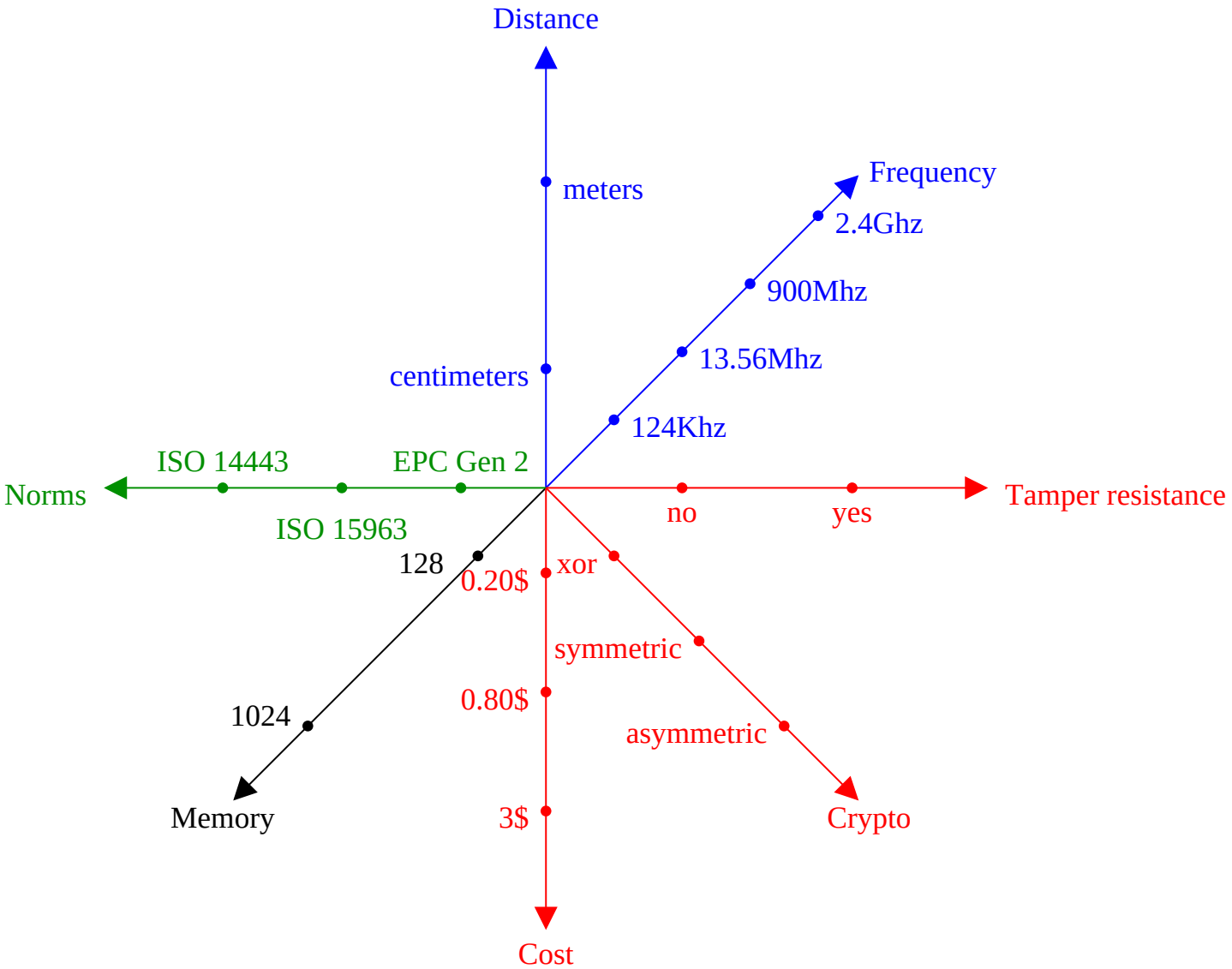
Radio Frequency IDentification





Radio Frequency IDentification

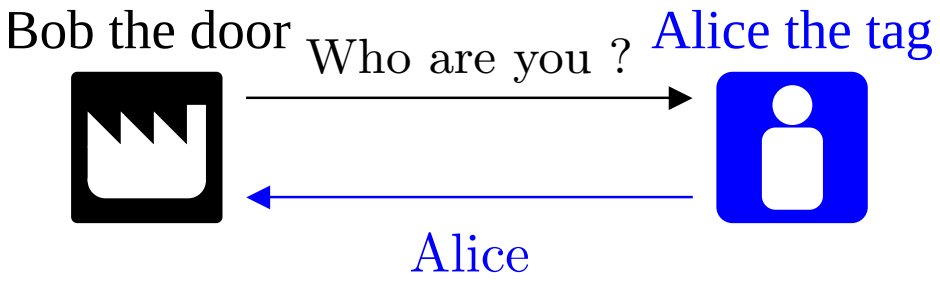
The big Napoleon



Radio Frequency IDentification

Identification

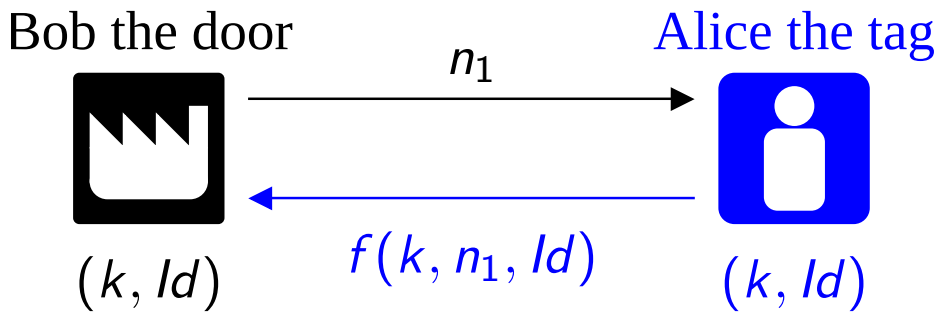
Definition The result of an identification protocol is the identity claimed by the queried RFID tag.



Radio Frequency IDentification

Authentification

Definition The result of an authentification protocol is the genuine identity of a(the) participant(s).



In brief:

$$\text{Authentification} = \text{Identity} + \text{Proof}.$$

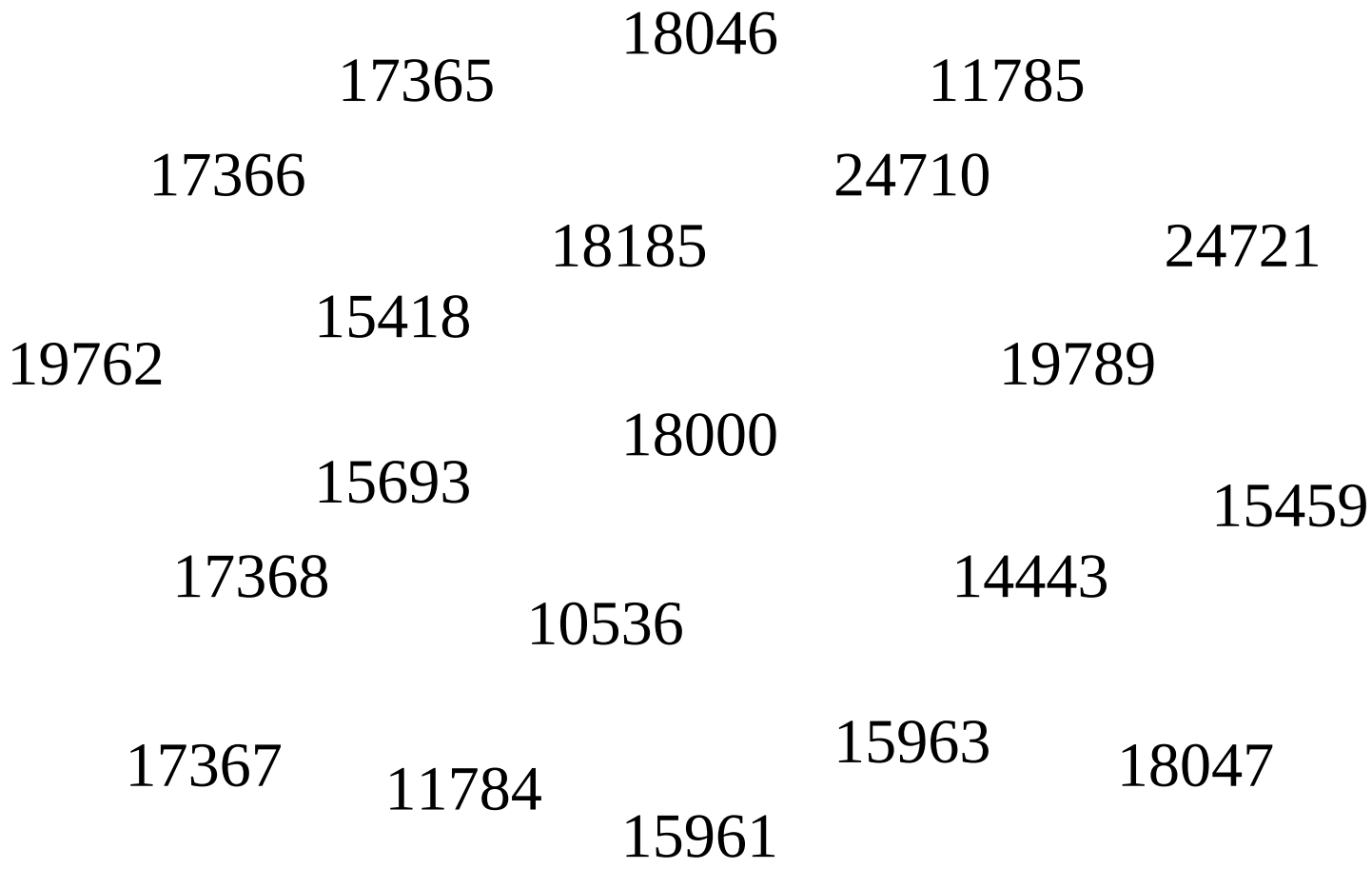
Frequency band

- 125–134 kHz (LF): Pet identification, livestock tracking...
- 13.553–13.567 MHz (HF): Smartcards, libraries...
- 860–960 MHz (UHF): Supply chain tracking...
- 2.4000–2.4835 GHz (UHF): Highway toll, vehicle fleet...

Norms

lost in translation ??

ISO Identification protocols:



Radio Frequency IDentification

Beijing Olympic Games

First event of this scale to use RFID:

- 16 millions RFID tags used (2^{24})

Tags usage:

- ticket anti-counterfeiting system
- food production and delivery monitoring
- subway and hotels access control

Next event, the Universal Exhibition (Shanghai 2010):

- 70 millions tickets (2^{26})

Radio Frequency IDentification

Beijing Olympic Games

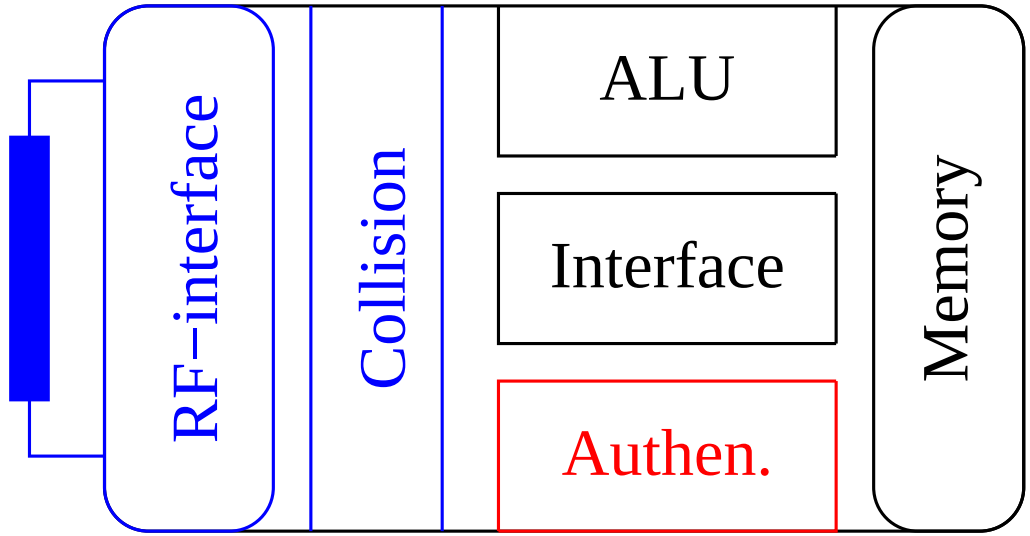
Tag technology:

- 13.56 Mhz range 1-10cm;
- ISO 14443B;
- No cryptographic capabilities;
- TMC products THR1064.

Reader technology:

- CPLD centric (reconfigurable);
- Software Defined Radio;
- PDA interface.

Tag



RFID and security

- Information leakage

  Okay, you got us. . . crypto what ?

- Malicious tracability

  We don't care !

- Relay attacks

  What the hell is that ?

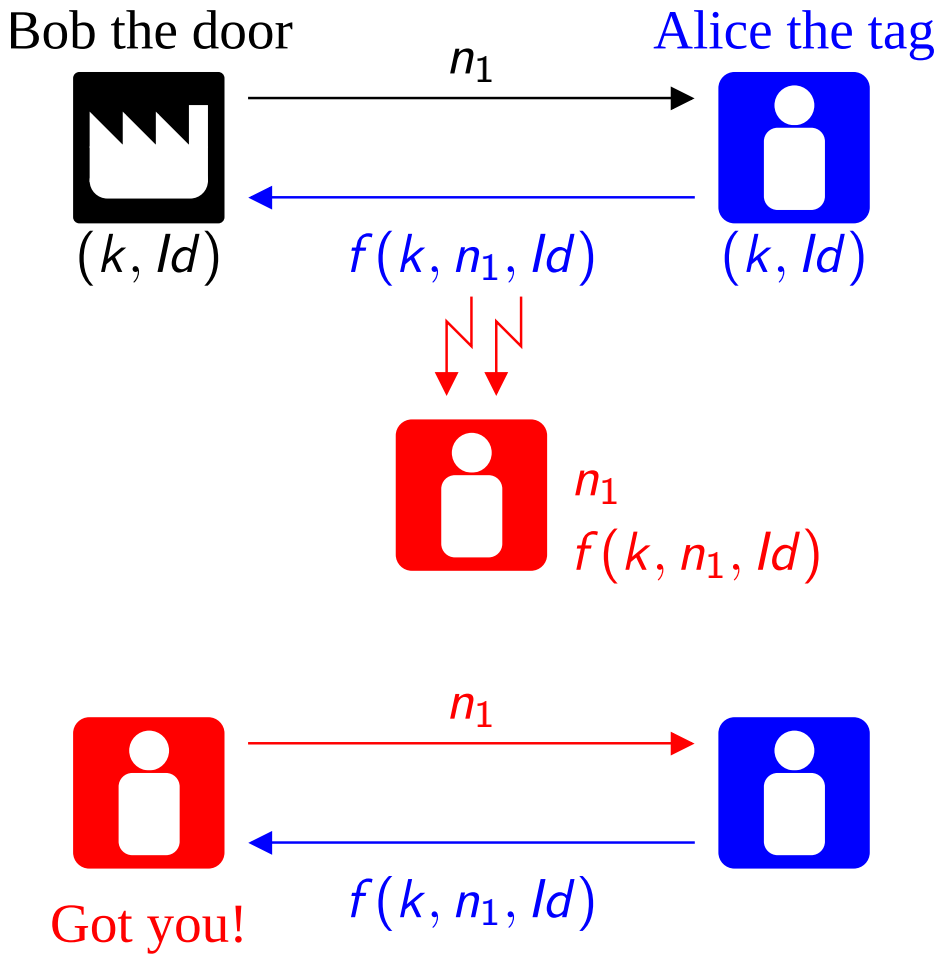
- Denial of service

  . . . . . ?

Definition

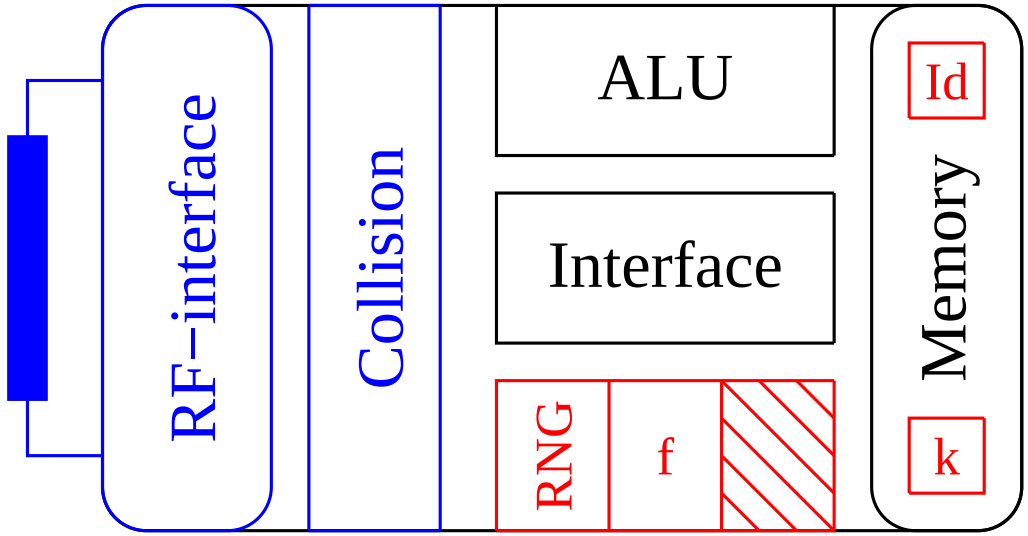
Malicious traceability

An adversary should not be able to track the tag holder: impossibility to correlate the tag interactions with the context of the usage.



Malicious traceability

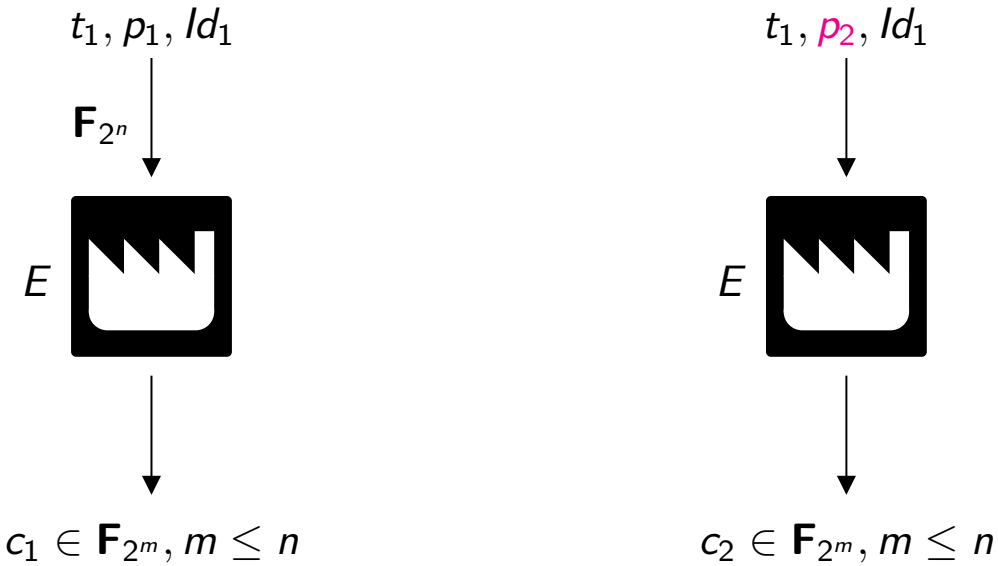
Tag architecture



Malicious traceability

Malicious traceability

Data analysis in forensic



Choices for E:

- plaintext, transposition — differential analysis
- adaptative compression — ??
- strict avalanche criteria functions — ??
- cryptography — side-channel attacks

Tonight word:

Definition

Anonymity – [...] the term typically refers to a person, and often means that the personal identity, or personally identifiable information of that person is not known.
More strictly, and in reference to an arbitrary element [...], within a well-defined set (called the "anonymity set"), "anonymity" of that element refers to the property of that element of not being identifiable within this set. If it is not identifiable, then the element is said to be "anonymous".
WIKIPEDIA

Definition

Anonymity – we don't put your data into the database.
STIB, RATP...

Relay attacks

Chess player problem

1. d4

1. .. Cf6

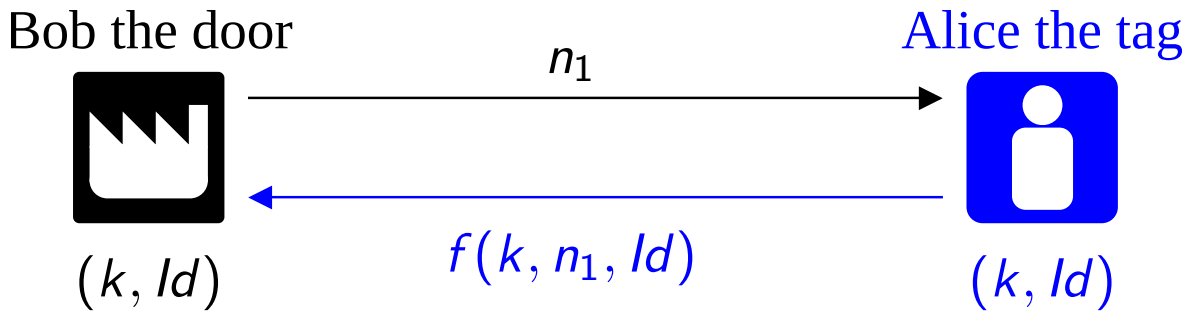
1. d4

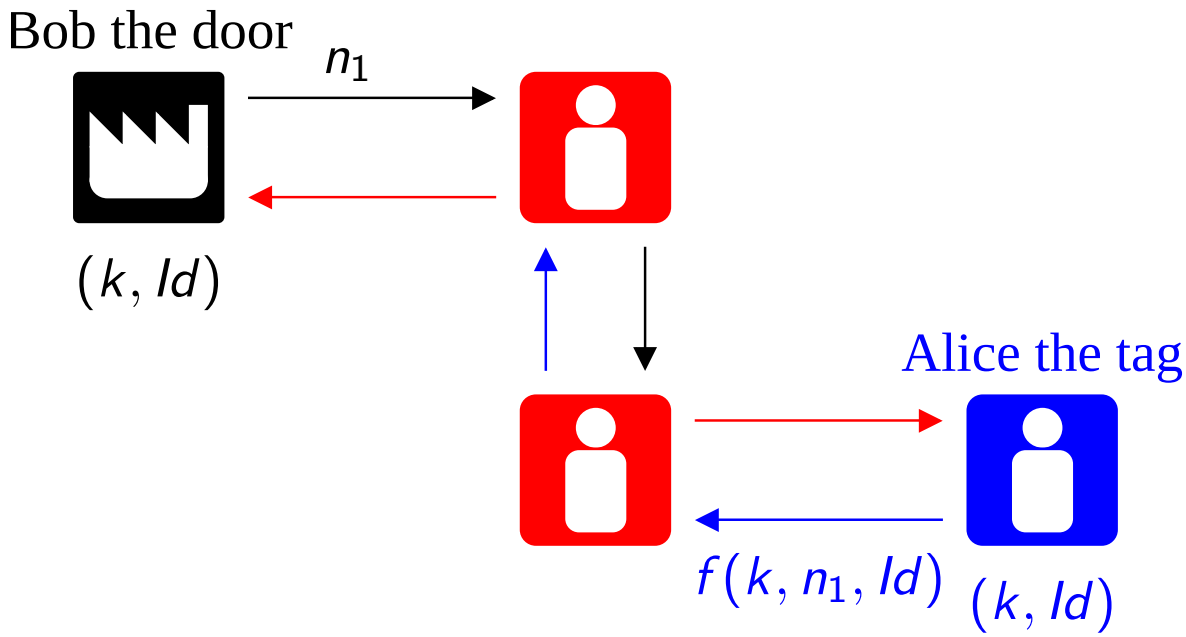
1. .. Cf6

Rusé ce Jean−Pierre !

Relay attacks

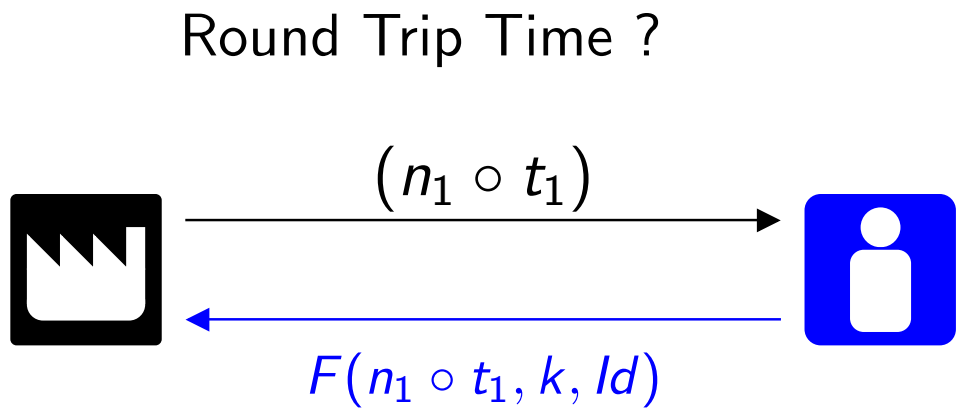
in RFID.





Relay attacks

Solution



Verification

- reception t_2
- $f^{-1}(n_1 \circ t_1, k, Id)$
- ok if $\delta_t < \sigma$

Problem

- σ ?
  - BCET
  - WCET

Relay attacks

More headaches !

- Attacker model:
  - freeze the time
  - speed the time
  - he is all-mighty !
- On tag solutions:
  - don't dream no clock !
  - any computation is a potential noise for the result.

Relay attacks

3 types of attacks

- Mafia fraud: the basic attack.
- Distance fraud: the prover cheats by sending early answer.
- Terrorism fraud: the prover colludes with the attacker without revealing its secret key.

The solutions are the distance-bounding protocols.

Denial of services

DoS is important in a competition context:

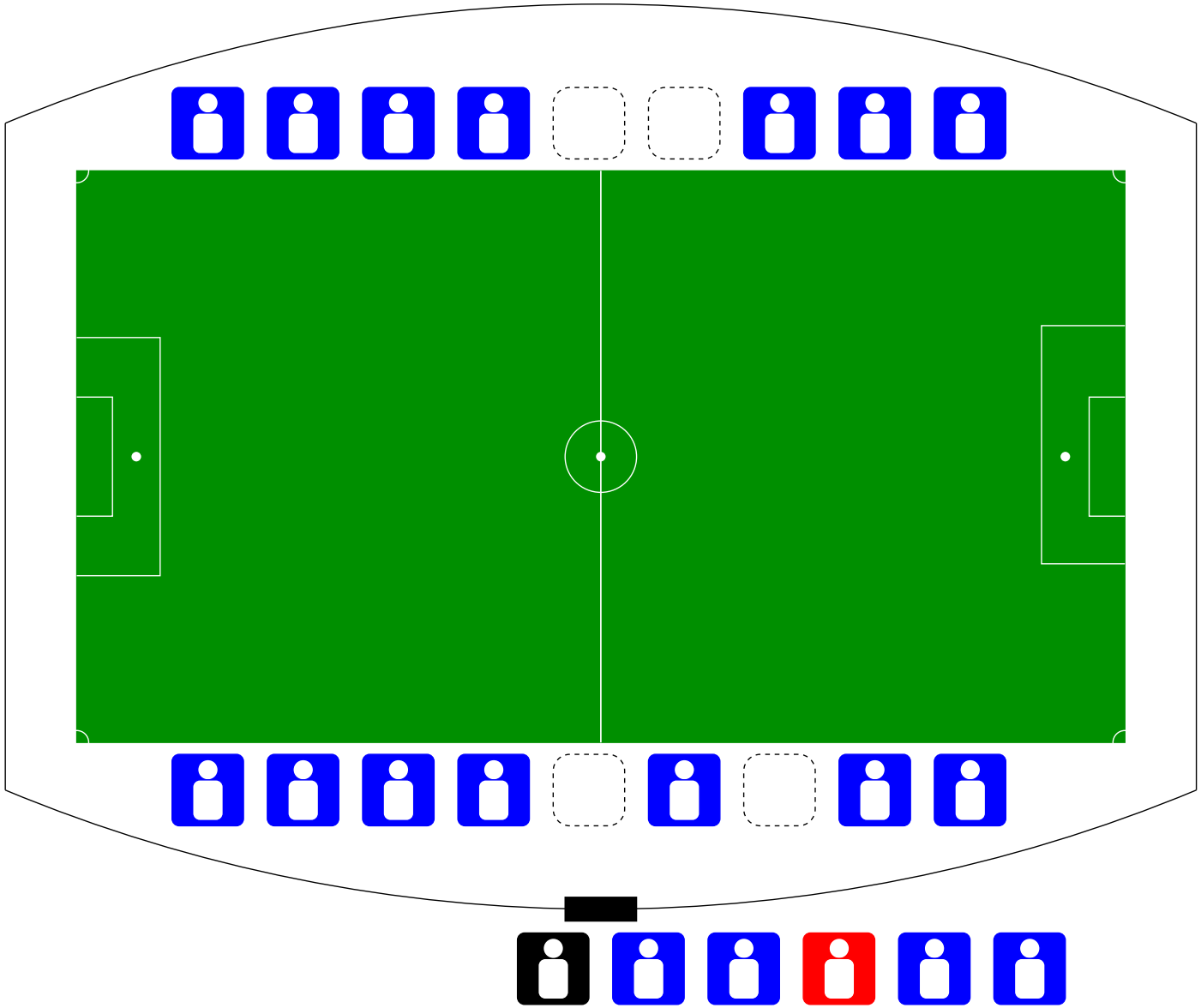
- RF Jammer: secure spread spectrum;
- Collision Jammer: improved algorithms;
- ElectroMagnetic Pulse: no possible solution.

Almost unvoidable attacks:

- Important to know your enemy;
- Critical to know what can do your commpetitor to ternish your reputation;
- Fun.

Ticketing applications

An access control problem



Ticketing problem

The players

The owner

- Designer of the system
- A few constraints: money, time...
- Collusion with the thief to increase profit

The steward

- Don’t want to know any complex stuffs
- Responsible for the customers line

The customer

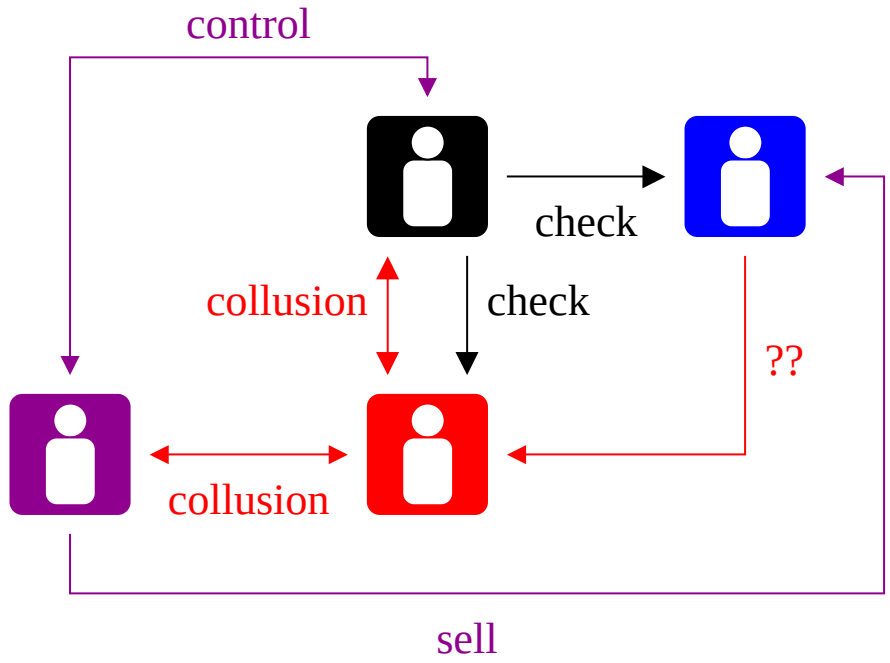
- Hold the ticket (don’t expect anything else)
- Don’t like to wait (short line)

The thief

- Smart: through time find always all the weaknesse
- Unlimited evilness
- Collusion with the owner

Ticketing problem

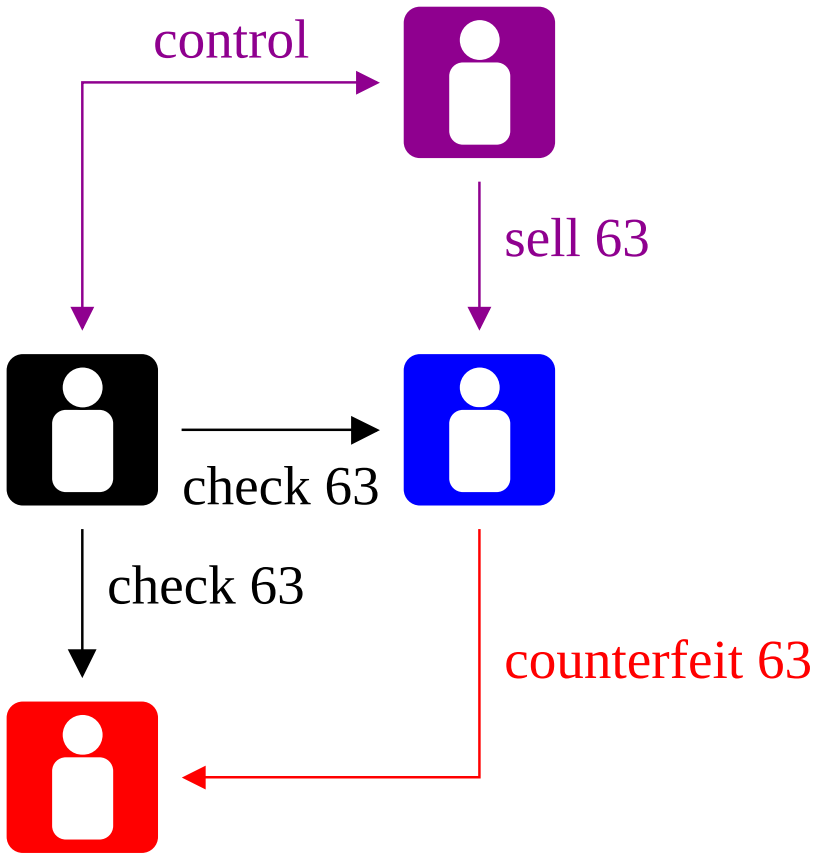
The rules



Specific attacks on ticketing systems:

- Counterfeit — one for many;
- Pass-back — a few for many;
- Illegal multiple sales — many for many;
- Black market — money for money.

Counterfeit



Counterfeit: ticket like bills ?

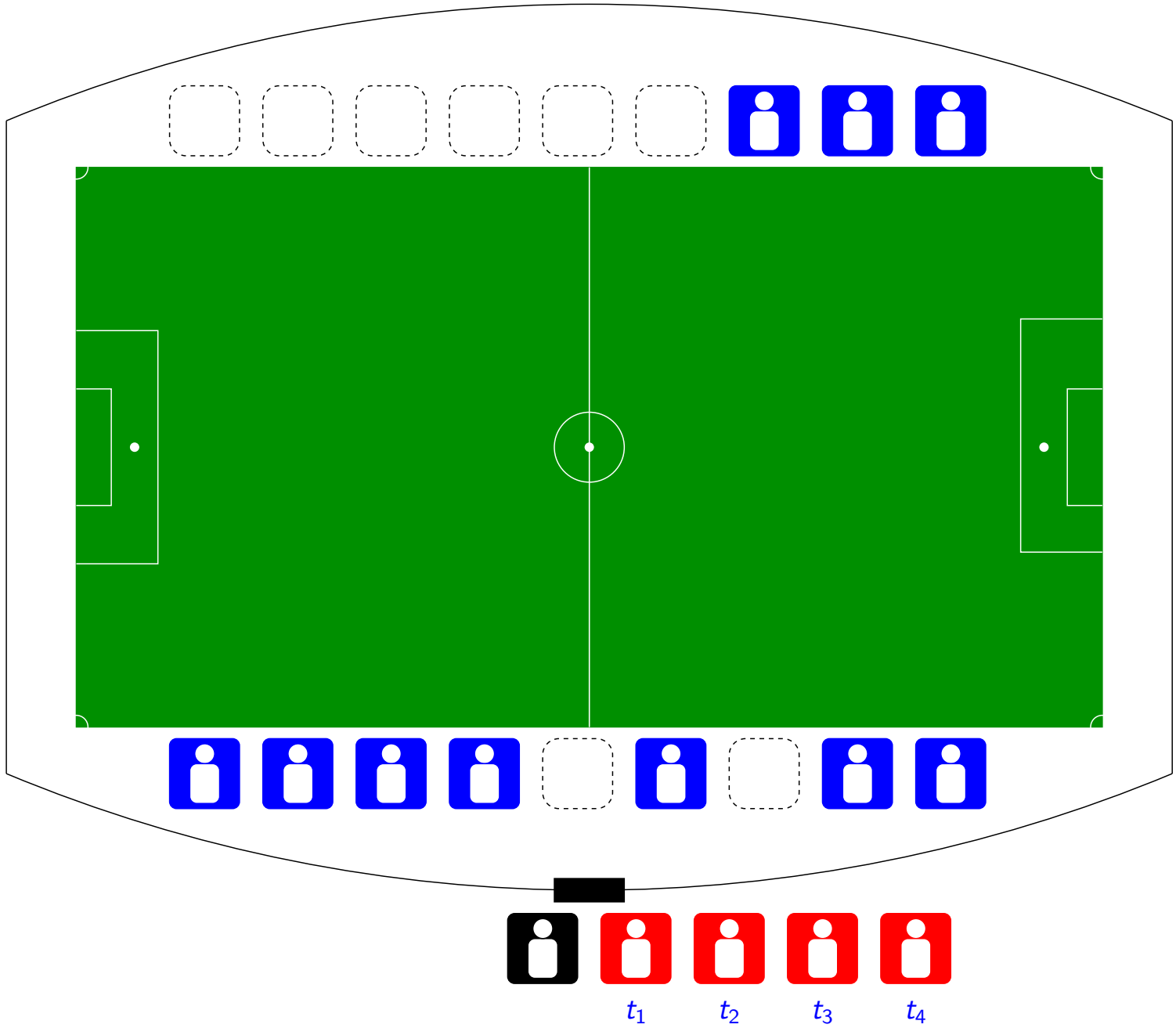
. . . or can we take advantage of money anti-counterfeiting system

Paper anti-counterfeiting system:

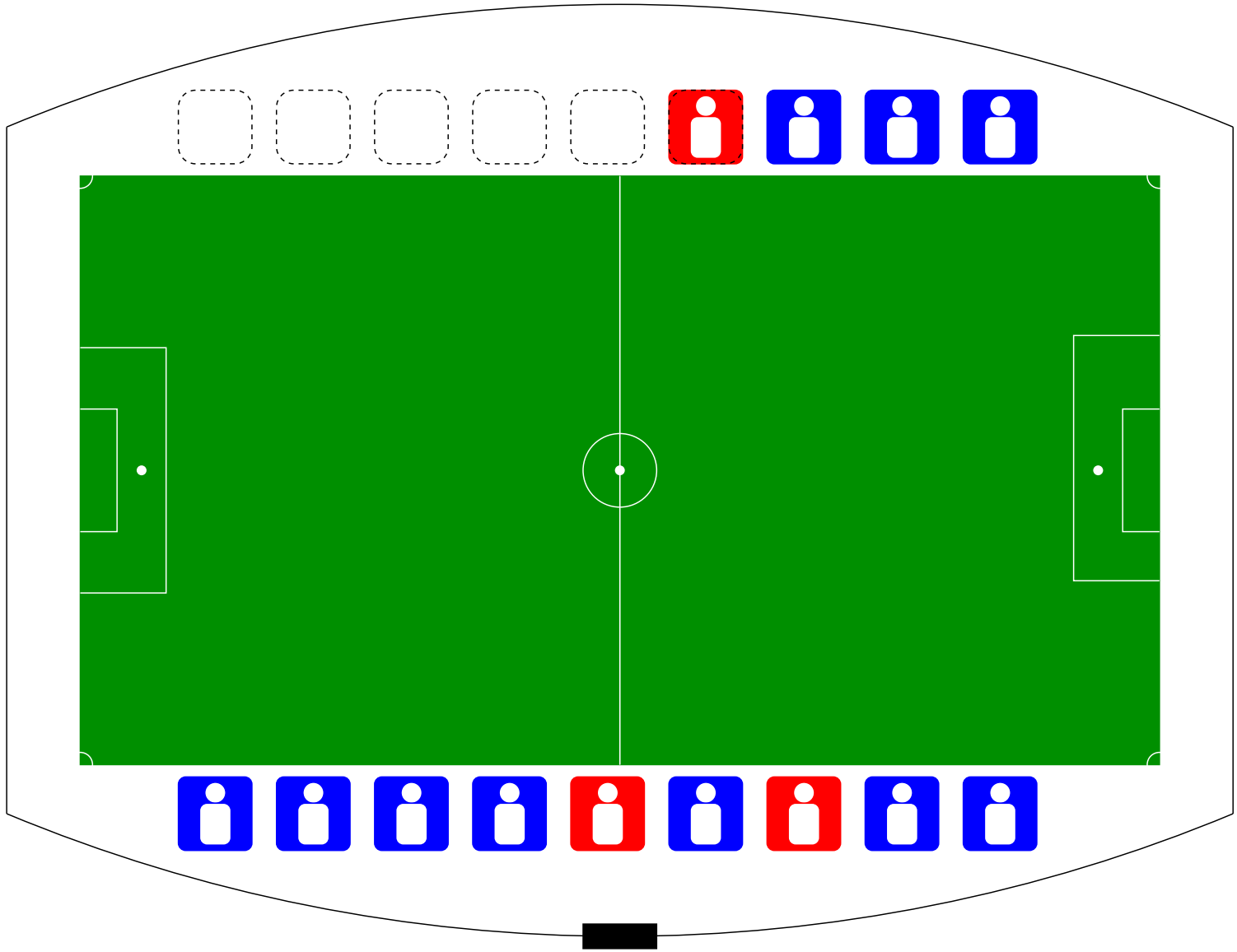
- special paper;
- special ink;
- holography;

Hard to check !

Pass-back

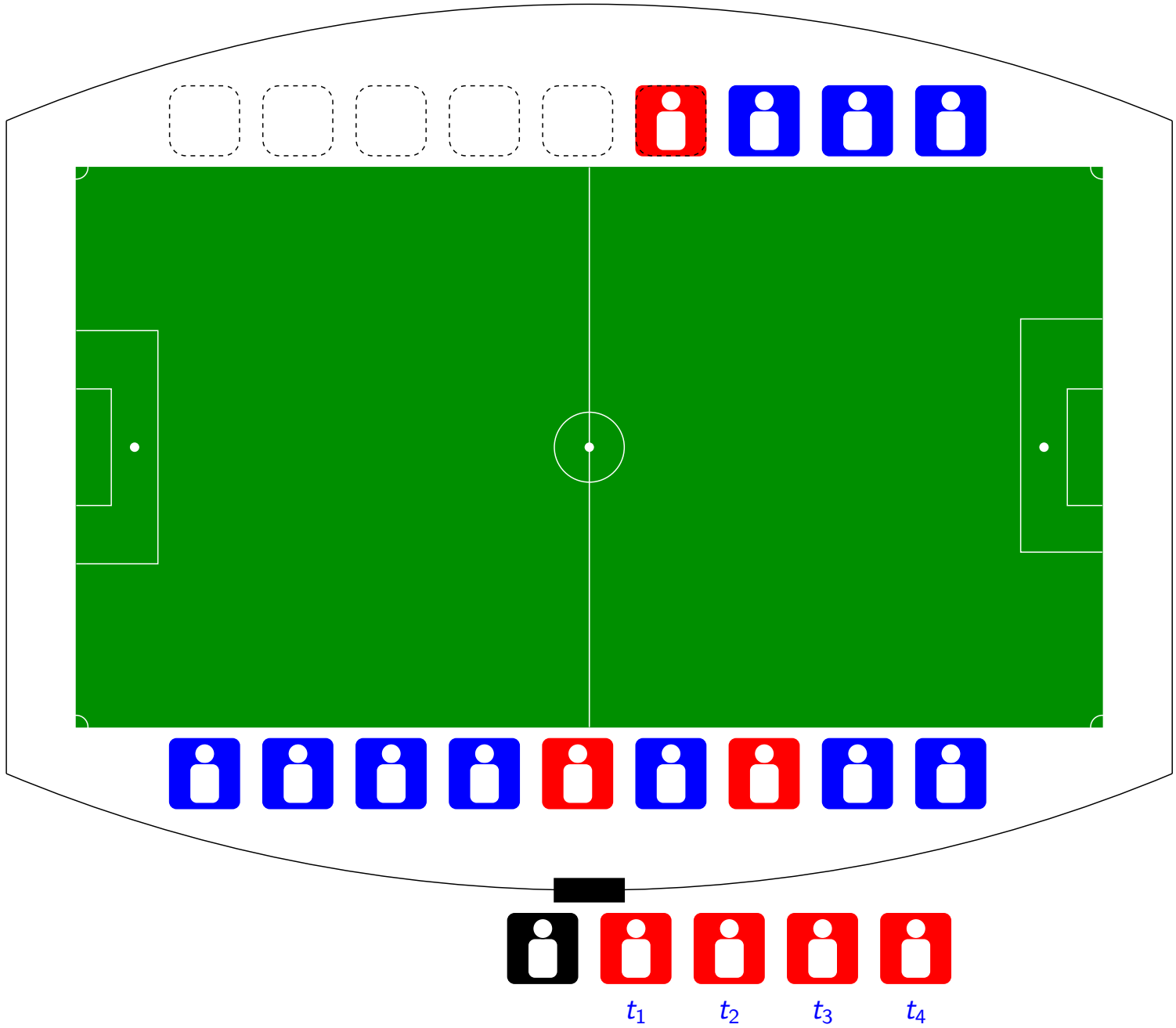


Pass-Back

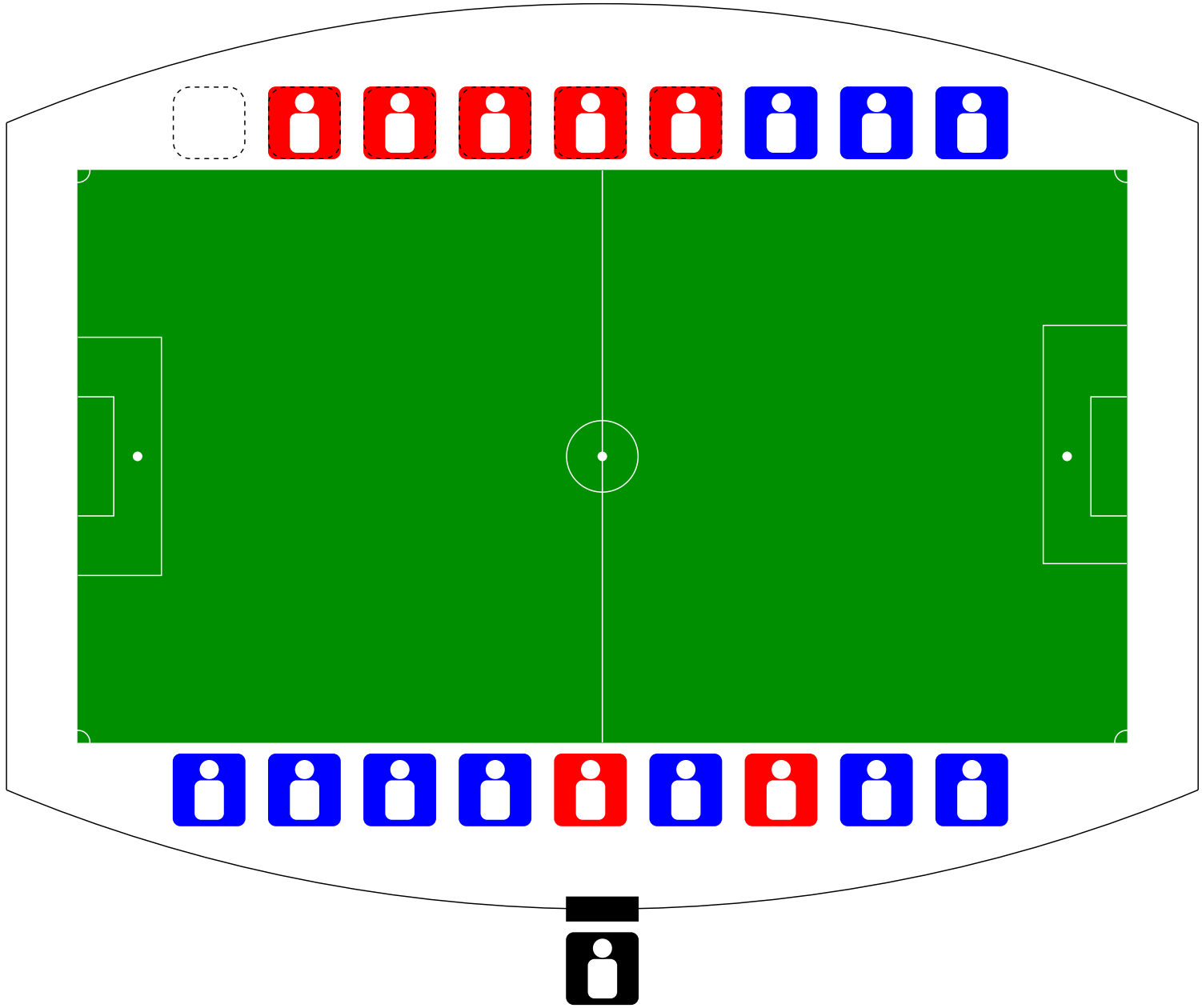


t_1, t_2, t_3, t_4

Pass-back



Pass-back



Pass-back

Coupon

Disavantages:

- one shot;
- not resistant to collusion;

Black market and illegal multiple sales

I am not Santa Claus !

RFID and ticketing

I have a dream of an RFID ticketing solutions that is:

- efficient;
- secure;
- cheap (no crypto on tag);
- compatible;
- simple (this is a dream);

I am free to forget:

- privacy;
- relay;
- other complex stuffs;