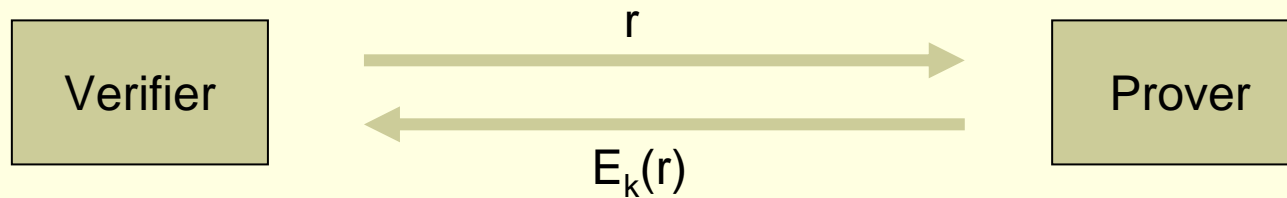

Relay Attacks in RFID:
Can Cryptography treat this Problem?

Gildas Avoine
UCL, Louvain-la-Neuve, Belgium

Challenge-Response ISO 9798-2 Mechanism

3

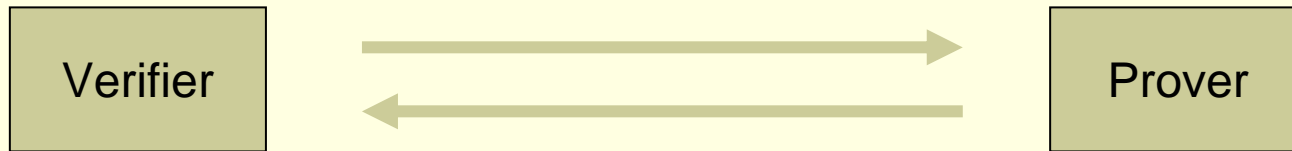


- Verifier and Prover share a secret k .
- E : Cipher.
- r : Nonce.

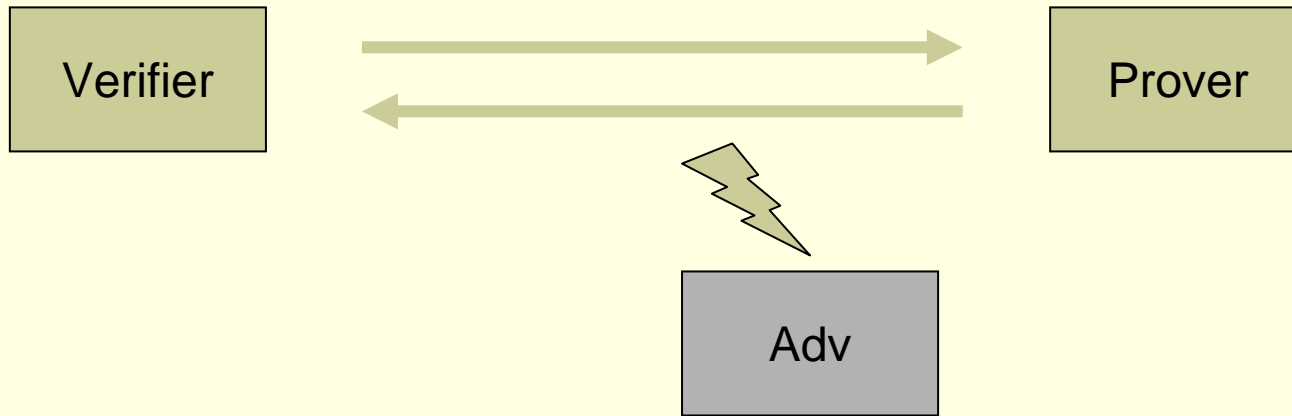
Problem Statement: What does authentication mean?

- “Literally this means determining the true identity of a person”.
Basic methods of cryptography, Jan C.A. Van Der Lubbe.
- “Entity authentication is a communication process (i.e., protocol) by which a principal establishes a lively correspondence with a second principal whose claimed identity should meet what is sought by the first”.
Modern Cryptography, Wenbo Mao.
- “Entity authentication is the process whereby one party is assured (through acquisition of corroborative evidence) of the identity of a second party involved in a protocol, and that the second has actually participated (i.e., is active at, or immediately prior to, the time the evidence is acquired)”.
Handbook of Applied Crypto, A. Menezes, P. van Oorschot, S. Vanstone.

Relay Attack



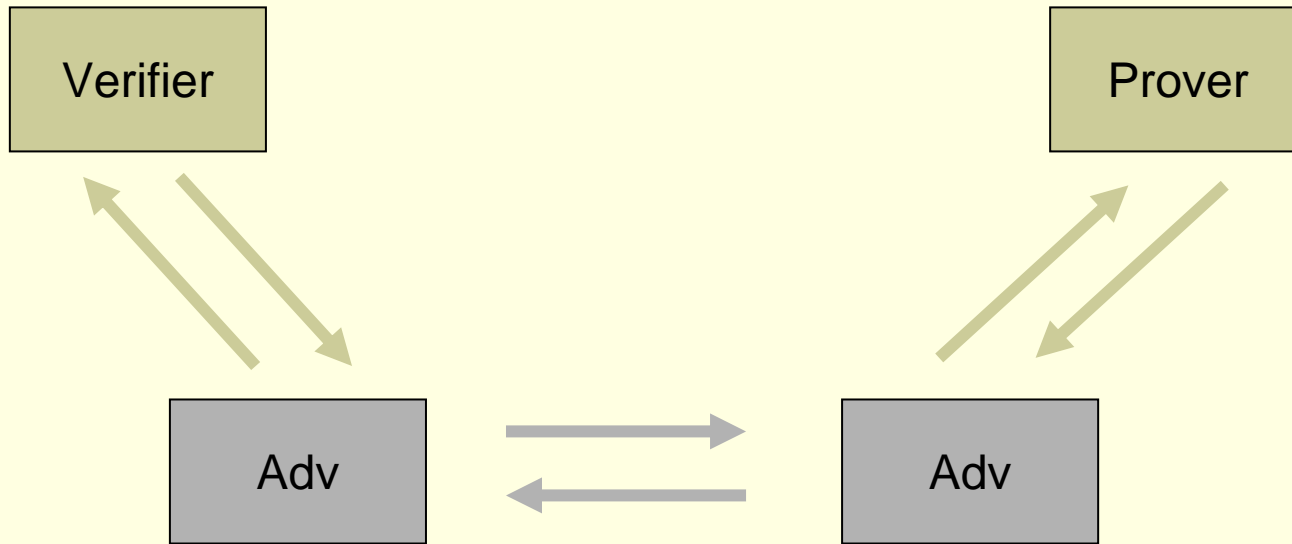
Relay Attack



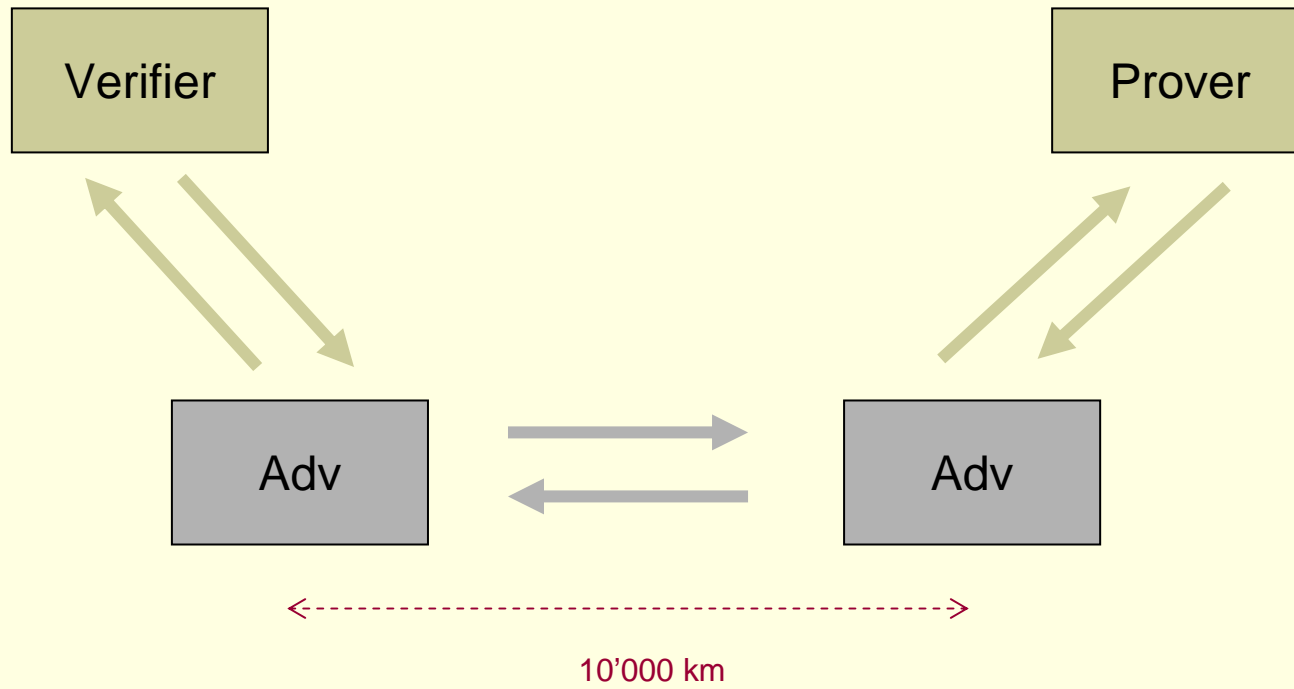
Relay Attack



Relay Attack



Relay Attack



Variants of Relay Attacks

- **Mafia fraud.**

- Shamir about Fiat-Shamir protocol [Crypto86]: “I can go to a Mafia-owned store a million successive times and they still will not be able to misrepresent themselves as me”.

(The NY Times, February 17, 1987, James Gleick)

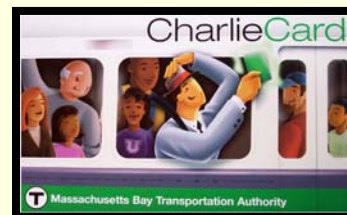
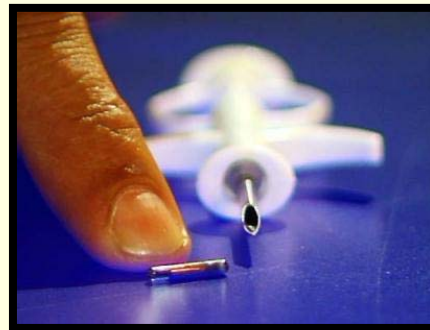
- Desmedt, Goutier, Bengio [Crypto87].
- The prover is unaware of the attack.

- **Terrorist fraud.**

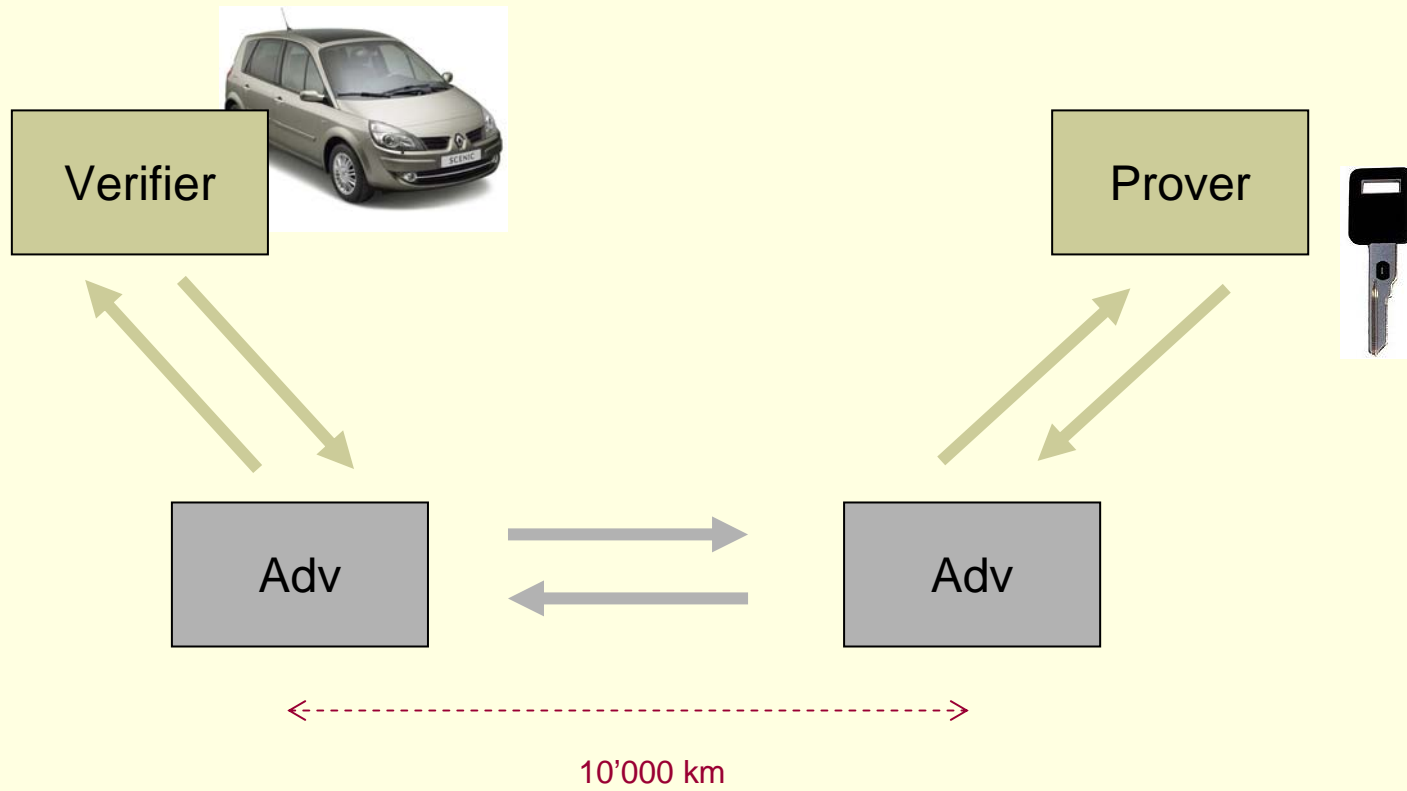
- Desmedt, Goutier, Bengio [Crypto87].
- Bengio, Brassard, Desmedt, Goutier, Quisquater [JoC91].
- The prover colludes with the adversary.

RFID in a Nutshell

- **RFID**: Radio Frequency Identification.
 - Tags are low-capability devices, passive.
 - Communication distance: a few cm to a few meters.
 - Tags answer **without agreement** of their holders.
 - Implicit agreement = being in the reader's field.



Relay Attack



Do-ability of Relay Attacks



- **Successful** attack
 - Co-axial cable over 50 cm (T. Gross 06).
 - Radio link over 50 meters (G. Hancke 05).

- Reader starts a **timer** when sending a message.
 - To avoid semi-open connections.

- **ISO 14443** “Proximity Cards”.
 - Used in most secure applications.
 - Standard on the low-layers (physical, collision-avoidance).
 - Default timer is around **5 ms**.
 - Prover can require more time, up to **4949 ms**.

Distance Bounding Protocols

- **Literature:**
 - Beth and Desmedt [Crypto90]
 - Brands and Chaum [Eurocrypt93]
 - Hancke and Kuhn [SecureComm05]
 - Etc.

- The verifier calculates the **round trip time** of a message.
 - Message needs to be **authenticated**.
 - Authentication is **time-consuming**.
 - Round trip time is noised.

Adversary model

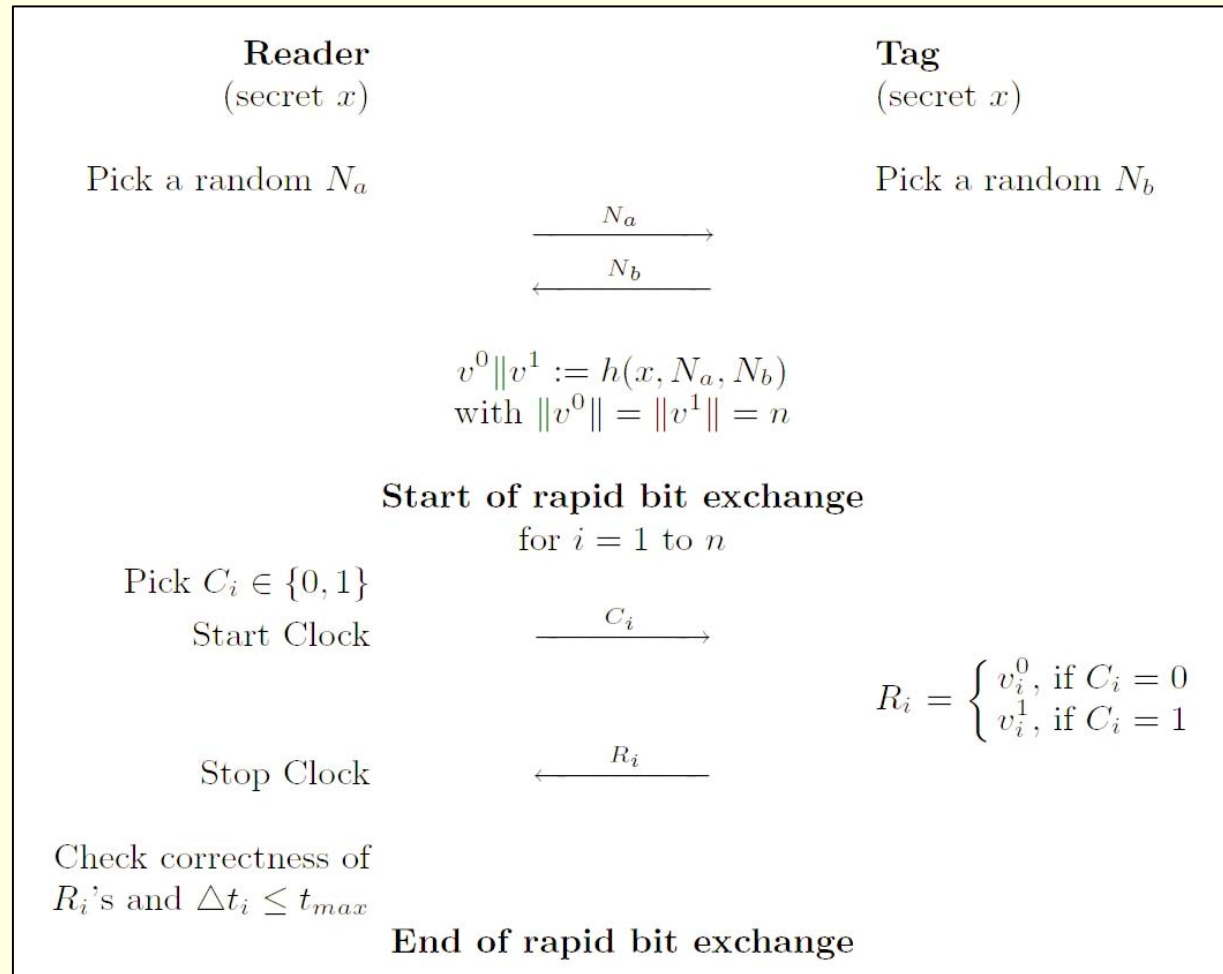
- **Adversary:**
 - Can eavesdrop, intercept, modify or inject messages.
 - Can increase the transmission speed on the channel up to a given bound (speed of light).
 - Cannot correctly encrypt, decrypt, or sign messages without knowledge of the appropriate key.
 - Can increase or decrease the clock frequency of a tag and thus the computation speed.

- **User:**
 - never reveals his secret key.

Adversary model

- We define a **neighborhood** as a zone around a reader.
- We consider that a tag present in a neighborhood **agrees to authenticate**.
- We say that a tag T has been **impersonated** if an execution of the protocol convinced a reader that it has authenticated T while the latter was not present inside the neighborhood during the said execution.

Hancke & Kuhn Distance Bounding Protocol



More Required Properties

	Mafia	M-FAR	Terrorist	T-FAR	Err. resis.	Privacy	MA	Comp.
BC	Yes	$(1/2)^n$	No	-	No	-	No	2
HK	Yes	$(3/4)^n$	No	-	Yes	-	No	1
Reid et al.	Yes	$(7/8)^n$	Yes	$(3/4)^v$	Yes	No	No	2
SP	Yes	$(1/2)^n$	No	-	Yes	-	No	1 + ECC
Capkun et al.	Yes	$(1/2)^n$	No	-	No	-	Yes	4
NV	Yes	$(1/2)^k$	No	-	No	-	No	$2k$

BC: Brand, Chaum

HK: Hancke, Kuhn

Reid et al.: Reid, Nieto, Tang, Senadji

Capkun et al.: Capkun, Buttyan, Hubaux

NV: Nikov, Vauclair

Conclusion and Limits of Distance Bounding

- Are such protocols realistic?
- Which parameters can be modified?
- No practical solution today.