



# Optimal Security Limits of RFID Distance Bounding Protocols

Orhun Kara – Süleyman Kardaş  
[Muhammed Ali Bingöl](#) – Gildas Avoine

RFIDsec 2010, Istanbul  
June 9, 2010

- Motivation
- Attacks Related to Distance
- Distance Bounding Protocols
- Current Challenge-Dependent (CCD) Protocol
- $k$ -Previous Challenge-Dependent ( $k$ -PCD) Protocols
- Natural Extension on CCD to 1-PCD
- Conclusion & Open Problems

# Motivation (Chess Grandmaster Attack)



**Karpov**



**Kasparov**

# Some RFID Applications: Need More Security

Identify friend or foe (1942)



Electronic passport



Car keys



Access control



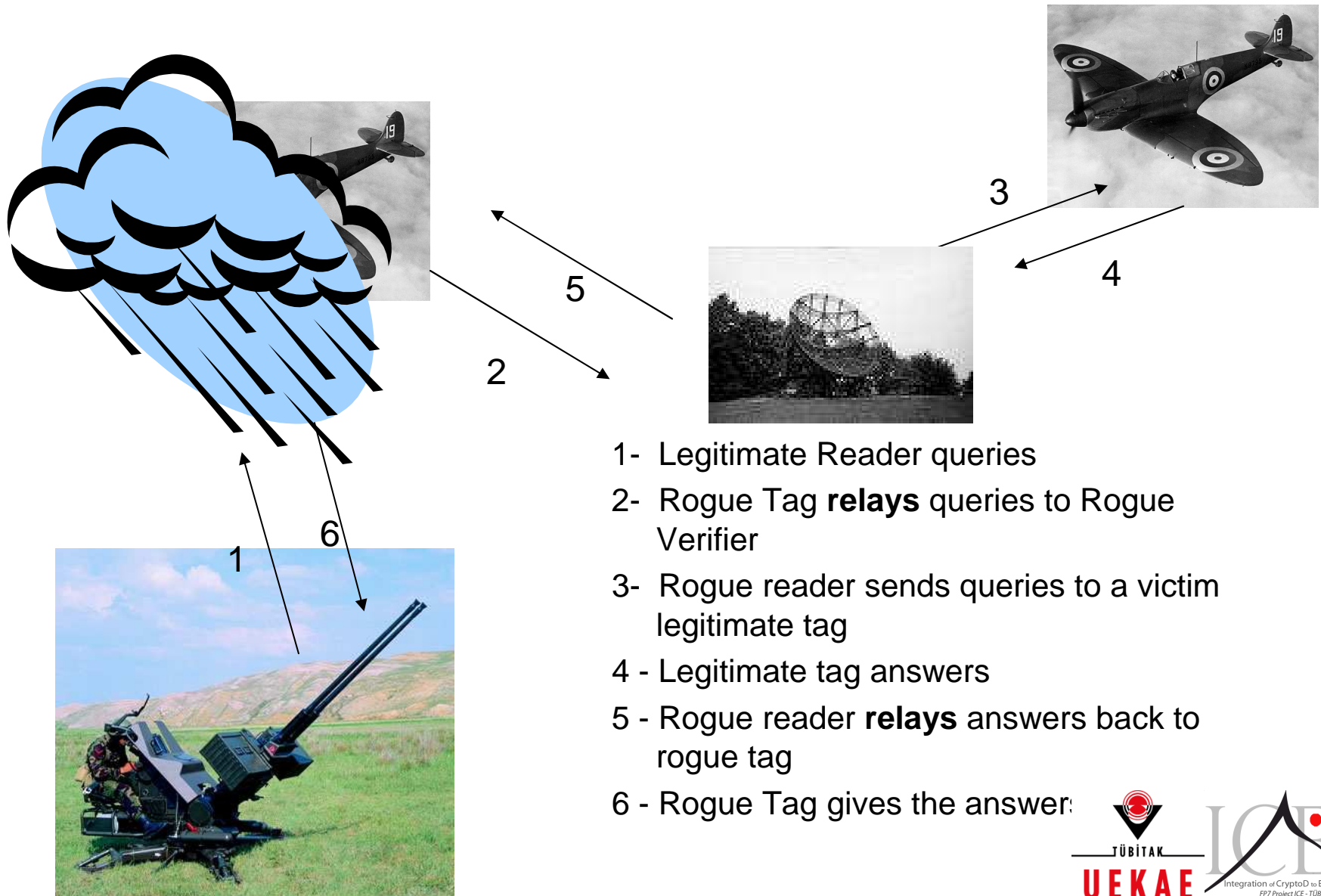
Contactless credit cards



Event ticketing



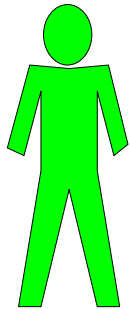
# Relay Attack: Identify Friend or Foe 1943



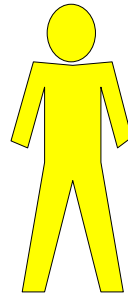
# Attacks Related to Distance

- ▶ Mafia Fraud
- ▶ Distance Fraud

## Characters:



Legitimate  
prover

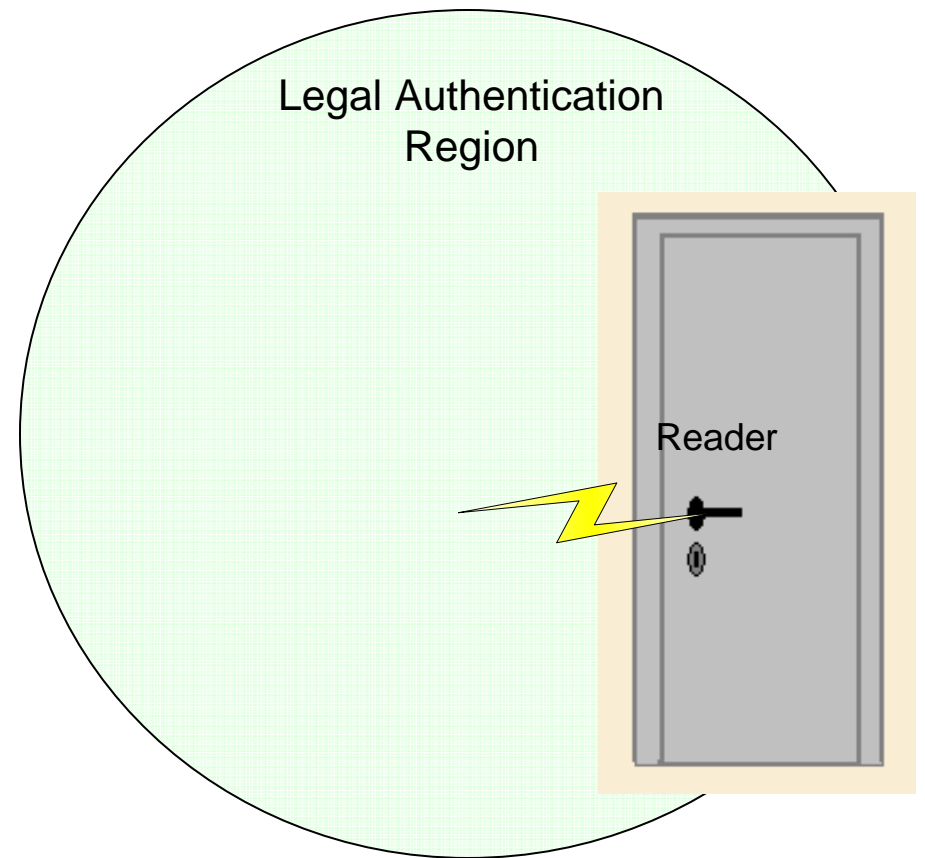
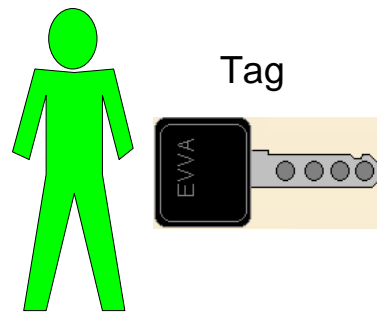


Legitimate  
prover acting  
in a bad way



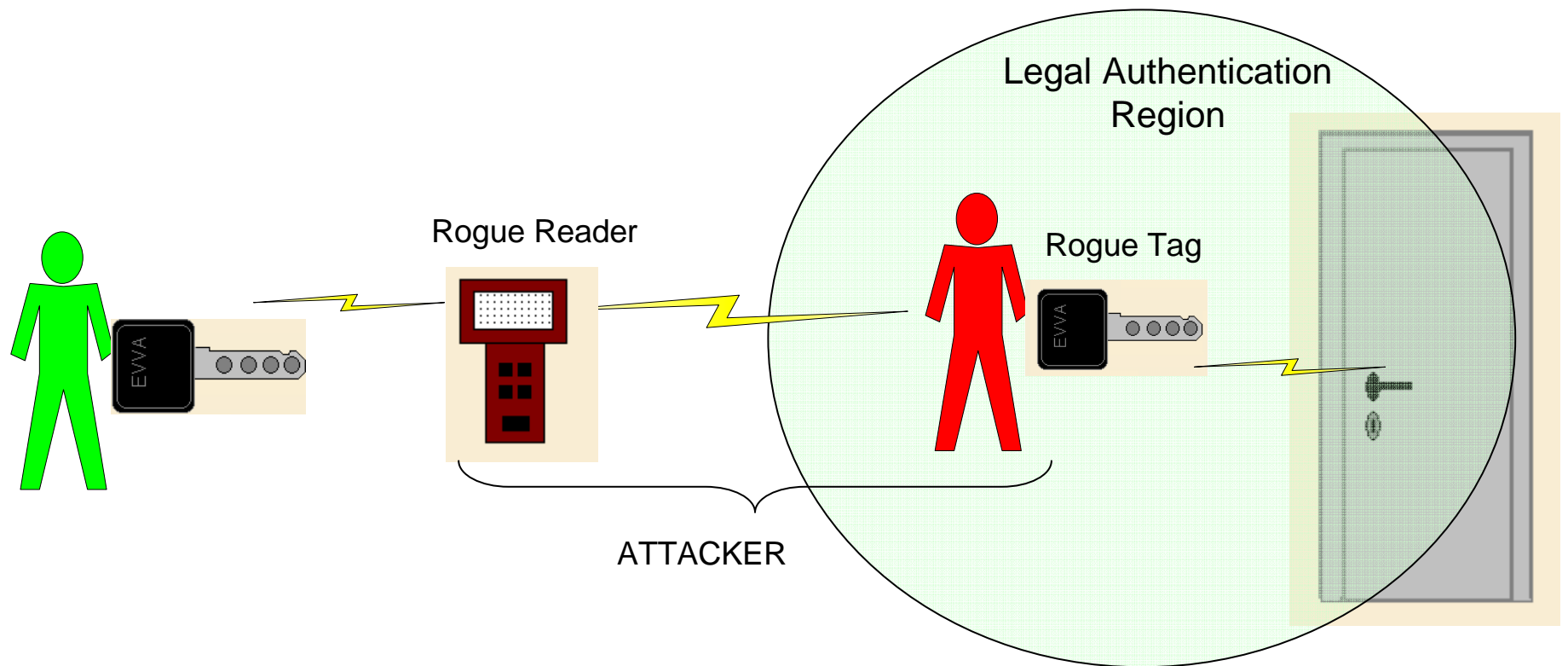
Adversary

# General Case



# Attacks Related to Distance

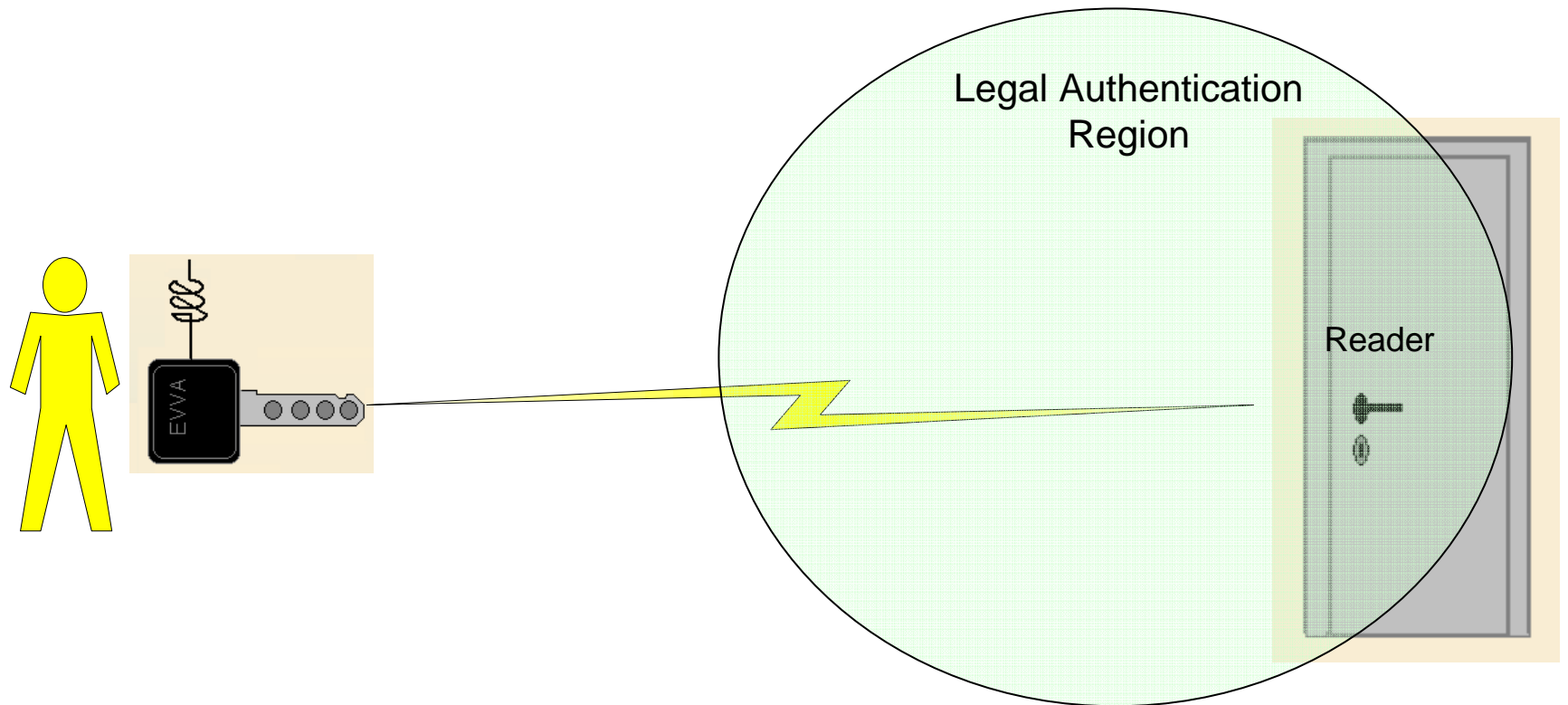
- ▶ Mafia Fraud
- ▶ Distance Fraud



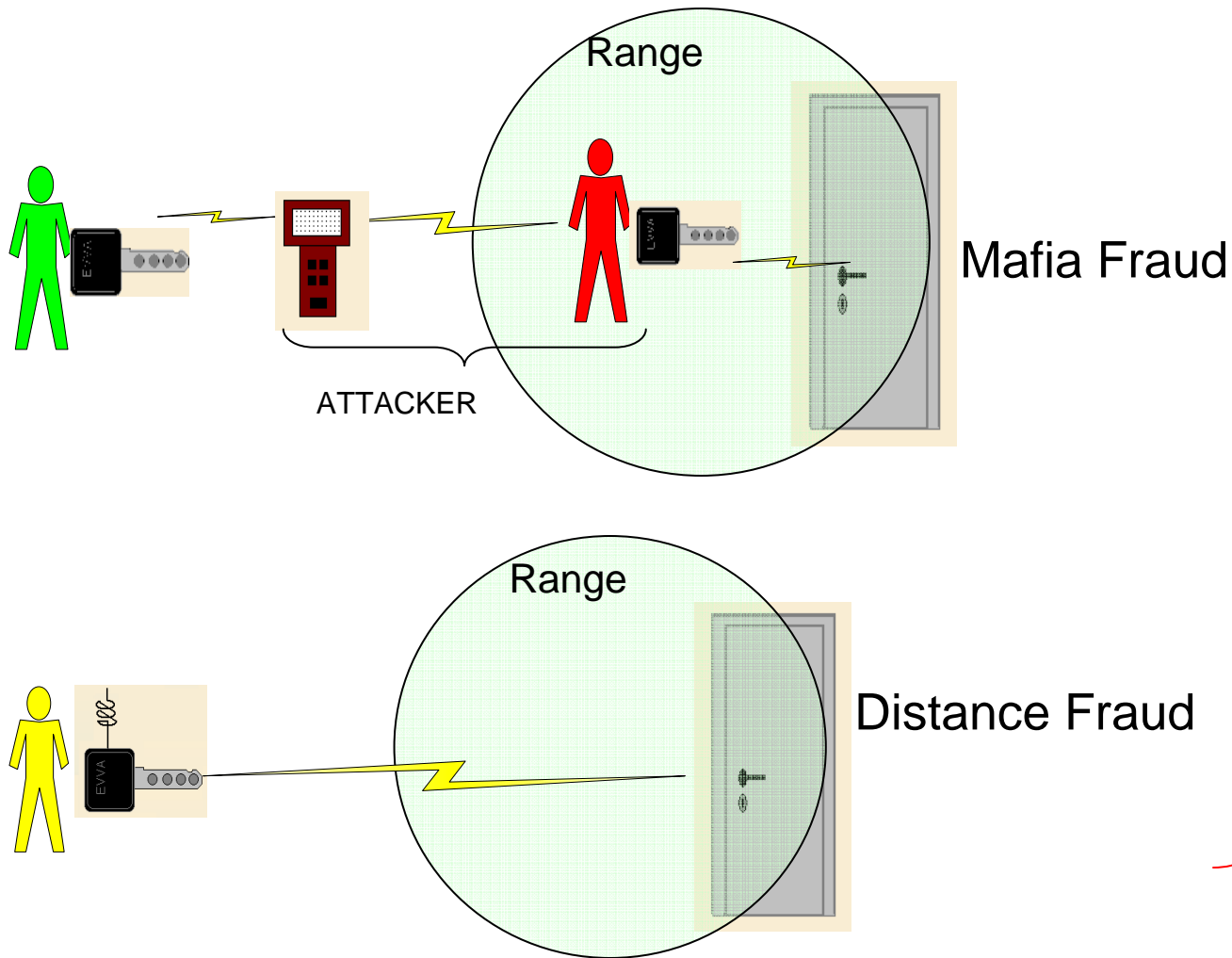
# Attacks Related to Distance

► Mafia Fraud

► Distance Fraud

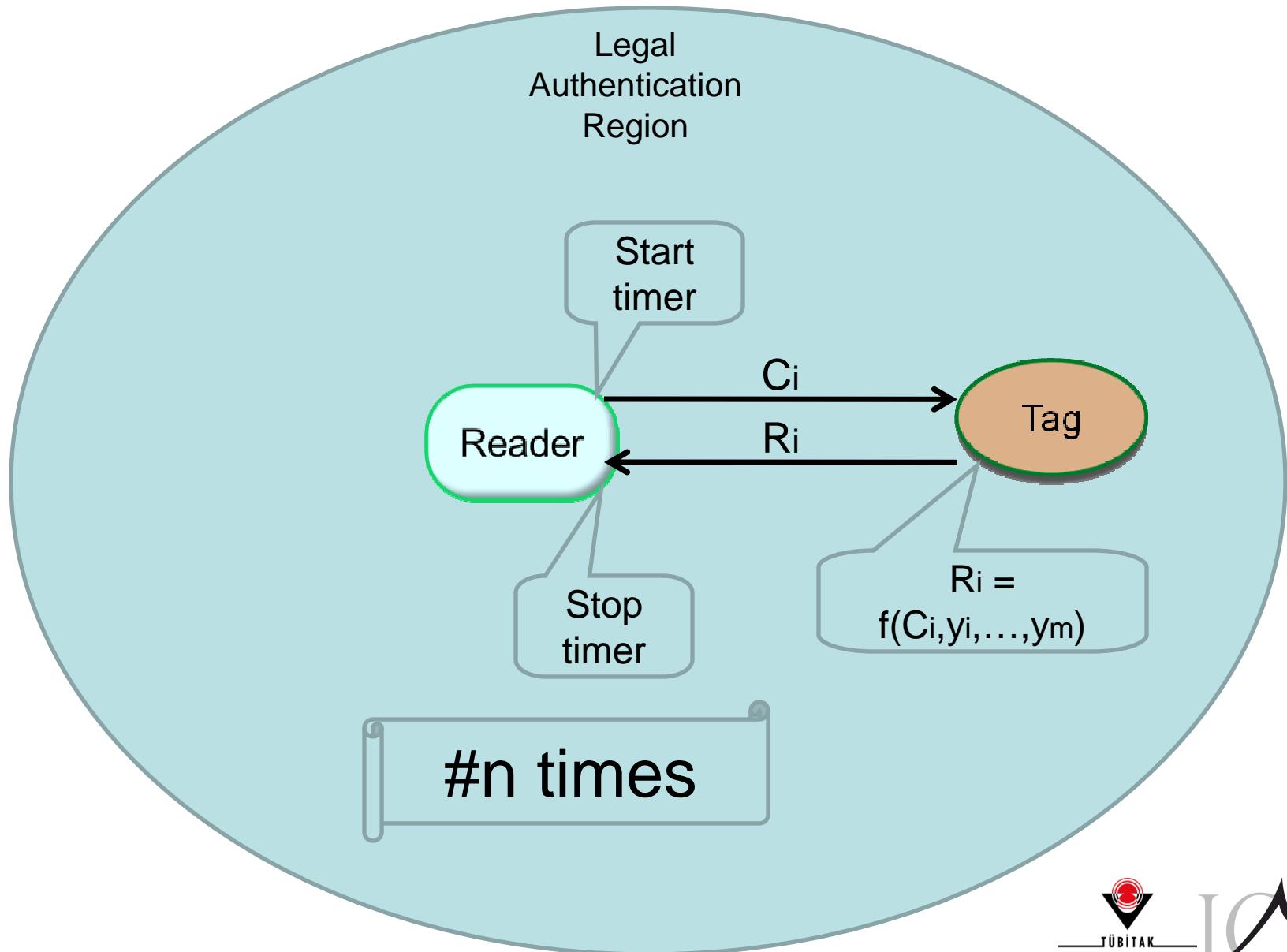


# How to Solve?



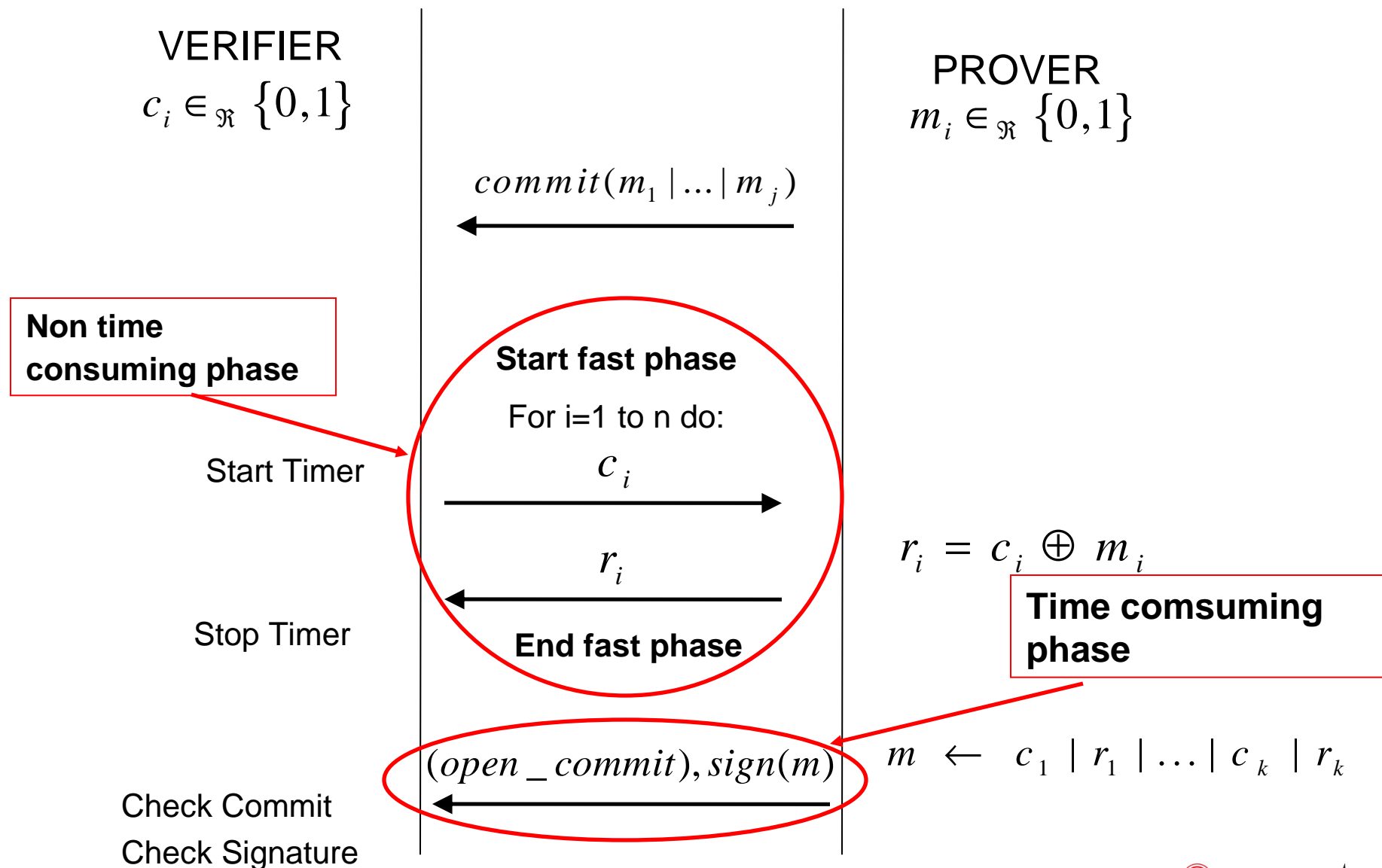
**Distance Bounding Protocols are Countermeasure to these Attacks!!**

# Round Trip Time Measurement

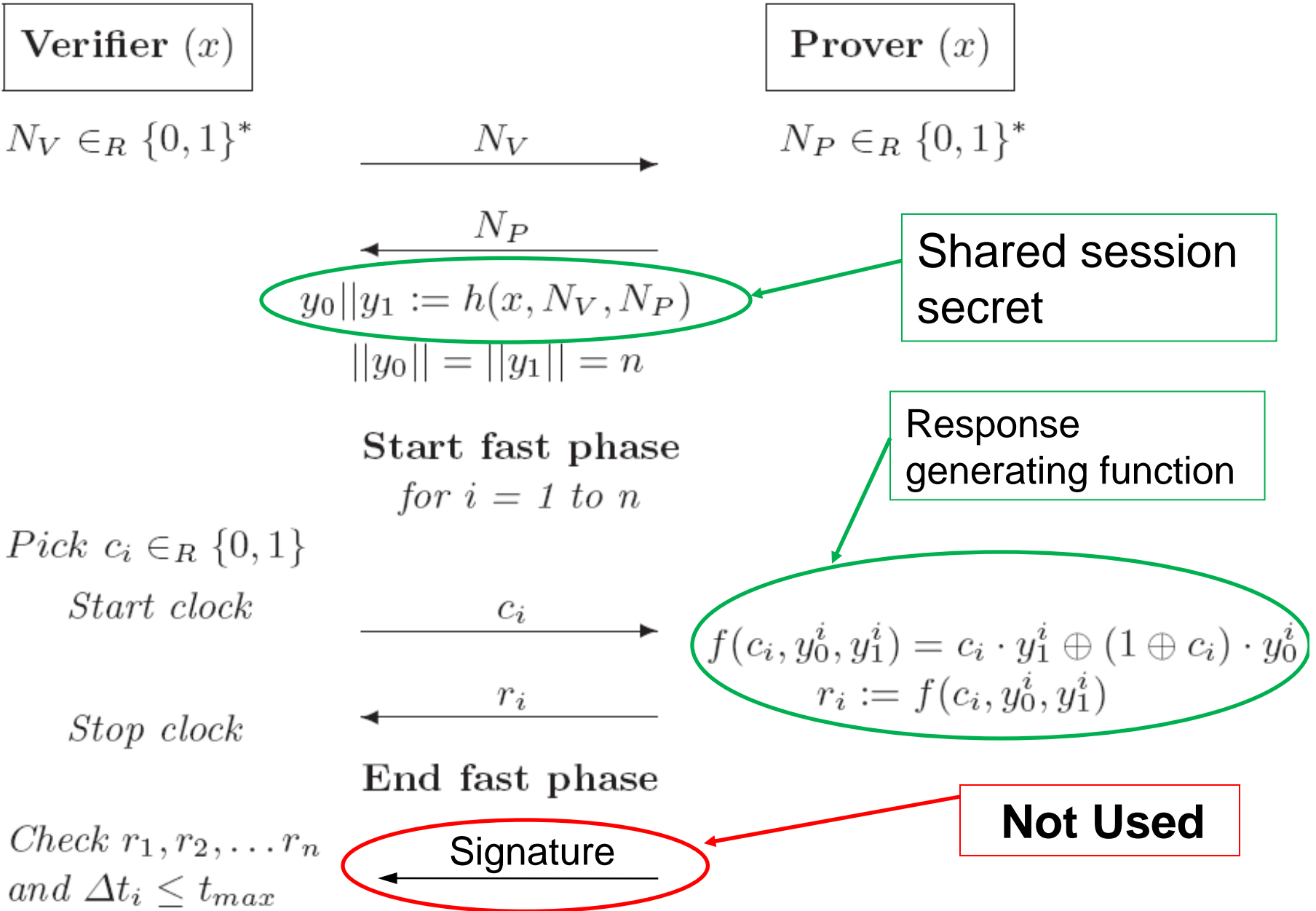


- Beth and Desmedt [Crypto90]
- Brands and Chaum [Eurocrypt93]
- Hancke and Kuhn [SecureComm05]
- ...

# Brands & Chaum's Distance Bounding Protocol



# Hancke & Kuhn's RFID Distance Bounding Protocol



## Focus of This Work

- We focus on the RFID distance bounding protocols having bitwise fast phases and no final signature.
- We first investigate Current Challenge Dependent (CCD) Protocols.

## Def: Current Challenge-Dependent (CCD) Protocol

Let  $f : \mathbb{F}_2^{m+1} \rightarrow \mathbb{F}_2$  be a Boolean function.

A CCD protocol  $P$  is a distance bounding protocol that satisfies:

(i) During the fast phase, each response bit  $r_i$  is computed as

$$r_i := f(c_i, y_0^i, \dots, y_{m-1}^i)$$

$i = 1, \dots, n$ , where  $n$  is the number of rapid bit exchanges.

(The current response depends on the current challenge)

(ii) There is no final signature.

## Attack Algorithms for CCD Protocols

- We have described two generic attacks for mafia and distance frauds that can be mounted on all CCD protocols.
- $P_{\text{maf}}$ : Success probability of correctly guessing one response bit for **mafia fraud**.
- $P_{\text{dis}}$ : Success probability of correctly guessing one response bit for **distance fraud**.

## Some Open Questions

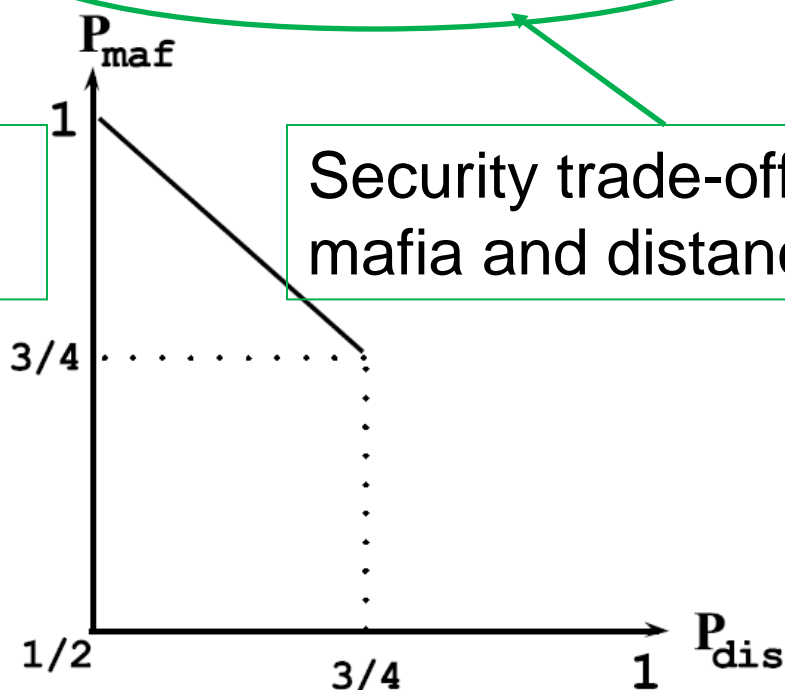
- Can we design a distance bounding protocol without final signature that resists to the Mafia fraud with probability better than  $3/4$ ?
- if  $P_{\text{dis}}$  is ideal (i.e.  $1/2$ ), what is the minimum value of  $P_{\text{maf}}$ .
- What are the best security levels for both mafia and distance frauds among all CCD protocols?
- ✓ The above-mentioned questions are answered in this work.

# Security Bound and Trade-off for CCD Protocols

**Theorem 1.** Let  $\mathcal{P}$  be a  $f(c_i, y_0^i, \dots, y_{m-1}^i) \rightarrow r_i$  CCD protocol. Assume that  $c_i$  and  $y_j^i$ s used during the fast phase of  $\mathcal{P}$  are uniformly random. Then, (i)  $P_{maf}(\mathcal{P}) \geq 3/4$ , and (ii)  $P_{maf}(\mathcal{P}) + P_{dis}(\mathcal{P}) \geq 3/2$ .

Security bound for Mafia Fraud

Security trade-off between mafia and distance frauds



**Corollary 1.** For a CCD protocol  $\mathcal{P}$ , if the security level for the distance fraud is ideal (i.e.  $P_{dis}(\mathcal{P}) = 1/2$ ) then,  $P_{maf}(\mathcal{P})$  is 1.

## How to Improve the Security Level with Almost No Cost

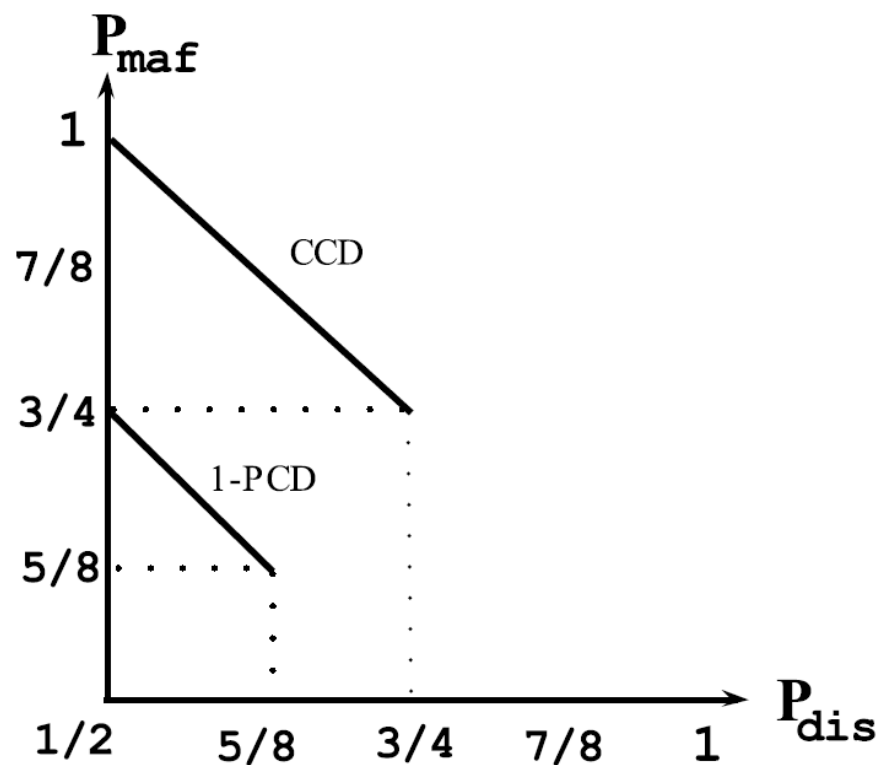
- Still we don't want to use final signature.
- We can use the previous challenges.
- *k-Previous Challenge Dependent (k-PCD) protocol: each response bit depends on the current and the k previous challenges.*
- k-previous challenges are used to generate a response bit.

$$r_i := g(c_i, \dots, c_{i-k}, y_0^i, \dots, y_{m-1}^i)$$

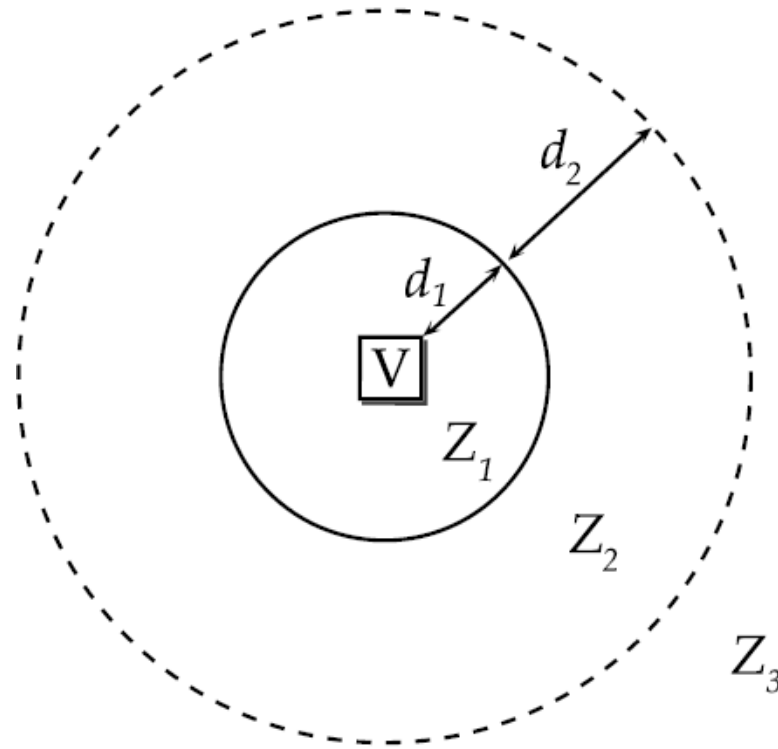
- A CCD protocol is a k-PCD protocol for  $k = 0$ .

# Security Bound and Trade-off for 1-PCD Protocols

**Theorem 2.** Let  $\mathcal{P}$  be a  $f(c_i, c_{i-1}y_0^i, \dots, y_{m-1}^i) \rightarrow r_i$  1-PCD protocol. Assume that  $c_i$ s and  $y_j^i$ s used in the fast phase of the protocol  $\mathcal{P}$  are uniformly random. Then  $P_{maf}(\mathcal{P}) \geq 5/8$ , and  $P_{maf}(\mathcal{P}) + P_{dis}(\mathcal{P}) \geq 5/4$ .



# Several Neighbourhoods for k-PCD Protocols



$P'$  is called a natural extension of  $P$  if  $g(c_i, c_{i-1}, y_0^i, \dots, y_{m-1}^i)$  is a Boolean function of the variables  $f(Q(c_i, c_{i-1}), y_0^i, \dots, y_{m-1}^i)$  and  $T(c_i, c_{i-1})$ , where  $Q$  and  $T$  are Boolean functions of two variables.

## Natural Extension for CCD to 1-PCD

- The objective is not proposing a new distance bounding protocol but enhancing the security level of a given protocol via extending its response function by using simple polynomial arithmetic.
- We show that the security level can be improved without using a computationally expensive final signature.

# A Natural Extension of HK Protocol for Improving Distance Fraud Resistance

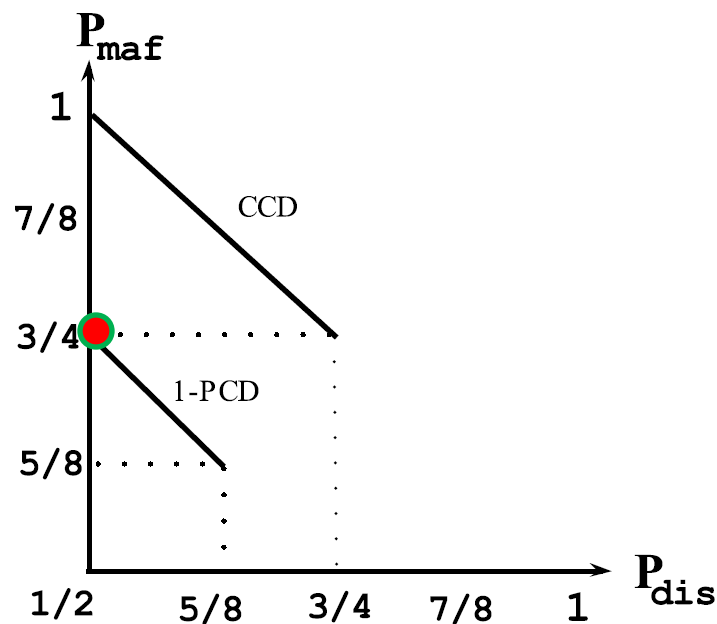
$$\begin{aligned}
 g(c_i, c_{i-1}, y_0^i, y_1^i) &= f(c_i, y_0^i, y_1^i) \oplus c_{i-1} \\
 &= c_i \cdot y_1^i \oplus ((1 \oplus c_i) \cdot y_0^i) \oplus c_{i-1} \\
 &= y_{c_i}^i \oplus c_{i-1}
 \end{aligned}$$

Original HK Protocol RGF

Previous challenge

$$P_{dis} = 1/2.$$

$$P_{maf} = \frac{3}{4}$$



# A Natural Extension of HK Protocol for Improving Mafia Fraud Resistance

$$g(c_i, c_{i-1}, y_0^i, y_1^i) = f(c_i, y_0^i, y_1^i) \oplus f((1 \oplus c_{i-1}), y_0^i, y_1^i)$$

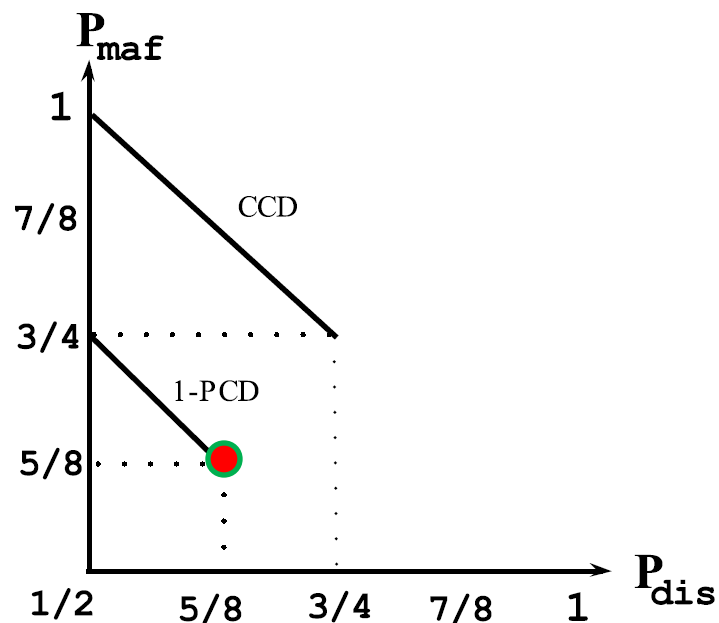
$$= y_{c_i}^i \oplus y_{\bar{c}_{i-1}}^i,$$

Original HK Protocol RGF

Complement of previous challenge into HK RGF

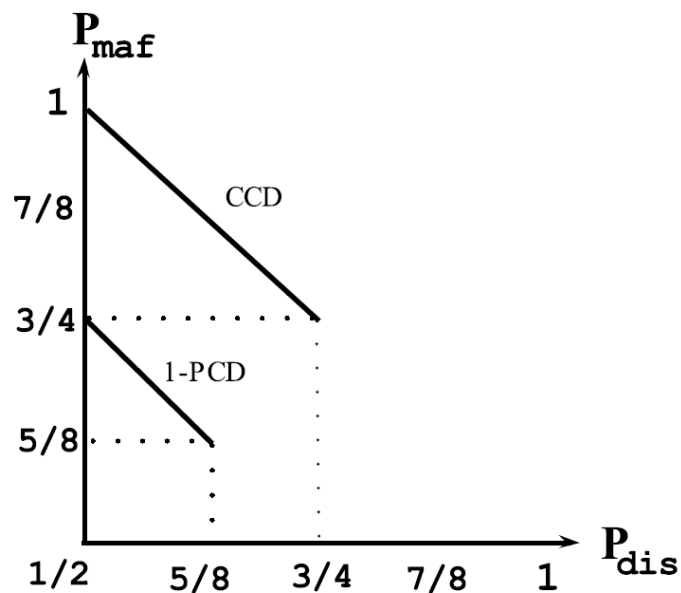
$$P_{maf} = 5/8$$

$$P_{dis} = 5/8$$



# Conclusion

- We introduced the notion of CCD protocols and k-PCD protocols.
- We developed generic attack algorithms that can be mounted on all CCD protocols and 1-PCD protocols.
- We have constructed trade-off curves both for CCD and 1-PCD protocols.
- We introduce the several neighbourhood concept.
- We give natural extension CCD protocols to 1-PCD protocols
- Case study extension of HK protocol



## Open Questions

- Is there a trade-off curve lying above the curve  $P_{\text{maf}} + P_{\text{dis}} = 3/2$  for CCD protocols?
- Similar question for 1-PCD protocols: Is there a trade-off curve lying above the curve  $P_{\text{maf}} + P_{\text{dis}} = 5/4$  for 1-PCD protocols?
- *Conjecture 1.* The best trade-off curve for  $k_1$ -PCD protocols lies above the best trade-off curve for  $k_2$ -PCD protocols where  $k_1 < k_2$ .
- *Conjecture 2.*  $P_{\text{maf}} + P_{\text{dis}}$  tends to 1 when  $k$  and  $n$  both tends to infinity.

# THANK YOU



THANKS FOR YOUR ATTENTION!  
QUESTIONS ?

