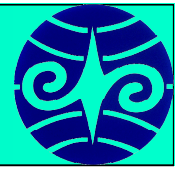
Threats & Challenges of RFID Authentication

Hung-Yu Chien

National Chi Nan University

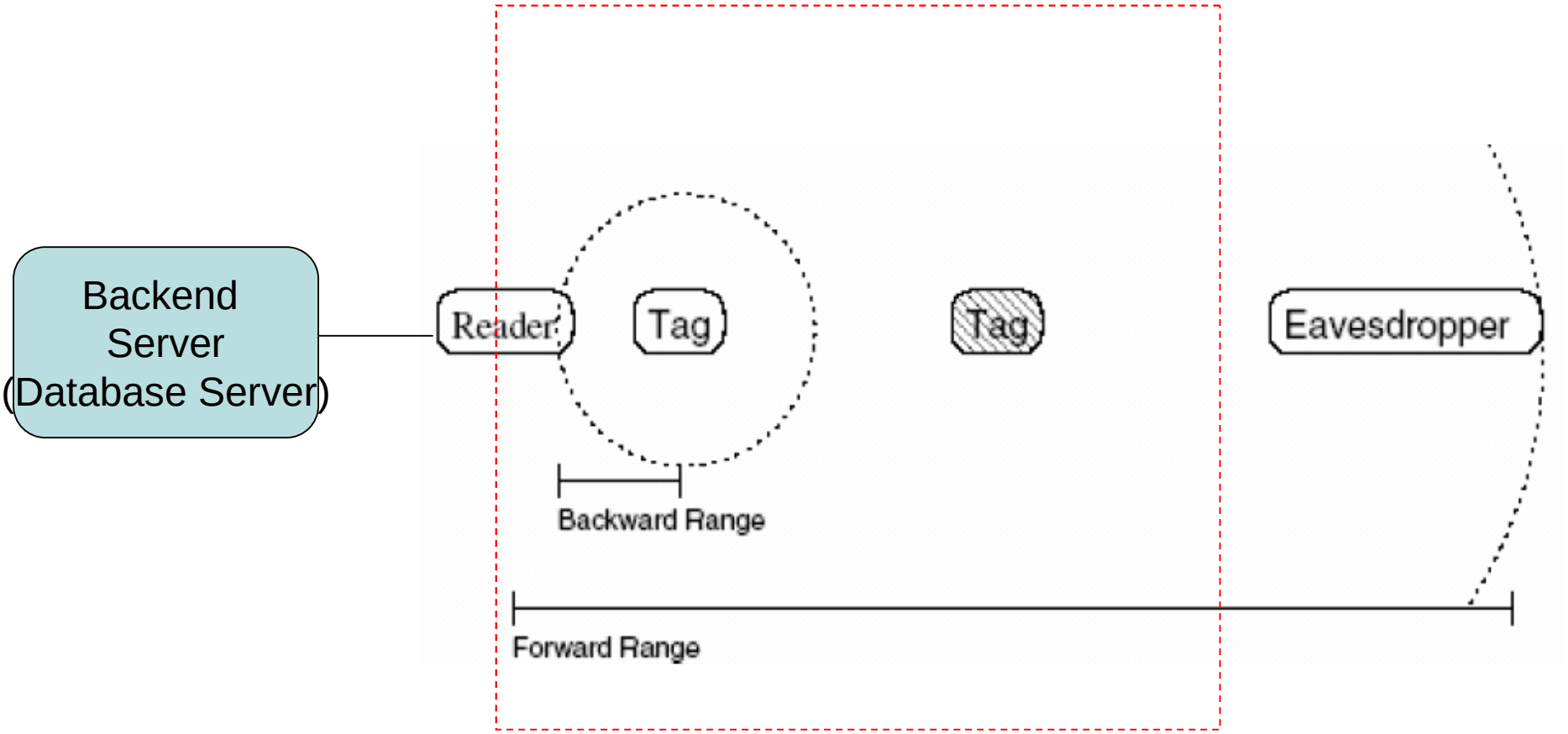
NCHU , 2008/3/14

Outline



- Basics of RFID Systems
- Security of RFID Authentications
- Variants of RFID Authentication Problems
- Classification of RFID Authentication Protocols
- Cryptographic Techniques to RFID Authentication
- Various Relay Attacks
- Conclusions

Basics of RFID Systems



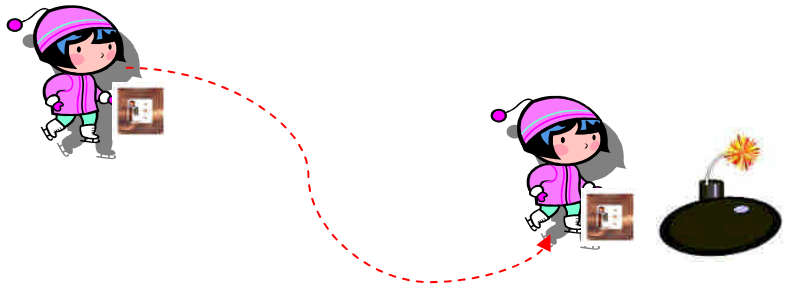
RFID tags will be *everywhere*…

http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/blocker/blocker_slides.pdf

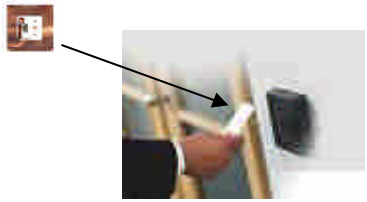
Security Threats

– *Eavesdropping*

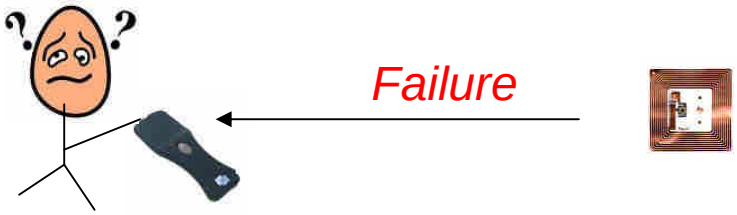
– *Traceability*



– *Spoofing*

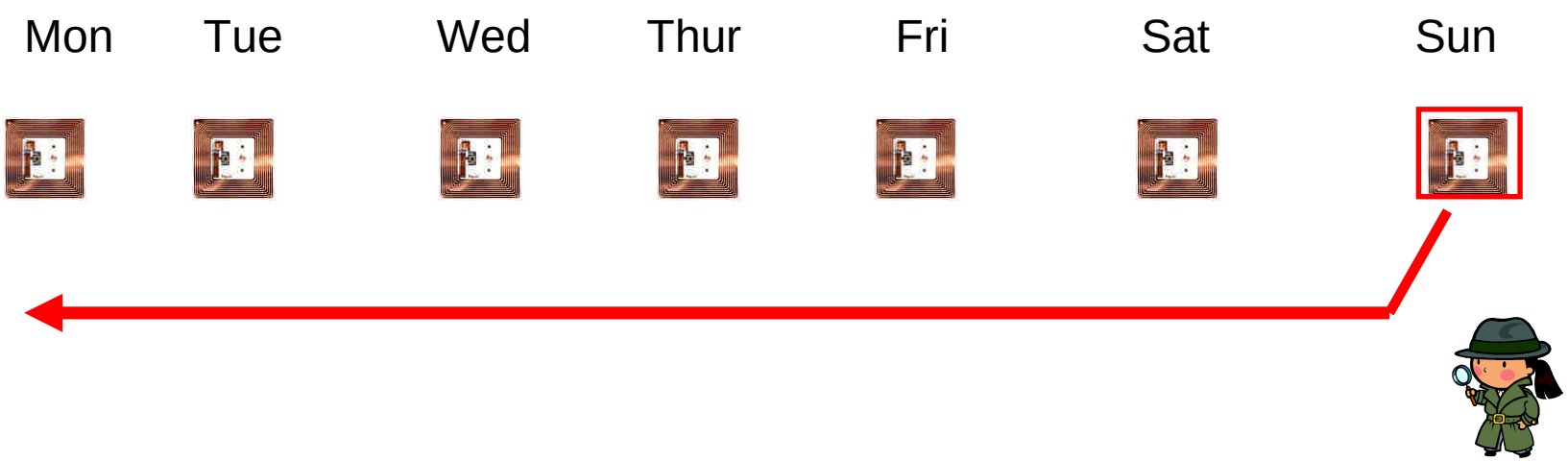


– Denial of Service (DoS)

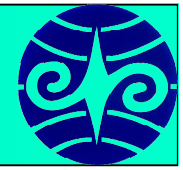


Security Requirements

- Privacy, authentication
- Anonymity
- Un-linkability
- Resistance to DOS attack
- Forward secrecy



Variants of RFID Authentication

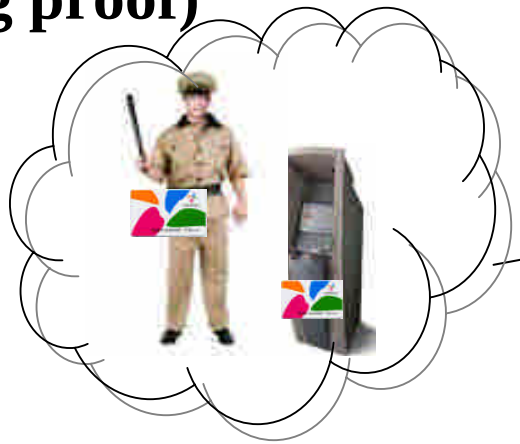


1. Pure Authentication

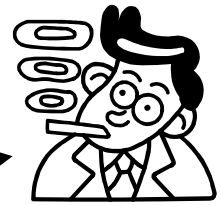
Which tag ?

Are you a legal reader ?

2. Yooking proof (grouping proof)

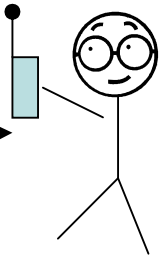


Does John check the ATM ?



3. Searching

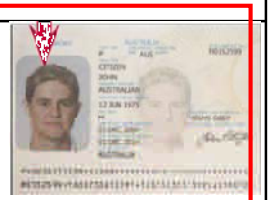
Where is my Honda car ?



Yes, I am here!

Classification of RFID Authentication Protocols

- Based on the required resources on ***tags***

Category	**Resources**	Application Examples
***full-fledged* class**	Symmetric encryption, asymmetric algorithms, biometric	E-passport Infineon SLE 66CLX641P 
***simple* class**	Hash function, optional symmetric encryption, but not public key algorithms	Access control, express pass Mifare card S50 
***lightweight* class**	Random number generator; optional ultra-light hash function	Supply chain management, EPC Class 1 Gen 2 tag (40,000 gates) 
***Ultra-lightweight* class**	Only bit-wise operations like AND, OR, NOT	Supply chain management Gen 1 tag (12,000 gates) 

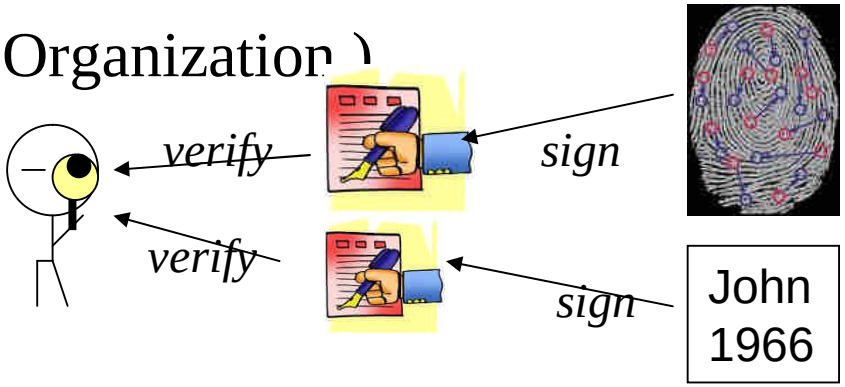
Full-Fledged Authentication Class

- E-passport

  ICAO（International Civil Aviation Organization）

  1. Passive Authentication

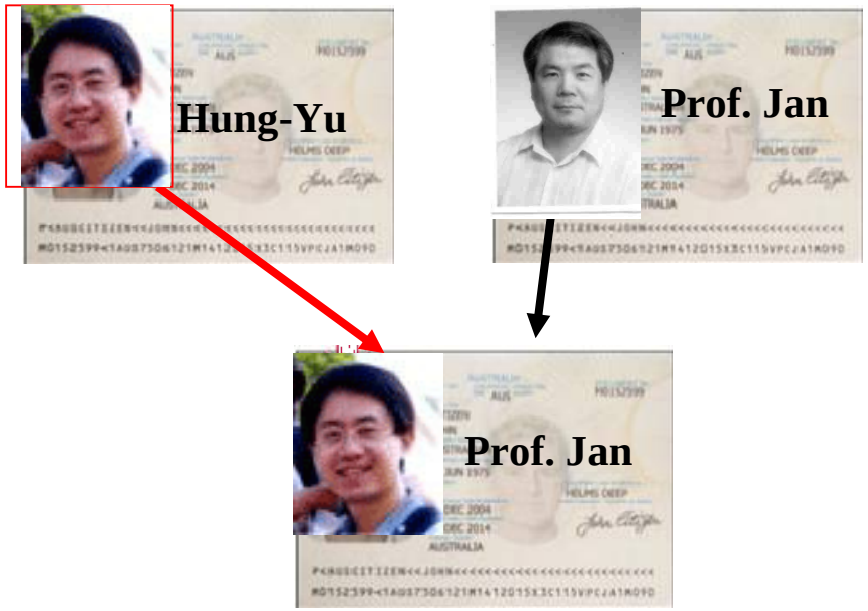
     only authenticate the data



2003 version: separate signing

counterfeiting

un-authorized disclosure, tracking



2004 version: joint signing

un-authorized disclosure, tracking

Full-Fledged Authentication Class

- E-passport
  2. Basic Access Control

Entropy of key is not enough
Key & data can be re-used once read

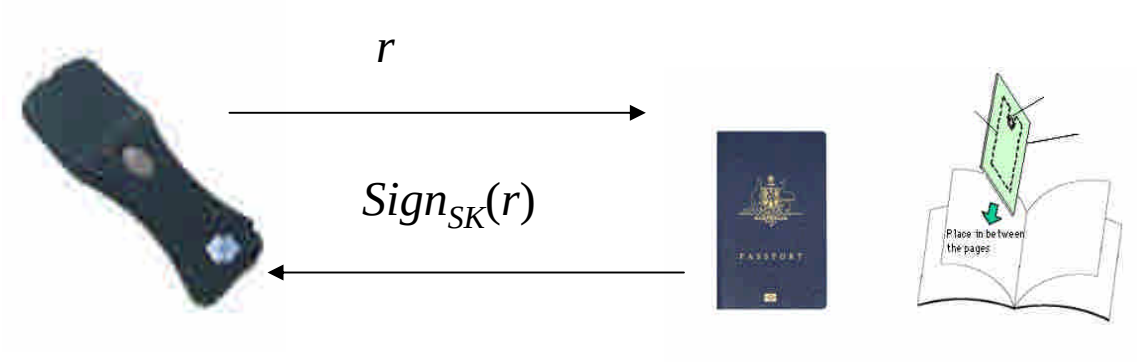
MRZ（Machine-Readable Zone)
Name, sex, birthday, expire date, …

Full-Fledged Authentication Class

- E-passport

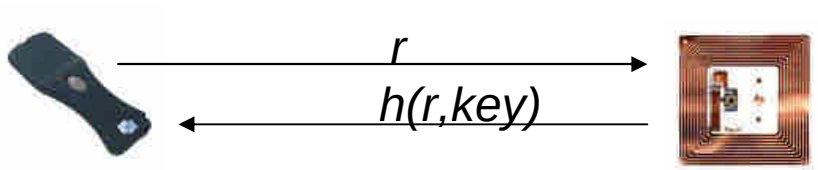
3. Active Authentication

anti-cloning,
does not prevent un-authorized reading
optional with Basic Access Control

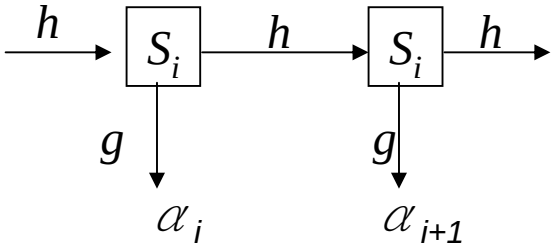


Simple Authentication Class

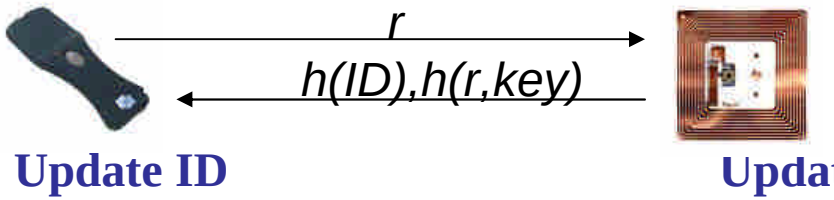
- Hash function, optional symmetric encryption, but not public key algorithms
- Weis 2003



- Ohkubo et al 2003



- Henrici et al., 2004 [varying identifier]

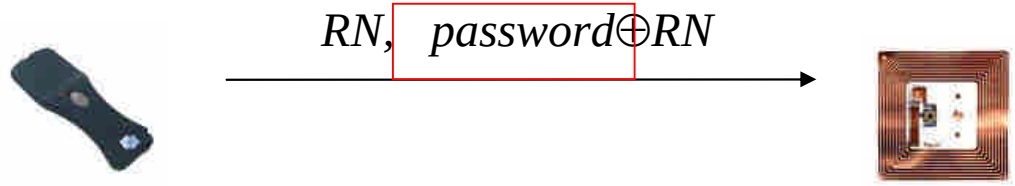


- Challenges

  efficiency + Forward secrecy + DOS attack resistance

Lightweight Authentication Protocol

- Random number generator; *optional ultra-light hash function*
- EPC Class 1 Gen 2



Password disclosure

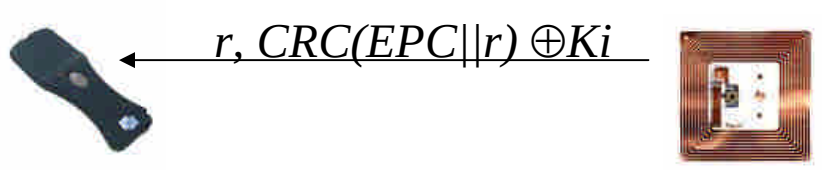
D. N. Duc, J. Park, H. Lee and K. Kim (2006)

Lightweight Authentication Protocol

- Duc et al. 2006

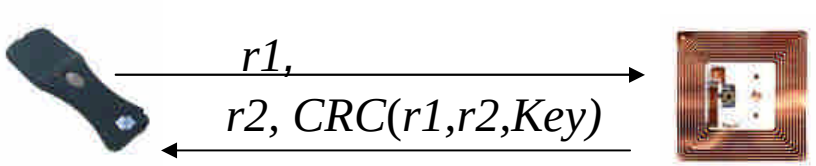
  No forward secrecy,

  No DOS resistance, spoofing



- Chien & Chen 2007

  Spoofing



- Challenges

  lightweight resources + authentication + forward secrecy + …

Ultra-Lightweight Authentication Protocol

- Only bit-wise operations- AND, OR, NOT, …
- Peris-Lopez et al.'s LMAP, EMAP, M2AP series 2006~2007
- *No protection of authentication,*

Integrity, DOS attack, spoofing

$$\mathrm{Re}ader \rightarrow Tag : A \| B \| C$$

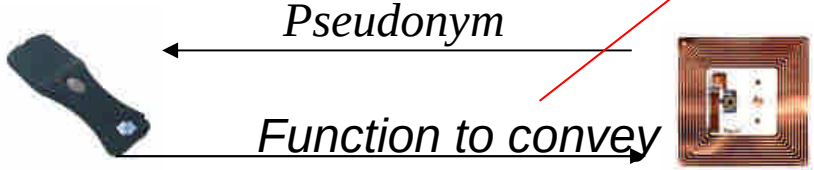
$$Tag \rightarrow \mathrm{Re}ader : D$$

$$A = IDS_{tag(i)}^{(n)} \oplus K1_{tag(i)}^{(n)} \oplus n1$$

$$B = (IDS_{tag(i)}^{(n)} \vee K2_{tag(i)}^{(n)}) + n1$$

$$C = IDS_{tag(i)}^{(n)} + K3_{tag(i)}^{(n)} + n2$$

$$D = (IDS_{tag(i)}^{(n)} + ID_{tag(i)}) \oplus n1 \oplus n2$$

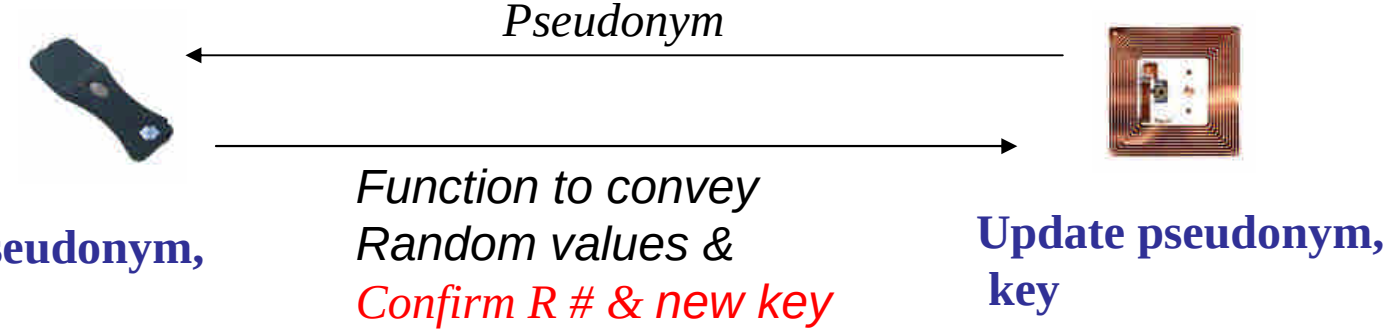


Update pseudonym, key

Update pseudonym, key

Ultra-Lightweight Authentication Protocol

Chien 2007



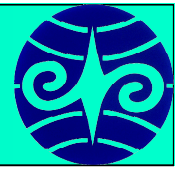
Entropy is not enough

(*96 possibilities for Gen 2*)

- **Challenges**

  avalanche effect or *ultra-lightweight hash*

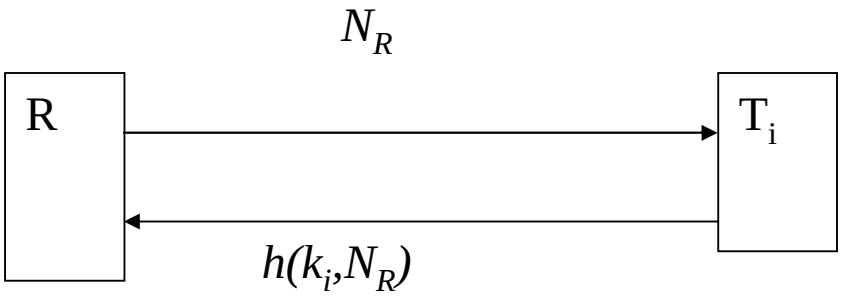
Techniques to authenticating RFID



- *Simple Challenge/Response approach*
- *Tree walking approach*
- *Hashing Chain approach*
- *Varying Pseudonym approach*

Techniques to authenticating RFID

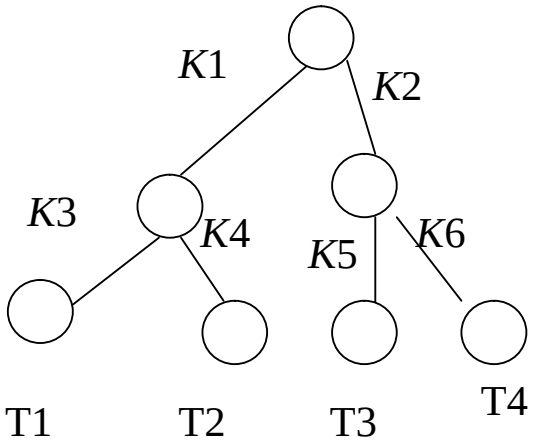
- **Simple challenge-response approach** (Rhee et al. 2005; Yang-Ren-Kim, …)

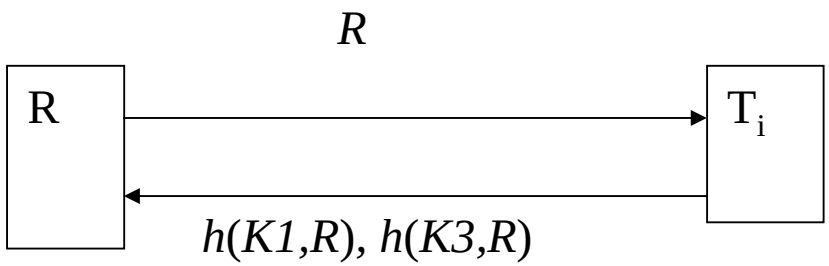


- *tag's storage space is* O(*1*) *but the computational cost for identifying a tag is* O(*n*)

Techniques to authenticating RFID

- **Tree-walking approach** (Molnar and D. Wagner 2005; Wang et al. 2007; Lu et al. Percom2007)



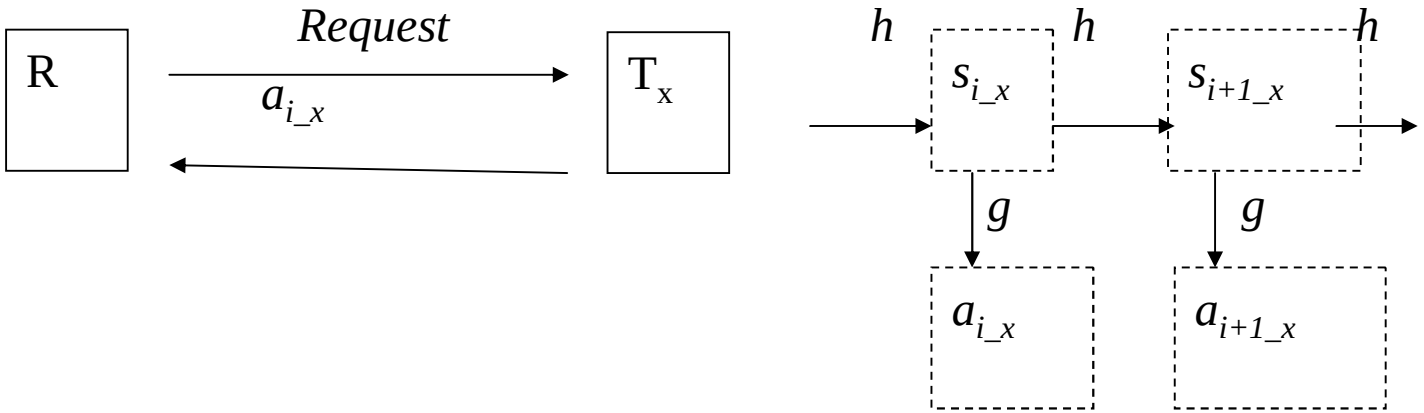


tag's storage space is O(log *n*) → O(1)

but the computational cost for identifying a tag is O(log *n*)

Techniques to authenticating RFID

- **Hash chains approach** (Ohkubo et al. 2003; Avoine et al. 2005)

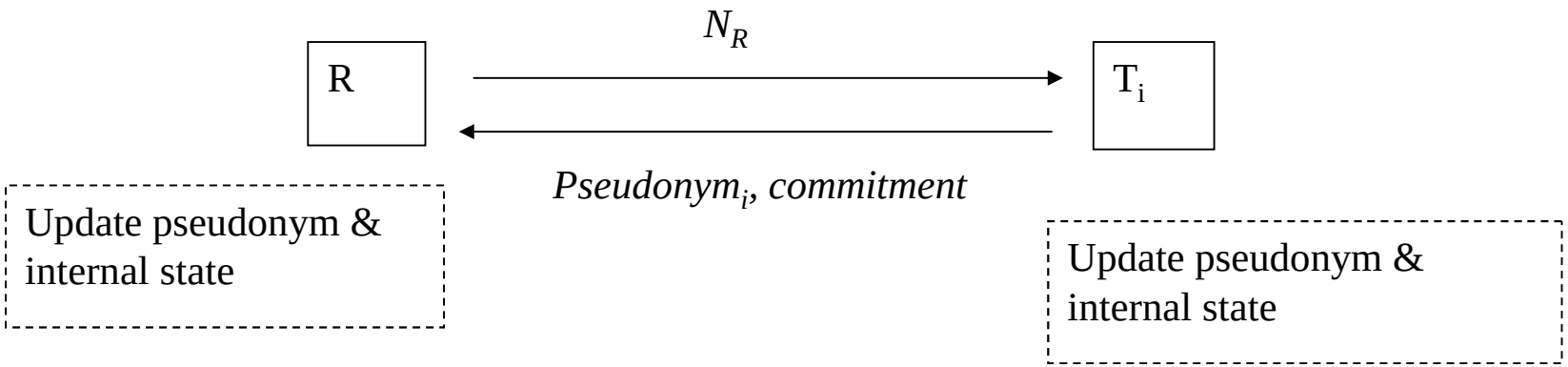


- - *forward secrecy*
- *tag's storage space is* O(*1*)

  but the computational cost for identifying a tag is O(*nm*)
- techniques to improve the computational at the cost of storage

Techniques to authenticating RFID

- **Varying Pseudonym (VP) approach (**Henrici and MÄuller; Peris-Lopez et al., Chien; Lee**)**



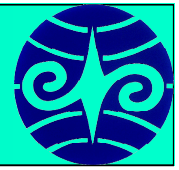
— *tag's storage space is* O(*1*)

but the computational cost for identifying a tag is O(*1*)

— Challenges

Resistance to DOS attack

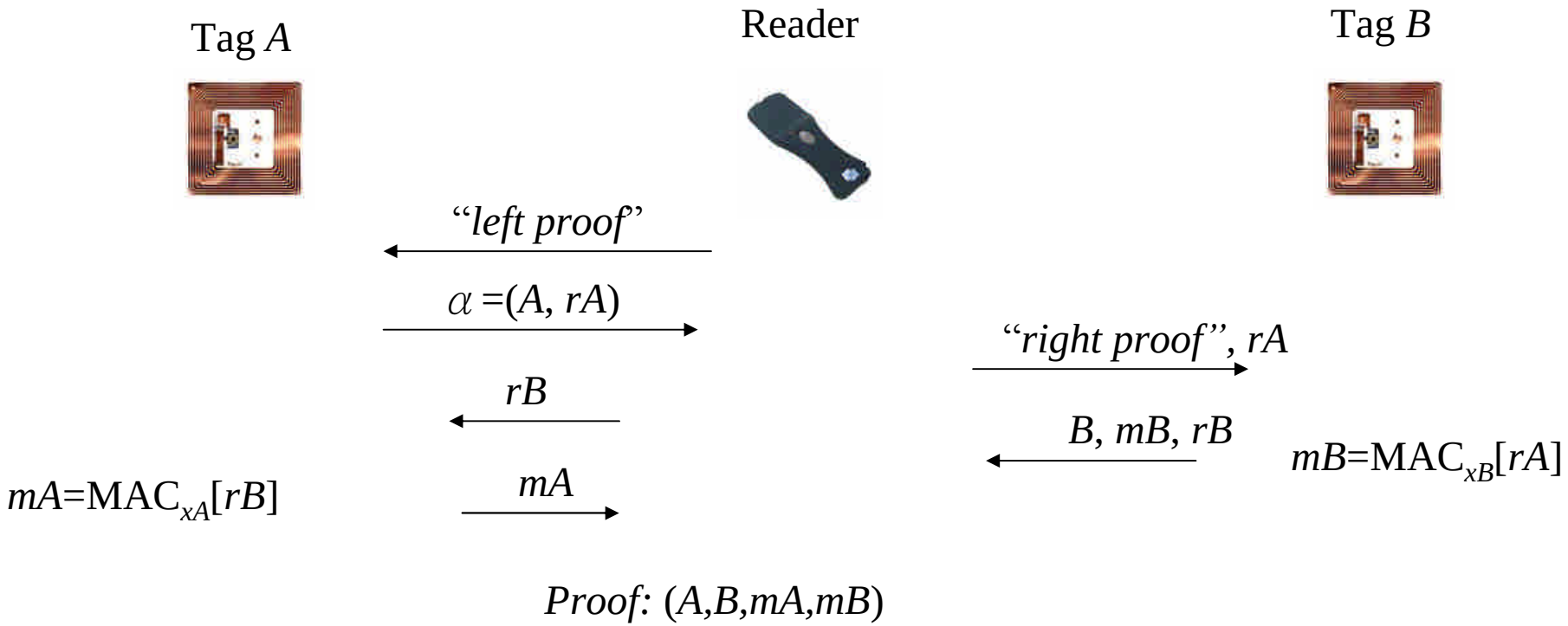
Grouping (Yooking) & Searching



- *Similar to pure authentication*

Yooking (Grouping)

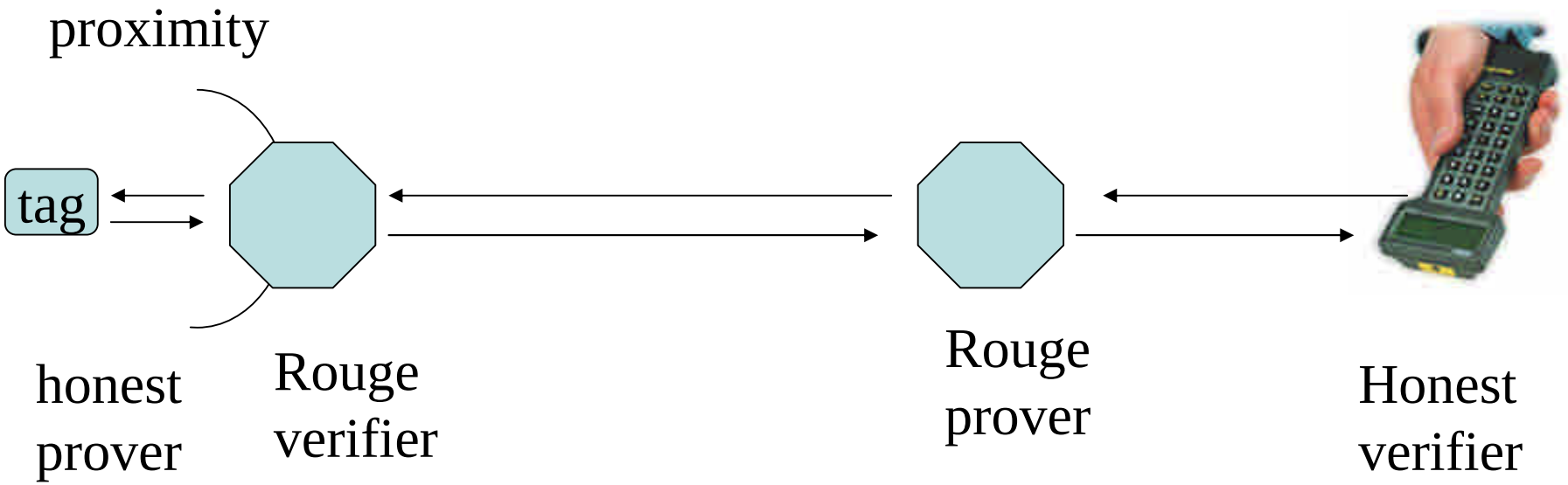
- Juels 2004



Saito & Sakurai 2005 ➔ *replay attack*

Various Relay attacks

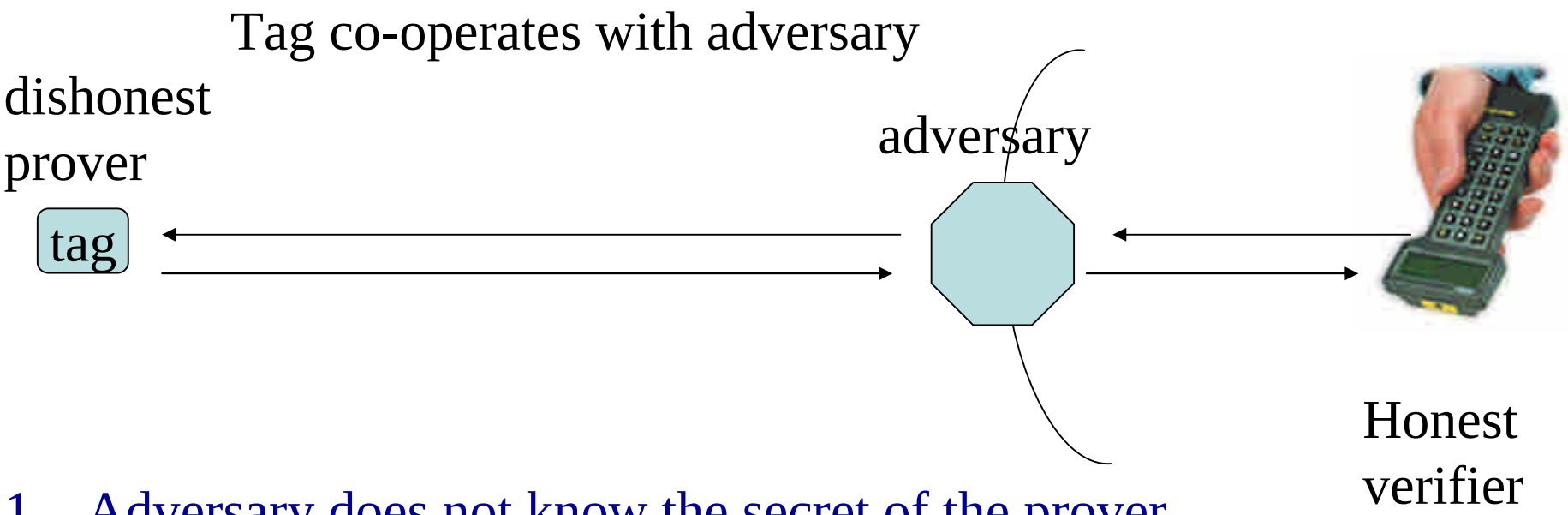
- Mafia (man-in-the-middle attack)



1. *No encryption could prevent this attack*
2. Brands and Chaum's distance bounding protocol

Various Relay attacks

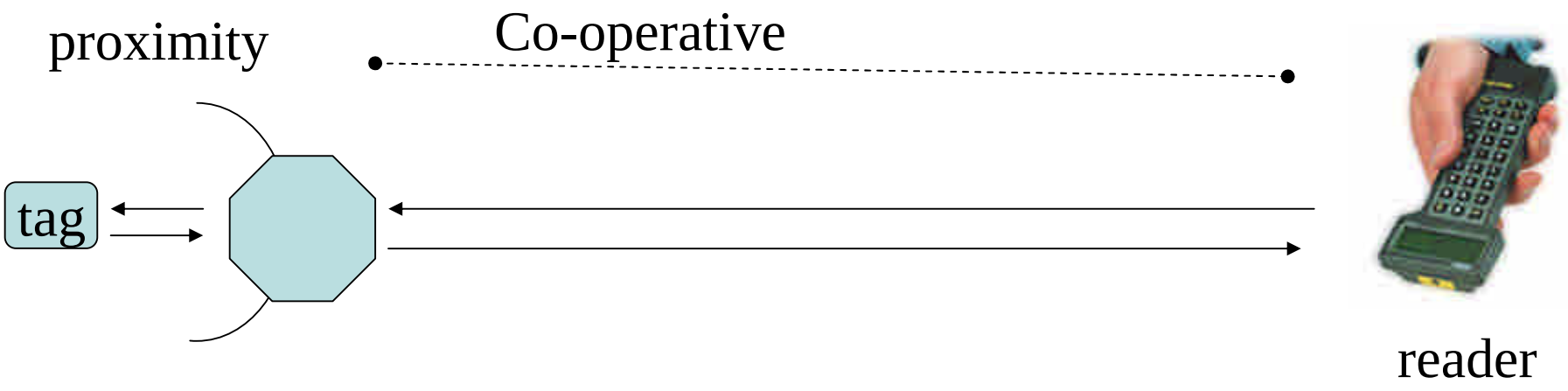
- Terrorist fraud attack



1. Adversary does not know the secret of the prover

Various Relay attacks

- *Jui-Chuan Hung & Chien reported*

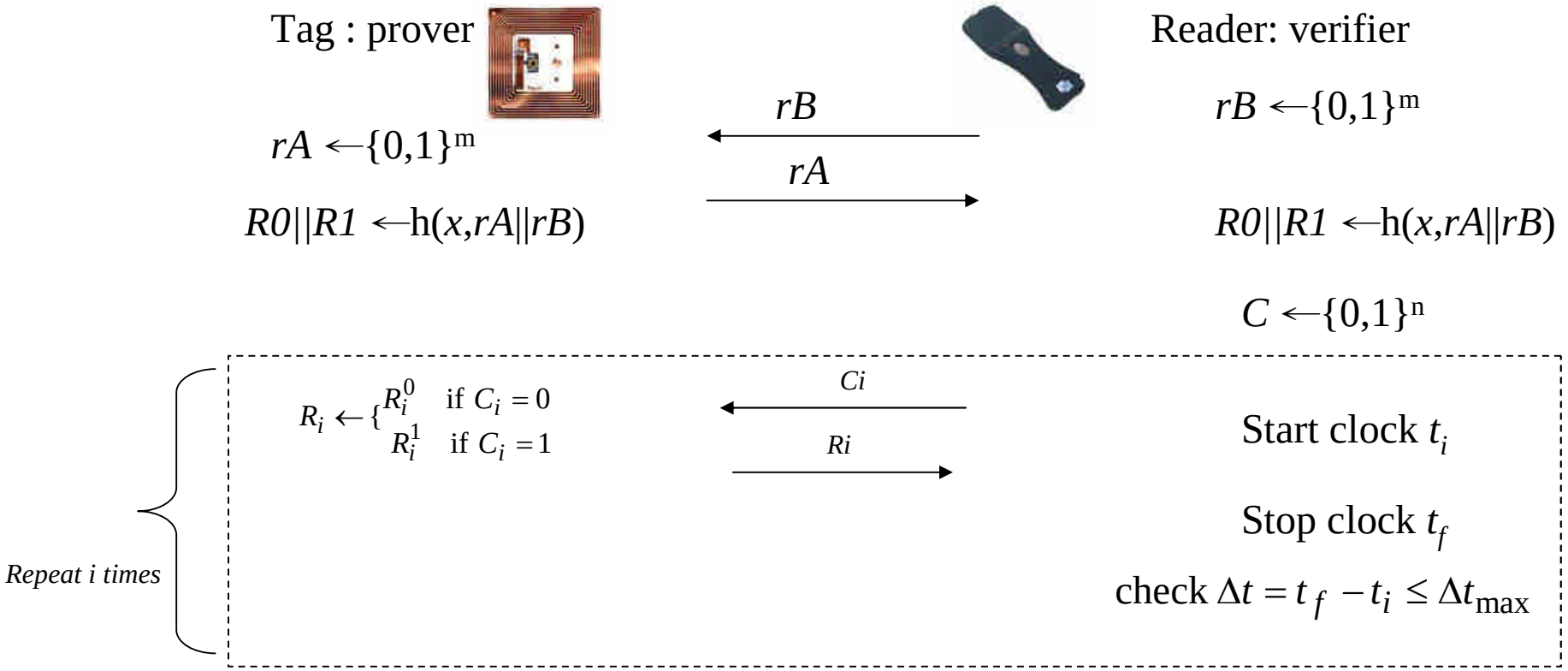


Possible vulnerable system: credit card, building access, passport

Countermeasures to Relay Attacks

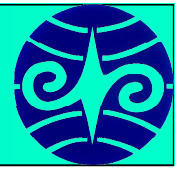
- Distance bounding protocol

  Hancke & Kuhn 2005



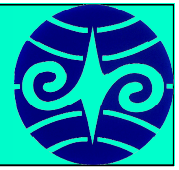
Secure against mafia attack, *but vulnerable to terrorist attack*

Various Relay Attacks



- Distance bounding protocol
  - *efficient enough for low-cost tag*?

Conclusions



- *Many Potential RFID Applications*, ***but …***

- Ultra-lightweight hash function
- Efficient distance bounding protocol
- New technique to authenticate the tag
- Formal Proof Model
- …..

Thanks for Listening