

MOBISSEC 

JUNE 3-5, 2009

TURIN, ITALY

Providing strong Security and high Privacy in low-cost RFID networks

Mathieu DAVID - Neeli R. Prasad

Aalborg University

June 4, 2009



Table of contents

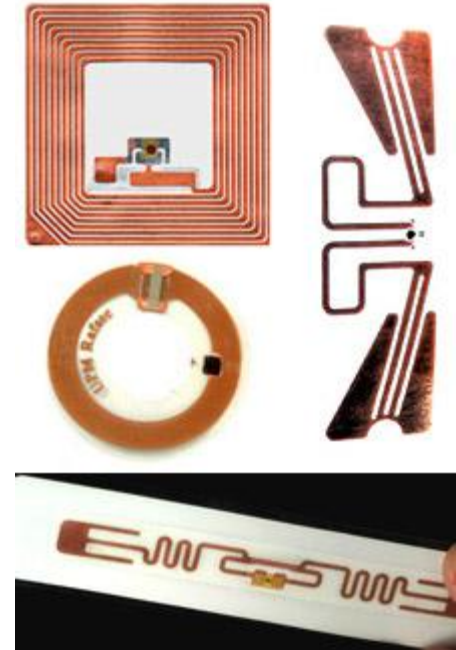
- **Introduction** to RFID Networks
- **Challenges**
- **Security Protocol**
- **Security Analysis**
- **Conclusion & Future Works**

Introduction to RFID Networks

Characteristics of RFID Tags:

- Ultra low computational capabilities
- Very Limited memory resources
- Very Limited energy resources

Architecture (simplified):



Introduction

Challenges

Security
Protocol

Security
Analysis

Conclusion

Challenges

Watch

Phone

Food

Clothes

Bags



Credit cards

Drinks (Bottles, Cans)

Laptop

Glasses

Wallet

Pencils

The Internet of Things

→ Need for security to ensure the consumer privacy

Introduction

Challenges

Security Protocol

Security Analysis

Conclusion

Security Protocol



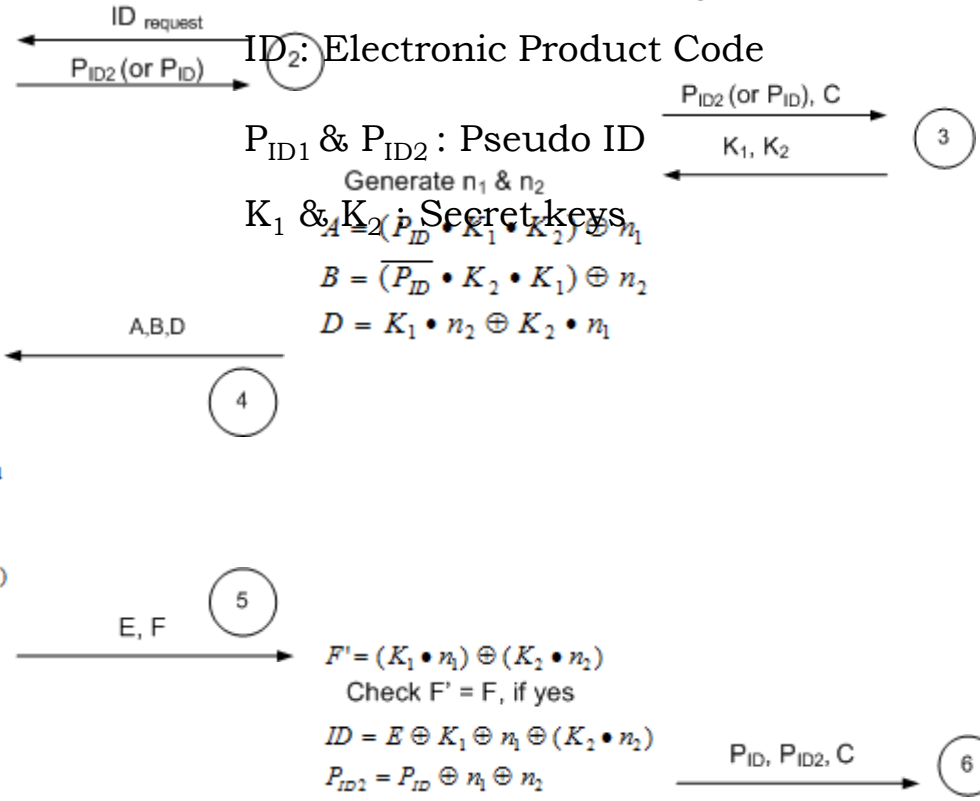
Introduction

Challenges

Security Protocol

Security Analysis

Conclusion



ID₂: Electronic Product Code

P_{ID1} & P_{ID2}: Pseudo ID

Generate n₁ & n₂

K₁ & K₂: Secret keys

$$A = \overline{(P_{ID} \cdot K_1 \cdot K_2)} \oplus n_1$$

$$B = \overline{(P_{ID} \cdot K_2 \cdot K_1)} \oplus n_2$$

$$D = K_1 \cdot n_2 \oplus K_2 \cdot n_1$$

$$n_1 = A \oplus (P_{ID} \cdot K_1)$$

$$n_2 = B \oplus (\overline{P_{ID}} \cdot K_2)$$

$$D' = K_1 \cdot n_2 \oplus K_2 \cdot n_1$$

Check D' = D, if yes

$$E = (K_1 \oplus n_1 \oplus D) \oplus (K_2 \cdot n_2)$$

$$F = (K_1 \cdot n_1) \oplus (K_2 \cdot n_2)$$

$$P_{ID2} = P_{ID} \oplus n_1 \oplus n_2$$

$$F' = (K_1 \cdot n_1) \oplus (K_2 \cdot n_2)$$

Check F' = F, if yes

$$ID = E \oplus K_1 \oplus n_1 \oplus (K_2 \cdot n_2)$$

$$P_{ID2} = P_{ID} \oplus n_1 \oplus n_2$$

Security Analysis

Introduction

Eavesdropping It is not possible to determine the values of the secrets keys or the ID of the tag, since the messages are encrypted (A, B, D, E and F).

Relay attack Impossible because tag and reader don not exchange data to authenticate each others directly. Any minor change in those values will be detected.

Challenges

Unauthorized tag reading and tag cloning Solved through the use of authentication.

Security Protocol

Tracking Impossible to track the tags over time.

However, between two successful authentications, a malicious reader will always receive either P_{ID} or P_{ID2} from its requests.

Replay attack The malicious tag won't be able to retrieve any information from A, B and D.

Security Analysis

De-synchronization attack The check of D (with D') and F (with F') prevent this kind of attack. If it is updated by mistake, the old value (P_{ID}) will be used to recover from the attack.

Forward Security It is impossible to find the previous data, since every exchange of data includes two random numbers.

Conclusion

Disclosure attack Any change is detected and the attacker won't receive any answer.

Conclusions

- Ultra-lightweight protocol (uses only bitwise operations)
- Secure against any attack over the radio
- Easy implementation on low-cost RFID Tags

Future Works

- Integrate a hash function to the protocol to remove the tracking issue
- Implementation in a real case scenario with multiple tags.
- Serverless protocol

Introduction

Challenges

**Security
Protocol**

**Security
Analysis**

Conclusion



Advanced Sensors and lightweight Programmable middleware for Innovative Rfid Enterprise applications

- Project supported by the European Commission (FP7)
- 10 partners within Europe
 - Aalborg University (DK)
 - INRIA (FR)
 - Université Joseph Fourier (FR)
 - Athens Information Technology (GR)
 - Instituto de telecomunicacoes (PT)
 - Sensap microsystems (GR)
 - Pôle Tracabilité (FR)
 - Open Source Innovation (UK)
 - Melexis (CH)
 - UEAPME (EU)

Aim

Programmable, Open Source, lightweight, royalty-free, **privacy-friendly**, standards-compliant, scalable, integrated and intelligent **RFID Middleware for SME**

Thank you
for
your attention

