BCRYPT

Belgian Science Policy

Belgian Fundamental Research on Cryptology and Information Security

KATHOLIEKE UNIVERSITEIT LEUVEN

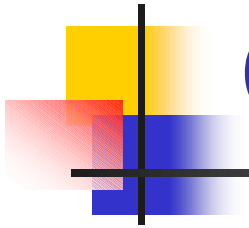
Designing Low-Cost Untraceable Authentication Protocols for RFID

Dave Singelée

IFIP WG 11.2 Seminar

Istanbul

June 07, 2010



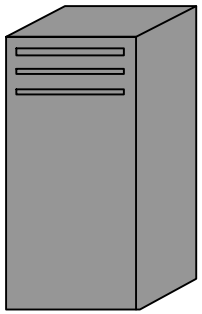
Outline of the talk

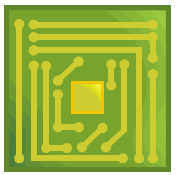
- Introduction
- RFID authentication protocols
  - Security requirements
  - Privacy requirements
  - Implementation requirements
- ECC-based RFID authentication protocols
- Design challenges
- Conclusion

RFID technology

- Radio Frequency Identification

- RFID setup
  - Back-end server
  - Reader
  - Tag





Online vs offline scenario

- Online

- Offline

RFID tags

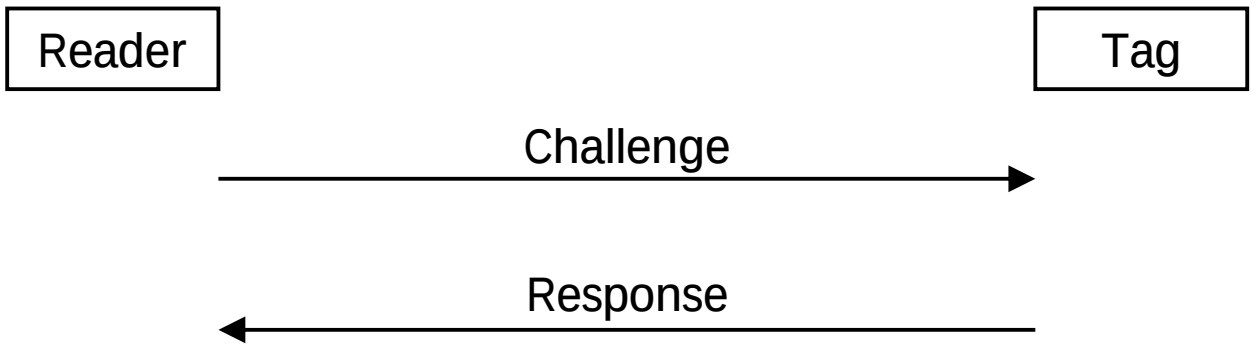
- Various types of tags

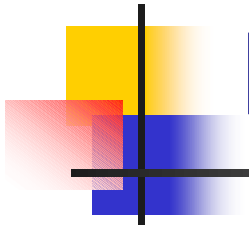



1. Passive tag
2. Battery assisted (BAP)
3. Active tag with onboard power source

RFID authentication protocols

- Tag proves its identity
- Challenge-response protocol



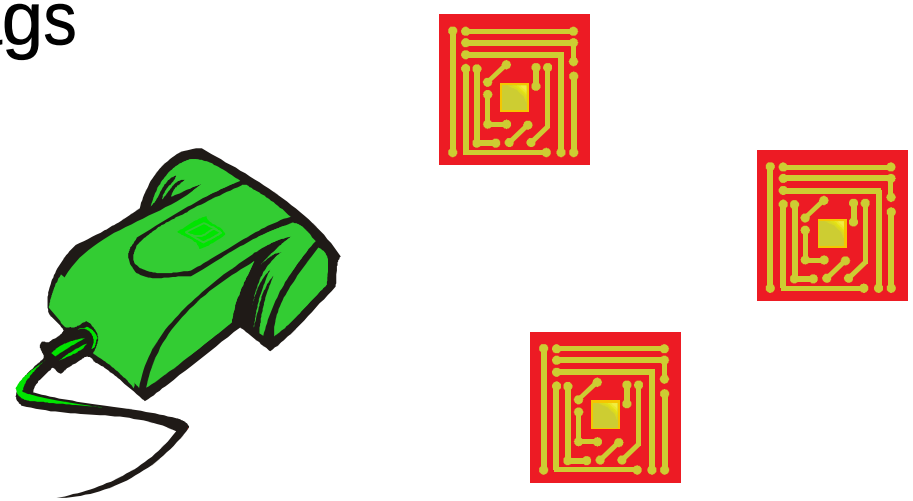


Requirements

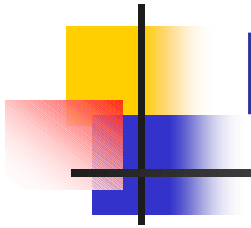
- Security
  - Entity authentication
- Privacy
  - Untraceability
- Implementation issues
  - Scalability
  - Low-cost

RFID security problems (I)

- Impersonation attacks
  - Genuine readers
  - Malicious tags



=> **Tag-to-server authentication**

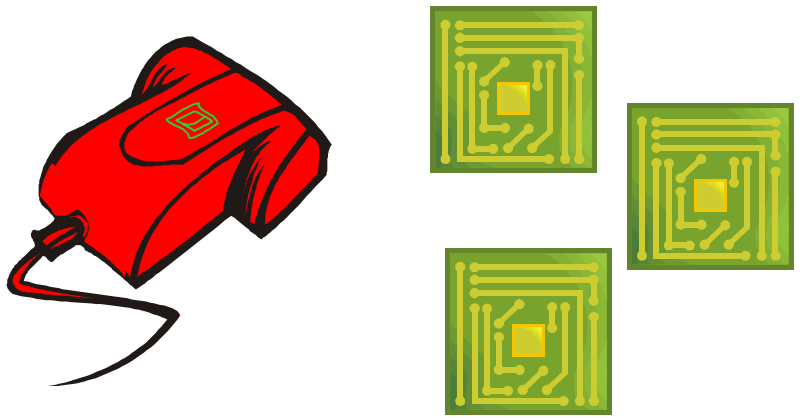


RFID security problems (II)

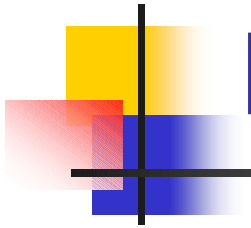
- Eavesdropping
- Replay attacks
- Man-in-the-middle attacks
- Cloning
- Side-channel attacks
- ...

RFID privacy problems (I)

- RFID Privacy problem
  - Malicious readers
  - Genuine tags



=> **Untraceability**

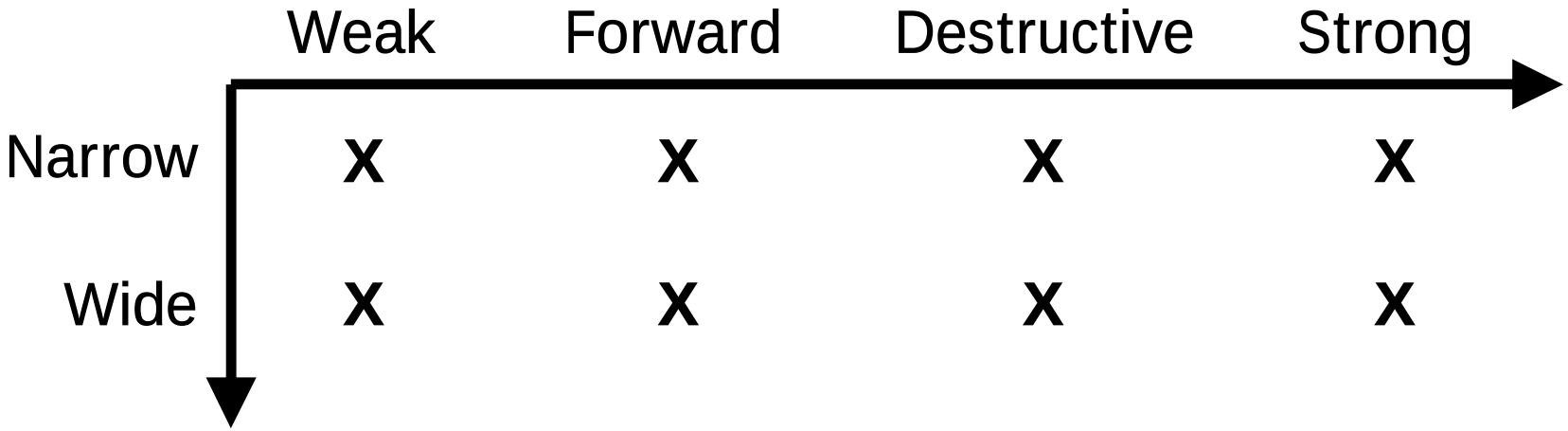


RFID privacy problems (II)

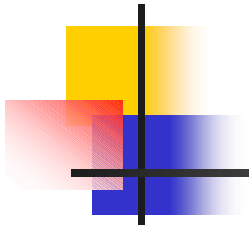
- Anonymity
  - The (fixed) identity of a tag must be impossible to determine
- **Untraceability**
  - Inequality of two tags: the (in)equality of two tags must be impossible to determine
- Untraceability > anonymity

RFID privacy problems (III)

- Theoretical framework
- Vaudenay [ASIACRYPT '07]:
  - 8 privacy classes



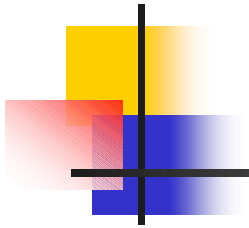
- Public-key cryptography needed to achieve certain privacy properties!!!



Implementation issues

- Scalability
- Low-cost implementation
  - Memory
  - Gate area
- Lightweight
- Efficient

=> **Depends on cryptographic building blocks used in the protocol**

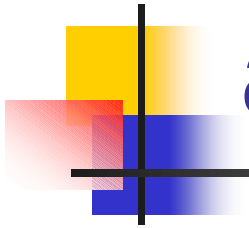


Implementation cost

- Symmetric encryption
  - AES: **3-4 kgates**
- Cryptographic hash function
  - SHA-3: **10 – 30 kgates**)
    [ECRYPT II: SHA-3 Zoo]
- Public-key encryption
  - Elliptic Curve Cryptography (ECC): **11-15 kgates**

=>Public key cryptography is suitable for RFID

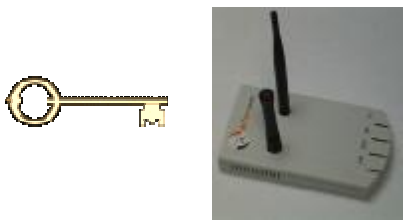
ECC-based RFID authentication protocols



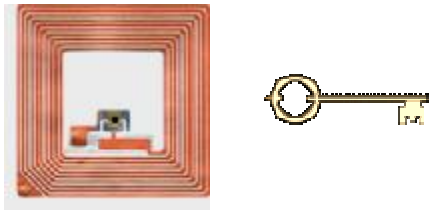
- **Rely exclusively on ECC !!!**
  - Security requirements
  - Privacy requirements
  - Implementation requirements
- Schnorr protocol
- Randomized Schnorr
- ID-transfer scheme
- **...**

ID-transfer scheme [WISEC 2010]

Server: y, $X = x_1 P$



Tag: x_1, $Y = yP$



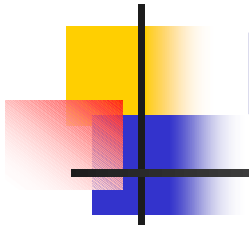
$r_{t1} \in \mathbb{Z}_q^*$, $T_1 \leftarrow r_{t1} P$

T_1 ←

$r_{s1} \in \mathbb{Z}_q^*$ → r_{s1}

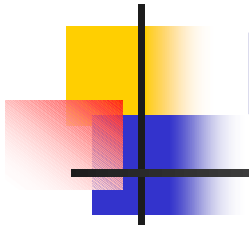
$T_2 \leftarrow (r_{t1} + r_{s1} x_1) Y$ ← T_2

$(y^{-1} T_2 - T_1)(r_{s1})^{-1} = x_1 P$



Design challenges (I)

- Readers share same private key y
  - Online scenario: OK
  - Offline scenario:
    - NOT OK
    - 1 compromised reader => no privacy
- How to solve the problem
  - Give unique private key to each reader?
  - Key updates / revocation / ... ??



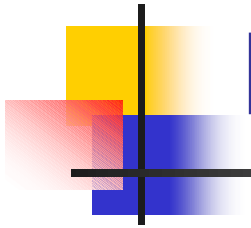
Design challenges (II)

- ECC-based RFID protocols in literature
  - Narrow-strong: OK
  - Wide-weak: NOT OK

- Man-in-the-middle attacks
- Insider attacks

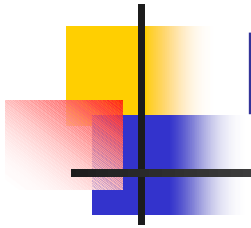
⇒ Increase privacy protection

⇒ Low cost solutions



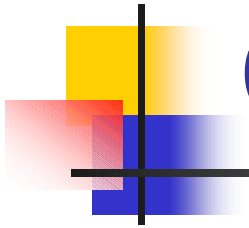
Design challenges (III)

- Secure and privacy-preserving extensions of basic RFID authentication protocols
  - Search protocol
  - Grouping proofs
  - ...
- Physical layer security
  - Distance bounding
  - Physical layer fingerprints
  - ...



Design challenges (IV)

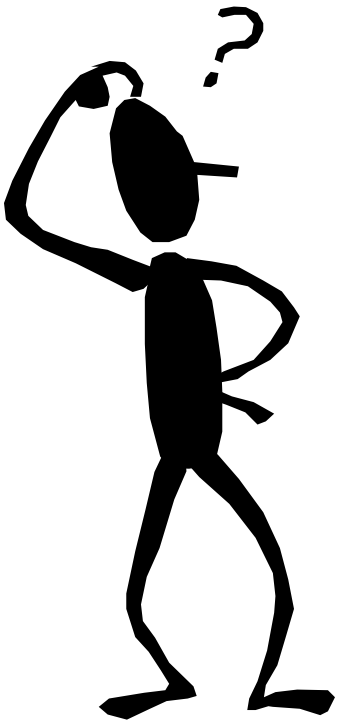
- Improve efficiency
  - Lower # EC point multiplications
  - Decrease communication cost
  - ...
- Further improve ECC hardware architecture
  - Area
  - Speed
  - Power consumption



Conclusion

- Security & privacy in RFID networks
- Need for public-key based RFID authentication protocols
- ECC is feasible on RFID
- Designing protocol is challenging task
  - Various open research problems

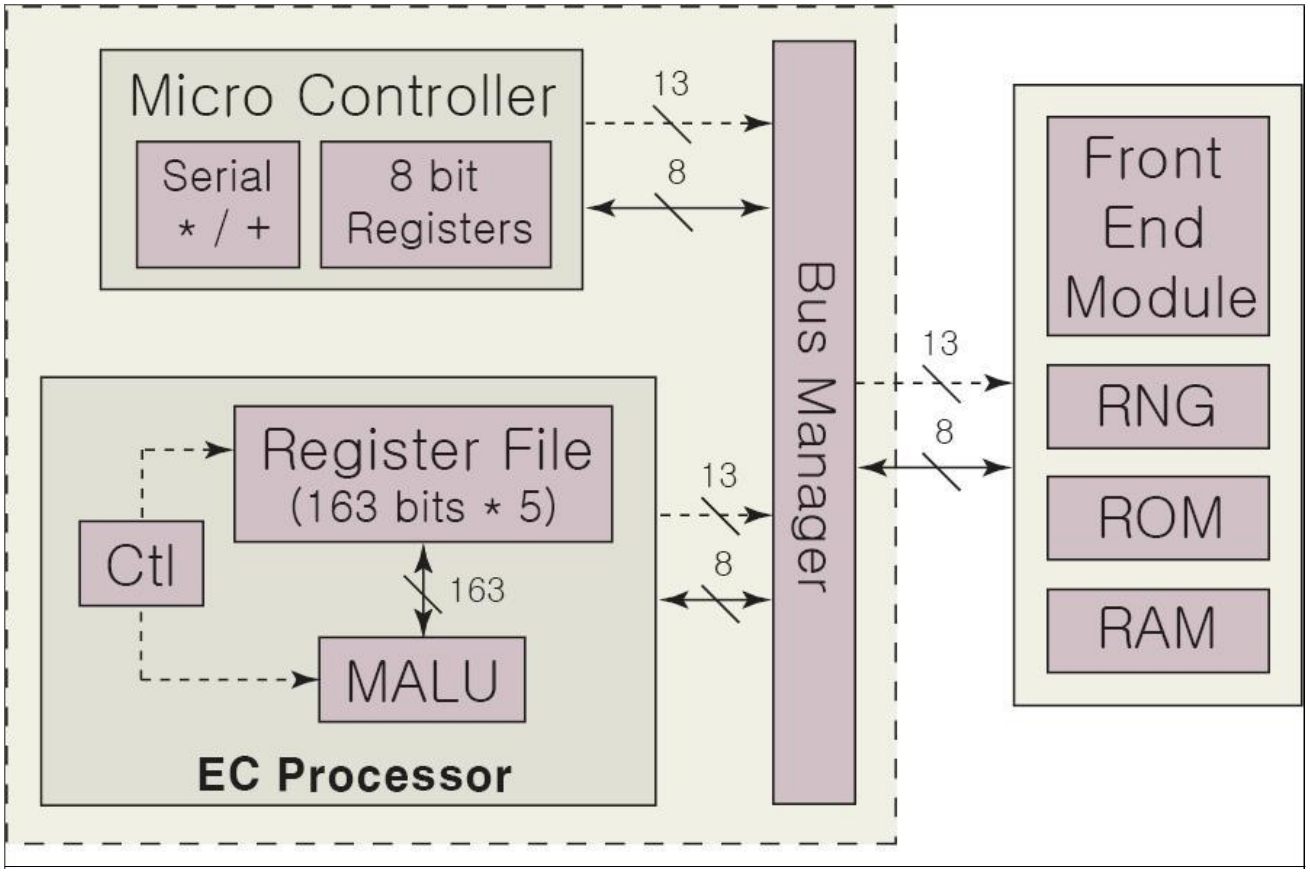
Questions??



Dave.Singelee@esat.kuleuven.be

EXTRA SLIDES

ECC hardware architecture



Performance results

Circuit Area (Gate Eq.)	14,566
Cycles for EC point multiplication	59,790
Frequency	700 KHz
Power	13.8 µW
Energy for EC point multiplication	1.18 µJ

Schnorr protocol [CRYPTO '89]

Server: $X = -xP$

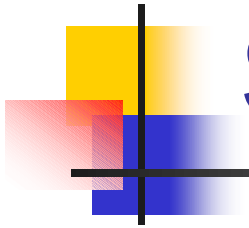
Tag: x

R_1 ← $r_1 \in \mathbb{Z}_q^*$, $R_1 \leftarrow r_1 P$

$r_2 \in \mathbb{Z}_q^*$ → r_2

v ← $v \leftarrow x r_2 + r_1$

$vP + r_2 X = R_1$



Schnorr protocol (II)

- Security: OK
- Privacy: vulnerable to tracking attacks

$$X = r_2^{-1} \cdot (R_1 - vP)$$

Randomized Schnorr [CANS '08]

Server: y, $X = xP$

Tag: x, $Y = yP$

$r_{t1}, r_{t2} \in \mathbb{Z}_q^*$

$T_1 = r_{t1}P \quad , \quad T_2 = r_{t2}Y$

T_1, T_2 ←

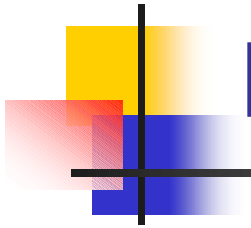
$r_{s1} \in \mathbb{Z}_q^*$

r_{s1} →

v ←

$v = r_{t1} + r_{t2} + x r_{s1}$

$r_{s1}^{-1} \cdot (vP - T_1 - y^{-1}T_2) = X$

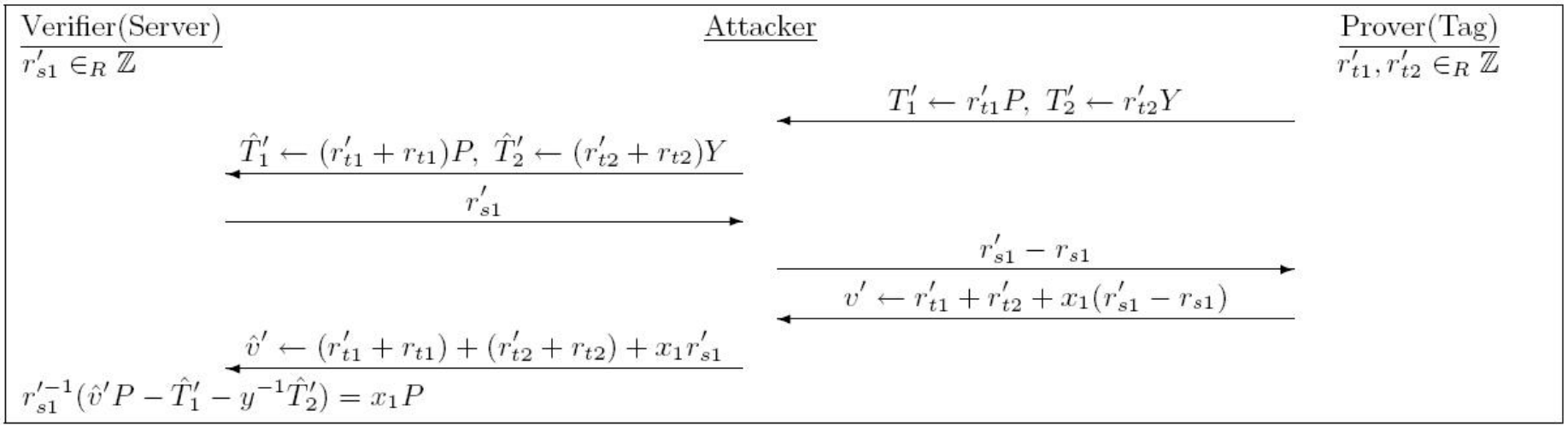


Randomized Schnorr (II)

- Security: OK
- Privacy
  - Narrow-strong
  - Not wide-weak: vulnerable to man-in-the-middle attack
    - Combine data from old protocol run with current protocol instance
    - Server accepts => same tag

    => Traceability

Randomized Schnorr (III)



ID-transfer scheme (protocol 1)

- Server's input: y
- Tag's input: x_1, $Y(=yP)$

	Verifier(Server)		Prover(Tag)
1)		$\xleftarrow{T_1}$	$r_{t1} \in_R \mathbb{Z}$, $T_1 \leftarrow r_{t1}P$
2)	$r_{s1} \in_R \mathbb{Z}$	$\xrightarrow{r_{s1}}$	
3)	$\dot{r}_{s1} \leftarrow x(r_{s1}P)$		$\dot{r}_{s1} \leftarrow x(r_{s1}P)$
4)		$\xleftarrow{T_2}$	$T_2 \leftarrow (r_{t1} + \dot{r}_{s1}x_1)Y$
5)	$(y^{-1}T_2 - T_1)\dot{r}_{s1}^{-1} = x_1P$		