Privacy Preserving Protocols

Workshop on Cryptography for the Internet of Things

Jens Hermans
KU Leuven - COSIC

20 November 2012

RFID

Car Keys

Access Control

Product Tracking

Why?

Industrial espionage

Why?

User privacy

Why?

User privacy

Why?

Wireless Gun

RFID Privacy: goals

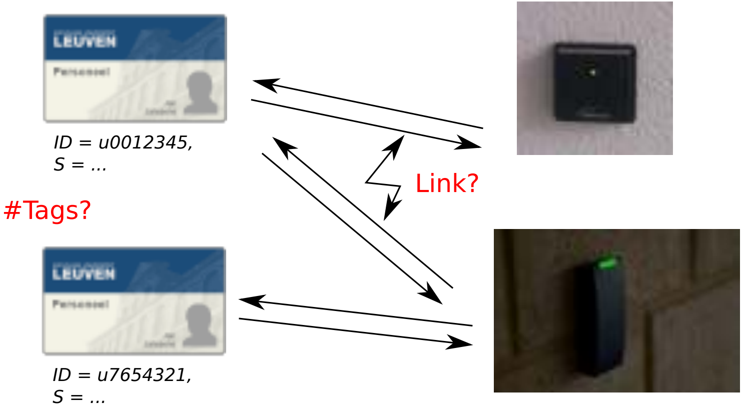
ID = u0012345,
S = ...

...

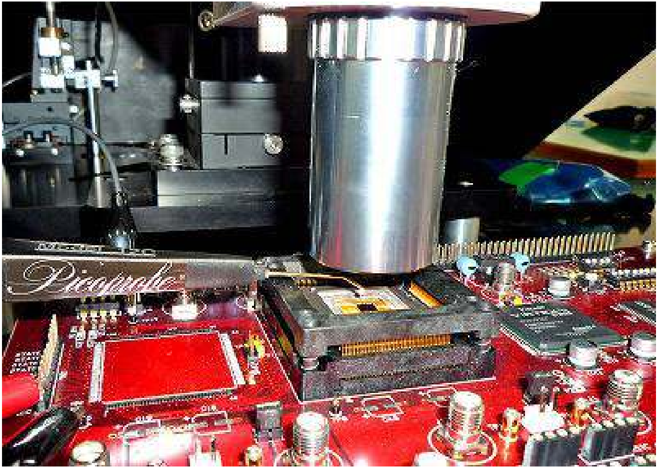
ID = ?

{ (ID=u0012345, P=...) , ...}

RFID Privacy: goals



Corrupting Tags



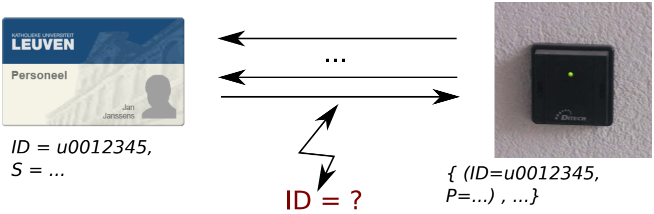
Different Privacy Solutions

- Protocol Level Privacy
- Kill Command
- Destroy Tag
- Shielding
- (Read Range Reduction)
- ...

Threat Analysis / Requirements

		Privacy: Low	Privacy: High
Security	Low	Supply Chain	Public Transport
Security	High	Car Keys	Payments Access Control Passports

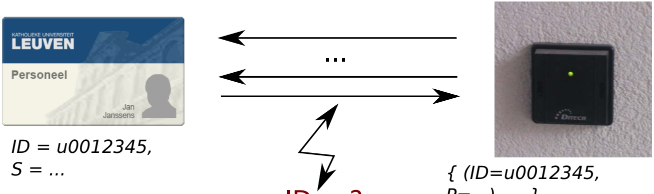
Protocol Analysis



Properties:

- Security
- Privacy: untraceability
- Allow corruption

Protocol Analysis



ID = u0012345,
S = ...

ID = ?

{ (ID=u0012345,
P=...) , ...}

Results

Many published protocols broken:
⇒ Lack of formal proofs!

Provable Security (Privacy)

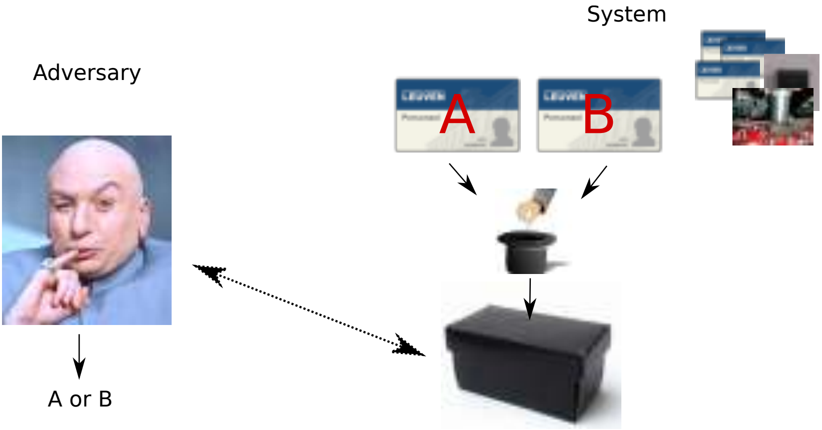
Provable Security (Privacy)

System

Adversary

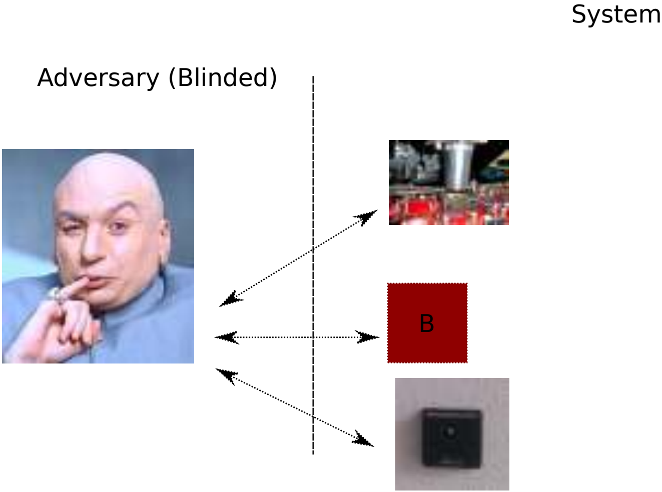
Adversary wins if ...

Juels-Weis model (2005)



Adversary wins if output is correct tag.

Vaudenay model (2007)



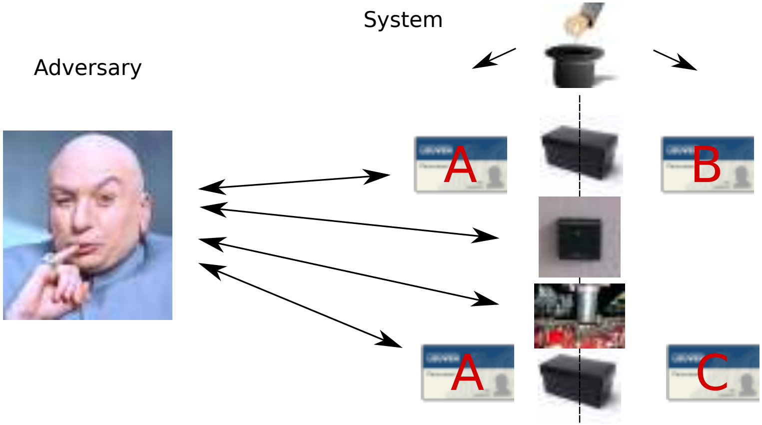
Adversary wins if output is *true* and not trivial

Privacy Model Hermans *et al.* (2011)

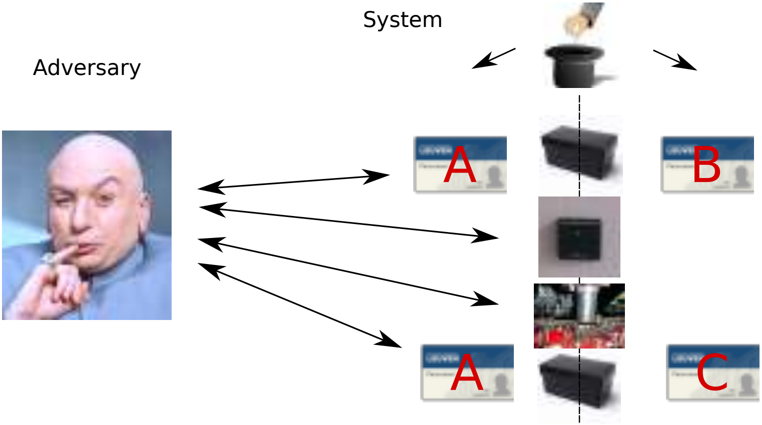
Design goals:

- Strong adversary: can always corrupt
- Solve issues with wide strong privacy
- Model 'reality'
- Easy to use

Privacy Model Hermans *et al.* (2011)



Privacy Model Hermans *et al.* (2011)

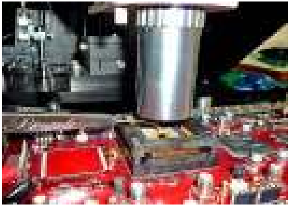


Adversary wins if random bit is guessed correctly.

Privacy Model Hermans *et al.* (2011)

New Features:

- corruption → on *real* tag
- wide strong privacy



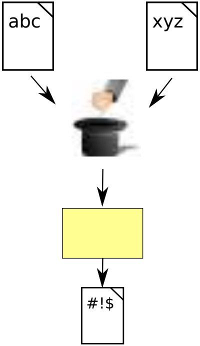
Features (reused):

- Virtual tag handles
- Indistinguishability based
- Single random bit for entire system

Indistinguishability

Encryption:

- RO
- IND-CPA
- IND-CCA
- IND-CCA2
- ...



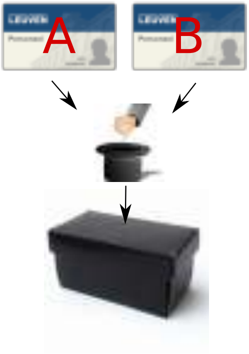
Privacy-models:

- Juels-Weis
- Vaudenay
- Hermans *et al.*

Indistinguishability

Encryption:

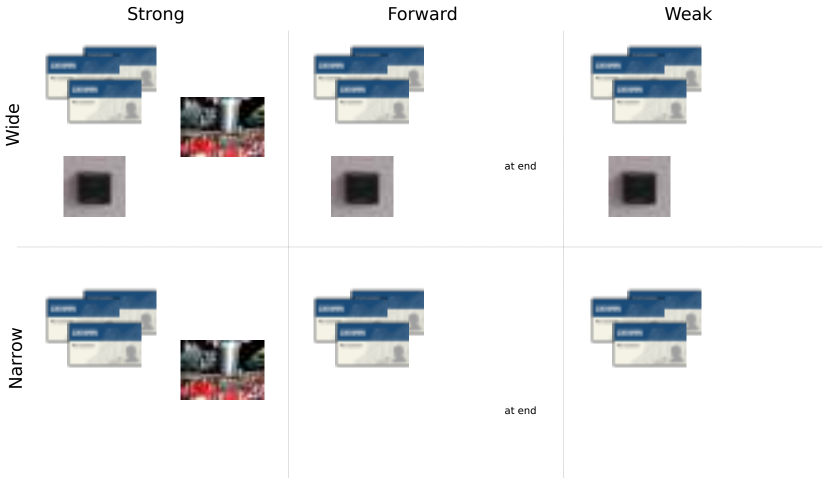
- RO
- IND-CPA
- IND-CCA
- IND-CCA2
- ...



Privacy-models:

- Juels-Weis
- Vaudenay
- Hermans *et al.*

Privacy Levels



Privacy Requirements

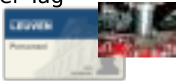
Privacy Level	**Application**
Narrow Weak	Supply Chain
Narrow Forward	Smart Products
Wide Weak	Car Keys
Wide Forward	Payments Access Tokens Passports Public Transport

Insider Attacks

System

Adversary

Insider Tag



Privacy Requirements

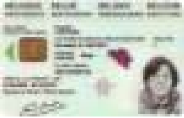
Privacy Level	**Application**
Narrow Weak	Supply Chain
Narrow Forward	Smart Products
Wide Weak	Car Keys
Wide Forward + Insider	Payments Access Tokens Passports Public Transport

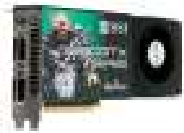
Privacy Requirements

Privacy Level	**Application**
Narrow Weak	Supply Chain
Narrow Forward	Smart Products
Wide Weak	Car Keys
~~Wide Forward + Insider~~ Currently: Wide Strong	Payments Access Tokens Passports Public Transport

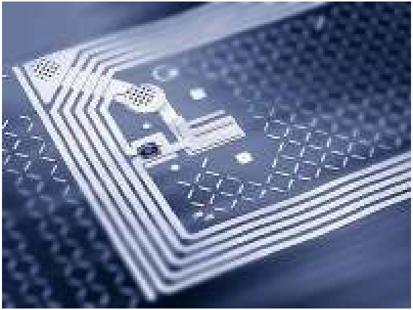
Lightweight Devices

$\leftrightarrow$





Lightweight Cryptography?



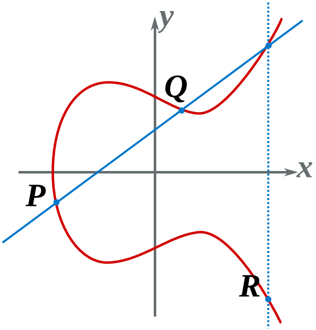
Limits:

- Area (€€€)
- Time
- Power
- Energy

Typical Ingredients for Protocols

Primitive	**Status**
RNG	OK?
Key Update	???
Block Cipher	OK
Hash Function	OK
ECC	OK
$\sum$	???

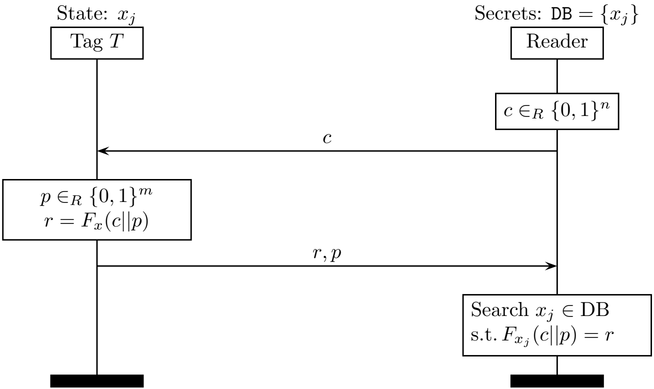
Lightweight Elliptic Curve Cryptography



Implementation [LBSV10]:

- Area (14.5 kGE)
- Time (85 ms)
- Power (13.8 μW)
- Energy (1.18 μJ)

PRF (Block cipher) based [ISO/IEC 9798-2]



Privacy

Wide-Weak

Symmetric Key and Efficiency

Damgård-Pedersen '08:

- Independent keys: inefficient $O(n)$
- Correlated keys:
  - efficient $O(\log(n))$
  - privacy loss

Symmetric Key and Efficiency

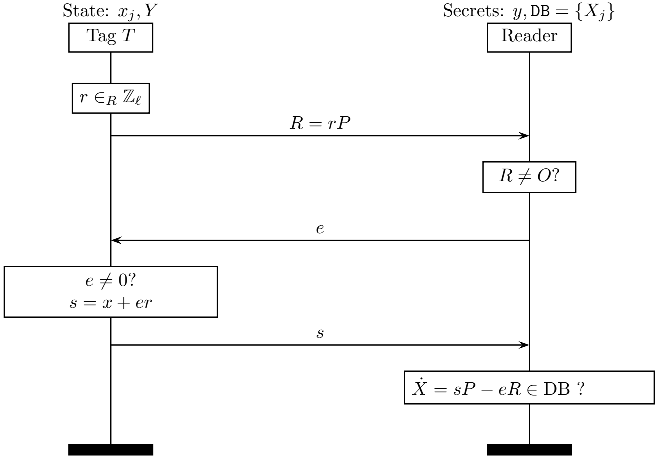
Damgård-Pedersen '08:

- Independent keys: inefficient $O(n)$
- Correlated keys:
  - efficient $O(\log(n))$
  - privacy loss

Key Updating

- Higher Privacy Level (narrow forward)
- Desynchronization Attacks / Efficiency Problems
- Implementation cost?

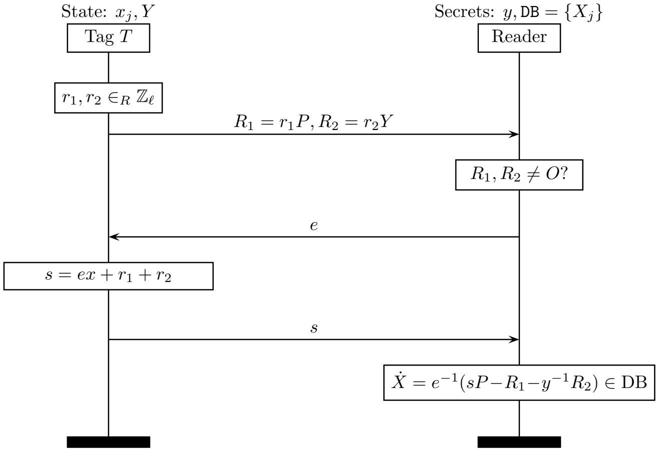
EC Schnorr Protocol



Privacy

None

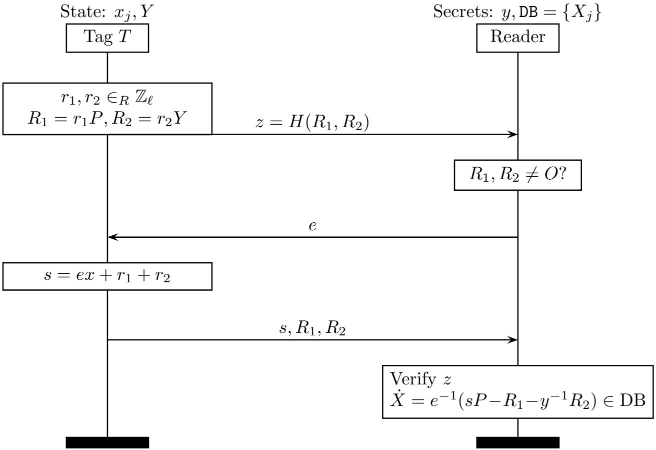
Randomized Schnorr [BCI08]



Privacy

Narrow Strong

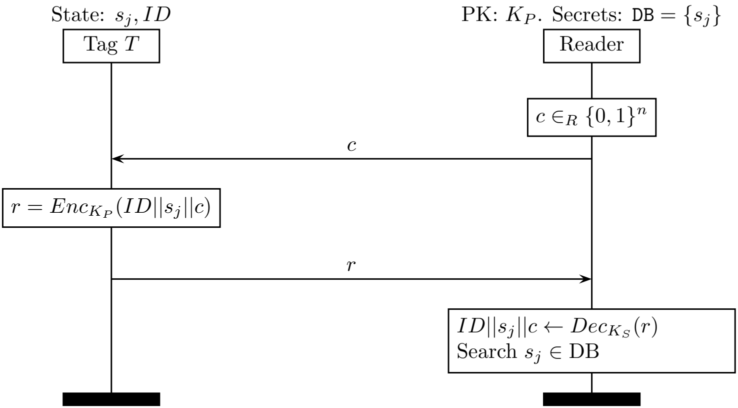
Randomized Hash GPS [BCI09]



Privacy

Narrow Strong and Wide Forward

IND-CCA2 Encryption [Vau07]



Privacy

Wide Strong

Performance

Protocol	Privacy	Ins.	Ext. Snd.	Operations
Schnorr	no	no	yes	1 EC mult
Randomized Schnorr	narrow-strong	no	yes	2 EC mult
Rand. Hashed GPS	narrow-strong wide-forward	no	yes	2 EC mult 1 hash

Performance

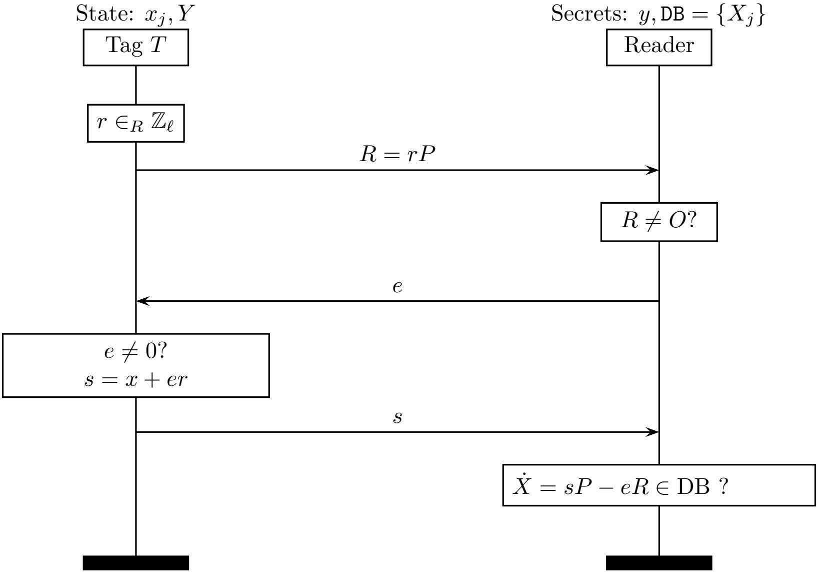
Protocol	Privacy	Ins.	Ext. Snd.	Operations
Schnorr	no	no	yes	1 EC mult
Randomized Schnorr	narrow-strong	no	yes	2 EC mult
Rand. Hashed GPS	narrow-strong wide-forward	no	yes	2 EC mult 1 hash
Vaudenay + DHIES	wide-strong	yes	no	2 EC mult 1 hash 1 MAC 1 symm enc
Hash ElGamal	wide-strong	yes	no	2 EC mult 1 hash 1 MAC

New Protocol [Peeters, Hermans 2012]

Design protocol:

- Correct
- Extended soundness
- (At least) Wide Forward + Insider privacy
- *Efficient*

EC Schnorr Protocol



Key Assumptions

Oracle Diffie-Hellman Assumption

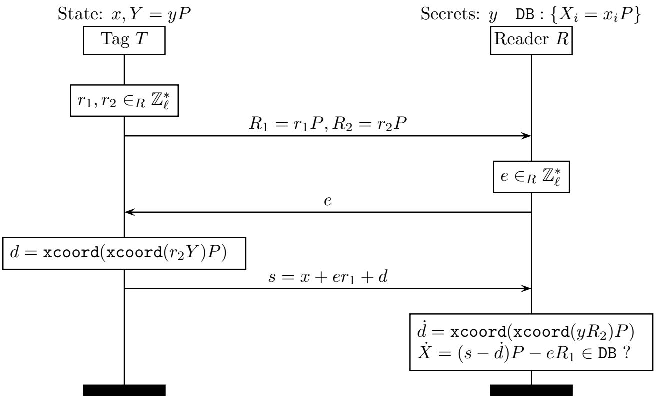
$$(A = aP, B = bP, abP) \sim (A = aP, B = bP, rP)$$

with extra $\mathcal{O}(Z) := \texttt{xcoord}(bZ)P$.

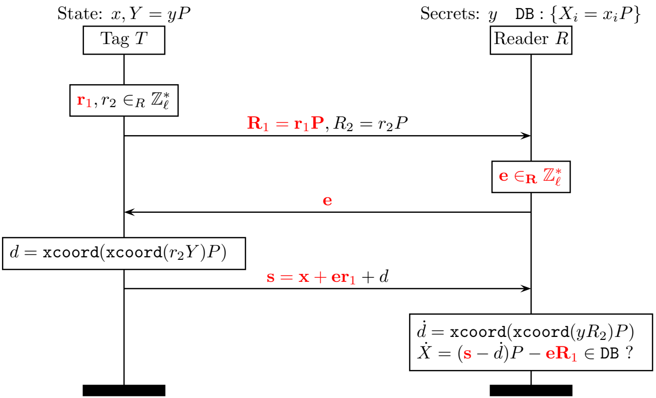
X Logarithm

$$\texttt{xcoord}(rP)P \sim r'P$$

New Protocol



New Protocol - Extended Soundness



Extended Soundness

Schnorr protocol $\Rightarrow$ extended soundness (OMDL assumption)

New Protocol - Privacy

State: $x, Y = yP$		Secrets: y $\mathtt{DB} : \{X_i = x_i P\}$
Tag T		Reader R
$r_1, \mathbf{r}_2 \in_R \mathbb{Z}_\ell^*$		
	$R_1 = r_1 P, \mathbf{R}_2 = \mathbf{r}_2 \mathbf{P}$ $\longrightarrow$	
		$e \in_R \mathbb{Z}_\ell^*$
	$\longleftarrow$ e	
$\mathbf{d} = \mathtt{xcoord}(\mathtt{xcoord}(\mathbf{r}_2 \mathbf{Y})\mathbf{P})$		
	$s = x + e r_1 + \mathbf{d}$ $\longrightarrow$	
		$\dot{\mathbf{d}} = \mathtt{xcoord}(\mathtt{xcoord}(\mathbf{y}\mathbf{R}_2)\mathbf{P})$ $\dot{X} = (s - \dot{\mathbf{d}})P - eR_1 \in \mathtt{DB}$?

Performance

Protocol	Privacy	Ins.	Ext. Snd.	Operations
Schnorr	no	no	yes	1 EC mult
Randomized Schnorr	narrow-strong	no	yes	2 EC mult
Rand. Hashed GPS	narrow-strong wide-forward	no	yes	2 EC mult 1 hash
Vaudenay + DHIES	wide-strong	yes	no	2 EC mult 1 hash 1 MAC 1 symm enc
Hash ElGamal	wide-strong	yes	no	2 EC mult 1 hash 1 MAC

Performance

Protocol	Privacy	Ins.	Ext. Snd.	Operations
Schnorr	no	no	yes	1 EC mult
Randomized Schnorr	narrow-strong	no	yes	2 EC mult
Rand. Hashed GPS	narrow-strong wide-forward	no	yes	2 EC mult 1 hash
Vaudenay + DHIES	wide-strong	yes	no	2 EC mult 1 hash 1 MAC 1 symm enc
Hash ElGamal	wide-strong	yes	no	2 EC mult 1 hash 1 MAC
Our Protocol - optimised version	wide-forward-insider wide-forward-insider	yes yes	yes yes	4 EC mult 2 EC mult

Summary

- Overview RFID Privacy Models & Privacy Levels
- Implementation Aspects
- RFID Protocols
- New Private & Efficient RFID Protocol

Future Perspectives

Privacy models

- ‘Fair’ comparison
- Restrictions on tag corruption
- Simulatability vs indistinguishability

Protocols

- New applications
- Other primitives $\rightarrow$ feasible?
- Analyze underlying assumptions (DDH-variants)

?