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
1 RFID Privacy
   Requirements

2 Privacy Models
   Protocol Analysis
   Provable Security (Privacy)
   Privacy Model
   Insider Attacks
   Requirements

3 Lightweight Cryptography

4 Existing Protocols

5 Protocol Design
   Design
   Performance

6 Conclusions and Future Perspectives
Why?

Industrial espionage
Why?

User privacy
Why?

User privacy
Why?

Wireless Gun
RFID Privacy: goals

\[ ID = u0012345, \quad S = \ldots \]
RFID Privacy: goals

ID = u0012345, 
S = ...

#Tags?

ID = u7654321, 
S = ...

Link?
Corrupting Tags
Different Privacy Solutions

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

Privacy Preserving Protocols
RFID Privacy
Requirements
## Threat Analysis / Requirements

<table>
<thead>
<tr>
<th>Security</th>
<th>Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Supply Chain</td>
</tr>
<tr>
<td>High</td>
<td>Car Keys</td>
</tr>
</tbody>
</table>
1 RFID Privacy
   Requirements

2 Privacy Models
   Protocol Analysis
   Provable Security (Privacy)
   Privacy Model
   Insider Attacks
   Requirements

3 Lightweight Cryptography

4 Existing Protocols

5 Protocol Design
   Design
   Performance

6 Conclusions and Future Perspectives
Protocol Analysis

Properties:
- Security
- Privacy: untraceability
- Allow corruption

ID = u0012345, S = ...

ID = ?

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

Results
Many published protocols broken:
⇒ Lack of formal proofs!
Provable Security (Privacy)
Provable Security (Privacy)

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

<table>
<thead>
<tr>
<th>Privacy Levels</th>
<th>Strong</th>
<th>Forward</th>
<th>Weak</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Wide</strong></td>
<td><img src="image1" alt="Images" /></td>
<td><img src="image2" alt="Images" /></td>
<td><img src="image3" alt="Images" /></td>
</tr>
<tr>
<td><strong>Narrow</strong></td>
<td><img src="image4" alt="Images" /></td>
<td><img src="image5" alt="Images" /></td>
<td><img src="image6" alt="Images" /></td>
</tr>
</tbody>
</table>
## Privacy Requirements

<table>
<thead>
<tr>
<th>Privacy Level</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Narrow Weak</td>
<td>Supply Chain</td>
</tr>
<tr>
<td>Narrow Forward</td>
<td>Smart Products</td>
</tr>
<tr>
<td>Wide Weak</td>
<td>Car Keys</td>
</tr>
<tr>
<td>Wide Forward</td>
<td>Payments</td>
</tr>
<tr>
<td></td>
<td>Access Tokens</td>
</tr>
<tr>
<td></td>
<td>Passports</td>
</tr>
<tr>
<td></td>
<td>Public Transport</td>
</tr>
</tbody>
</table>
Insider Attacks

Adversary

System

Insider Tag
### Privacy Requirements

<table>
<thead>
<tr>
<th>Privacy Level</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Narrow Weak</td>
<td>Supply Chain</td>
</tr>
<tr>
<td>Narrow Forward</td>
<td>Smart Products</td>
</tr>
<tr>
<td>Wide Weak</td>
<td>Car Keys</td>
</tr>
<tr>
<td><strong>Wide Forward + Insider</strong></td>
<td>Payments</td>
</tr>
<tr>
<td></td>
<td>Access Tokens</td>
</tr>
<tr>
<td></td>
<td>Passports</td>
</tr>
<tr>
<td></td>
<td>Public Transport</td>
</tr>
</tbody>
</table>
## Privacy Requirements

<table>
<thead>
<tr>
<th>Privacy Level</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Narrow Weak</td>
<td>Supply Chain</td>
</tr>
<tr>
<td>Narrow Forward</td>
<td>Smart Products</td>
</tr>
<tr>
<td>Wide Weak</td>
<td>Car Keys</td>
</tr>
<tr>
<td><strong>Wide Forward + Insider</strong></td>
<td>Payments</td>
</tr>
<tr>
<td>Currently: <strong>Wide Strong</strong></td>
<td>Access Tokens</td>
</tr>
<tr>
<td></td>
<td>Passports</td>
</tr>
<tr>
<td></td>
<td>Public Transport</td>
</tr>
</tbody>
</table>
Privacy Preserving Protocols

1 RFID Privacy
   Requirements

2 Privacy Models
   Protocol Analysis
   Provable Security (Privacy)
   Privacy Model
   Insider Attacks
   Requirements

3 Lightweight Cryptography

4 Existing Protocols

5 Protocol Design
   Design
   Performance

6 Conclusions and Future Perspectives
Lightweight Devices
Lightweight Cryptography?

Limits:
- Area (€€€)
- Time
- Power
- Energy
## Typical Ingredients for Protocols

<table>
<thead>
<tr>
<th>Primitive</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>RNG</td>
<td>OK?</td>
</tr>
<tr>
<td>Key Update</td>
<td>???</td>
</tr>
<tr>
<td>Block Cipher</td>
<td>OK</td>
</tr>
<tr>
<td>Hash Function</td>
<td>OK</td>
</tr>
<tr>
<td>ECC</td>
<td>OK</td>
</tr>
<tr>
<td>$\sum$</td>
<td>???</td>
</tr>
</tbody>
</table>
Lightweight Elliptic Curve Cryptography

Implementation [LBSV10]:
- Area (14.5 kGE)
- Time (85 ms)
- Power (13.8 μW)
- Energy (1.18 μJ)
1 RFID Privacy Requirements

2 Privacy Models
   Protocol Analysis
   Provable Security (Privacy)
   Privacy Model
   Insider Attacks
   Requirements

3 Lightweight Cryptography

4 Existing Protocols

5 Protocol Design
   Design
   Performance

6 Conclusions and Future Perspectives
PRF (Block cipher) based [ISO/IEC 9798-2]

State: $x_j$
Tag $T$

Secrets: $DB = \{x_j\}$

Reader

$c \in_R \{0, 1\}^n$

$p \in_R \{0, 1\}^m$
$r = F_x(c||p)$

Search $x_j \in DB$
s.t. $F_{x_j}(c||p) = r$

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

State: \( x_j, Y \)
- Tag \( T \)
- \( r \in R \mathbb{Z}_\ell \)

Secrets: \( y, DB = \{X_j\} \)
- Reader

\[ R = rP \]

\[ R \neq O? \]

\[ e \neq 0? \]
- \( s = x + er \)

\[ s \]

\[ \hat{X} = sP - eR \in DB? \]

Privacy
None
Randomized Schnorr [BCI08]

State: $x_j, Y$

Tag $T$

Secrets: $y, \text{DB} = \{X_j\}$

Reader

$R_1 = r_1 P, R_2 = r_2 Y$

$R_1, R_2 \neq O$?

$s = ex + r_1 + r_2$

$e$

$s$

$\dot{X} = e^{-1}(sP - R_1 - y^{-1}R_2) \in \text{DB}$

Privacy

Narrow Strong
Randomized Hash GPS [BCI09]

State: $x_j, Y$

Tag $T$

$R_1 = r_1 P, R_2 = r_2 Y$

$z = H(R_1, R_2)$

Secrets: $y, DB = \{X_j\}$

Reader

$R_1, R_2 \neq O?$

$e$

$s = ex + r_1 + r_2$

$s, R_1, R_2$

Verify $z$

$\hat{X} = e^{-1}(sP - R_1 - y^{-1}R_2) \in DB$

Privacy

Narrow Strong and Wide Forward
IND-CCA2 Encryption [Vau07]

State: $s_j, ID$

Tag $T$

$PK: K_P$. Secrets: $DB = \{s_j\}$

Reader

$c \in_R \{0, 1\}^n$

$ID \| s_j \| c \leftarrow Dec_{K_S}(r)$

Search $s_j \in DB$

Privacy

Wide Strong
## Performance

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Schnorr</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>1 EC mult</td>
</tr>
<tr>
<td>Randomized Schnorr</td>
<td>narrow-strong</td>
<td>no</td>
<td>yes</td>
<td>2 EC mult</td>
</tr>
<tr>
<td>Rand. Hashed GPS</td>
<td>narrow-strong wide-forward</td>
<td>no</td>
<td>yes</td>
<td>2 EC mult 1 hash</td>
</tr>
</tbody>
</table>
# Performance

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Schnorr</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>1 EC mult</td>
</tr>
<tr>
<td>Randomized Schnorr</td>
<td>narrow-strong</td>
<td>no</td>
<td>yes</td>
<td>2 EC mult</td>
</tr>
<tr>
<td>Rand. Hashed GPS</td>
<td>narrow-strong</td>
<td>no</td>
<td>yes</td>
<td>2 EC mult</td>
</tr>
<tr>
<td>Vaudenay + DHIES</td>
<td>wide-strong</td>
<td>yes</td>
<td>no</td>
<td>2 EC mult</td>
</tr>
<tr>
<td>Hash ElGamal</td>
<td>wide-strong</td>
<td>yes</td>
<td>no</td>
<td>2 EC mult</td>
</tr>
</tbody>
</table>

- 1 EC mult
- 1 hash
- 1 MAC
- 1 symm enc
1 RFID Privacy
   Requirements

2 Privacy Models
   Protocol Analysis
   Provable Security (Privacy)
   Privacy Model
   Insider Attacks
   Requirements

3 Lightweight Cryptography

4 Existing Protocols

5 Protocol Design
   Design
   Performance

6 Conclusions and Future Perspectives
New Protocol [Peeters, Hermans 2012]

Design protocol:
- Correct
- Extended soundness
- (At least) Wide Forward + Insider privacy
- Efficient
EC Schnorr Protocol

State: $x_j, Y$

Tag $T$

$r \in_R \mathbb{Z}_l$

Secrets: $y, DB = \{X_j\}$

Reader

$R = rP$

$R \neq O?$

$e \\neq 0?$

$s = x + er$

$s$

$\hat{X} = sP - eR \in DB ?$
Key Assumptions

Oracle Diffie-Hellman Assumption

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

with extra \(O(Z) := x\text{coord}(bZ)P.\)

X Logarithm

\[x\text{coord}(rP)P \sim r'P\]
New Protocol

State: \( x, Y = yP \)

Tag \( T \)

\( r_1, r_2 \in_R \mathbb{Z}_\ell^* \)

Secrets: \( y \ DB : \{ X_i = x_iP \} \)

Reader \( R \)

\( R_1 = r_1P, R_2 = r_2P \)

\( e \in_R \mathbb{Z}_\ell^* \)

\( d = \text{xcoord}(\text{xcoord}(r_2Y)P) \)

\( s = x + er_1 + d \)

\( \hat{d} = \text{xcoord}(\text{xcoord}(yR_2)P) \)

\( \hat{X} = (s - \hat{d})P - eR_1 \in DB ? \)
New Protocol - Extended Soundness

State: \( x, Y = yP \)

Tag \( T \)

Secrets: \( y \) \( \text{DB: } \{ X_i = x_iP \} \)

Reader \( R \)

\( r_1, r_2 \in_R \mathbb{Z}_\ell^* \)

\( R_1 = r_1P, R_2 = r_2P \)

\( e \in_R \mathbb{Z}_\ell^* \)

\( e \)

\( d = \text{xcoord(xcoord}(r_2Y)P) \)

\( s = x + er_1 + d \)

Extended Soundness

Schnorr protocol \( \Rightarrow \) extended soundness (OMDL assumption)
New Protocol - Privacy

State: $x, Y = yP$

Tag $T$

$R_1 = r_1P, R_2 = r_2P$

Secrets: $y$ DB : $\{X_i = x_iP\}$

Reader $R$

$e \in R \mathbb{Z}_*^\ell$

$d = x\text{coord}(x\text{coord}(r_2Y)P)$

$s = x + er_1 + d$

$\dot{d} = x\text{coord}(x\text{coord}(yR_2)P)$

$\dot{X} = (s - \dot{d})P - eR_1 \in \text{DB}$
## Performance

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Schnorr</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>1 EC mult</td>
</tr>
<tr>
<td>Randomized Schnorr</td>
<td>narrow-strong</td>
<td>no</td>
<td>yes</td>
<td>2 EC mult</td>
</tr>
<tr>
<td>Rand. Hashed GPS</td>
<td>narrow-strong wide-forward</td>
<td>no</td>
<td>yes</td>
<td>2 EC mult 1 hash</td>
</tr>
<tr>
<td>Vaudenay + DHIES</td>
<td>wide-strong</td>
<td>yes</td>
<td>no</td>
<td>2 EC mult 1 hash 1 MAC 1 symm enc</td>
</tr>
<tr>
<td>Hash EIGamal</td>
<td>wide-strong</td>
<td>yes</td>
<td>no</td>
<td>2 EC mult 1 hash 1 MAC</td>
</tr>
</tbody>
</table>
# Performance

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Schnorr</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>1 EC mult</td>
</tr>
<tr>
<td>Randomized Schnorr</td>
<td>narrow-strong</td>
<td>no</td>
<td>yes</td>
<td>2 EC mult</td>
</tr>
<tr>
<td>Rand. Hashed GPS</td>
<td>narrow-strong</td>
<td>no</td>
<td>yes</td>
<td>2 EC mult 1 hash</td>
</tr>
<tr>
<td>Vaudenay + DHIES</td>
<td>wide-strong</td>
<td>yes</td>
<td>no</td>
<td>2 EC mult 1 hash 1 MAC 1 symm enc</td>
</tr>
<tr>
<td>Hash ElGamal</td>
<td>wide-strong</td>
<td>yes</td>
<td>no</td>
<td>2 EC mult 1 hash 1 MAC</td>
</tr>
<tr>
<td>Our Protocol - optimised version</td>
<td>wide-forward-insider</td>
<td>yes</td>
<td>yes</td>
<td>4 EC mult 2 EC mult</td>
</tr>
</tbody>
</table>
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 → feasible?
- Analyze underlying assumptions (DDH-variants)