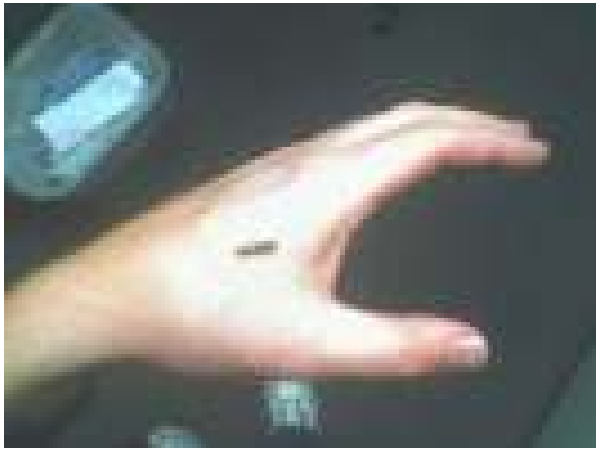
RFID Authentication: Security, Privacy and the Real World

ESC 2013

Jens Hermans
KU Leuven - COSIC

15 January 2013

RFID



Security - Why?

Privacy - Why?

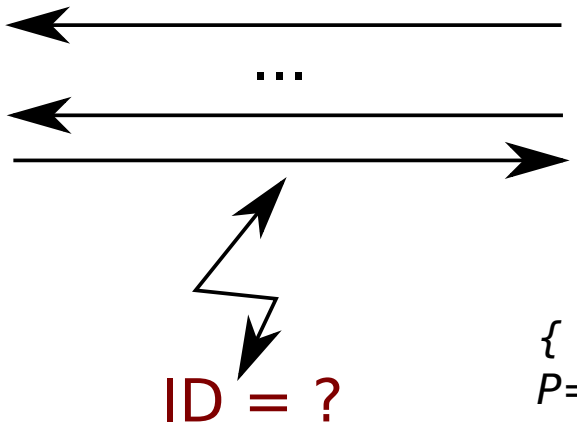
Industrial espionage, user privacy

Threat Analysis / Requirements

		Privacy	
		−	+
Security	−	Supply Chain	Public Transport
	+	Car Keys	Payments Access Control Passports

RFID Privacy: goals

ID = u0012345,
S = ...



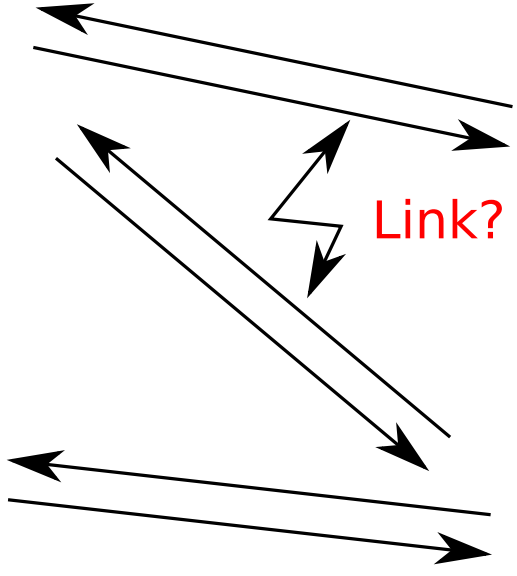
{ (ID=u0012345, P=...) , ...}

RFID Privacy: goals

ID = u0012345,
S = ...

#Tags?

ID = u7654321,
S = ...

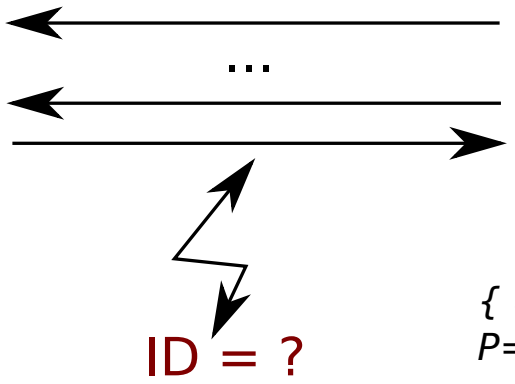


Different Privacy Solutions

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

Protocol Analysis

ID = u0012345,
S = ...



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

Properties:

- Security
- Privacy: untraceability
- Allow corruption

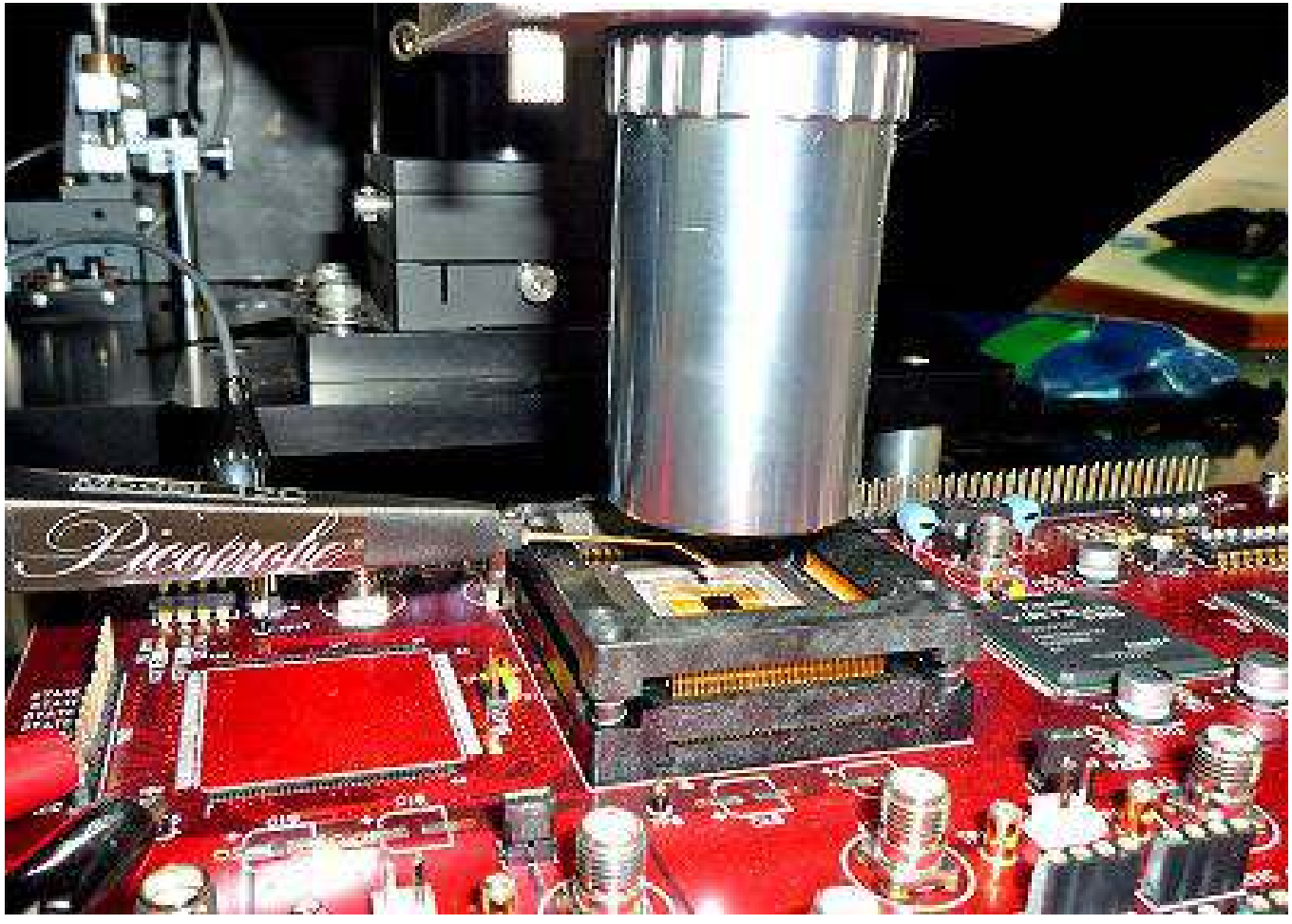
Provable Security & Privacy

System

Adversary

Adversary wins if ...

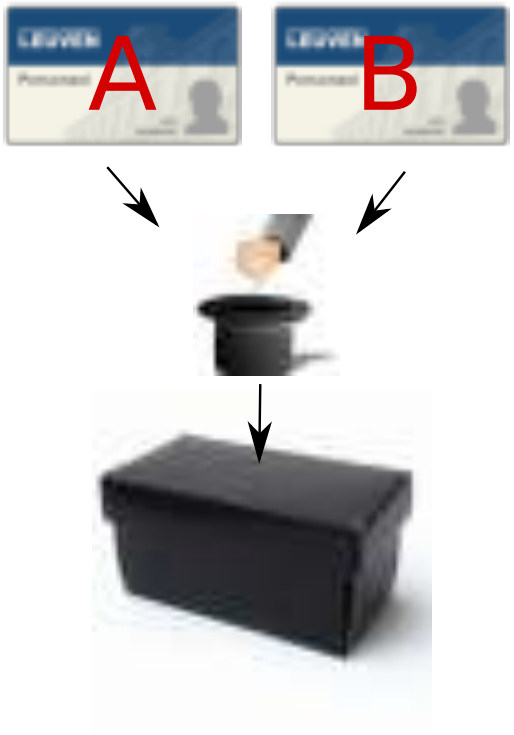
Corrupting Tags



Privacy Models - Indistinguishability

Encryption:

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



Privacy-models:

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

Privacy Levels

	Strong	Forward	Weak
Wide		 at end	
Narrow		 at end	

Privacy Requirements

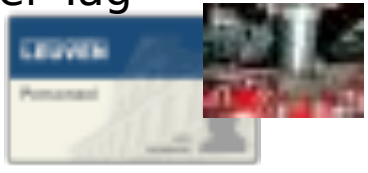
Privacy Level	**Application**
Narrow Weak	Supply Chain
Narrow Forward	Smart Products
Wide Weak	Car Keys
Wide Forward	Payments Access Tokens Passports Public Transport

Insider Attacks

System

Adversary

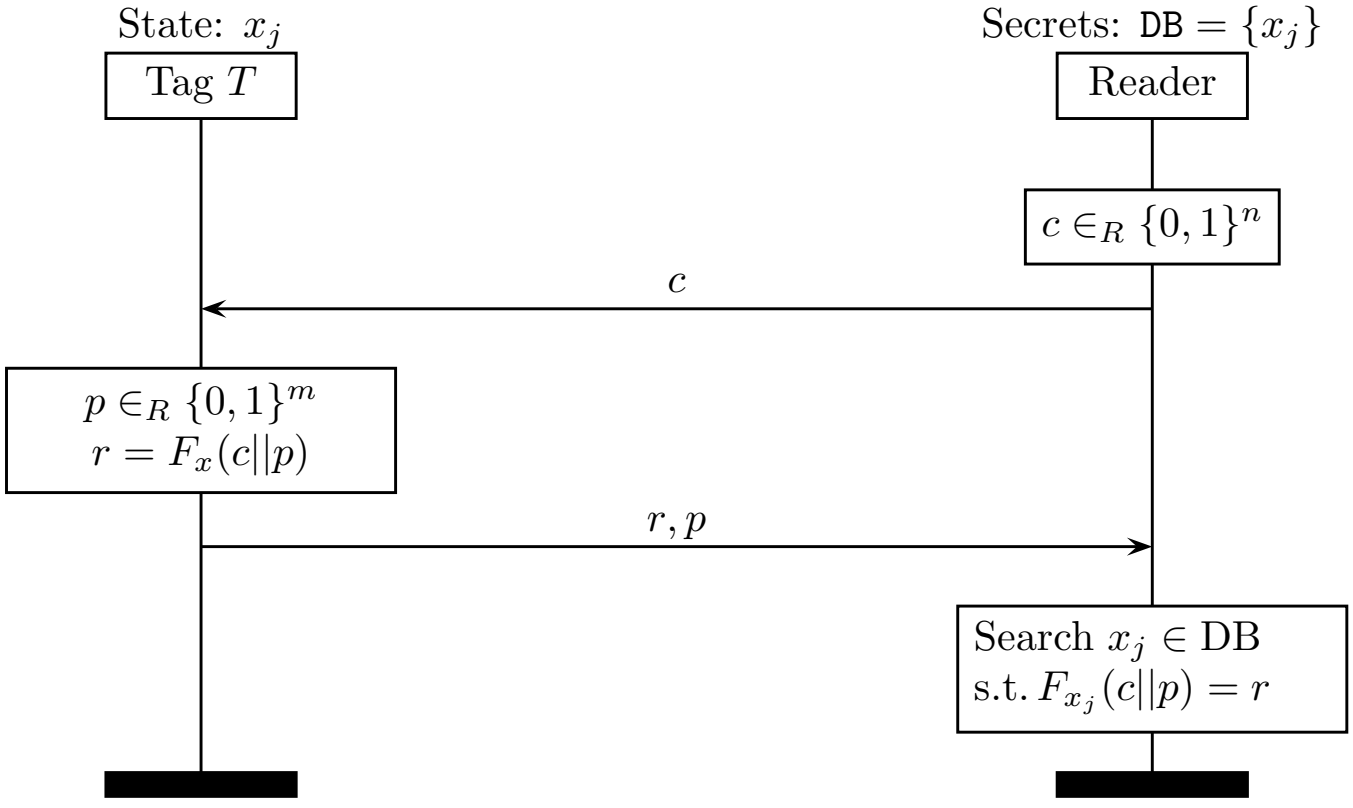
Insider Tag



Privacy Requirements

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

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



Privacy

Wide-Weak

Symmetric Key and Efficiency

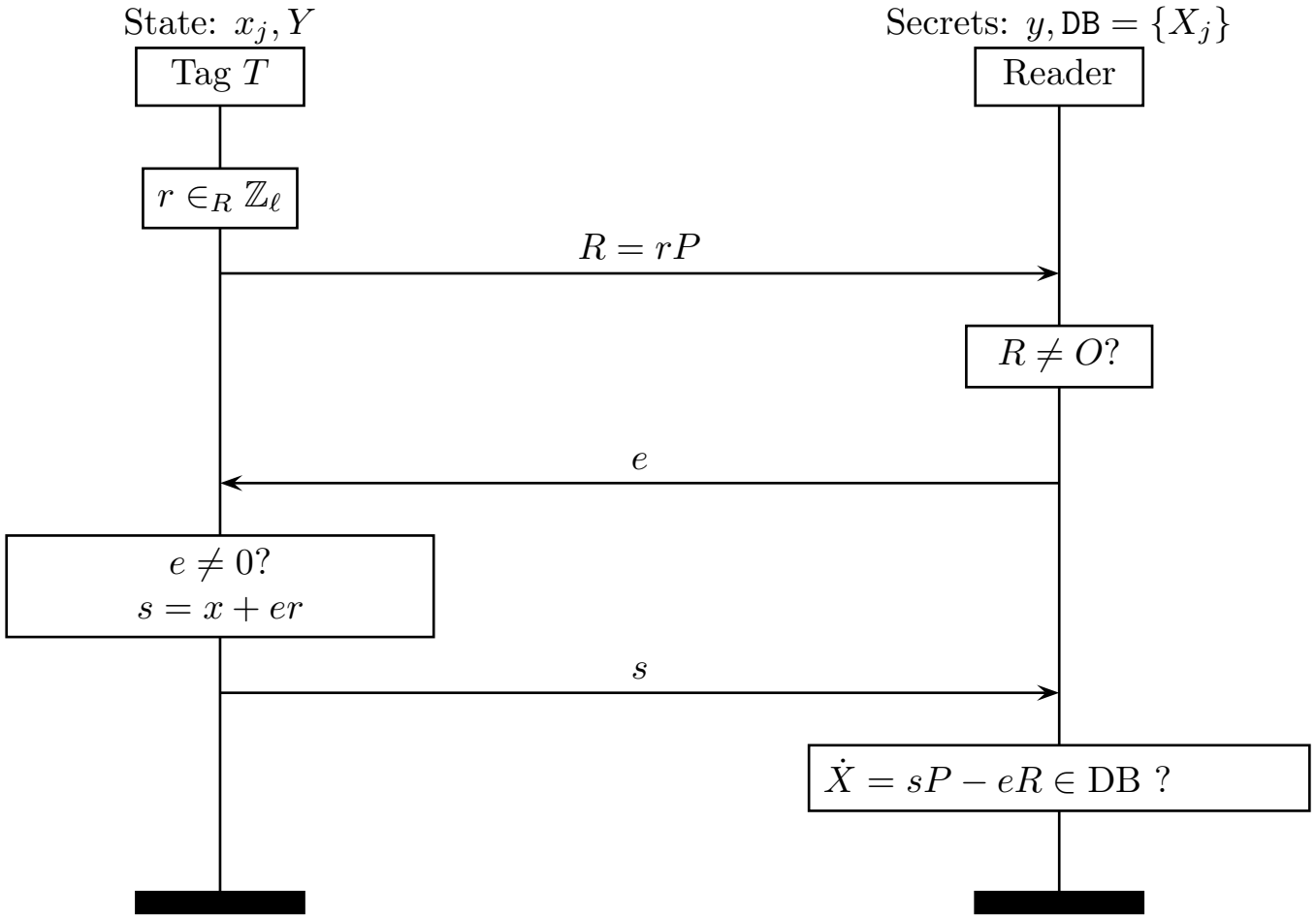
Damgård-Pedersen '08:

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

Key Updating

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

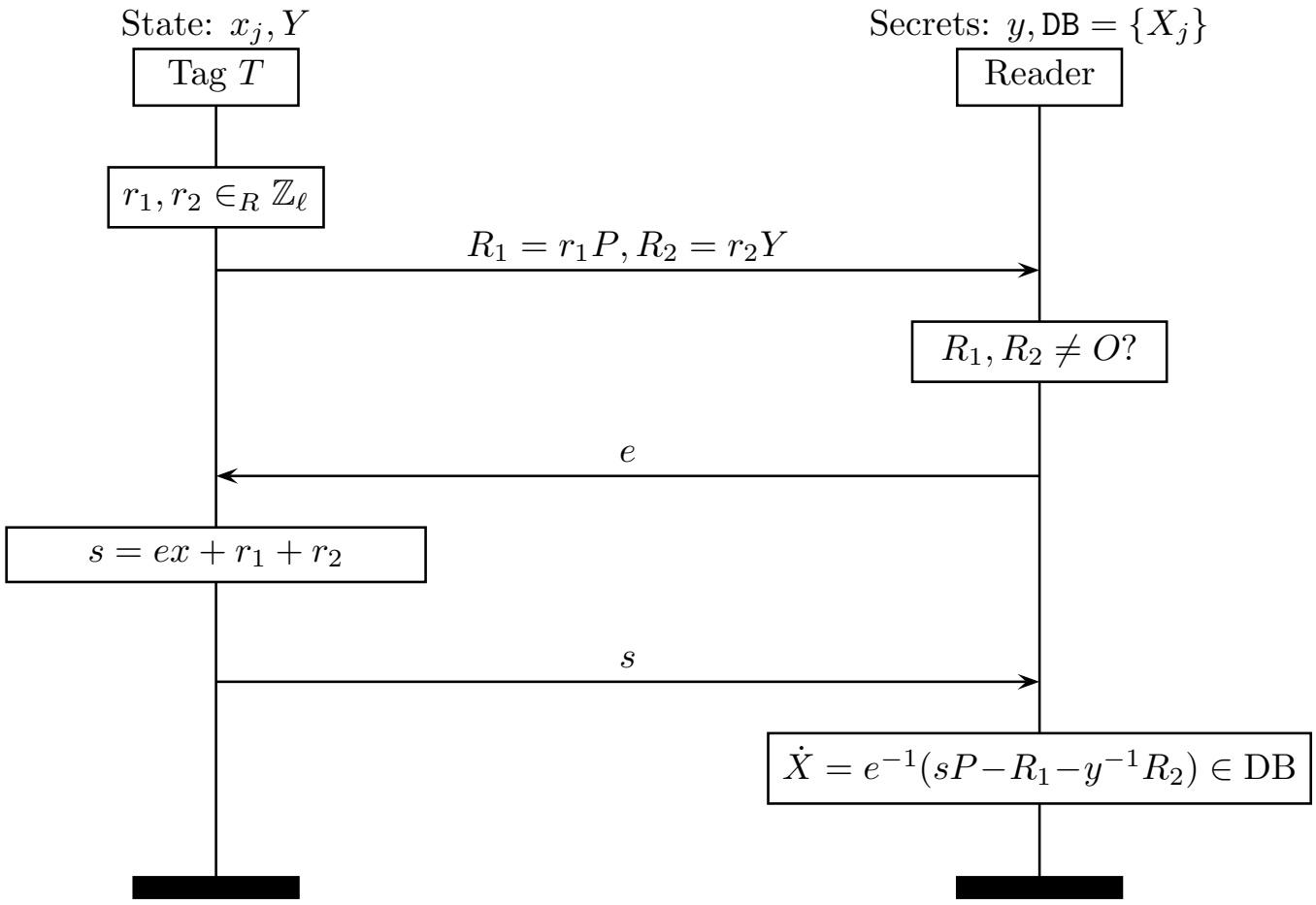
EC Schnorr Protocol



Privacy

None

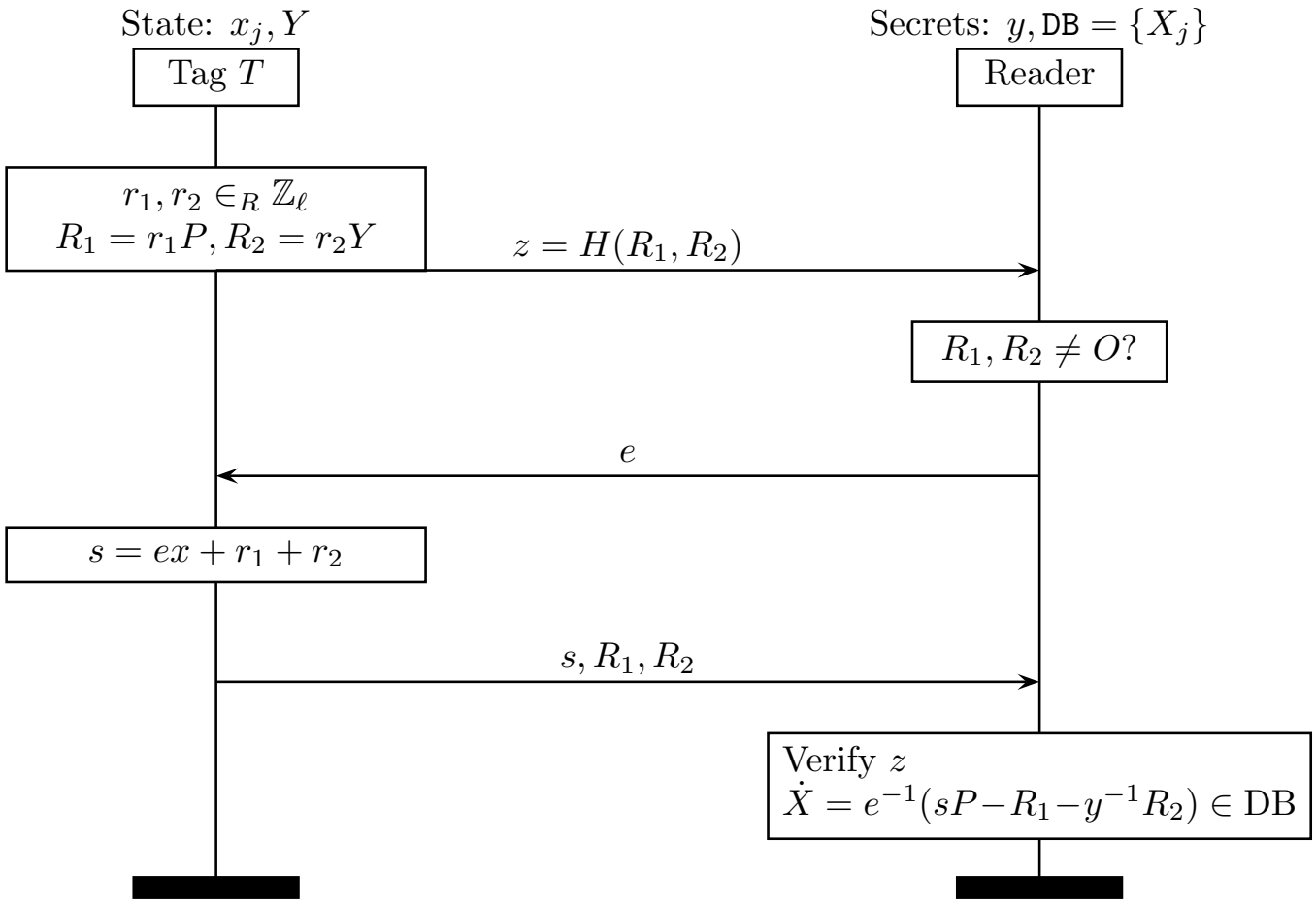
Randomized Schnorr [BCI08]



Privacy

Narrow Strong

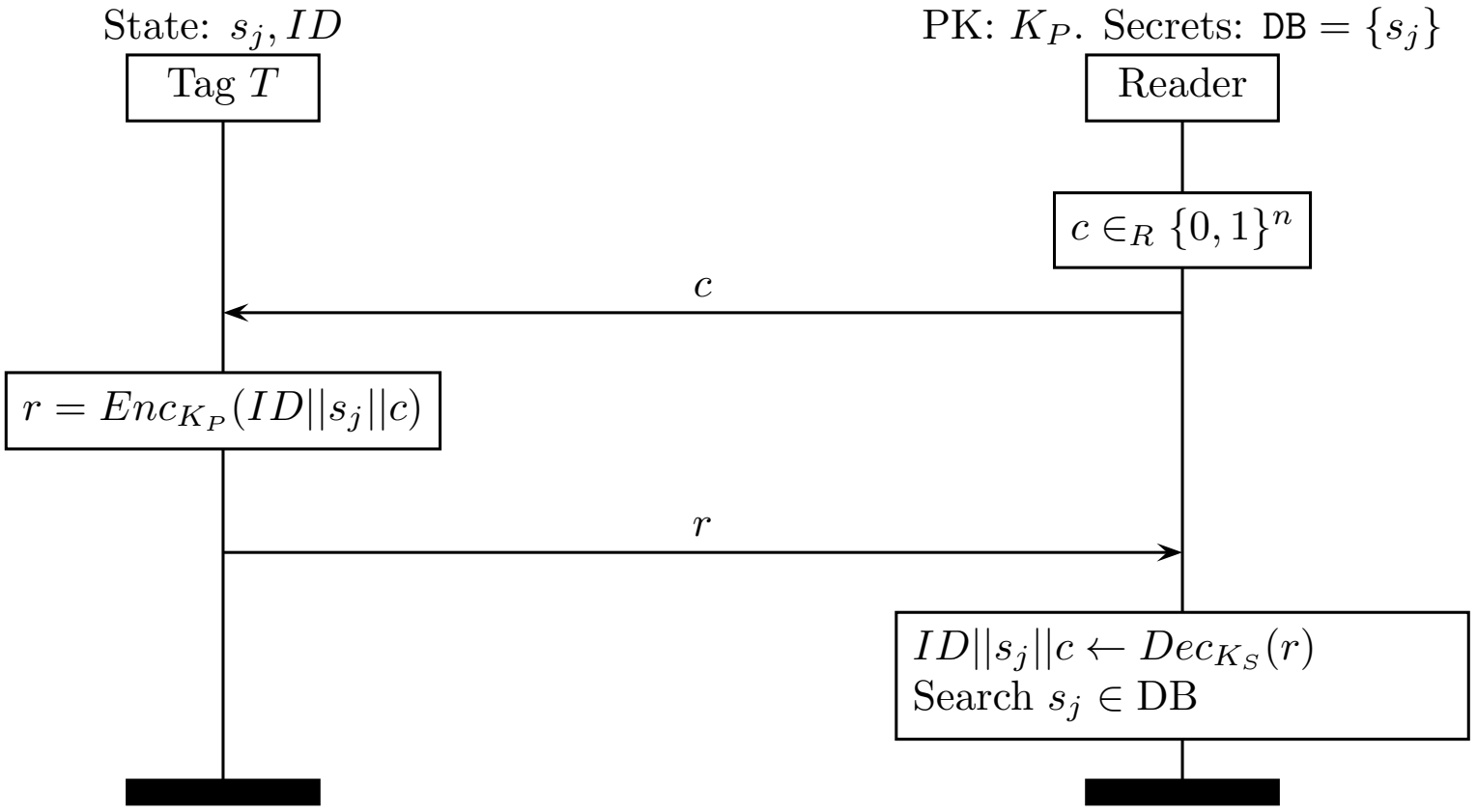
Randomized Hash GPS [BCI09]



Privacy

Narrow Strong and Wide Forward

IND-CCA2 Encryption [Vau07]



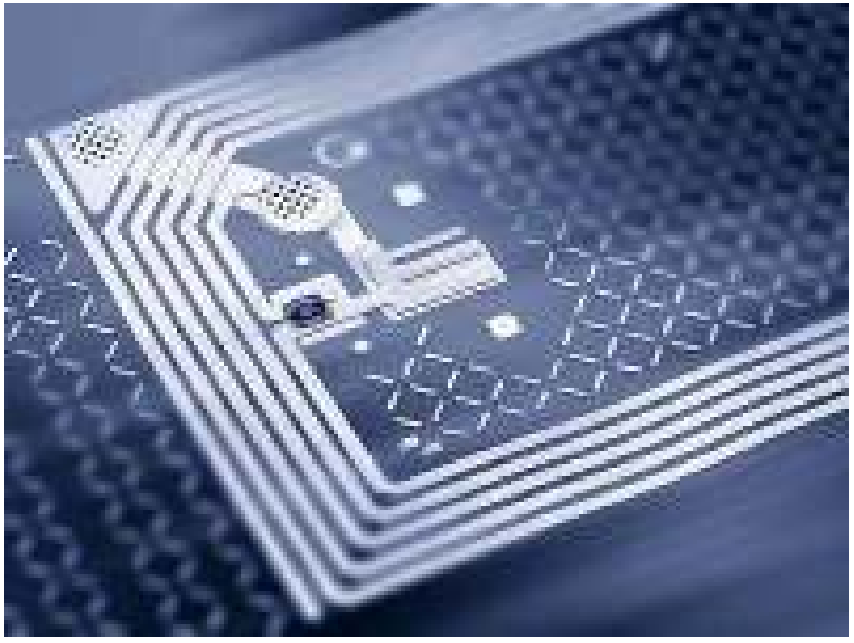
Privacy

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
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

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
$\sum$	???

Scope

ISO/IEC JTC 1 SC31: Automatic identification and data capture techniques

Features:

- Tag authentication
- Reader authentication
- Mutual authentication
- Secure data exchange

Target platform: passive & active tags.

Proposals

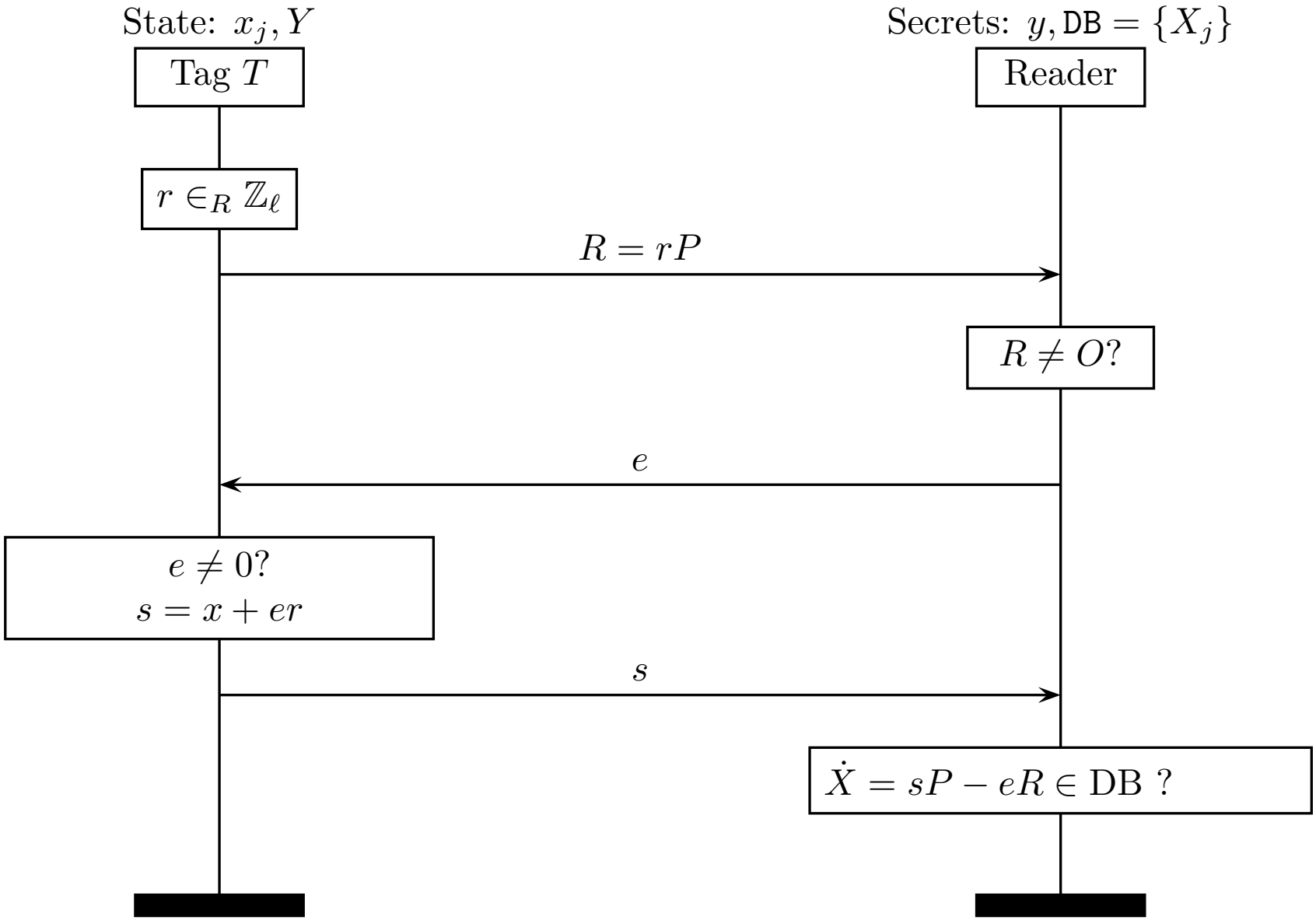
Protocol	Tag Auth	Reader Auth	Mutual Auth	Privacy
Block cipher based (3)	✓	(✓)	(✓)	
HB-2	✓	✓	✓	(✓)
Stream cipher based	✓	✓	✓	
XOR	~~✓~~	~~✓~~	~~✓~~	
ECC Static DH	✓			
CryptoGPS	✓			
ECDSA/DH TLS	✓	✓	✓	
PK Encryption - Rabin	✓	✓	✓	✓

New Protocol [Peeters, Hermans 2012]

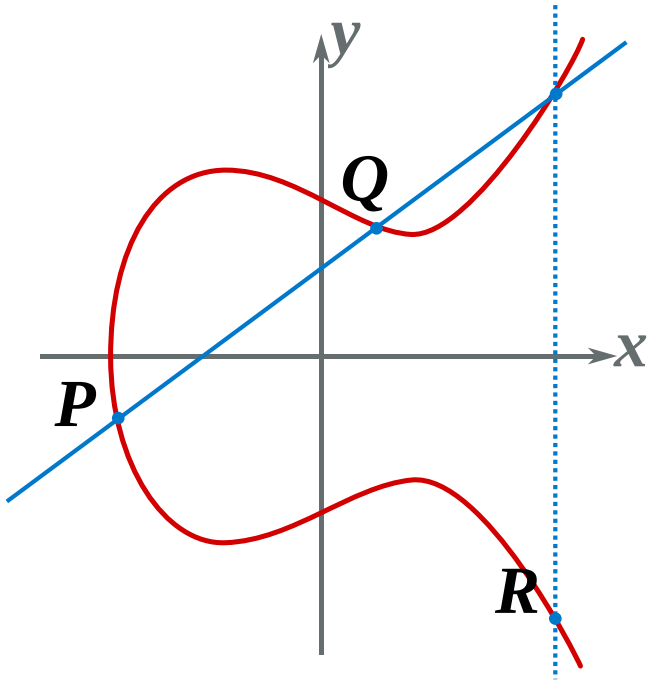
Design protocol:

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

EC Schnorr Protocol



Lightweight Elliptic Curve Cryptography



Implementation [LBSV10]:

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

Key Assumptions

Oracle Diffie-Hellman Assumption

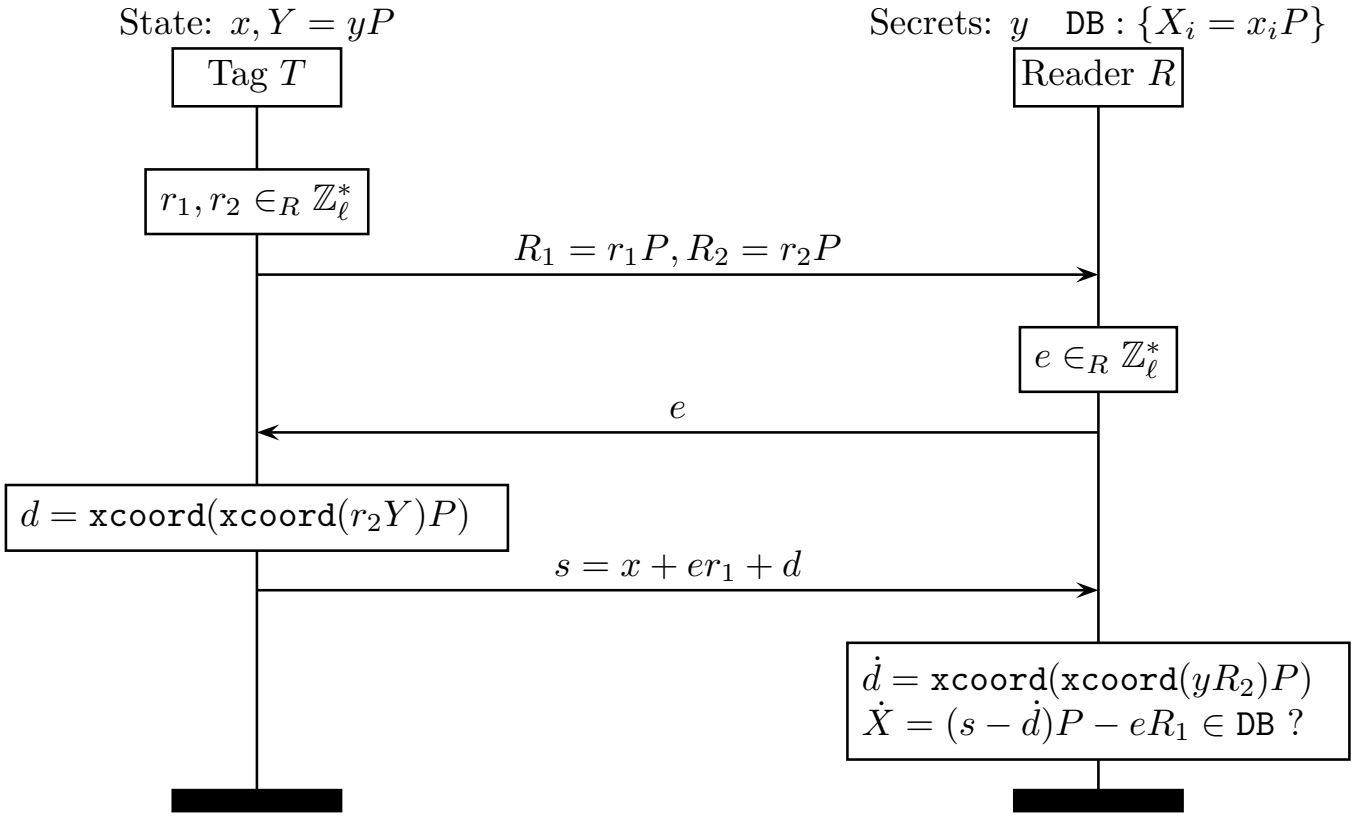
$$(A = aP, B = bP, abP) \sim (A = aP, B = bP, rP)$$

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

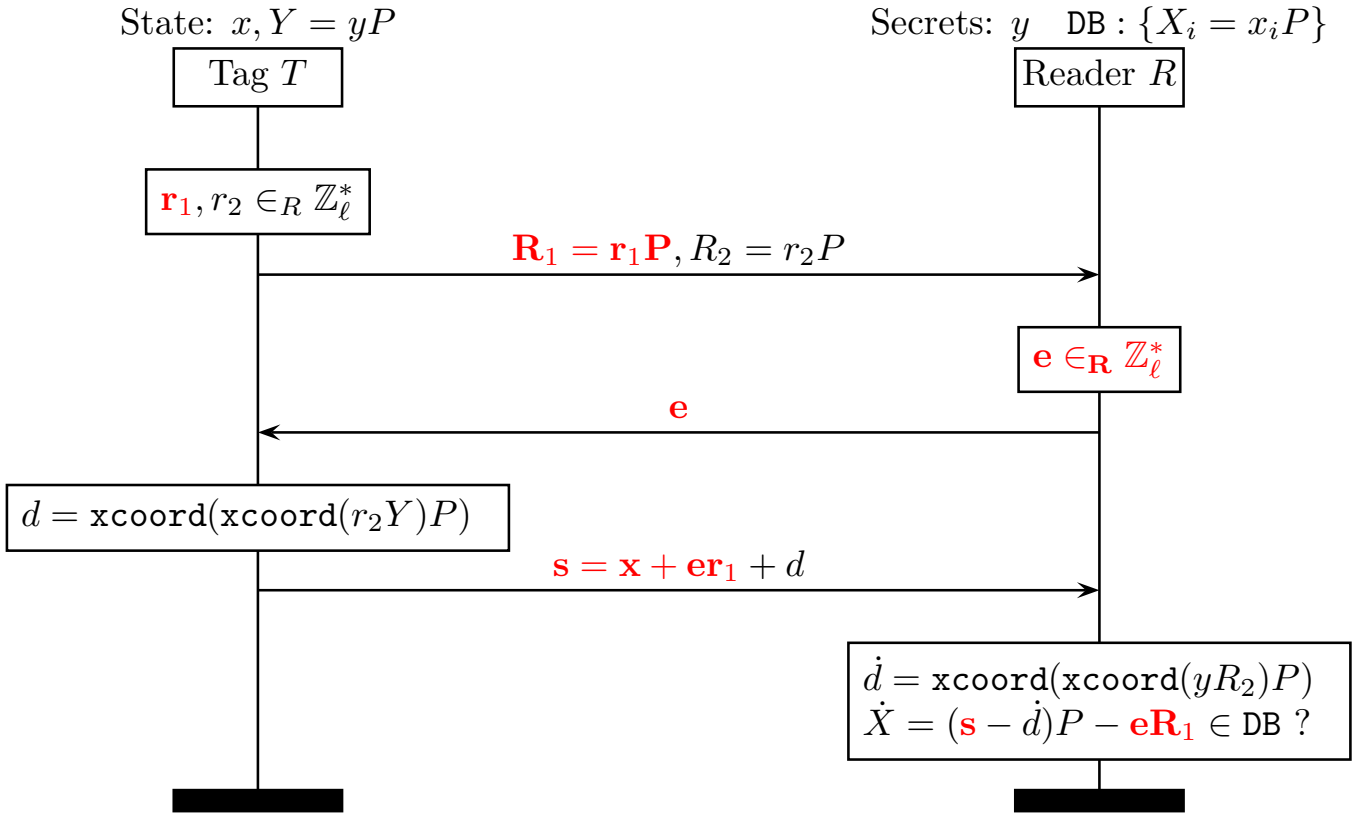
X Logarithm

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

New Protocol



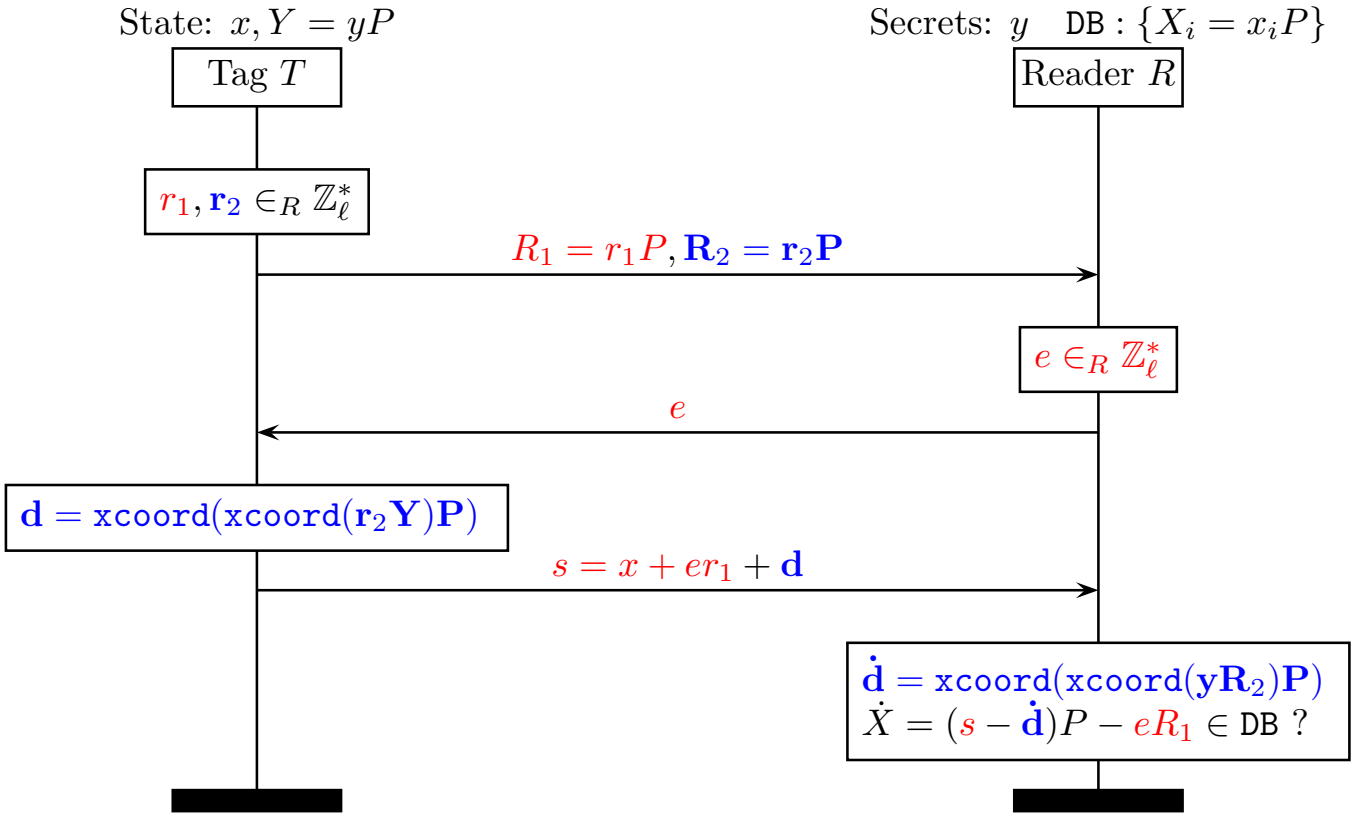
New Protocol - Extended Soundness



Extended Soundness

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

New Protocol - Privacy



Something symmetric?

Final step: $s = x + d + er_1$

Assume set $\mathcal{X} = \{x_0, \ldots, x_n\}$ and set $\mathcal{I} = \{\iota_0, \ldots, \iota_m\}$.

1. Adversary gets $\mathcal{I}$
2. Set of oracles:
   - $\mathcal{O}_1(\alpha, \beta) := \begin{cases} x_\alpha \oplus d_i & \text{if } b = 0 \\ x_\beta \oplus d_i & \text{if } b = 1 \end{cases}$, $d_i \in_R \{0,1\}^l$
   - $\mathcal{O}_2(s, i) := s \oplus d_i \in \mathcal{X} \cup \mathcal{I}$
   - $\mathcal{O}_3(s) := s \in \mathcal{X} \cup \mathcal{I}$
3. Adversary gets $\mathcal{X}$, outputs guess g

Something for wide strong privacy?

Assume set $\mathcal{X} = \{x_0, \ldots, x_n\}$

1. Adversary gets $\mathcal{X}$
2. Interact with oracles:
   - $\mathcal{O}_1(\alpha, \beta) := \begin{cases} x_\alpha d_i + e_i & \text{if } b = 0 \\ x_\beta d_i + e_i & \text{if } b = 1 \end{cases}$, $\quad d_i, e_i \in_R \mathbb{Z}_l$
   - $\mathcal{O}_2(s, i) := d_i^{-1}(s - e_i) \in \mathcal{X}$
3. Output guess g.

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
Wide-Strong protocol	wide-strong	yes	yes	4-5 EC mult

Summary

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

?