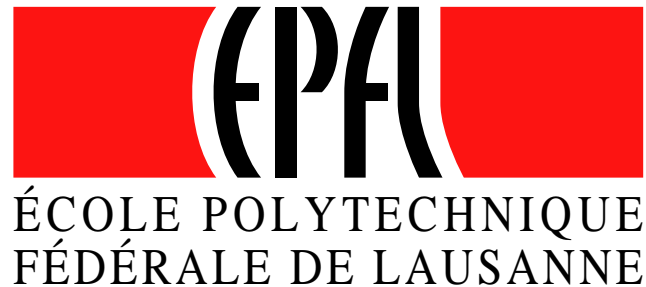


On Privacy Models for RFID

Serge Vaudenay



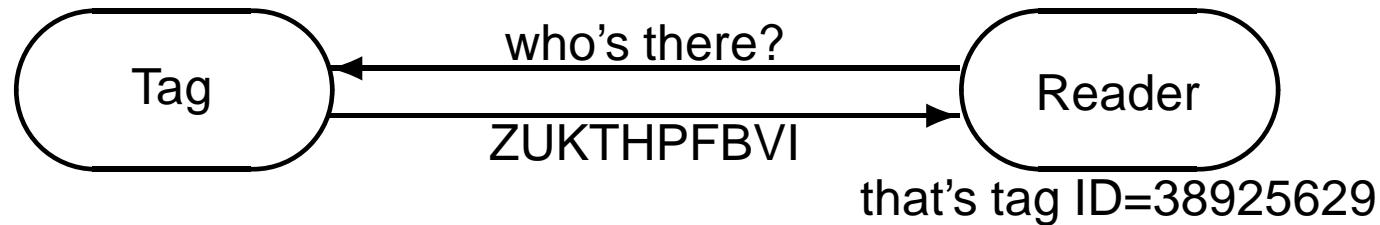
<http://lasecwww.epfl.ch/>

LASEC

- 1 Introduction: The RFID Technology**
- 2 Case Studies: Some RFID Schemes**
- 3 Definitions: 4×2 Adversarial Models**
- 4 Results**
- 5 Extension to Mutual Authentication**

- 1 Introduction: The RFID Technology**
- 2 Case Studies: Some RFID Schemes
- 3 Definitions: 4×2 Adversarial Models
- 4 Results
- 5 Extension to Mutual Authentication

The RFID Concept



- stocks management (Wal-Mart)
- libraries (Santa Clara, KU Leuven)
- pets identification, meat traceability
- sensors (Michelin tires)
- access control (EPFL Labs)
- localization of people (amusement parks, hospitals)
- electronic documents (traveling passports)
- transport tickets

Nabaztag



- several designs (ears)
- blinks, moves ears, speaks
- obeys voice
- clock
- reads out RSS
- plays podcasts, music
- reads, sings, dances emails
- chat
- detects and react to RFID
- read books (with RFID) to kids

Current Cheap RFID Tags

- communicate up to decimeters
- 1Kb of memory
- very little cryptography
- passive
- no battery (tag-to-reader signal pretty weak)
- not tamper resistant

This Talk

Covered:

- single system multiple tags
- identification of tag to reader
- authentication of tag to reader
- security and privacy

Uncovered:

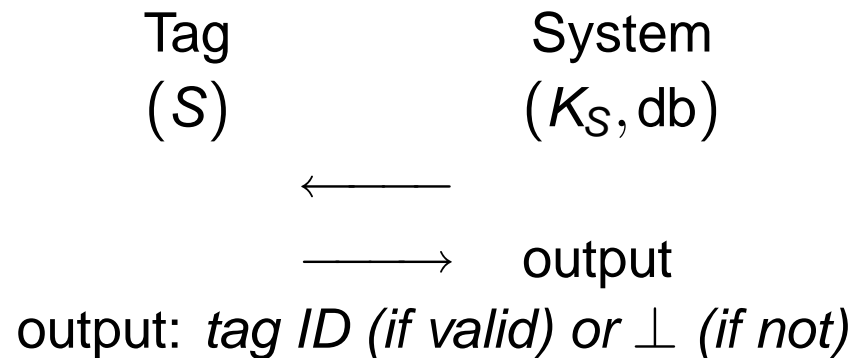
- multiple systems
- authentication of reader to tag
- key agreement
- secure communication

- 1 Introduction: The RFID Technology
- 2 Case Studies: Some RFID Schemes**
- 3 Definitions: 4×2 Adversarial Models
- 4 Results
- 5 Extension to Mutual Authentication

RFID Scheme

Components:

- SetupReader: generate key materials (K_S, K_P) + reset database
- SetupTag $_{K_P}$: tag ID is given an initial state S and $(ID, data)$ is inserted in database
- Protocols:



Functionality:

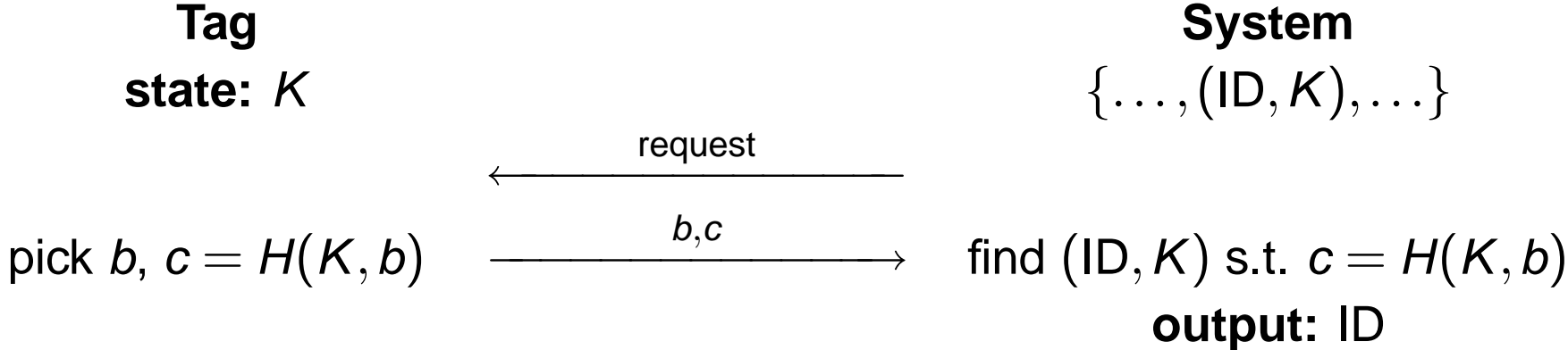
- correctness: identification under normal execution

Crypto properties (whenever required):

- security: adversary cannot impersonate a tag
- privacy: anonymity, unlikability

Weis-Sarma-Rivest-Engel 2003 [WSRE 2003]

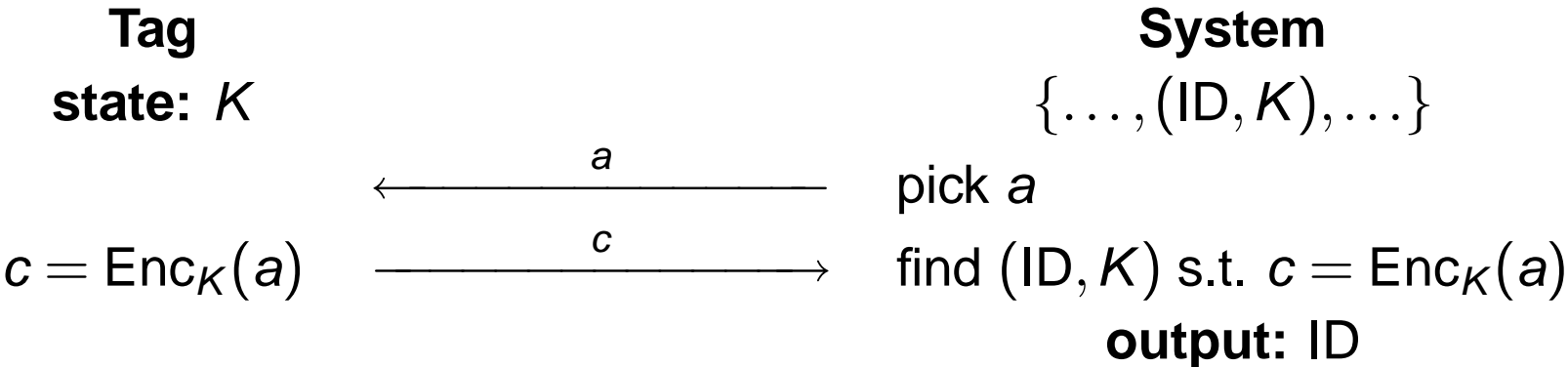
Randomized Hash-Lock Identification



not secure: can replay (b, c) or intercept it and play it later

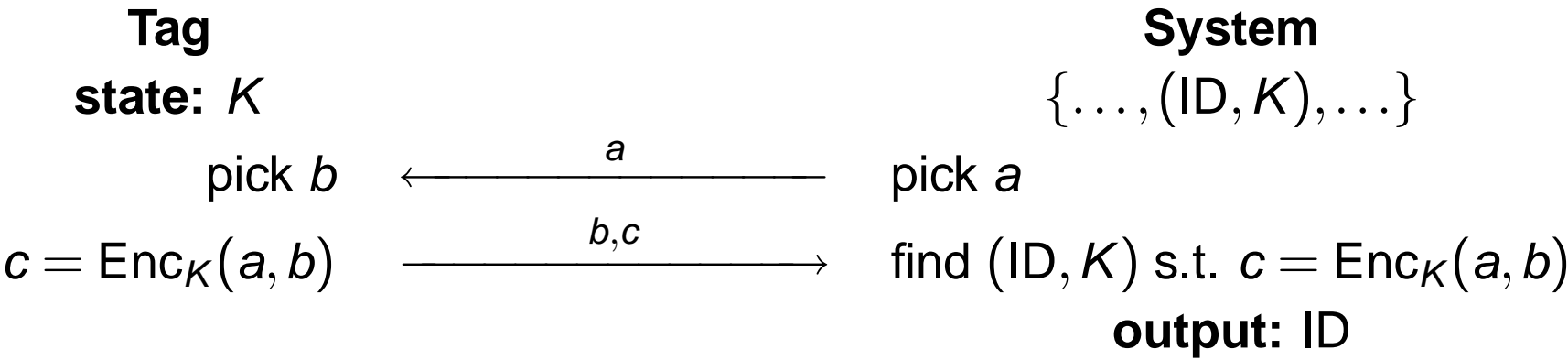
Feldhofer-Dominikus-Wolkerstorfer 2004 [FDW 2004]

ISO/IEC 9798-2 2-Pass Unilateral Authentication



traceability: replaying a leads to the same c

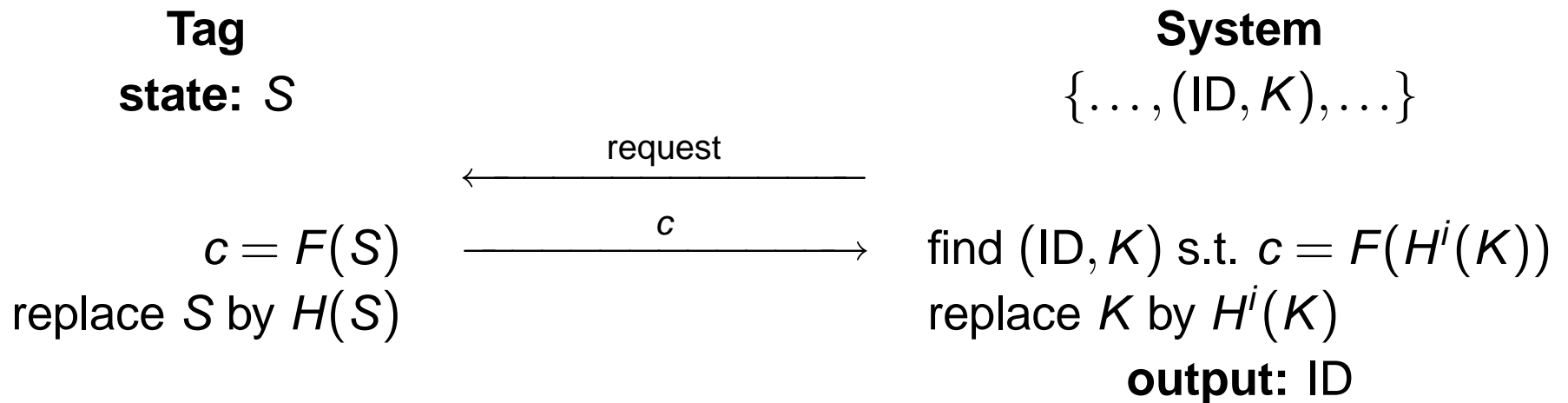
Variant



no forward privacy: trace tag by corrupting it in the future

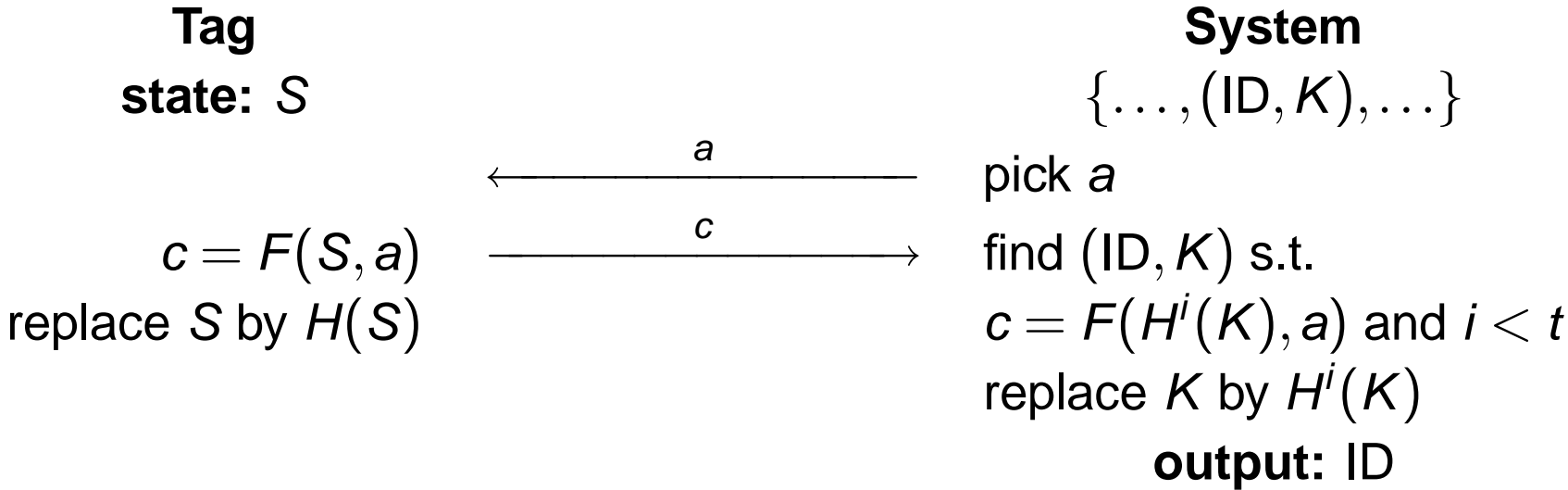
Ohkubo-Suzuki-Kinoshita 2003 [OSK 2003]

Introducing Forward Privacy



not secure: can intercept c and play it later (\equiv hash lock)

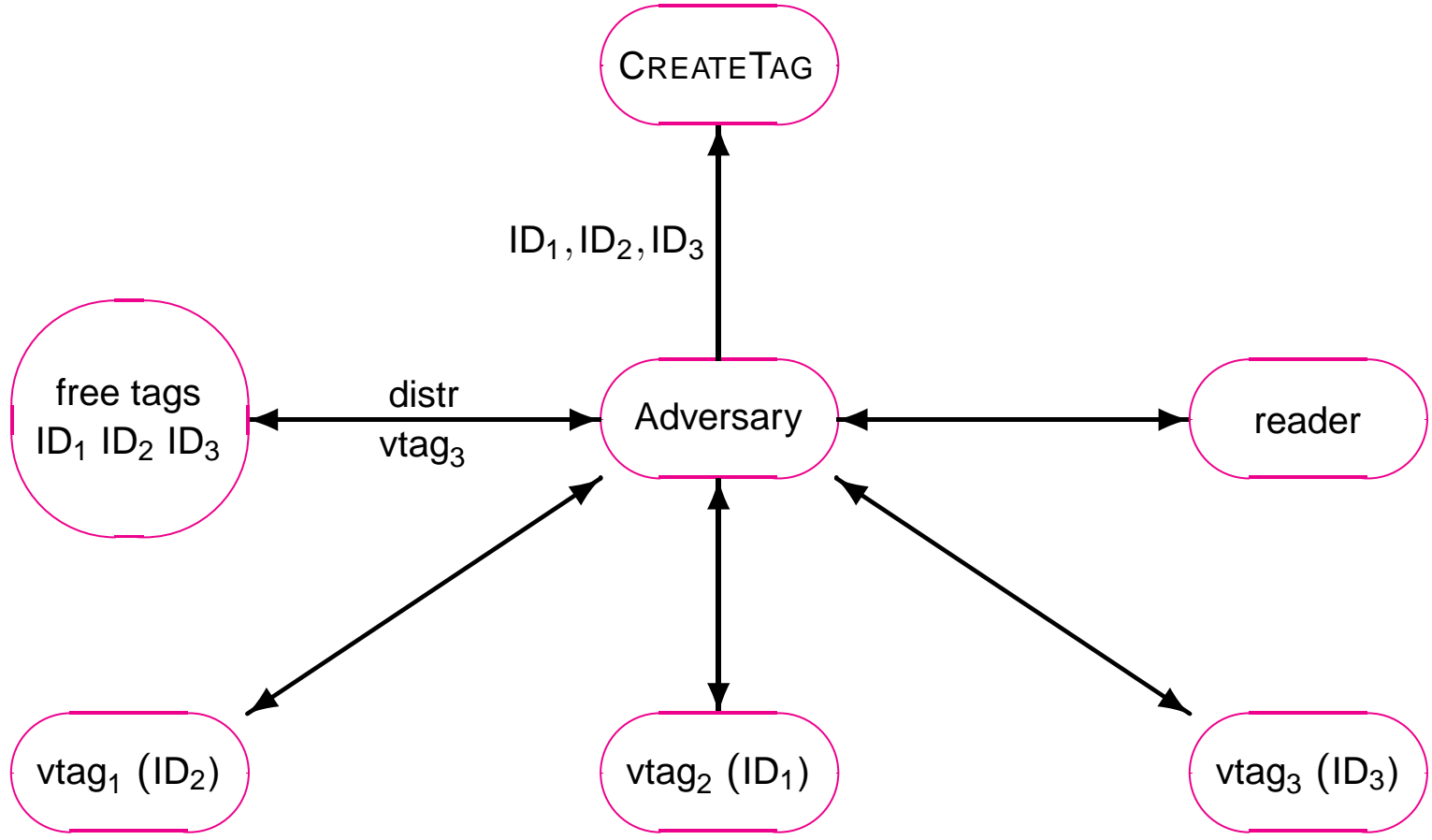
Variant



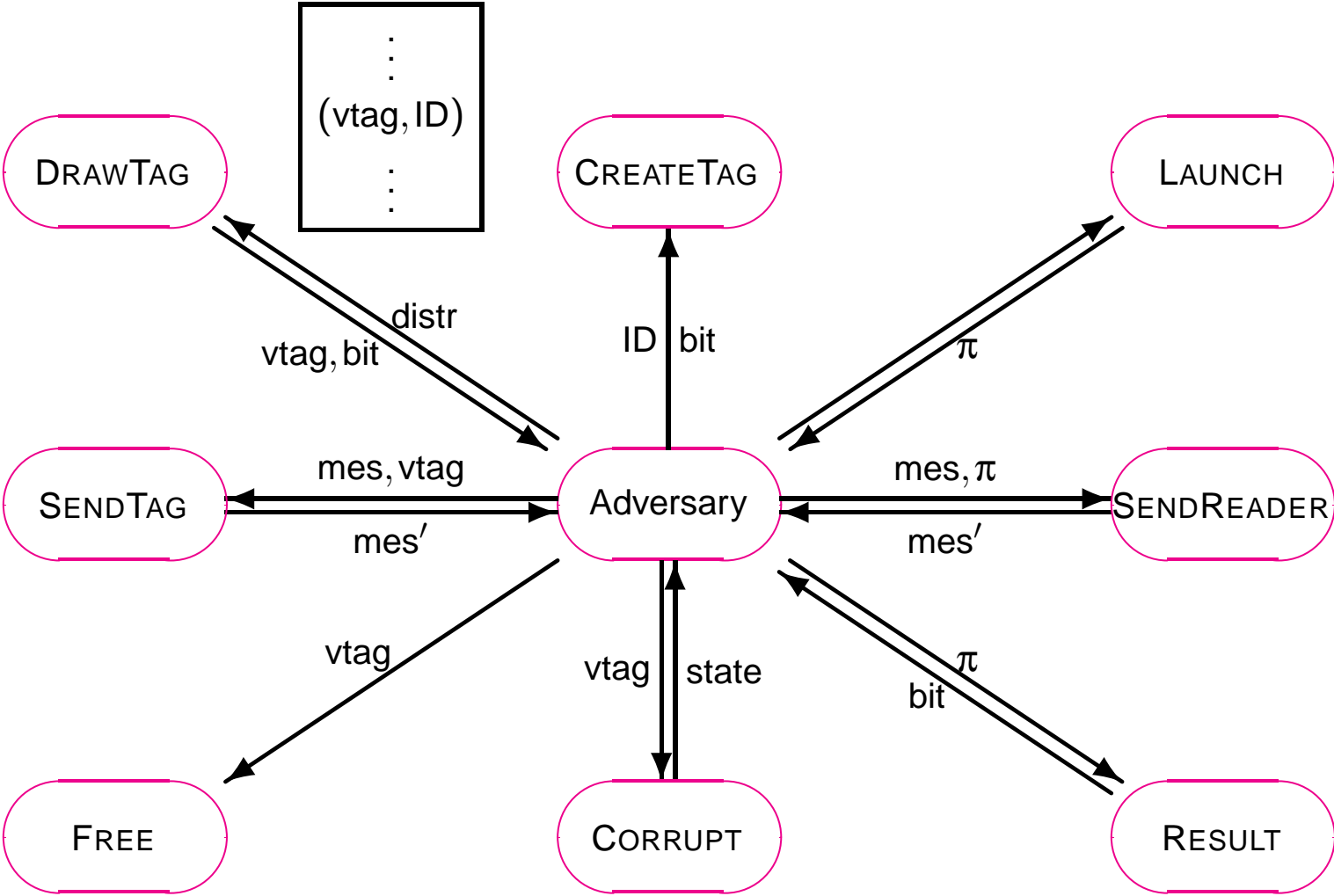
no privacy with a side channel: DoS [JW 2006]

- 1 Introduction: The RFID Technology
- 2 Case Studies: Some RFID Schemes
- 3 Definitions: 4×2 Adversarial Models**
- 4 Results
- 5 Extension to Mutual Authentication

Adversarial Model



Oracle Accesses



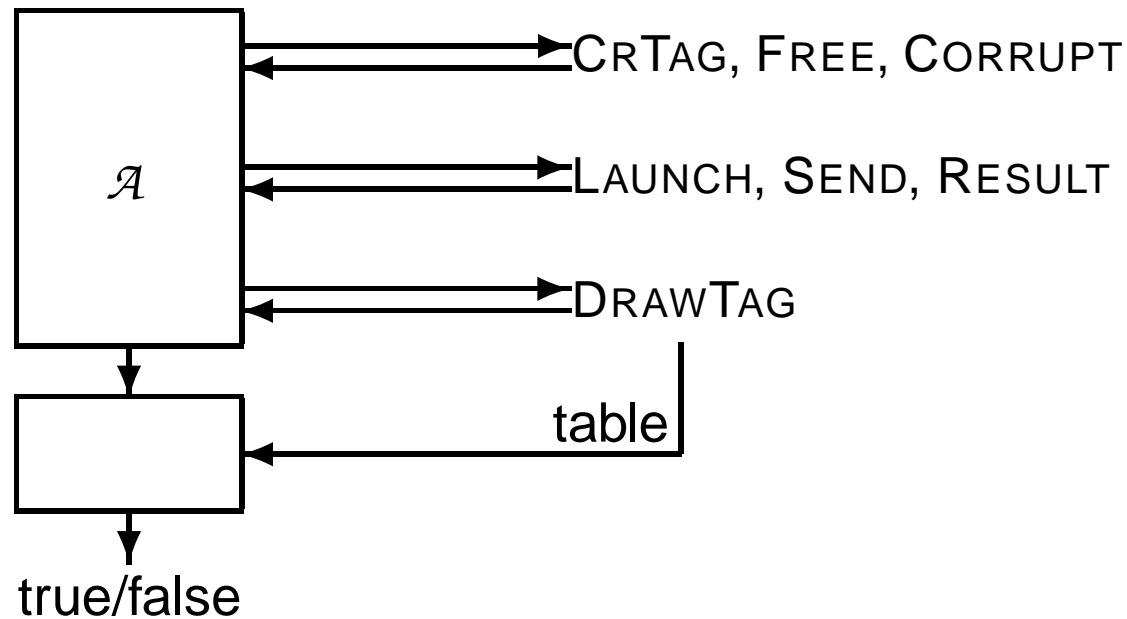
Security

Winning condition: one reader-protocol instance π identified ID but this tag did not have any matching conversation (i.e. same transcript and well interleaved messages).

Definition

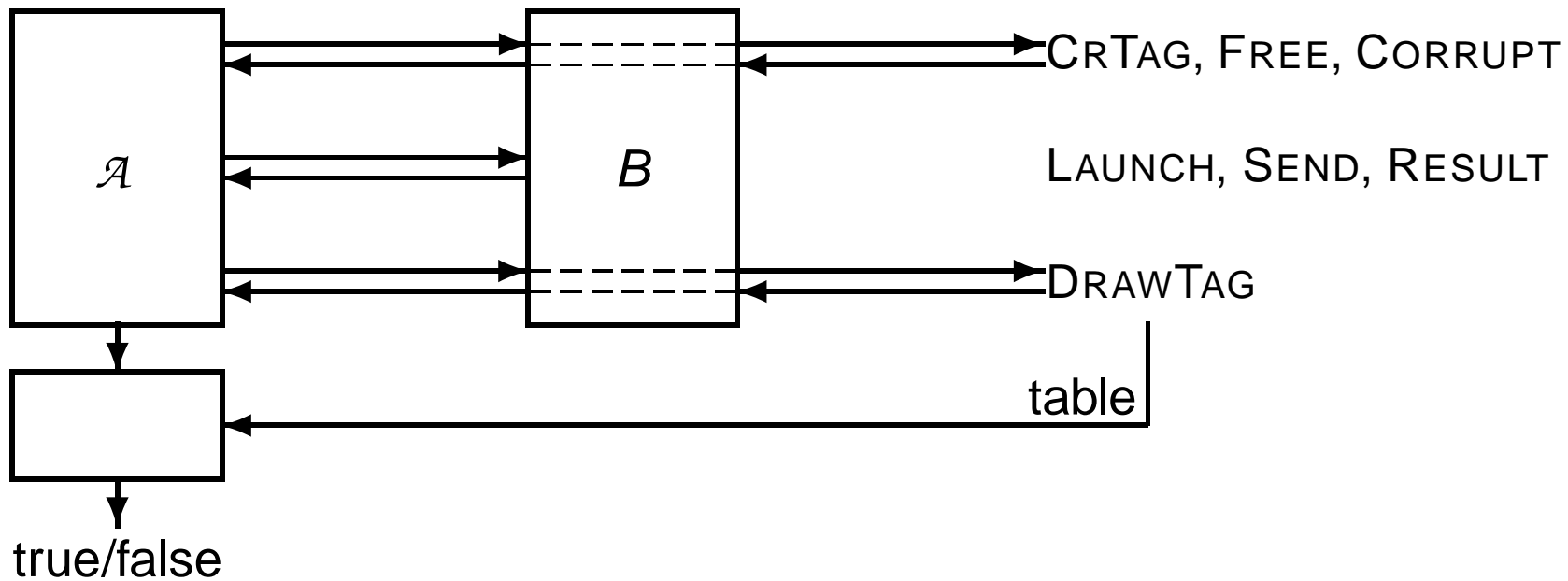
An RFID scheme is secure if for any polynomially bounded adversary the probability of success is negligible.

Privacy Adversary



- Wining condition: the adversary outputs true
- **Problem:** there are trivial wining adversaries (e.g. an adversary who always answers true)

Blinders

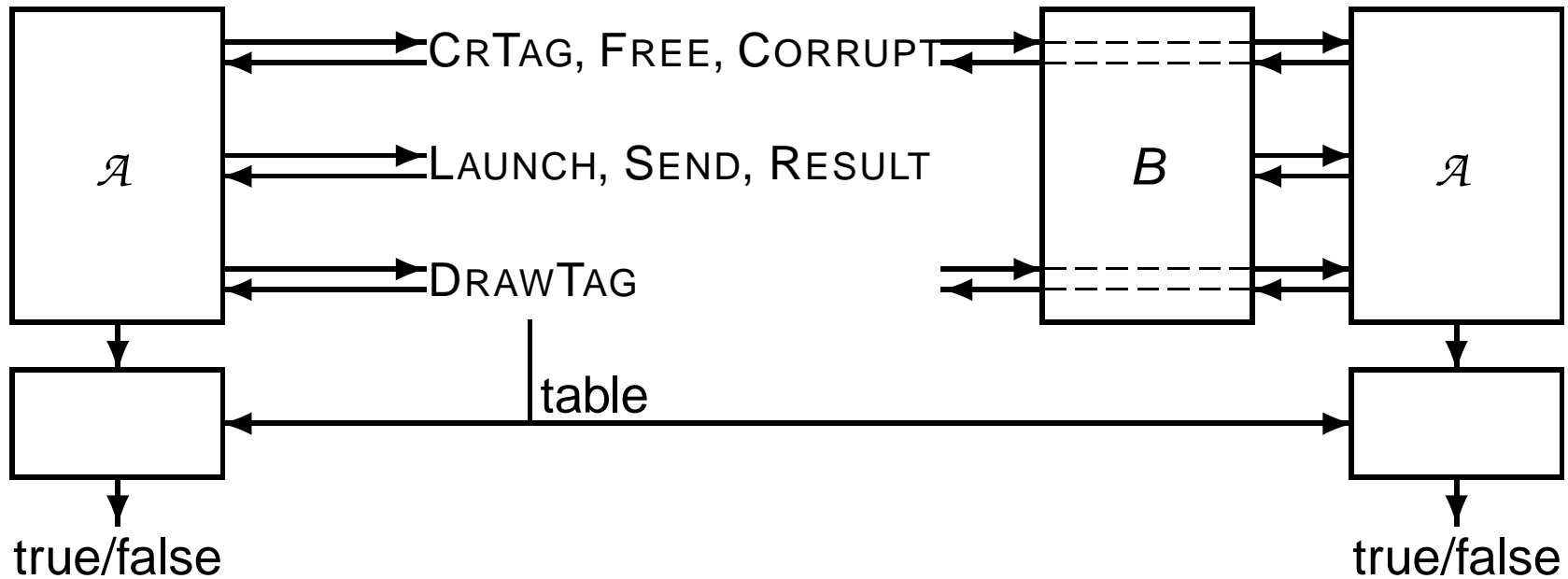


Definition

A blinder is an interface between the adversary and the oracles that

- passively looks at communications to `CREATE TAG`, `DRAW TAG`, `FREE`, and `CORRUPT` queries
- simulates the oracles `LAUNCH`, `SEND READER`, `SEND TAG`, and `RESULT`

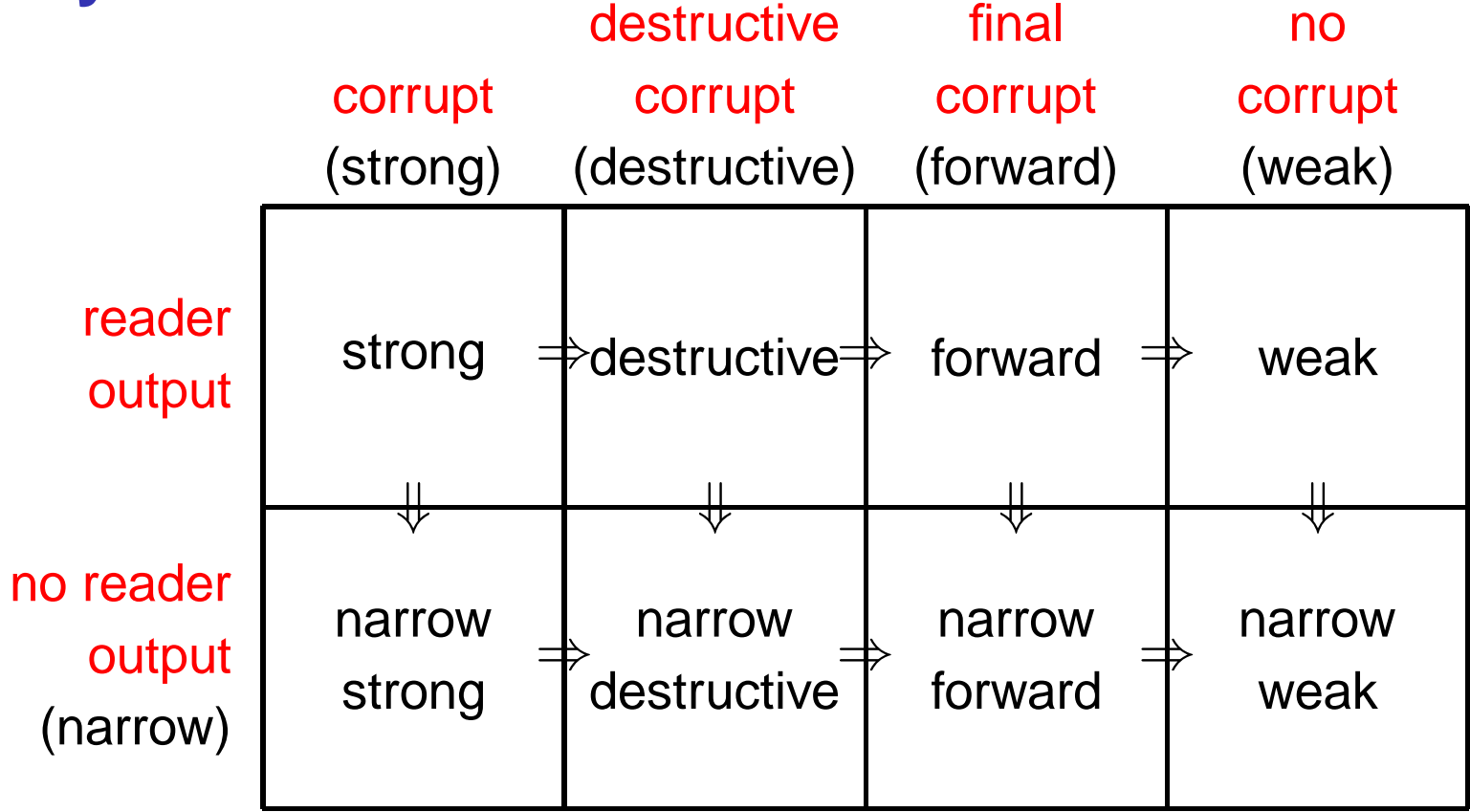
Privacy



Definition

An RFID scheme protects privacy if for any polynomially bounded \mathcal{A} there exists a polynomially bounded blinder B such that $\Pr[\mathcal{A} \text{ wins}] - \Pr[\mathcal{A}^B \text{ wins}]$ is negligible.

Privacy Models



- possible:

 (PRF)

 (ROM)

 (PKC)
- impossible:

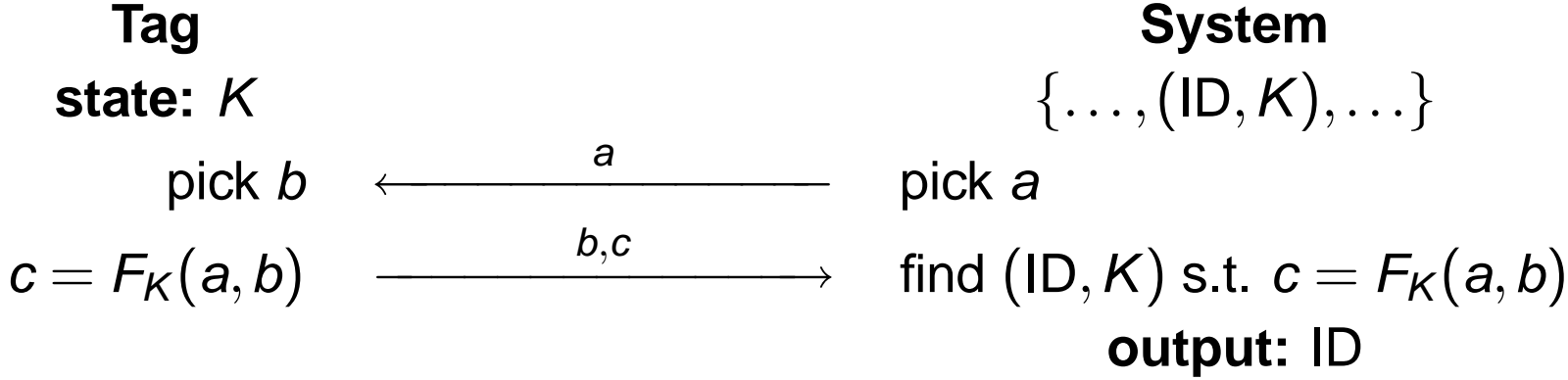
 (w/o KA)
- open:

 (w/o ROM)

 (w/o PKC)

- 1 Introduction: The RFID Technology
- 2 Case Studies: Some RFID Schemes
- 3 Definitions: 4×2 Adversarial Models
- 4 Results**
- 5 Extension to Mutual Authentication

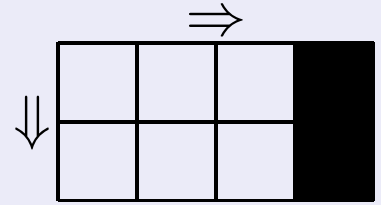
Challenge-Response RFID Scheme



Theorem

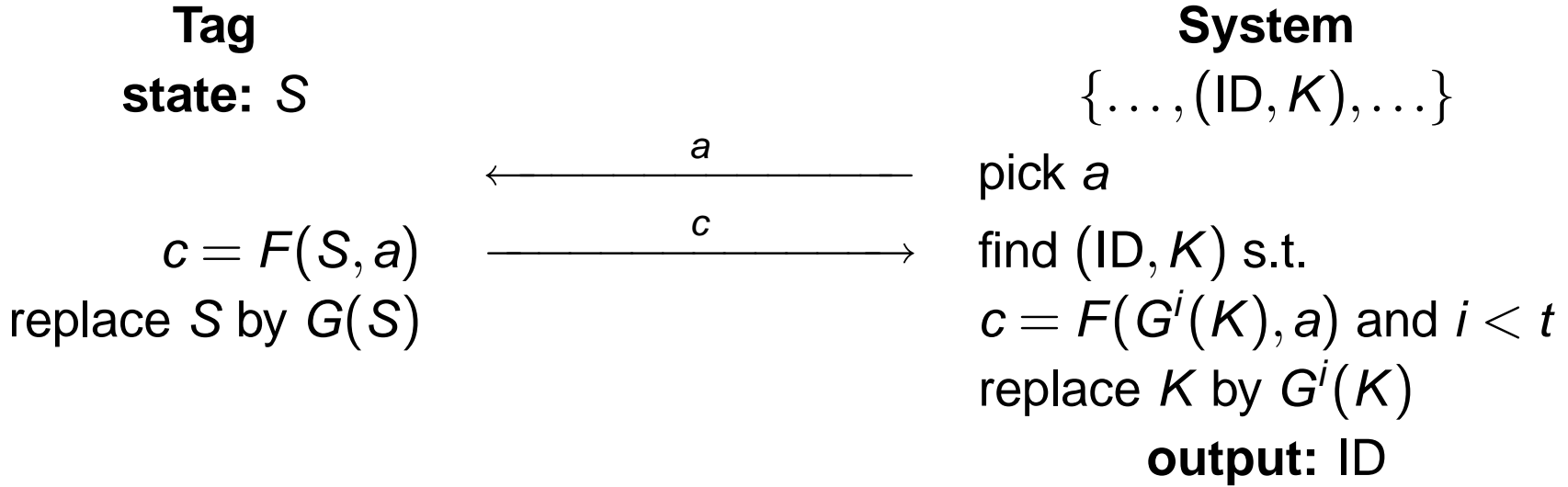
Assuming that F is a pseudorandom function, this RFID scheme is

- correct
- secure
- **weak private**



no forward privacy: trace tag by corrupting it in the future

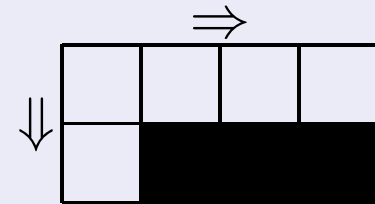
Modified Ohkubo-Suzuki-Kinoshita



Theorem

Assuming that F and G are random oracles, this RFID scheme is

- correct
- secure
- **narrow-destructive private**



no privacy with a side channel: DoS [JW 2006]

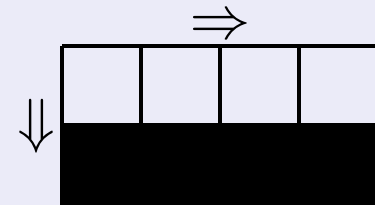
Narrow-Strong Privacy Implies Public-Key Cryptography

Theorem

An RFID scheme that is

- *correct*
- *narrow-strong private*

can be transformed into a secure key agreement protocol.



no narrow-strong privacy without public-key crypto!

Idea

Alice

SetupReader $\rightarrow (K_S, K_P)$
SetupTag $_{K_P}(ID_0) \rightarrow (S_0, K_0)$
SetupTag $_{K_P}(ID_1) \rightarrow (S_1, K_1)$

reader: $K_S, \{(ID_0, K_0), (ID_1, K_1)\}$
simulate reader

key: k

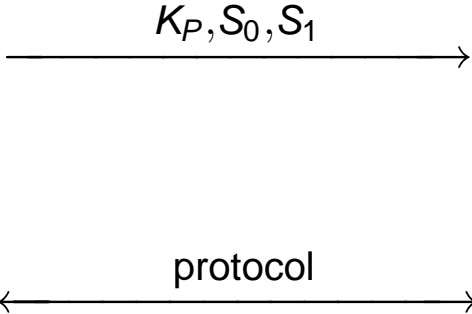
Bob

pick k

tag: S_k

simulate tag

key: k



Public-Key-Based RFID Scheme

Tag

state: K_P, ID, K

$$c = \text{Enc}_{K_P}(ID || K || a)$$

System

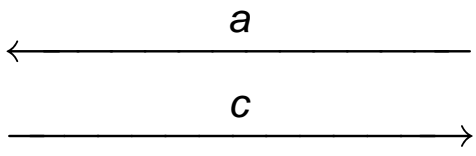
secret key: K_S
 $\{\dots, (ID, K), \dots\}$

pick a

$$\text{Dec}_{K_S}(c) = ID || K || a$$

check $a, (ID, K)$

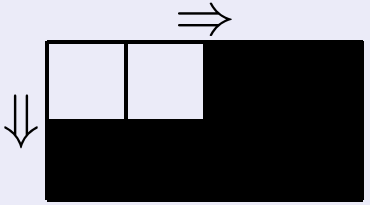
output: ID



Theorem

Assuming that Enc/Dec is an IND-CCA public-key cryptosystem, this RFID scheme is

- correct
- secure
- **narrow-strong** and **forward** private



Not Destructive Private

```
1: CREATETAG(0)
2: (vtag0, ·) ← DRAWTAG(0)
3: S0 ← CORRUPT(vtag0)
4: (·, S1) ← SETUPTAGKP(1)
5: flip a coin  $b \in \{0, 1\}$ 
6:  $\pi \leftarrow \text{LAUNCH}$ 
7: simulate a tag of state  $S_b$  with
   reader instance  $\pi$ 
8:  $x \leftarrow \text{RESULT}(\pi)$ 
9: if  $\mathcal{T}(x) = b$  then
10:   output true
11: else
12:   output false
13: end if
```

We have $\Pr[\mathcal{A} \text{ wins}] \approx 1$.

A blinder who computes x translates into an IND-CPA adversary against the public-key cryptosystem, thus $\Pr[\mathcal{A}^B \text{ wins}] \approx \frac{1}{2}$ for any B .

Hence, \mathcal{A} is a significant destructive adversary.

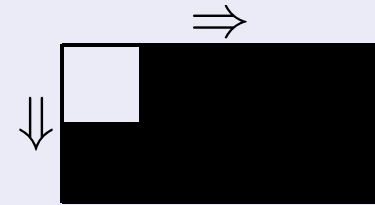
Strong Privacy is Infeasible

Theorem

An RFID scheme cannot be

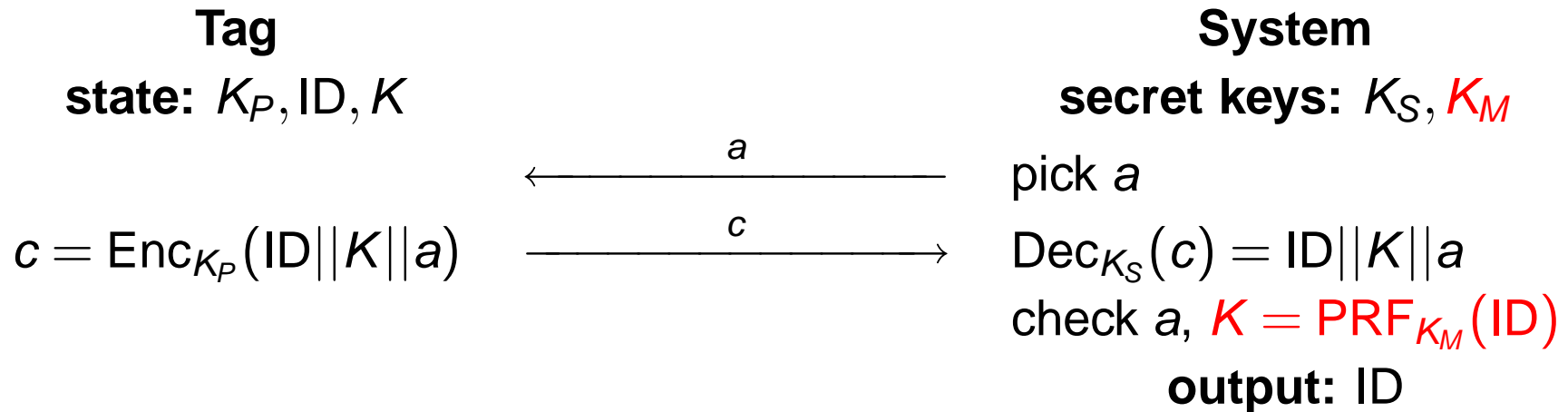
- *correct*
- *narrow-strong and destructive private*

at the same time.



no strong privacy!

Scheme with No Database



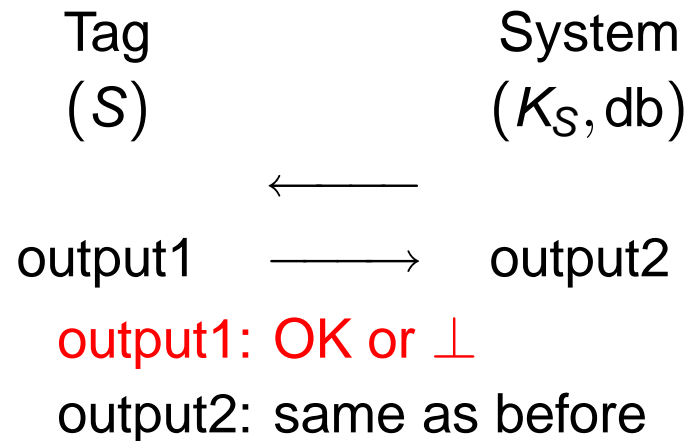
- SetupTag must now use a secret key K_M
- all the theory remains valid if SetupTag produces keys which are indistinguishable from simulated ones

- 1 Introduction: The RFID Technology
- 2 Case Studies: Some RFID Schemes
- 3 Definitions: 4×2 Adversarial Models
- 4 Results
- 5 Extension to Mutual Authentication**

RFID Scheme with Mutual Authentication

Components:

- SetupReader: same as before
- SetupTag $_{K_P}$: same as before
- Protocols:



Functionality:

- tag identification: same as before + **output1 is OK**

Crypto properties (whenever required):

- tag authentication + tag privacy: same as before
- reader authentication: **adversary cannot impersonate a reader**

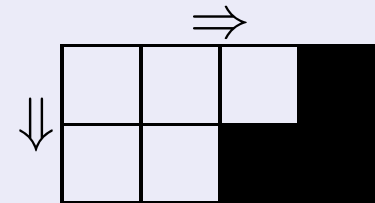
Forward Privacy is Infeasible

Theorem

An RFID scheme cannot be

- *correct*
- *with secure reader authentication*
- *narrow-forward private*

at the same time.



Idea

- in the protocol, we say that a message from reader to tag is **crucial** if there exists a simulator who can generate further messages from reader and make the tag happy but this message cannot be simulated
- if a protocol provides secure reader authentication, there must be a message from reader which is crucial
- consider this adversary:
 - 1 run a protocol between a tag and the reader
 - 2 guess which message is crucial and does not forward it
 - 3 release the tag and draw one
 - 4 corrupt it
 - 5 simulate the tag with this state with the crucial message and a simulator for further messages is a
 - 6 yield output1

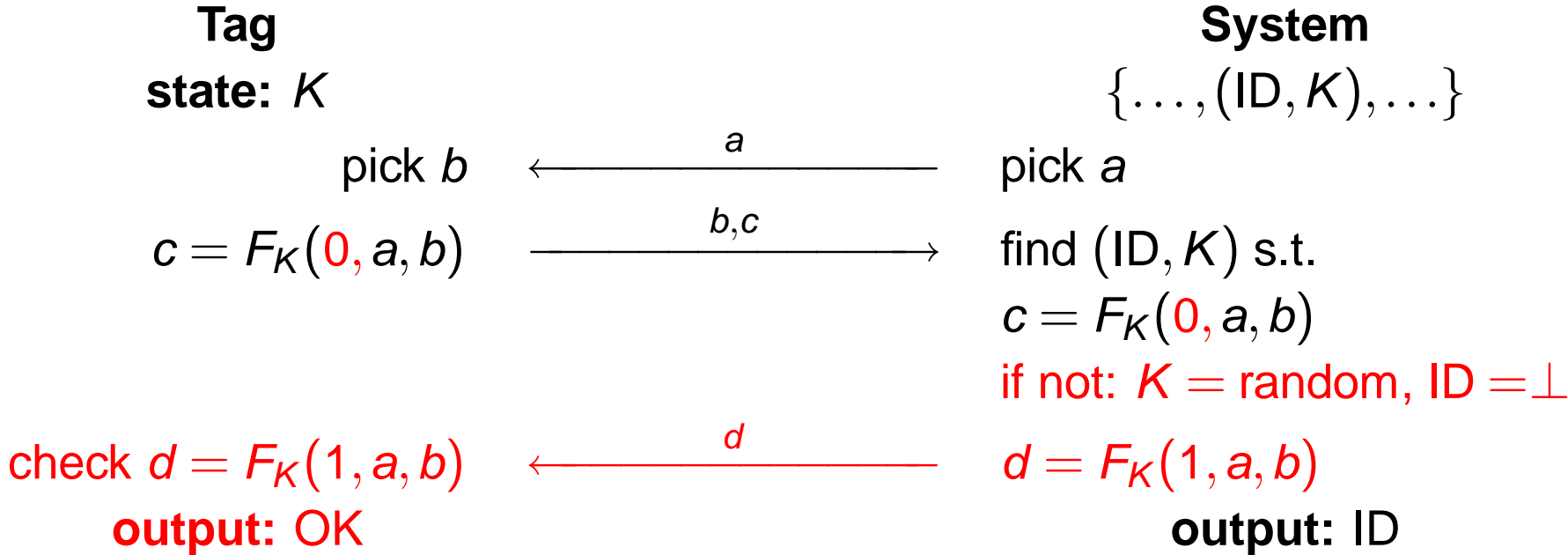
This is a **significant narrow-forward adversary**

How to Study Mutual Authentication?

assume that tags have volatile memory which resets itself when the tag is freed

consequence: adversaries can no continue an interrupted protocol after freeing and drawing a tag again

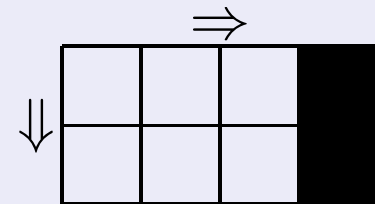
Challenge-Response RFID Scheme



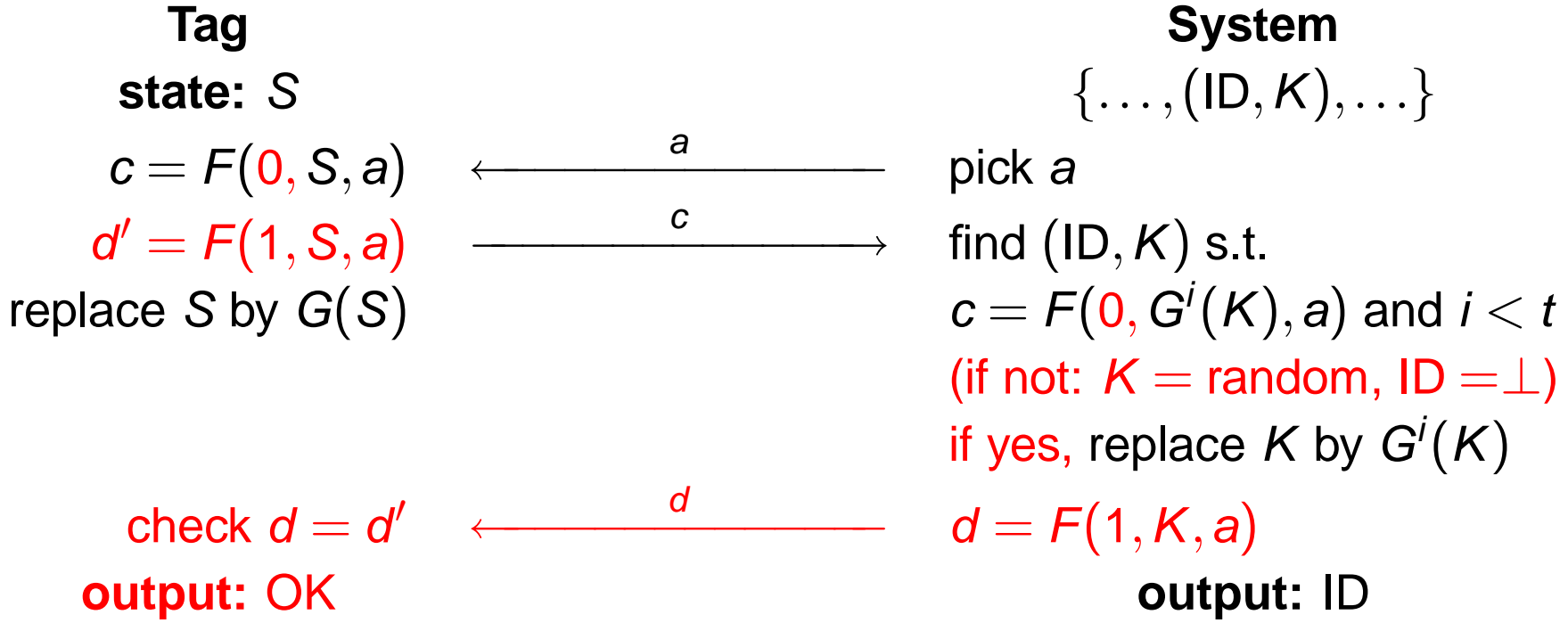
Theorem

Assuming that F is a pseudorandom function, this RFID scheme is

- correct
- secure
- **weak private**



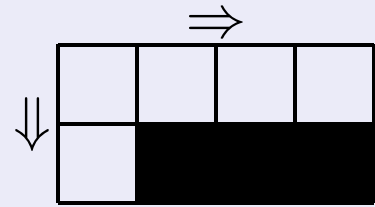
Modified Ohkubo-Suzuki-Kinoshita



Theorem

Assuming that F and G are random oracles, this RFID scheme is

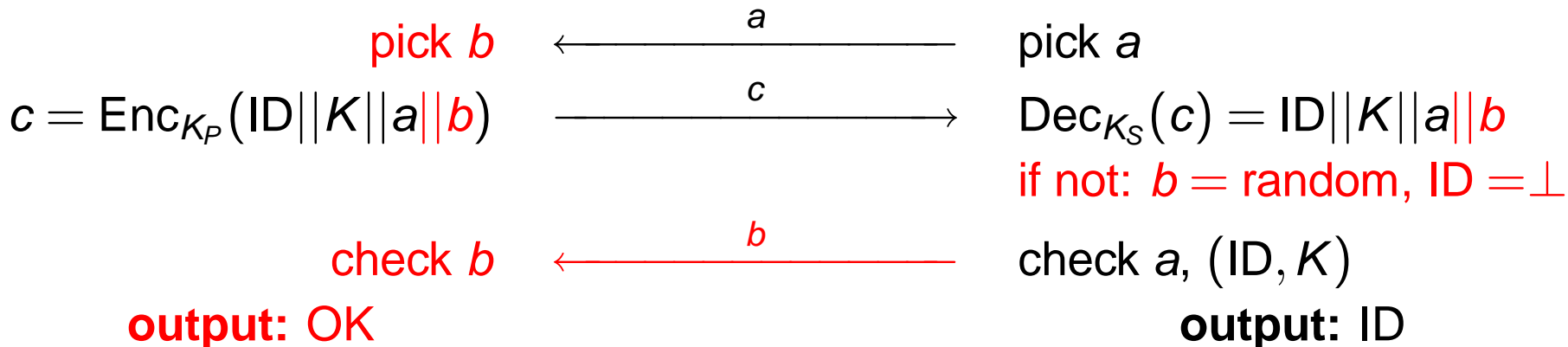
- correct
- secure
- **narrow-destructive private**



Public-Key-Based RFID Scheme

Tag
state: K_P, ID, K

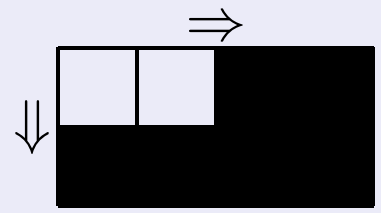
System
secret key: K_S
 $\{\dots, (ID, K), \dots\}$



Theorem

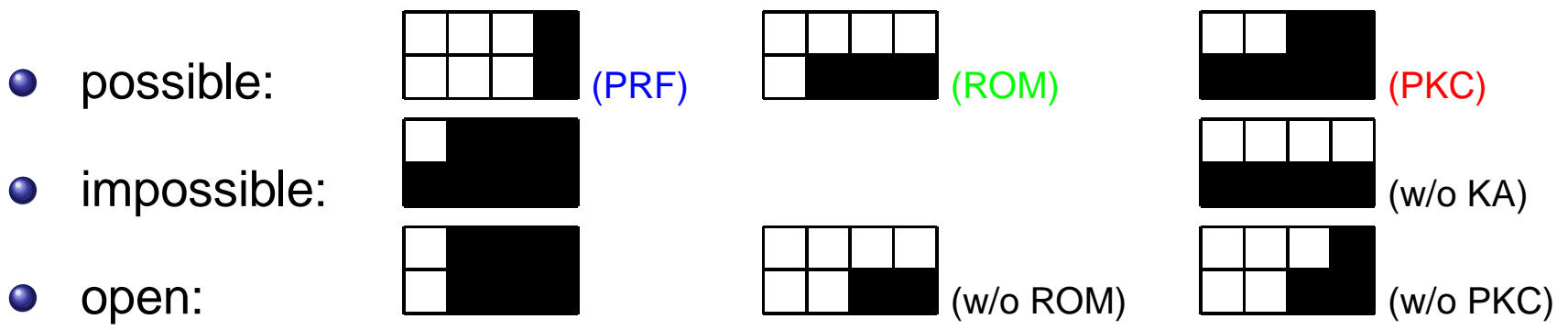
Assuming that Enc/Dec is an IND-CCA public-key cryptosystem, this RFID scheme is

- correct
- secure
- **narrow-strong and forward private**



Conclusion

	corrupt	destructive corrupt	final corrupt	no corrupt
reader output	impossible	??	doable with PK-crypto	doable with PRF
no reader output	equiv to PK-crypto	doable in ROM		



Q & A

References

- Feldhofer-Dominikus-Wolkerstrofer 2004: CHES 2004
- Juels-Weis 2006: <http://eprint.iacr.org/2006/137>
- Ohkubo-Suzuki 2005: Communications of the ACM 2005
- Ohkubo-Suzuki-Kinoshita 2003: RFID Privacy Workshop 2003
- Paise-Vaudenay 2008: ASIACCS 2008
- Vaudenay 2007: ASIACRYPT 2007
- Weis-Sarma-Rivest-Engel 2003: SPC 2003