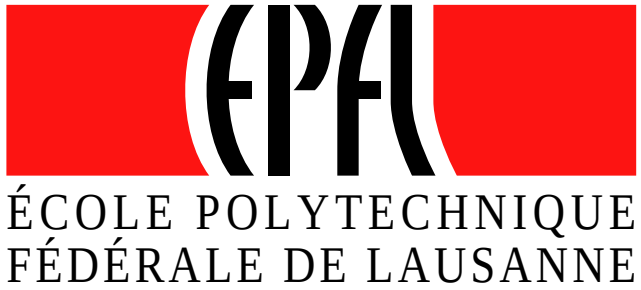
On Privacy Models for RFID

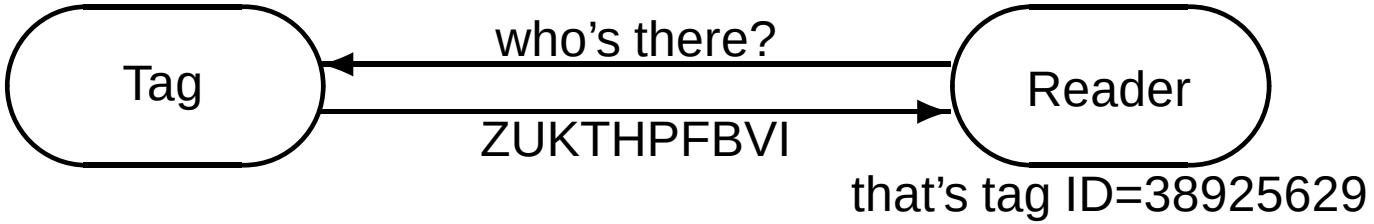
Serge Vaudenay



http://lasecwww.epfl.ch/

LASEC

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 lout 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

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 $(\mathsf{ID}, \mathsf{data})$ is inserted in database
- Protocols:

Tag		System
(S)		(K_S, db)
	$\longleftarrow$	
	$\longrightarrow$	output

output: *tag ID (if valid) or* $\perp$ *(if not)*

Functionality:

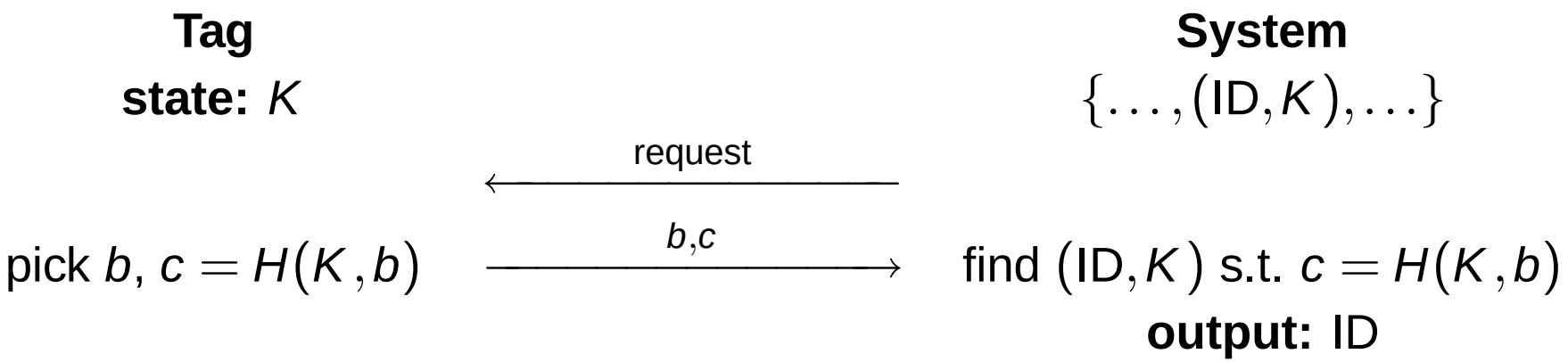
- correctness: identification under normal execution

Crypto properties (whenever required):

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

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

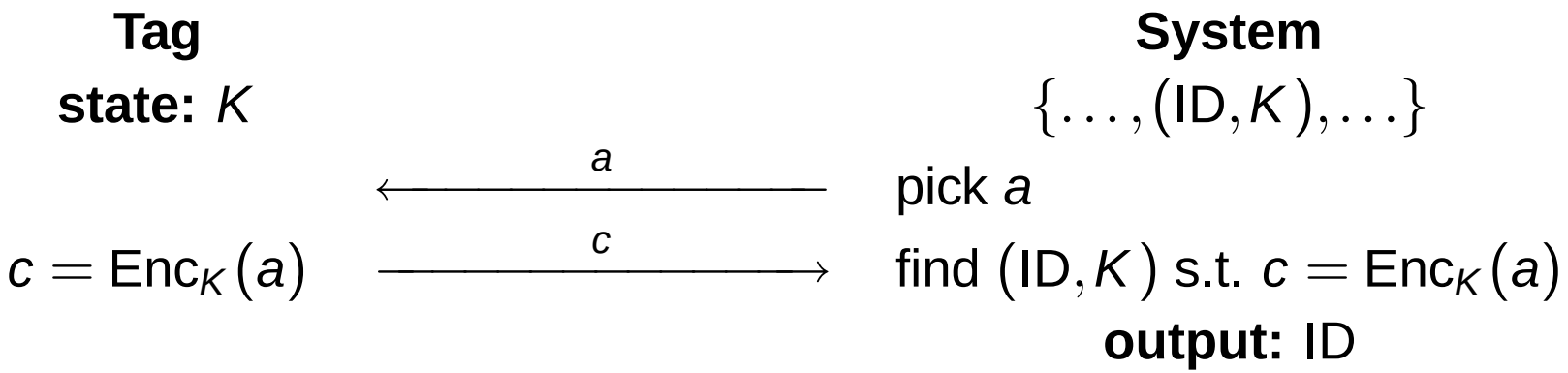
Randomized Hash-Lock Identification



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

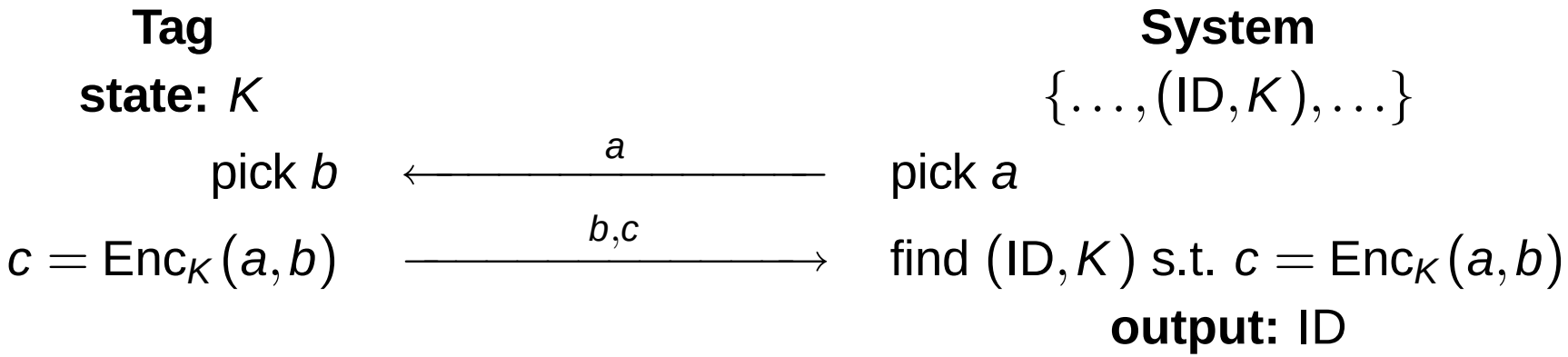
Feldhofer-Dominikus-Wolkerstorfer 2004 [FDW 2004]

ISO/IEC 9798-2 2-Pass Unilateral Authentication



traceability: replaying a leads to the same c

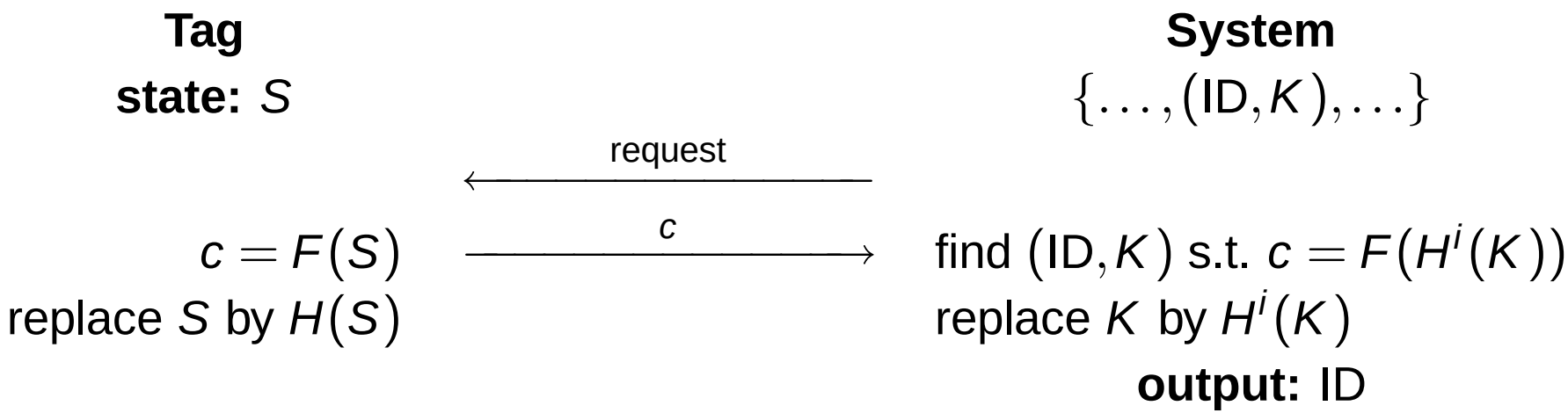
Variant



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

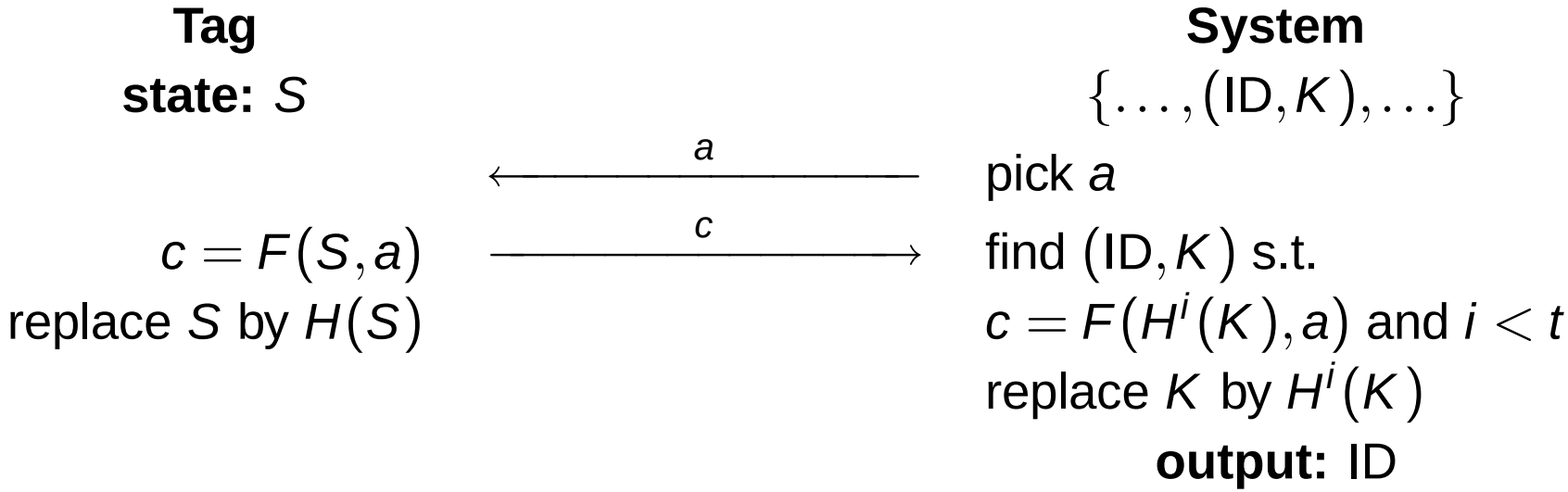
Ohkubo-Suzuki-Kinoshita 2003 [OSK 2003]

Introducing Forward Privacy



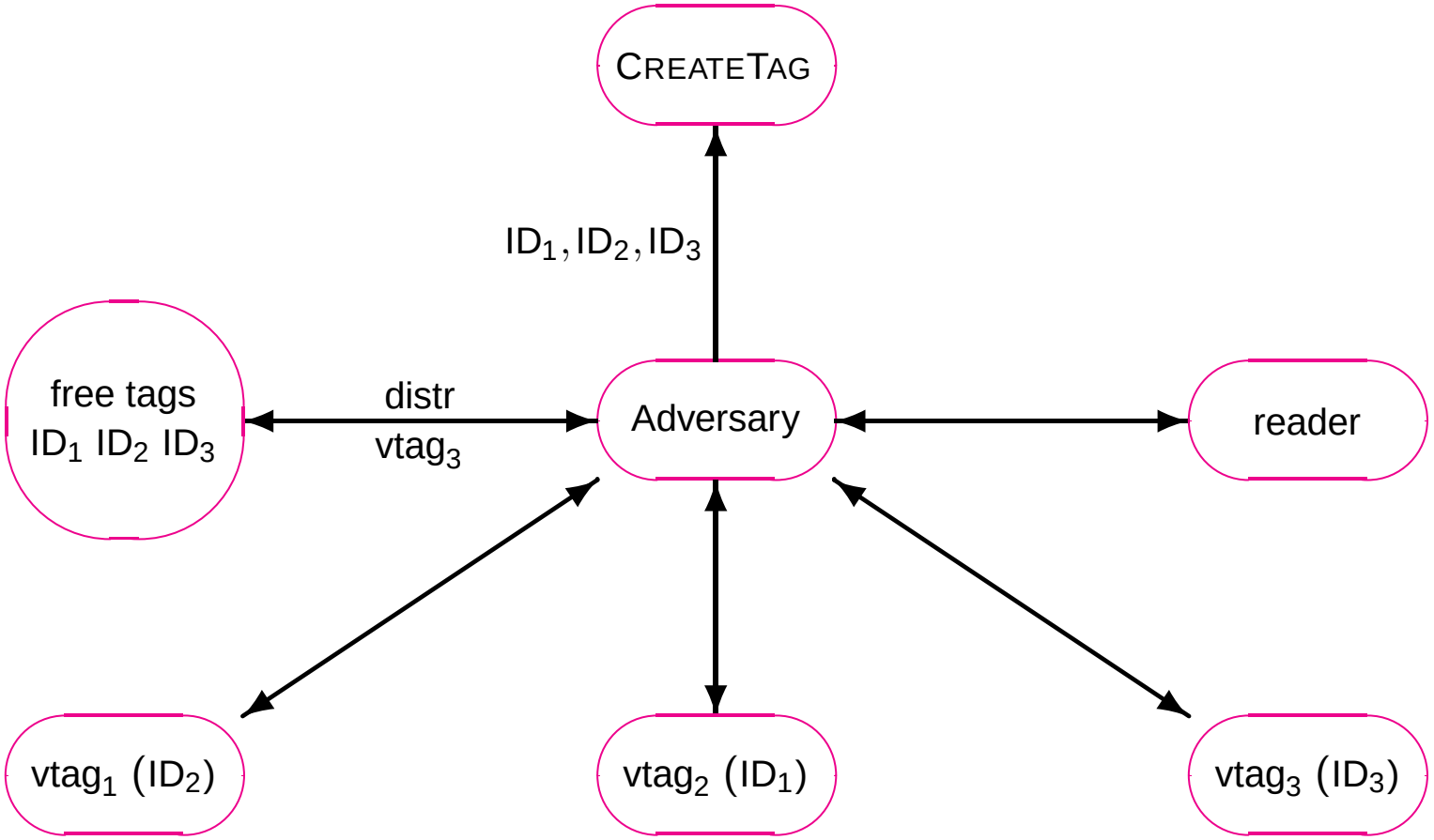
not secure: can intercept c and play it later ($\equiv$ hash lock)

Variant

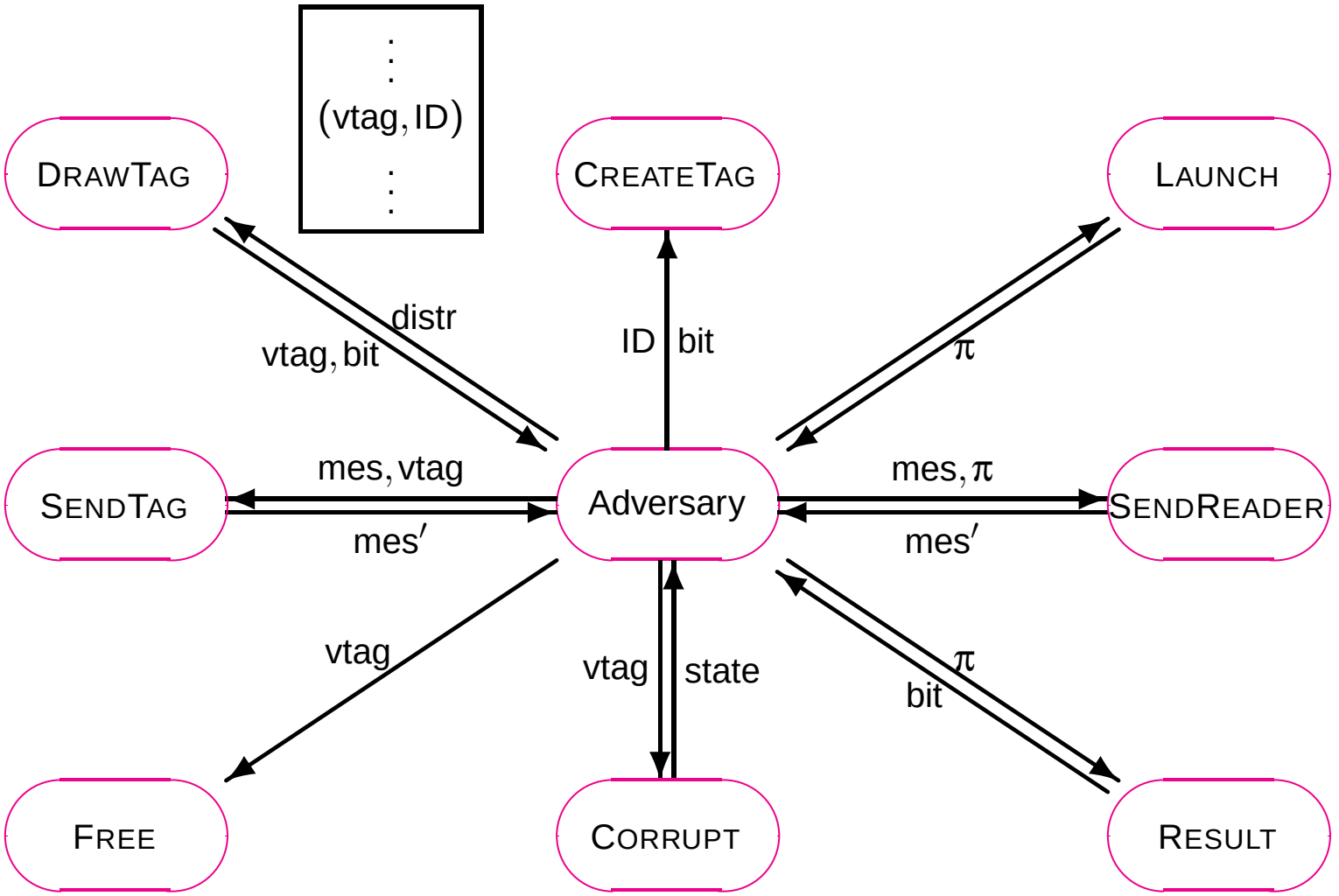


no privacy with a side channel: DoS [JW 2006]

Adversarial Model



Oracle Accesses



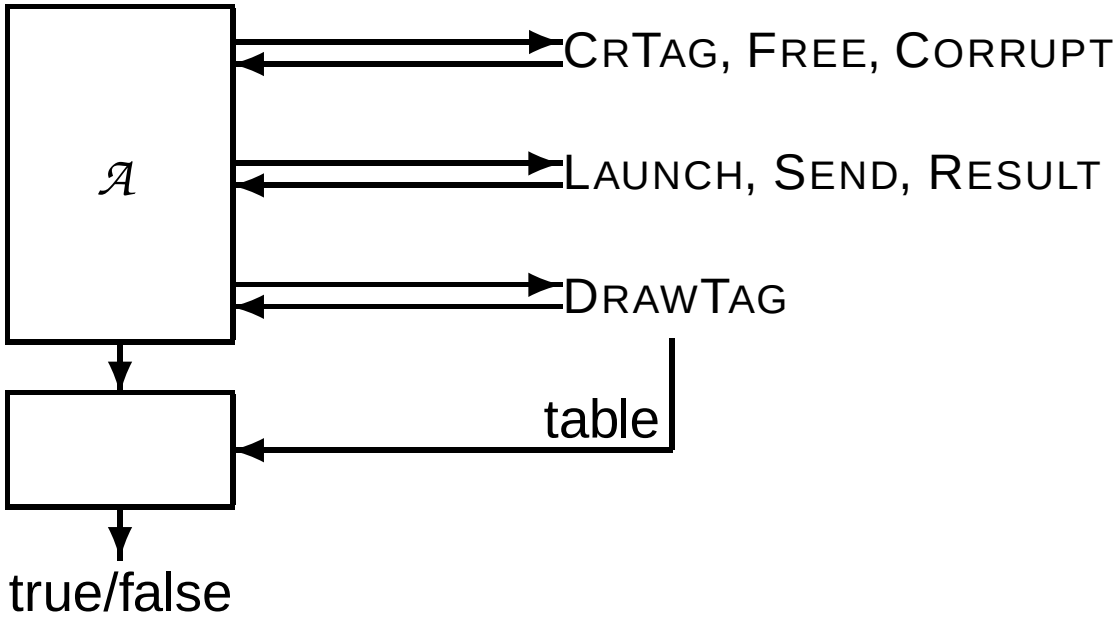
Security

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

Definition

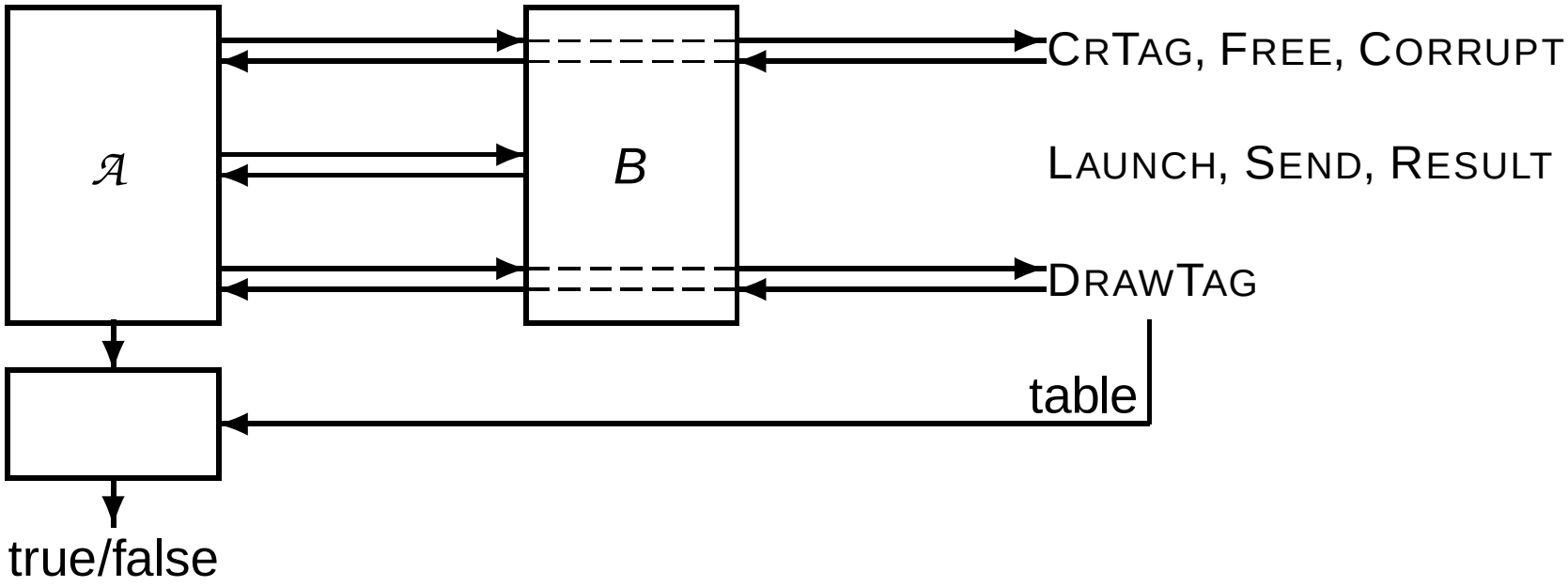
An RFID scheme is secure if for any polynomially bounded adversary the probability of success is negligible.

Privacy Adversary



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

Blinders

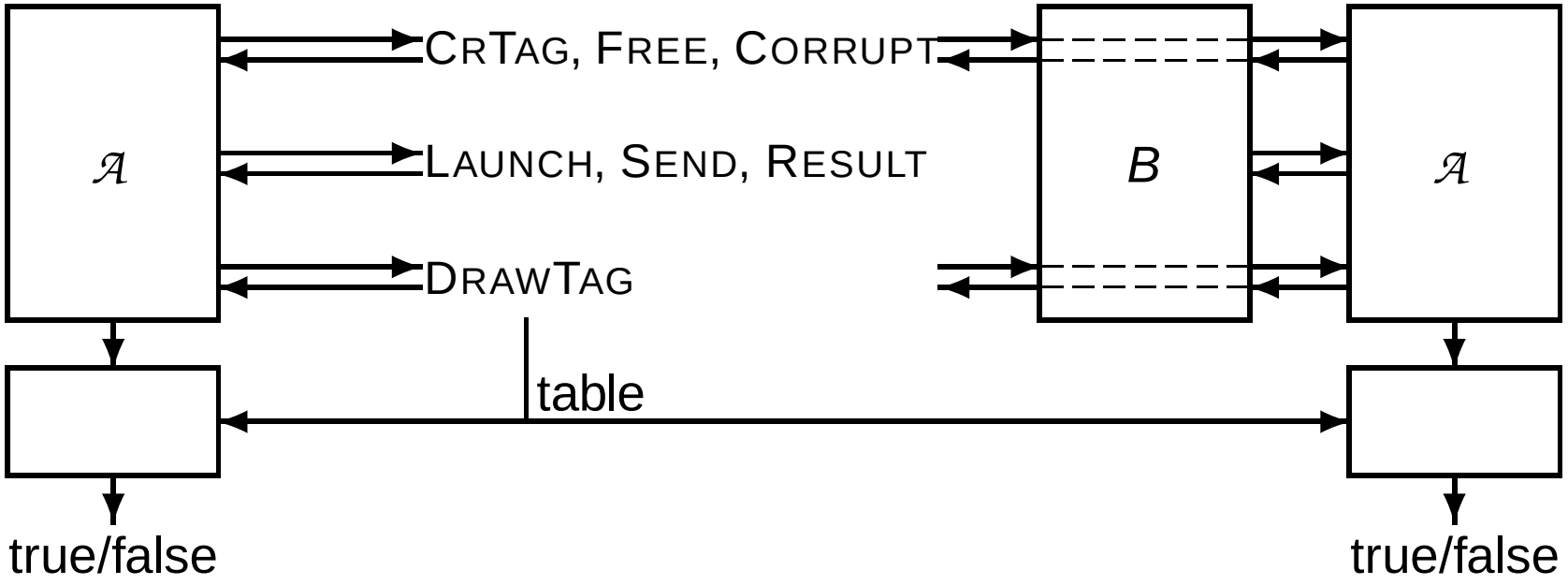


Definition

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

- passively looks at communications to CreateTag, DrawTag, Free, and Corrupt queries
- simulates the oracles Launch, SendReader, SendTag, and Result

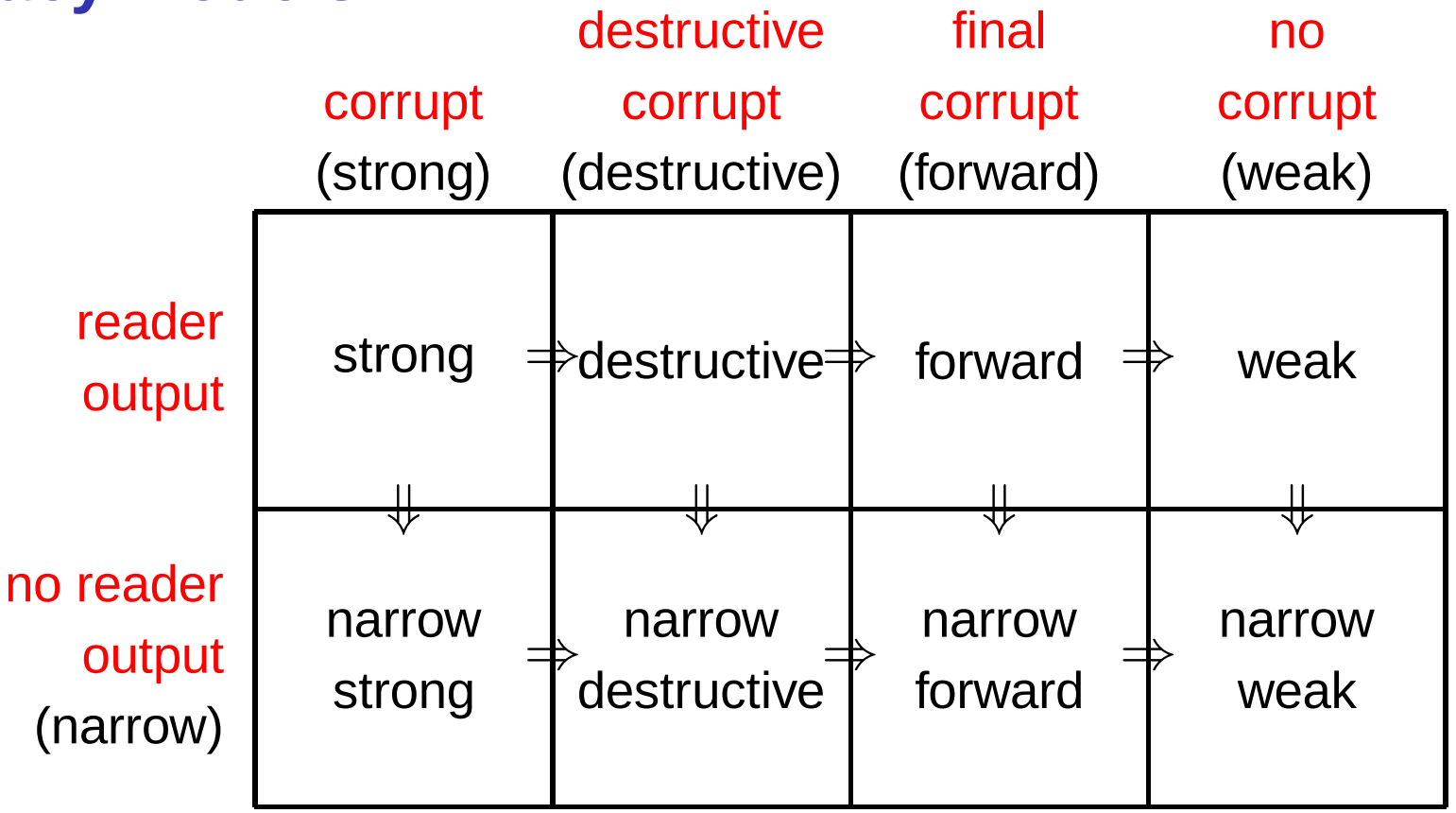
Privacy



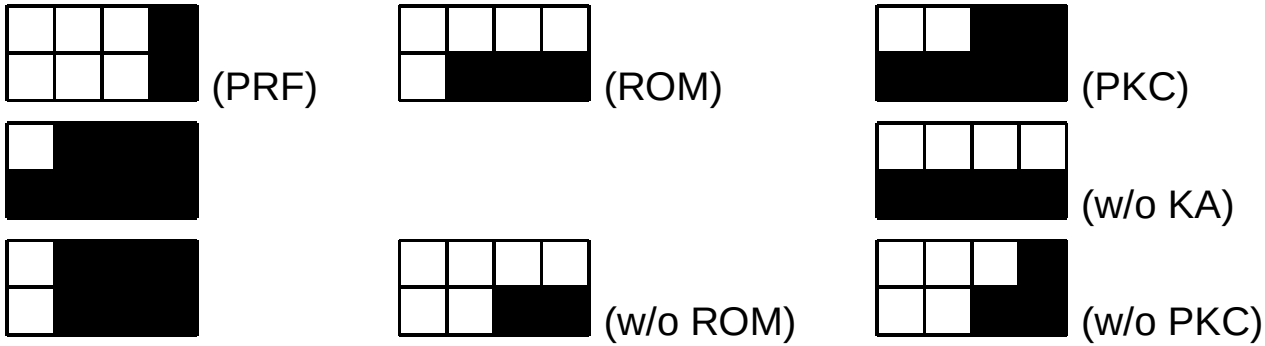
Definition

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.

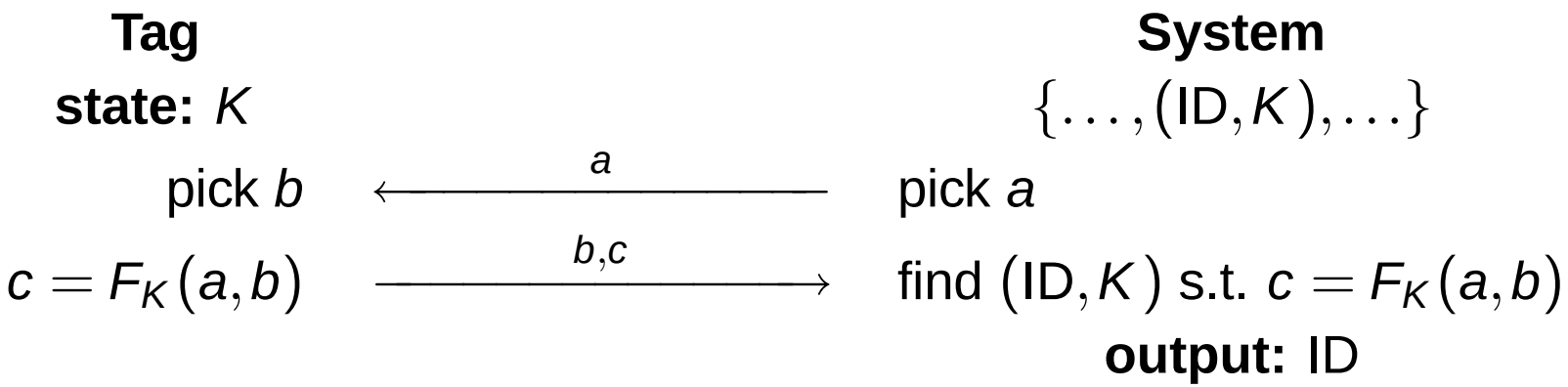
Privacy Models



- possible:
- impossible:
- open:



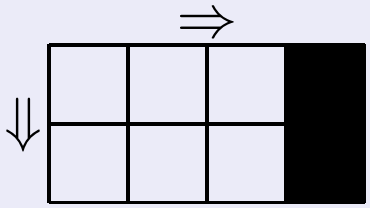
Challenge-Response RFID Scheme



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

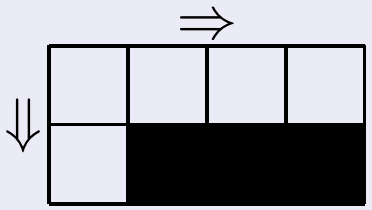
Modified Ohkubo-Suzuki-Kinoshita

Tag		**System**
state: S		$\{\ldots,(\mathsf{ID},K),\ldots\}$
	$\xleftarrow{a}$	pick a
$c = F(S,a)$	$\xrightarrow{c}$	find (ID,K) s.t.
replace S by $G(S)$		$c = F(G^i(K),a)$ and $i < t$
		replace K by $G^i(K)$
		output: ID

Theorem

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

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



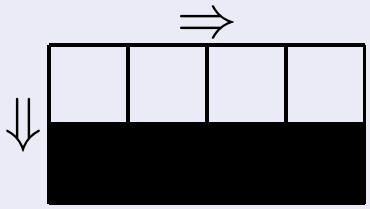
no privacy with a side channel: DoS [JW 2006]

Narrow-Strong Privacy Implies Public-Key Cryptography

Theorem

An RFID scheme that is

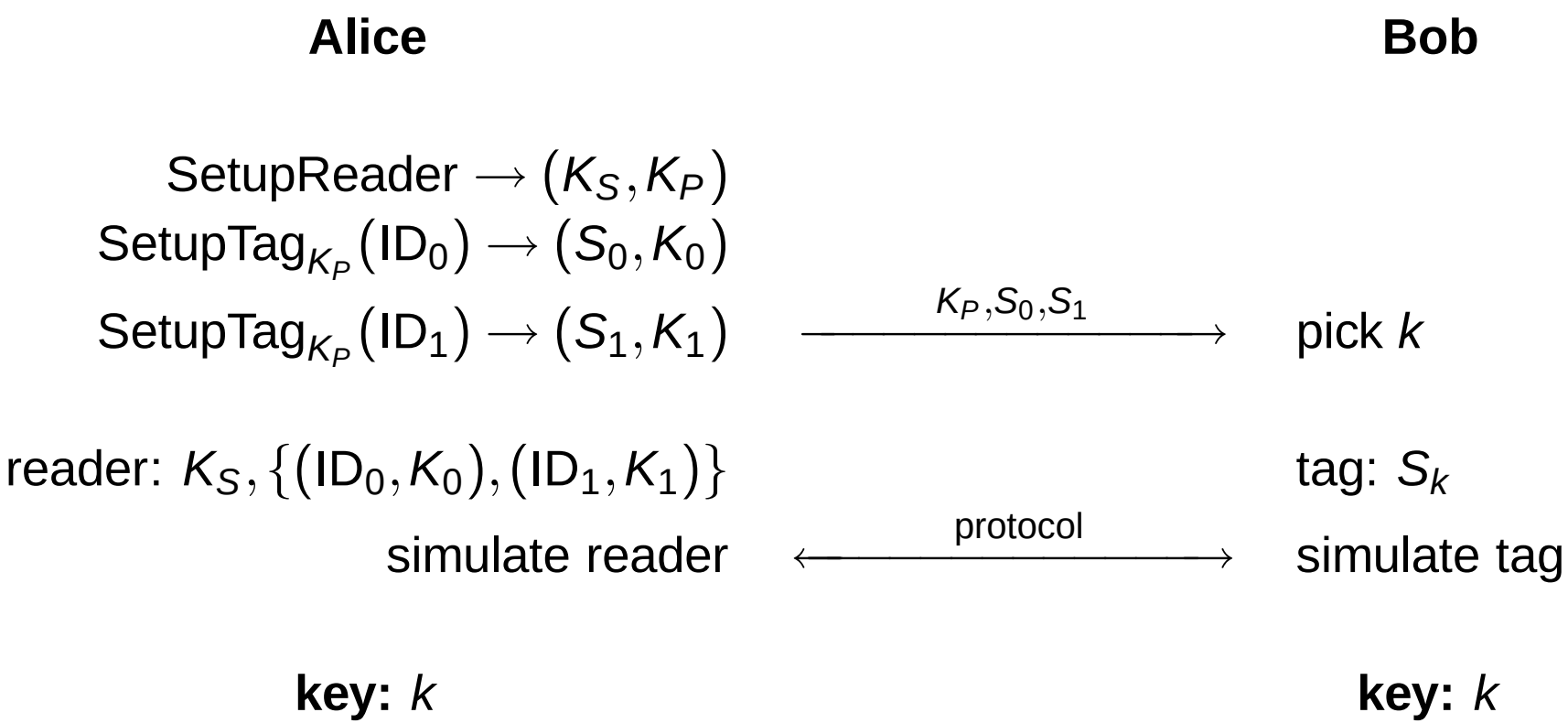
- *correct*
- *narrow-strong private*



can be transformed into a secure key agreement protocol.

no narrow-strong privacy without public-key crypto!

Idea


Alice
Bob
SetupReader $\longrightarrow (K_S, K_P)$
SetupTag$_{K_P}(\mathrm{ID}_0) \longrightarrow (S_0, K_0)$
SetupTag$_{K_P}(\mathrm{ID}_1) \longrightarrow (S_1, K_1)$
K_P, S_0, S_1
pick k
reader: $K_S, \{(\mathrm{ID}_0, K_0), (\mathrm{ID}_1, K_1)\}$
tag: S_k
protocol
simulate reader
simulate tag
key: k
key: k

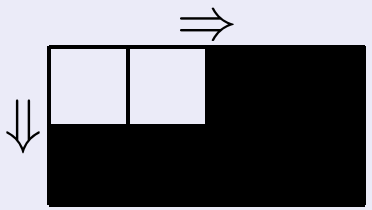
Public-Key-Based RFID Scheme

Tag		**System**
state: K_P, ID, K		**secret key:** K_S
		$\{\ldots, (\mathsf{ID}, K), \ldots\}$
	$\xleftarrow{\quad a \quad}$	pick a
$c = \mathsf{Enc}_{K_P}(\mathsf{ID}\|\|K\|\|a)$	$\xrightarrow{\quad c \quad}$	$\mathsf{Dec}_{K_S}(c) = \mathsf{ID}\|\|K\|\|a$
		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: $\textsc{CreateTag}(0)$
2: $(\text{vtag}_0, \cdot) \leftarrow \textsc{DrawTag}(0)$
3: $S_0 \leftarrow \textsc{Corrupt}(\text{vtag}_0)$
4: $(\cdot, S_1) \leftarrow \textsc{SetupTag}_{K_P}(1)$
5: flip a coin $b \in \{0,1\}$
6: $\pi \leftarrow \textsc{Launch}$
7: simulate a tag of state S_b with reader instance π
8: $x \leftarrow \textsc{Result}(\pi)$
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.

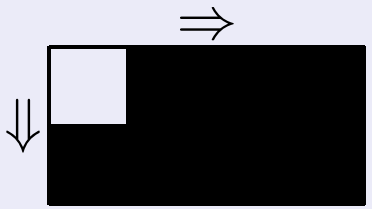
Strong Privacy is Infeasible

Theorem

An RFID scheme cannot be

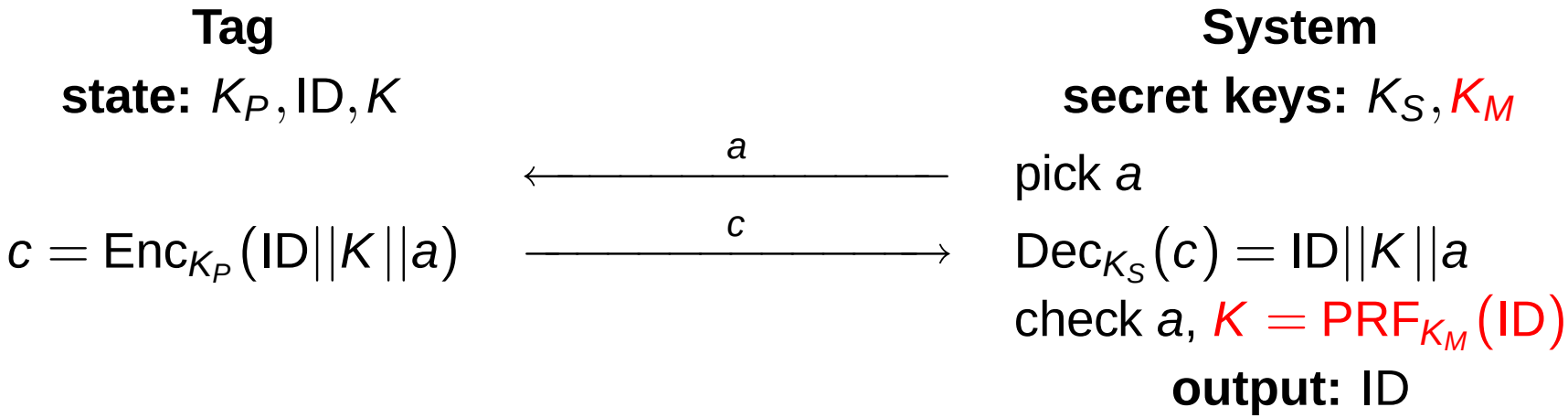
- *correct*
- *narrow-strong and destructive private*

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

RFID Scheme with Mutual Authentication

Components:

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

Tag		System
(S)		(K_S, db)
	$\longleftarrow$	
output1	$\longrightarrow$	output2

output1: OK or $\perp$

output2: same as before

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

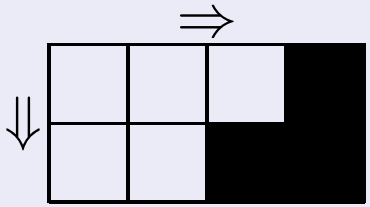
Forward Privacy is Infeasible

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 freeed

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

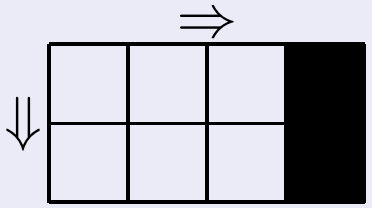
Challenge-Response RFID Scheme

Tag		**System**
state: K		$\{\ldots,(\mathsf{ID},K),\ldots\}$
pick b	$\xleftarrow{a}$	pick a
$c = F_K(0,a,b)$	$\xrightarrow{b,c}$	find (ID,K) s.t. $c = F_K(0,a,b)$ if not: $K =$ random, $\mathsf{ID} = \perp$
check $d = F_K(1,a,b)$	$\xleftarrow{d}$	$d = F_K(1,a,b)$
output: OK		**output:** ID

Theorem

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

- *correct*
- *secure*
- ***weak** private*



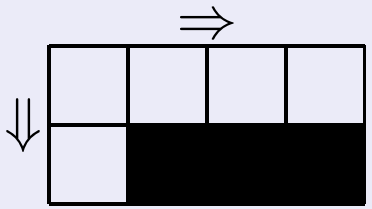
Modified Ohkubo-Suzuki-Kinoshita

Tag		**System**
state: S		$\{\ldots,(\mathsf{ID},K),\ldots\}$
$c = F(0,S,a)$	$\xleftarrow{a}$	pick a
$d' = F(1,S,a)$	$\xrightarrow{c}$	find (ID,K) s.t.
replace S by $G(S)$		$c = F(0,G^i(K),a)$ and $i < t$
		(if not: $K =$ random, $\mathsf{ID} = \perp$)
		if yes, replace K by $G^i(K)$
check $d = d'$	$\xleftarrow{d}$	$d = F(1,K,a)$
output: OK		**output:** ID

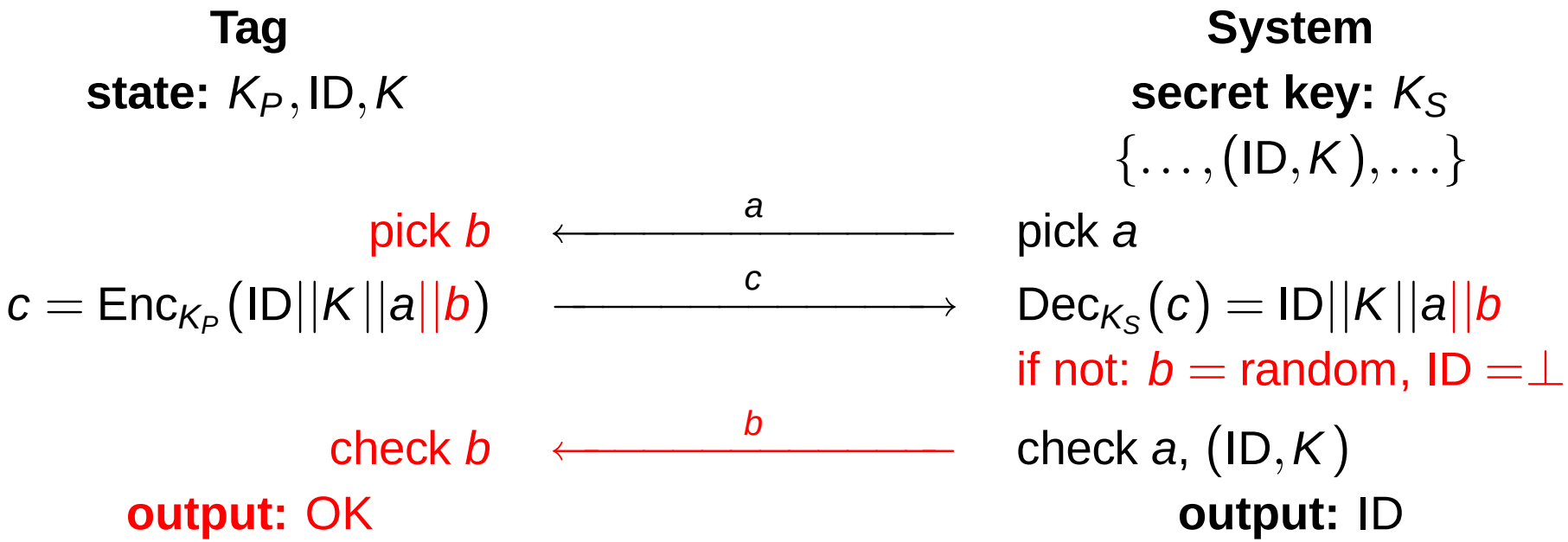
Theorem

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

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



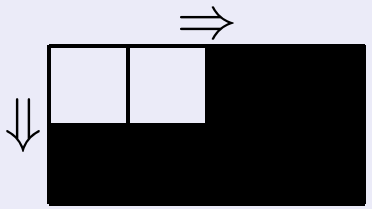
Public-Key-Based RFID Scheme



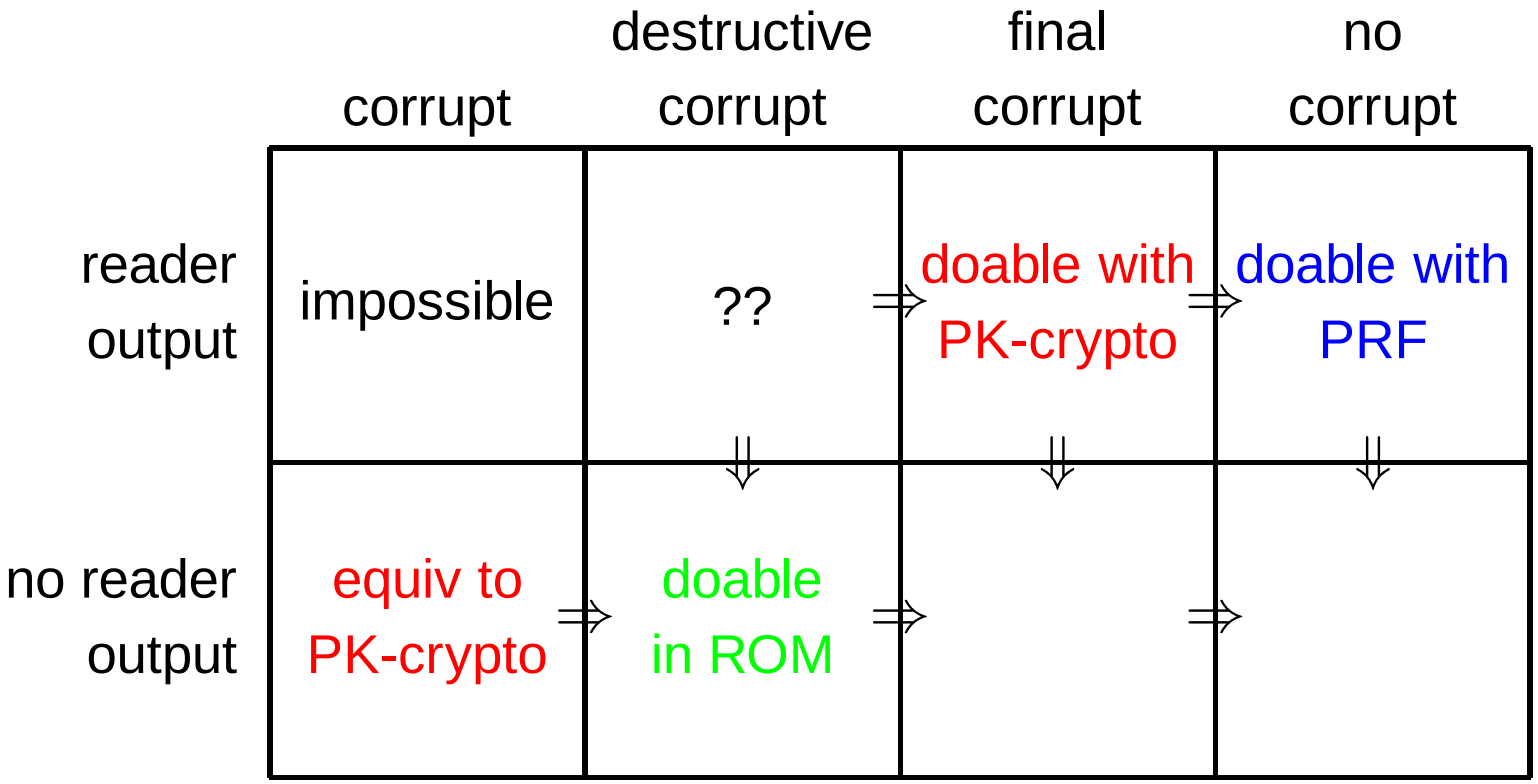
Theorem

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

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



Conclusion



- possible: (PRF) (ROM) (PKC)
- impossible: (w/o KA)
- open: (w/o ROM) (w/o PKC)

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