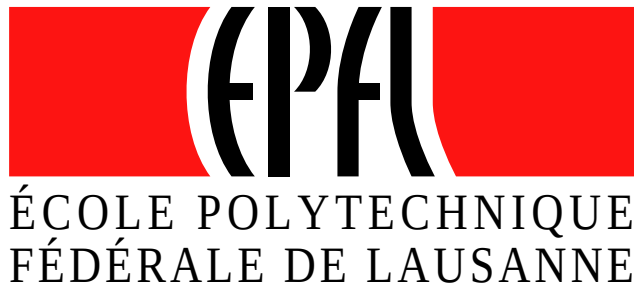
Strong Privacy for RFID Systems from Plaintext-Aware Encryption

Khaled Ouafi and Serge Vaudenay

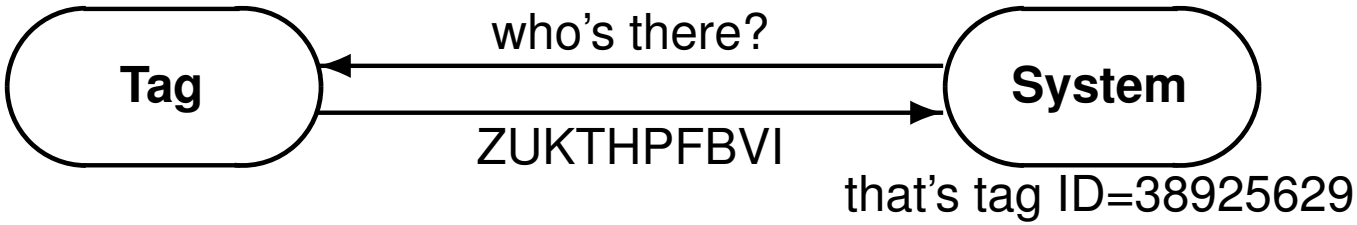


http://lasec.epfl.ch/

supported by the ECRYPT project

LASEC

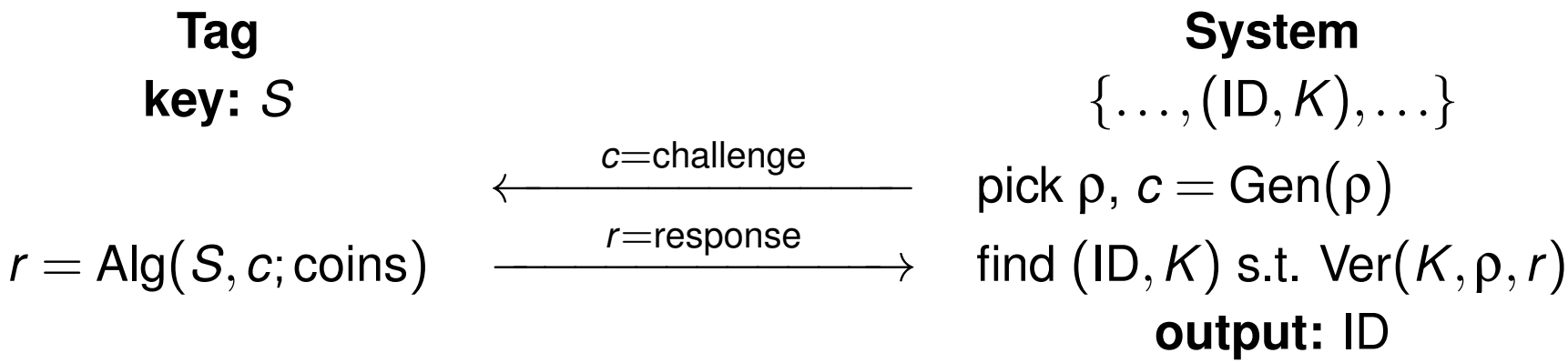
Our Problem



- **one system** (may include several readers), many tags
- tags: **passive** (no battery), limited capabilities, not tamper-proof
- primary concern (industry driven): **security**
  if System identifies tag ID, it must be tag ID
- secondary concern (user driven): **privacy**
  tags could only be identified/traced/linked by System
- problem: formal model

LASEC

A Typical Protocol



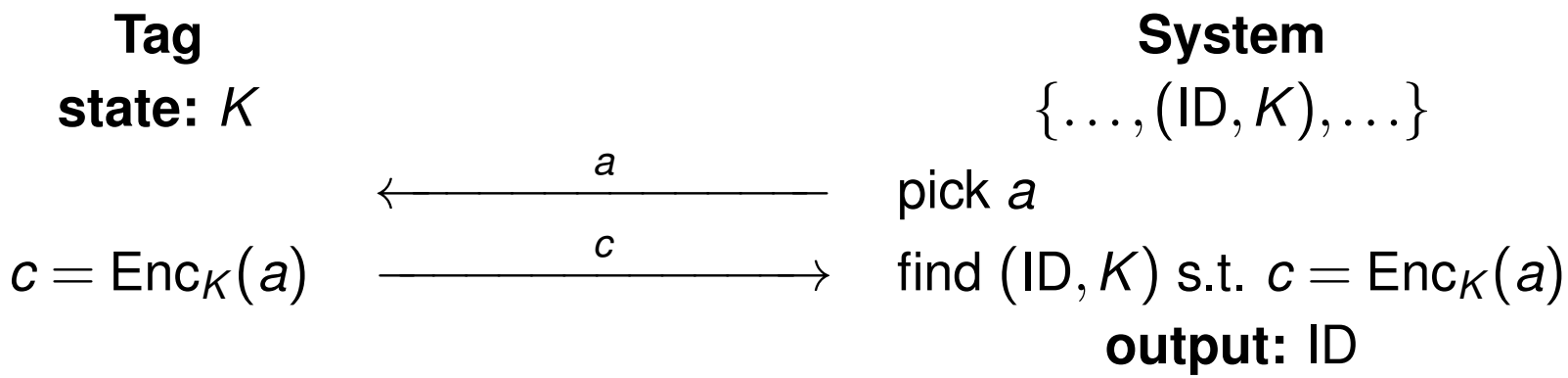
- stateless
- 2-round

1. Towards a Formal Model
2. Definitions and Results
3. Strong Privacy is Possible

LASEC

LASEC

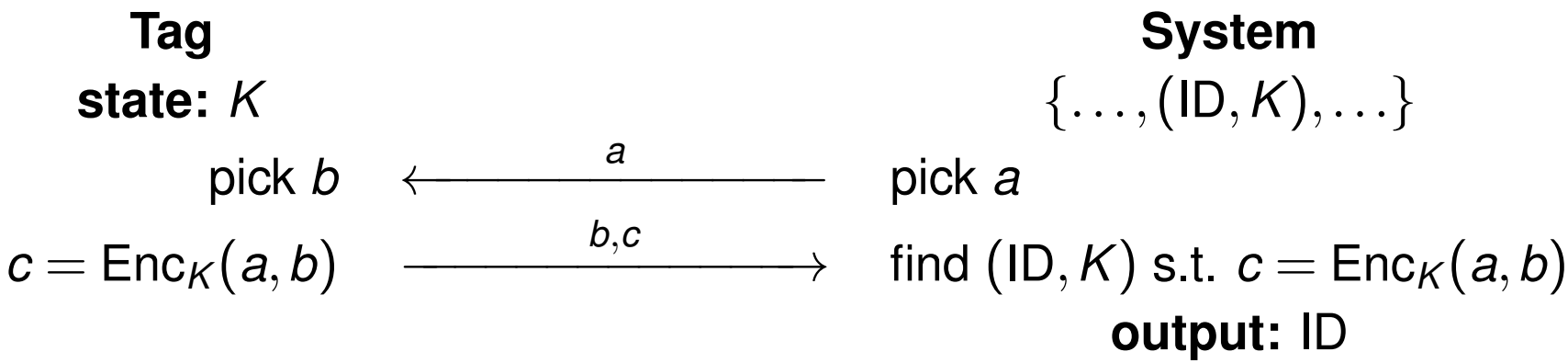
ISO/IEC 9798-2 2-Pass Unilateral Authentication



pro stateless, symmetric crypto

con replay attack $\longrightarrow$ tag traceability

Variant



pro stateless, symmetric crypto, secure, weak privacy

con tag corruption $\longrightarrow$ tag traceability

Evolution of Privacy Protocols

- early: did not address corruption or result channel
- OSK03: corruption at the end only (forward privacy)
- ADO06: early corruption considered
- JW06: result channel considered
- Vau07: 2×4 matrix (result channel $\times$ corruption model)

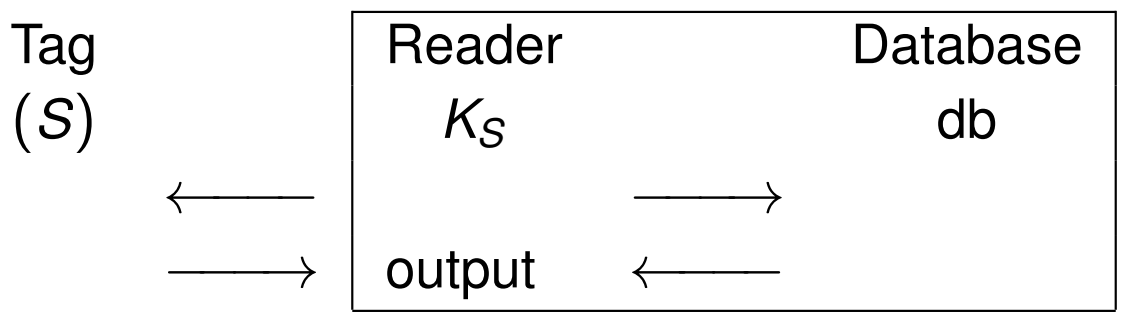
LASEC

LASEC

RFID Scheme

Components:

- System = (stateless) Reader $\overset{\text{securely connected}}{\longleftrightarrow}$ (stateful) Database
- SetupReader $\rightarrow (K_S, K_P)$:
  generate keys (K_S, K_P), store in Reader, and empty database
- SetupTag$_{K_P}$(ID) $\rightarrow (K, S)$:
  S is an initial state for tag ID
  (ID, data) is to be inserted in database
- Protocols:

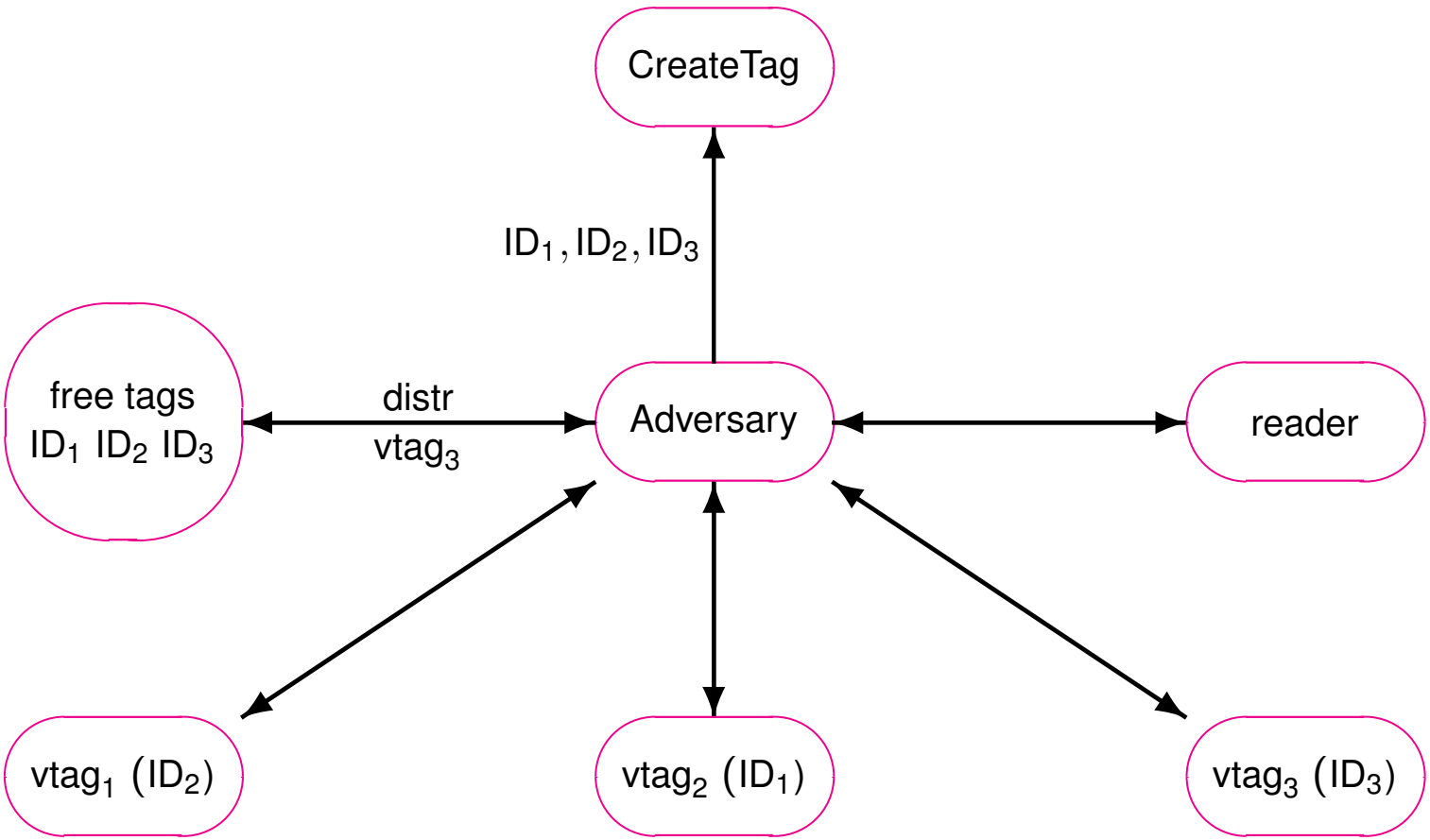


output: *tag ID (if valid) or* $\perp$ *(if not)*

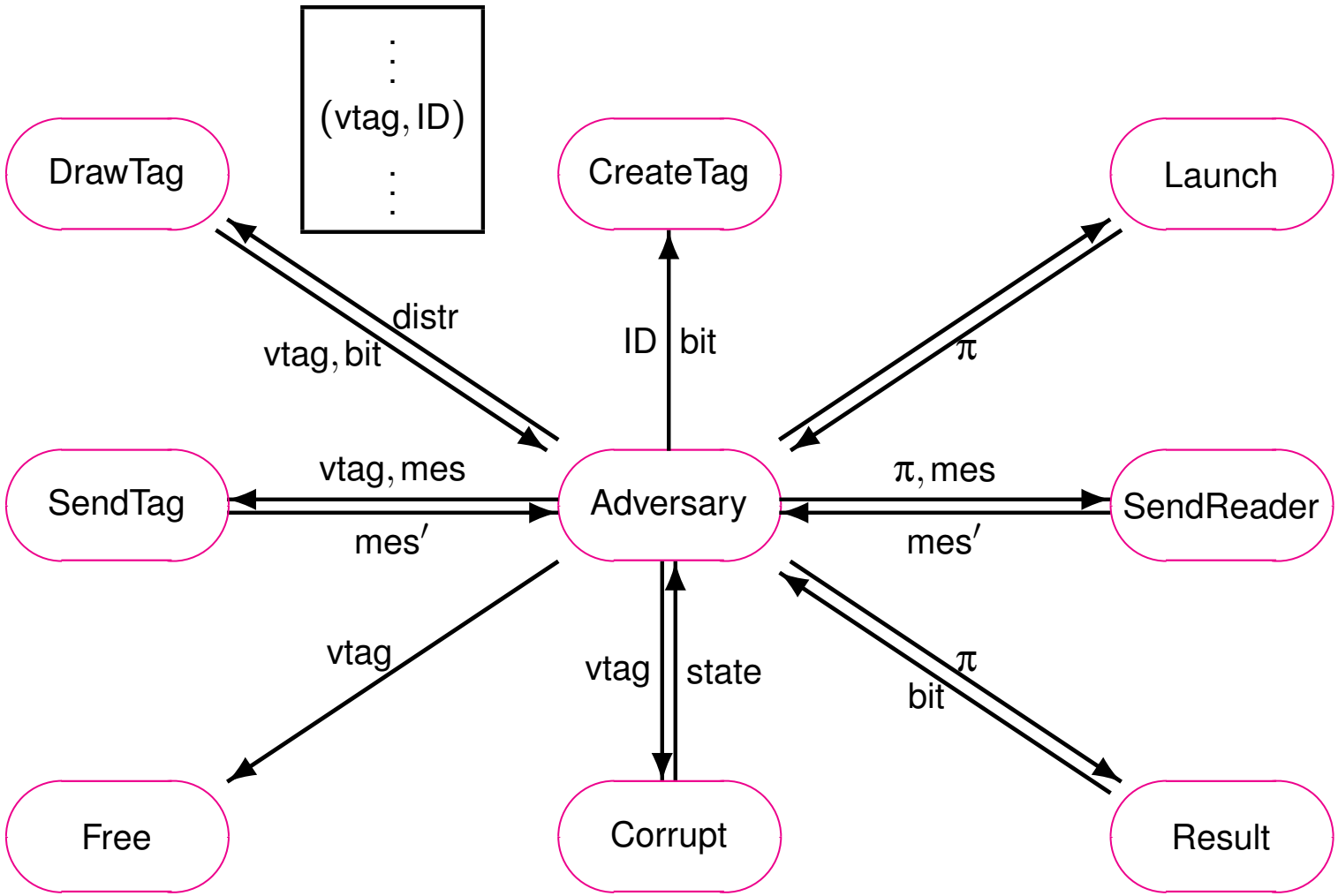
Functionality:

- correctness: identification under normal execution

Adversarial Model



Oracle Accesses



Security

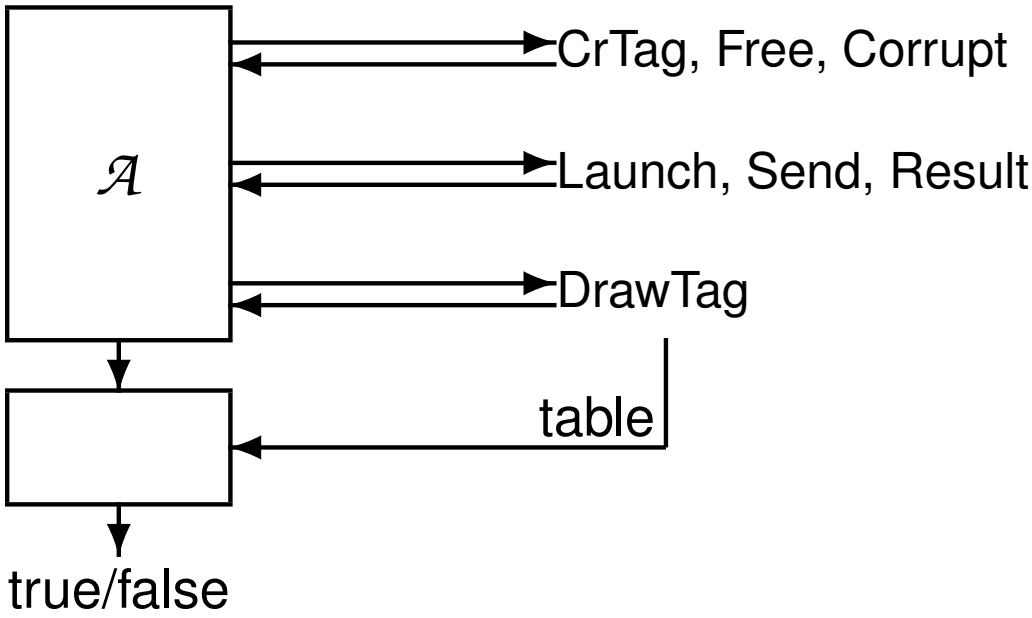
Wining condition: one reader-protocol instance π identified ID but this tag did not have any matching conversation
(i.e. same transcript and well interleaved messages).

Definition

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

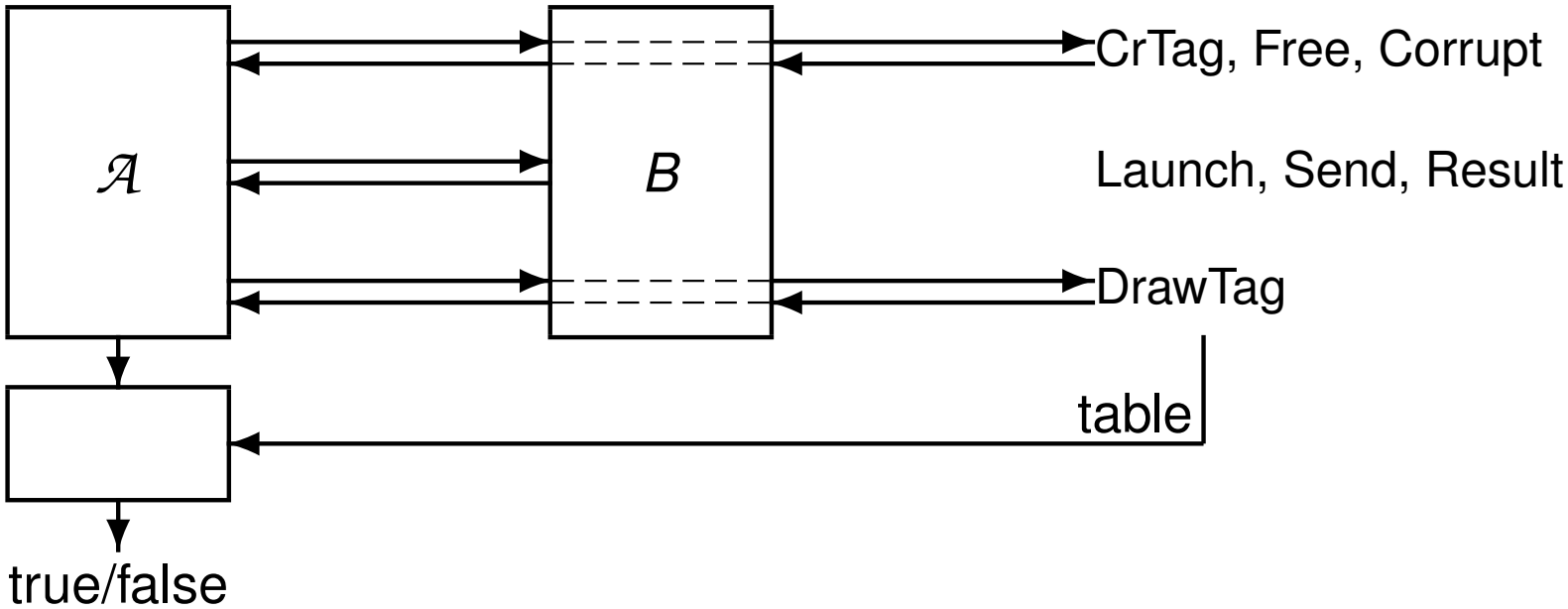
LASEC

Privacy Adversary



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

Blinders

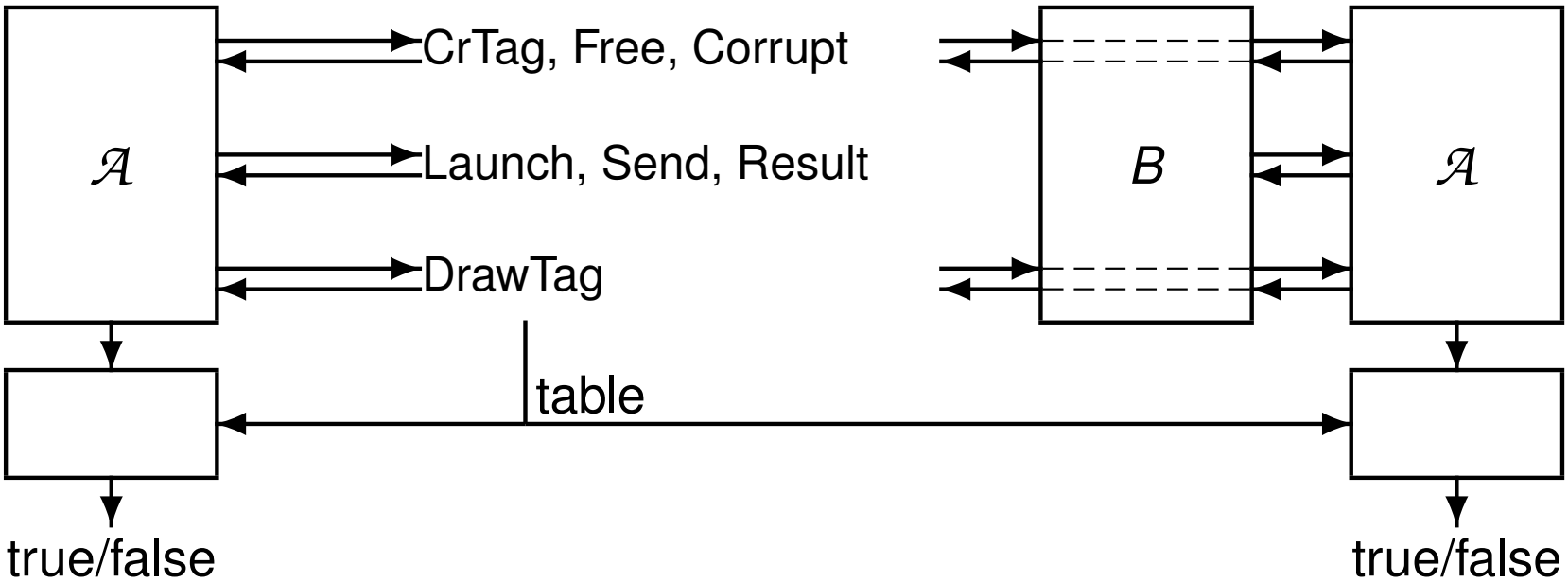


Definition

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

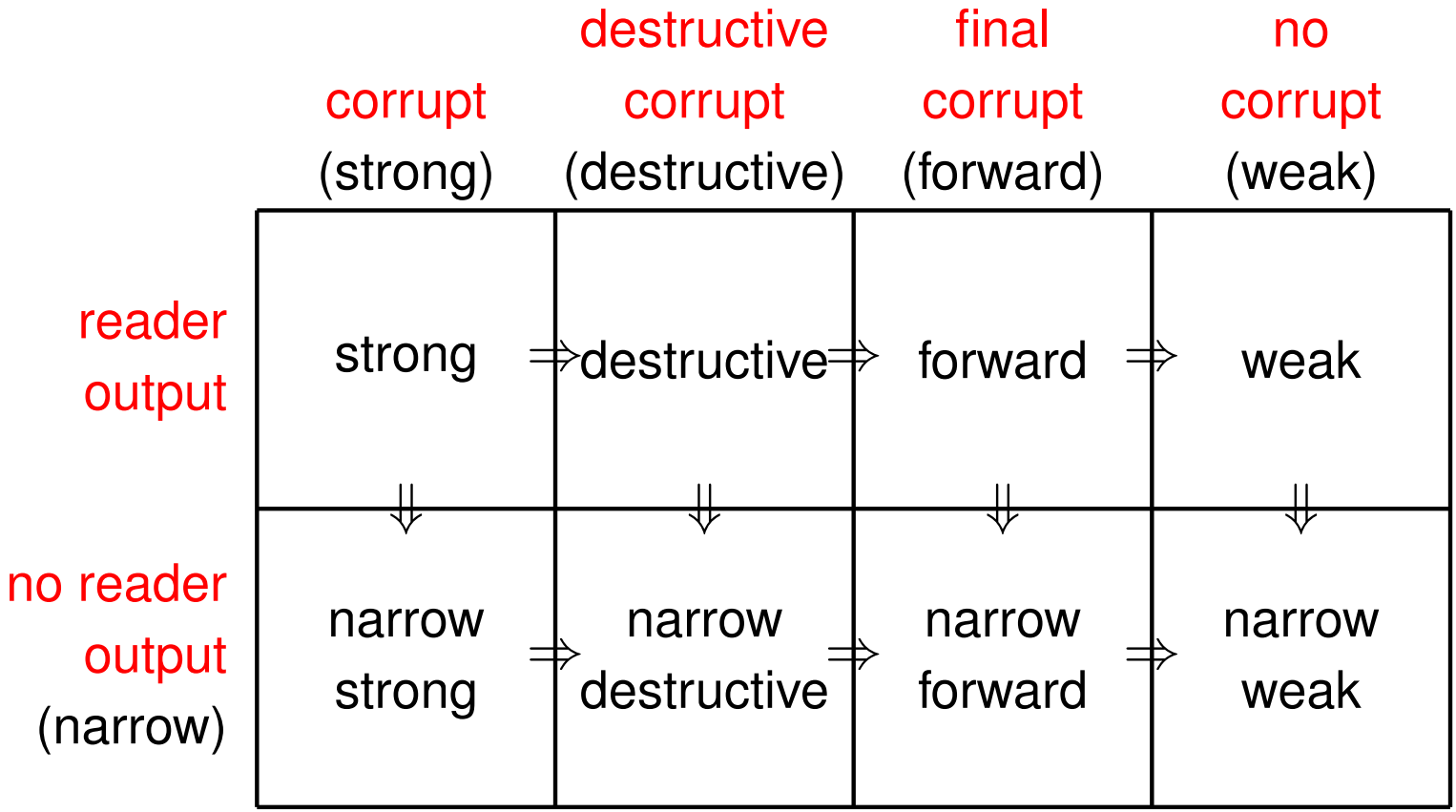
Privacy



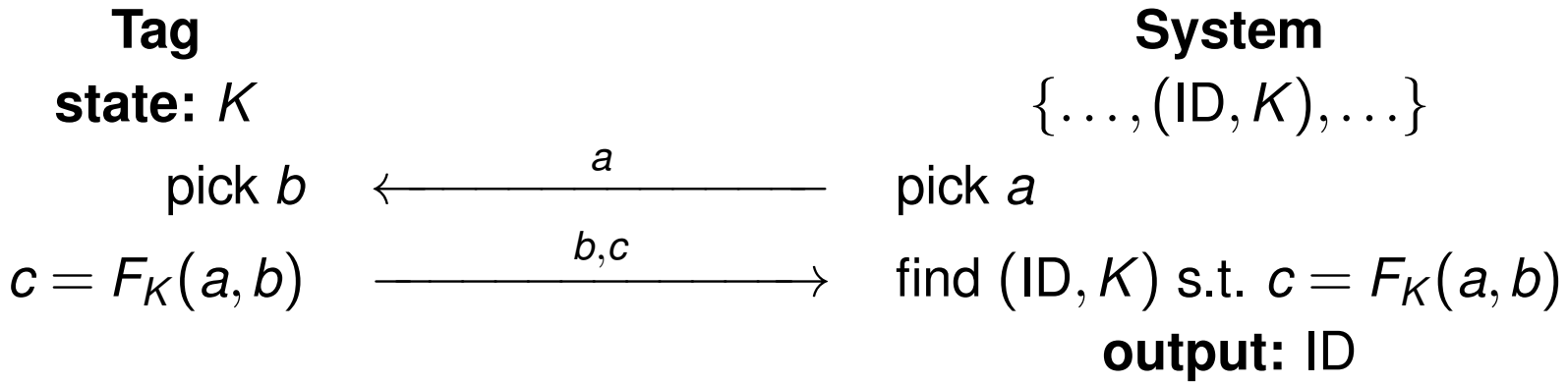
Definition

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



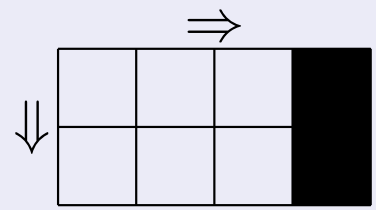
Challenge-Response RFID Scheme



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

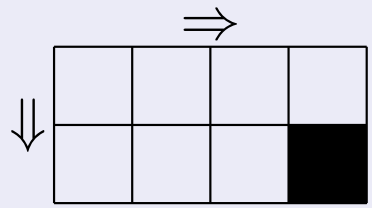
Narrow-Weak Privacy Implies One-Way Function

Theorem

An RFID scheme that is

- *correct*
- *narrow-weak private*

can be transformed into a one-way function.



no privacy without any crypto!

Proof idea:

1. the function mapping the initial states and random coins to the protocol transcript must be one-way (otherwise compute new states and identify in future sessions)

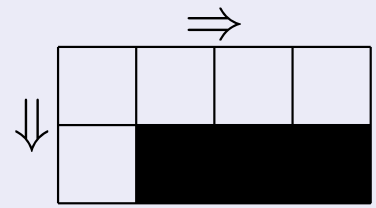
Modified OSK

Tag		**System**
state: S		$\{\ldots,(\mathsf{ID},K),\ldots\}$
	$\xleftarrow{\quad a \quad}$	pick a
$c = F(S,a)$	$\xrightarrow{\quad c \quad}$	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]

LASEC

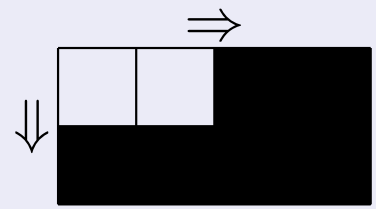
Public-Key-Based RFID Scheme

Tag		**System**
state: K_P, ID, K		**secret key:** K_S
		$\{\ldots, (\mathsf{ID}, K), \ldots\}$
	$\xleftarrow{\quad a \quad}$	pick a
$c = \mathsf{Enc}_{K_P}(\mathsf{ID} \Vert K \Vert a)$	$\xrightarrow{\quad c \quad}$	$\mathsf{Dec}_{K_S}(c) = \mathsf{ID} \Vert K \Vert a$
		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*

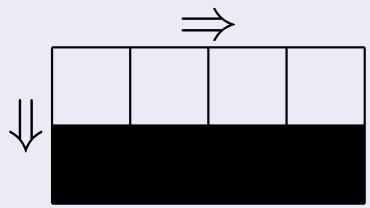


Narrow-Strong Privacy Implies Public-Key Cryptography

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!

Proof idea:

1. Alice creates two legitimate tags 0 and 1, sends their states to Bob, and simulate the system for Bob
2. Bob flips a bit b and simulate tag b to Alice
3. Alice identifies b which is an agreed key bit

LASEC

Caveat: Not Destructive Private

1: CreateTag(0)
2: $\text{vtag}_0 \leftarrow \text{DrawTag}(0)$
3: $S_0 \leftarrow \text{Corrupt}(\text{vtag}_0)$
4: $(\cdot, S_1) \leftarrow \text{SetupTag}_{K_P}(1)$
5: flip a coin $b \in \{0,1\}$
6: $\pi \leftarrow$ Launch
7: simulate a tag of state S_b with reader instance π
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.

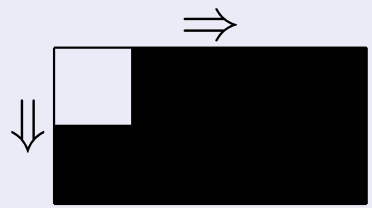
Strong Privacy is Infeasible

Theorem

An RFID scheme cannot be

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

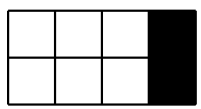
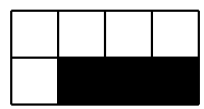
at the same time.



no strong privacy!

Results about Privacy Models (2007 Version)

	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		equiv to PRF

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

1 Towards a Formal Model

2 Definitions and Results

3 **Strong Privacy is Possible**

LASEC

Impossibility Proof

take the following adversary (for destructive privacy)

1: $(\cdot, S_0) \leftarrow \mathsf{SetupTag}_{K_P}(0)$
2: $\mathsf{CreateTag}(1)$
3: $\mathsf{vtag} \leftarrow \mathsf{DrawTag}(1)$
4: $S_1 \leftarrow \mathsf{Corrupt}(\mathsf{vtag})$ (destroy it)
5: flip a coin $b \in \{0,1\}$
6: $\pi \leftarrow$ Launch
7: simulate tag of state S_b with π
8: $x \leftarrow \mathsf{Result}(\pi)$
9: output $1_{x=b}$

a blinder $\mathcal{B}$ for this advesary gets S_1, simulate reader interacting with $b = 0$ or 1 and can guess b

$\mathcal{B}$ defines an adversary (for narrow-strong privacy)

1: create tag 0 and tag 1
2: draw both tags
3: corrupt both tags and get their states S_0 and S_1
4: free both tags
5: draw a random tag: $\mathsf{vtag} \leftarrow \mathsf{DrawTag}(0 \text{ or } 1)$
6: simulate B with input K_P, S_1, and interacting with vtag and get bit x
7: output $1_{\mathcal{T}(\mathsf{vtag})=x}$

LASEC

Ng-Susilo-Mu-Safavi-Naini 2008

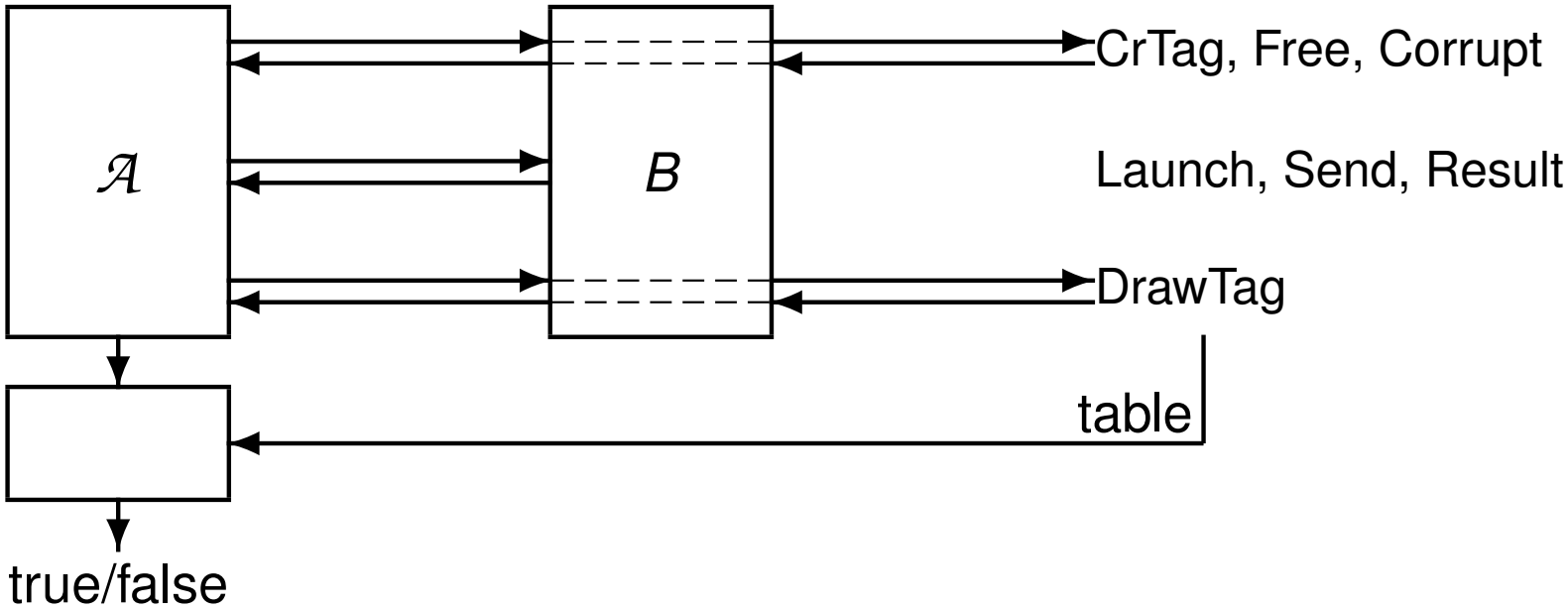
- not strong private because the adversary asks questions for which he knows the answer but the blinder cannot guess it
- notion of “wise” adversary (cannot ask question for which he knows the answer)

we take a different approach:

we let the blinder be able to read the adversary’s thoughts

LASEC

New 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
- see the adverary's random coins

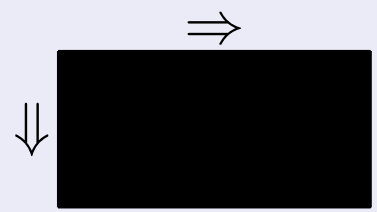
Public-Key-Based RFID Scheme

Tag		**System**
state: K_P, ID, K		**secret key:** K_S
		$\{\ldots, (\mathsf{ID}, K), \ldots\}$
	$\xleftarrow{\quad a \quad}$	pick a
$c = \mathsf{Enc}_{K_P}(\mathsf{ID} \Vert K \Vert a)$	$\xrightarrow{\quad c \quad}$	$\mathsf{Dec}_{K_S}(c) = \mathsf{ID} \Vert K \Vert a$
		check a, (ID, K)
		output: ID

Theorem

Assuming that Enc/Dec *is a PA2+IND-CPA public-key cryptosystem, this RFID scheme is*

- *correct*
- *secure*
- ***strong*** *private*

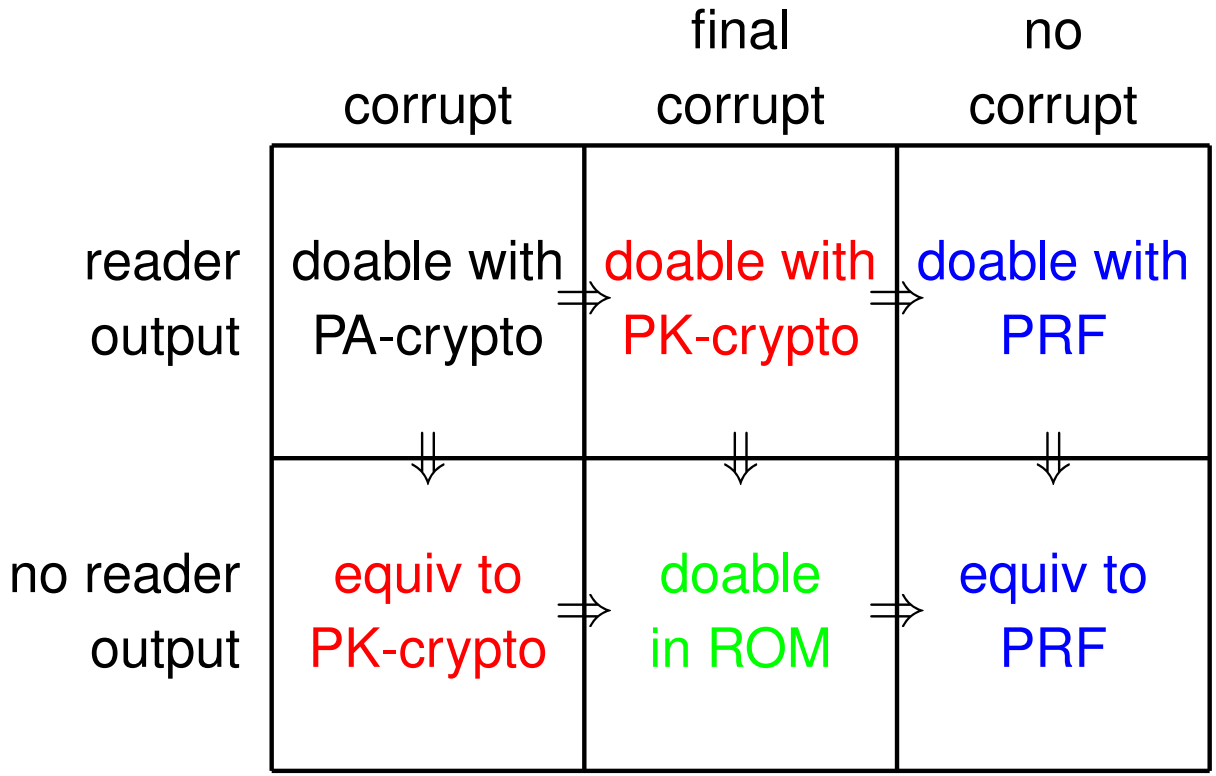


PA2 Trick

- PA2 means for all valid ciphertexts form the adversary, either it is reused or the adversary must know the plaintext (Bellare-Palacio 2004)
- know the plaintext $\Longrightarrow$ blinder can get it be reading his thoughts
- PA2 needed because the blinder must simulate Result by decrypting ciphertexts forged by the adversary (they could be based on corrupted states)

LASEC

Conclusion



- we have a good framework to study privacy
- strong privacy is possible, but only with PK-crypto
- some open problems
  - forward privacy based on PRF (or ROM)?
  - narrow-forward privacy based on PRF (no ROM)?
  - separation with a concurrent model based on indistinguishability

Q & A