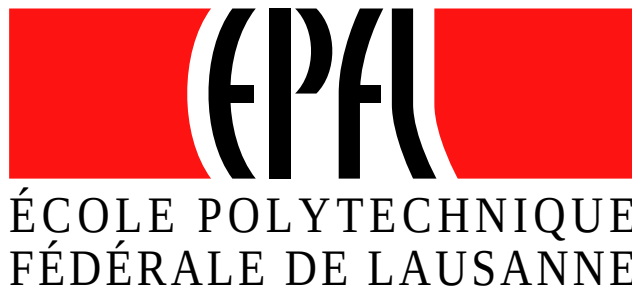
On Privacy for RFID

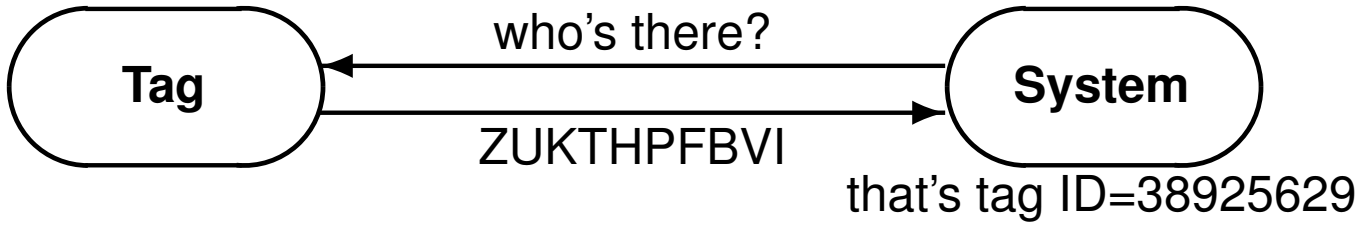
Serge Vaudenay



http://lasec.epfl.ch/

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

Evolution of Privacy Models

- early models: distinguish between two honest tags
- OSK03: allow corruption at the end of the attack (forward privacy)
- ADO06: earlier corruption considered
- JW06: result channel considered
- V07: complete simulation-based definition + impossibility result
- NSMS08: “wise adversary”
- HPVP11 model: complete left-or-right game
- OV12 extension: the simulator can read the adversary’s thoughts

possible extensions: mutual authentication, with distance bounding, ...

Reference

On Privacy Models for RFID

Serge Vaudenay

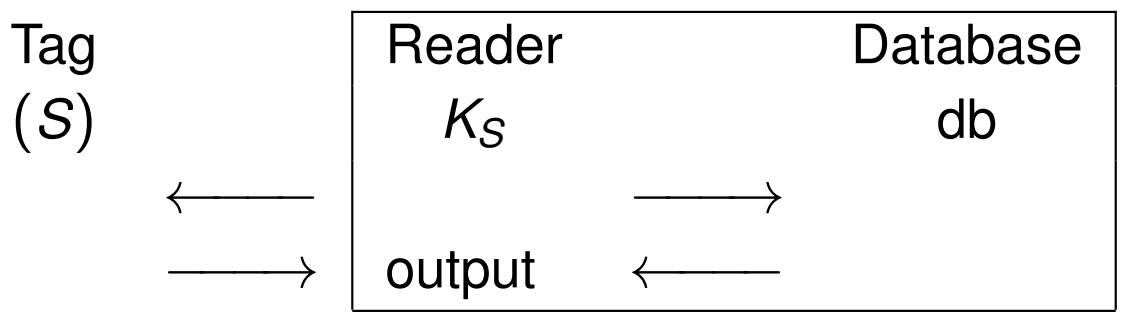
Asiacrypt 2007

- security and privacy models for single-system RFID
- feasibility and infeasibility results

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) $\rightarrow$ (data, S):
  S is an initial state for tag ID
  (ID, data) is to be inserted in database
- Protocols:

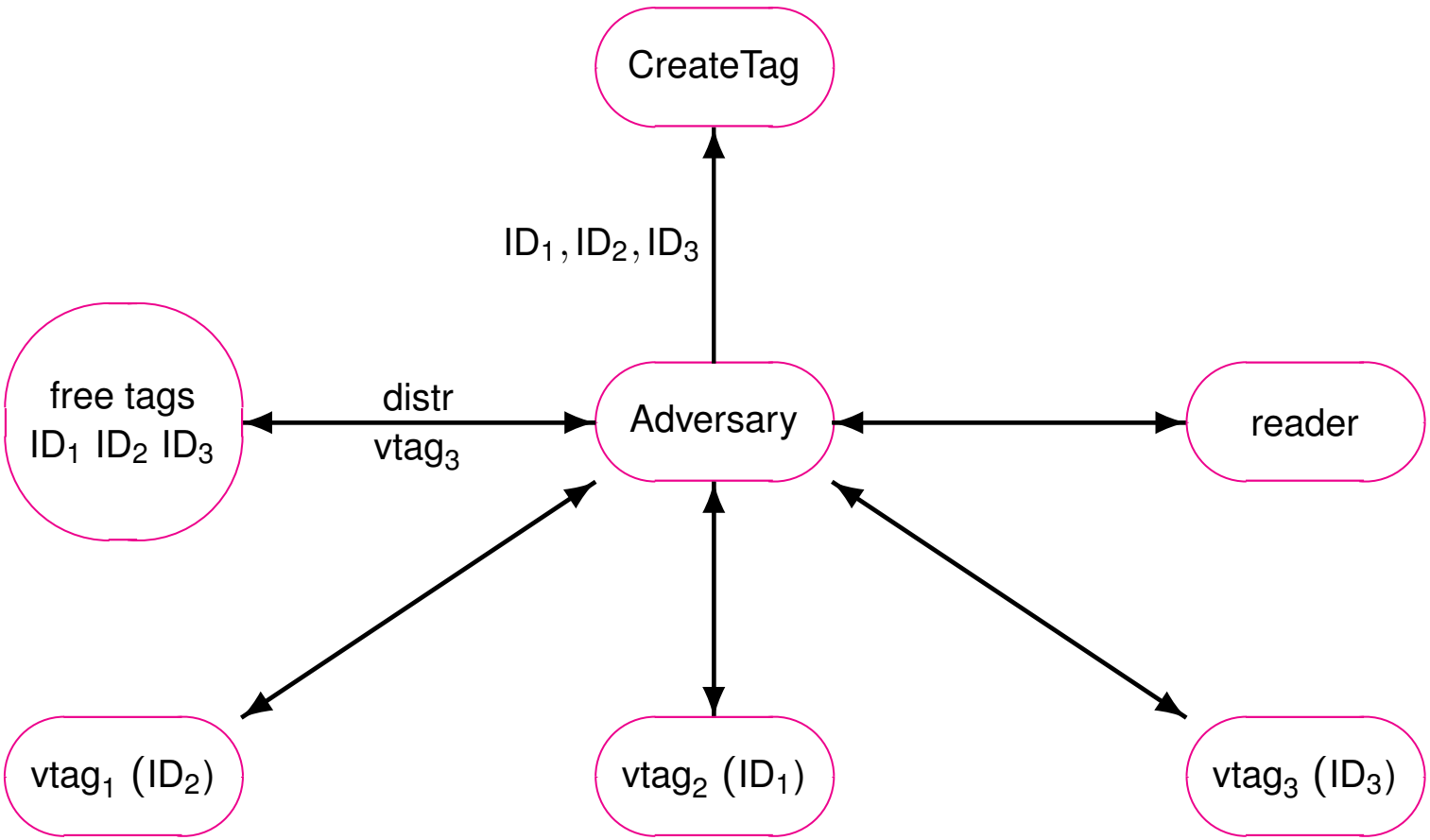


output: *tag ID (if valid) or* $\perp$ *(if not)*

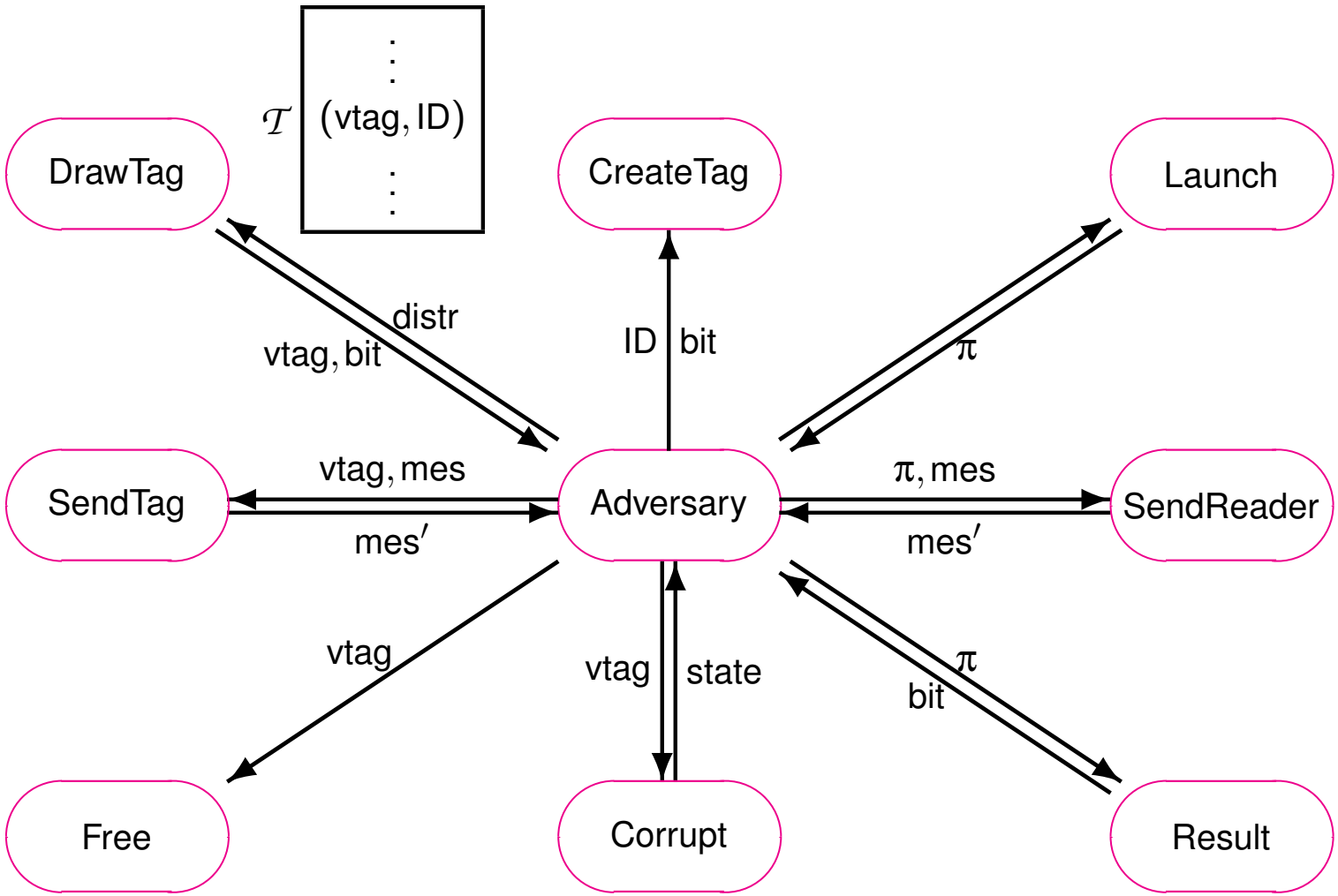
Functionality:

- correctness: identification under normal execution

Adversarial Model



Oracle Accesses



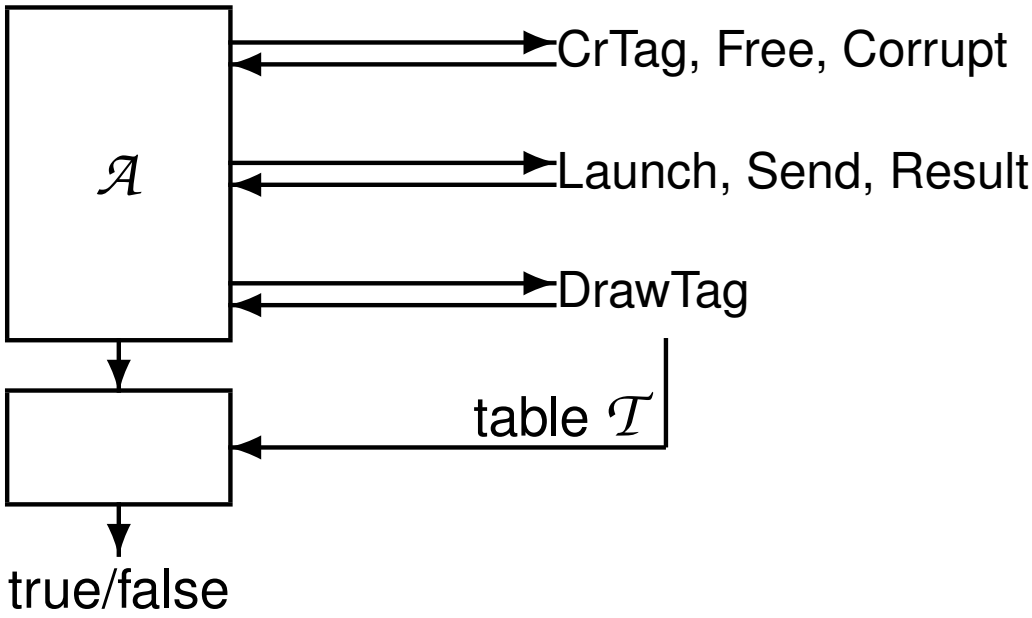
Security

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

Definition

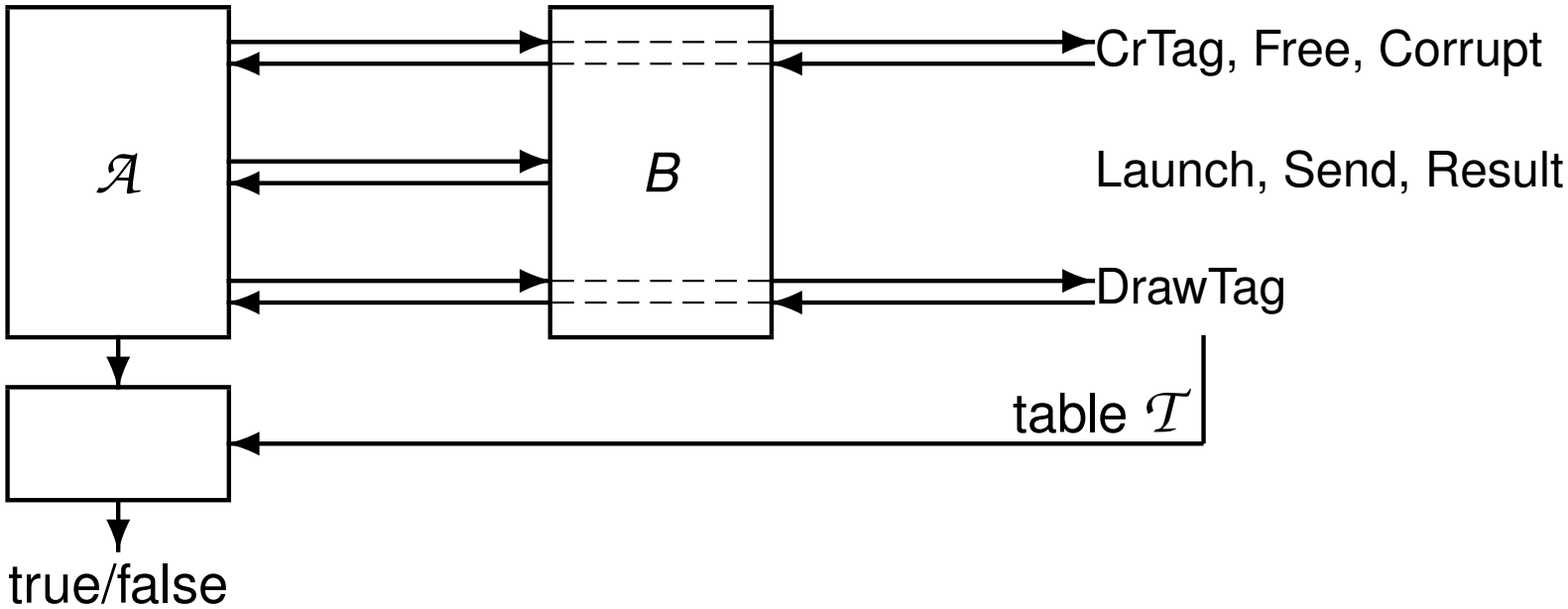
An RFID scheme is secure if for any polynomially bounded adversary the probability of success is negligible.

Privacy Adversary



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

Blinders

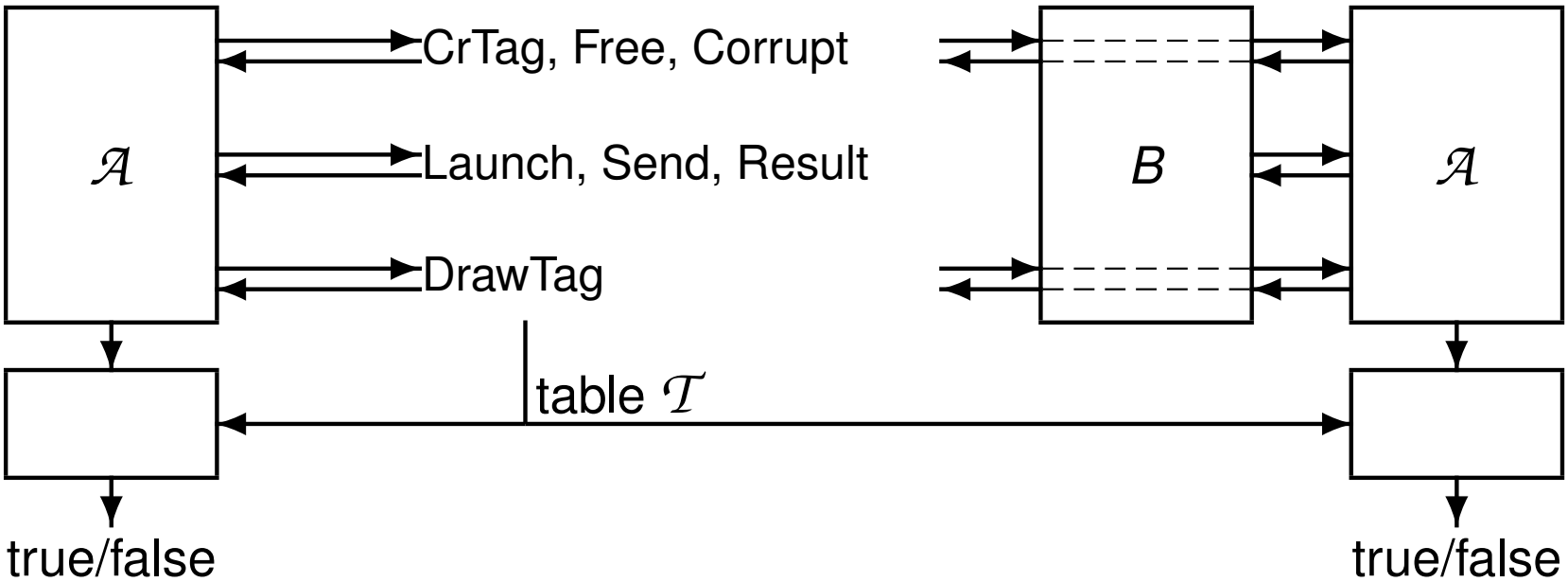


Definition

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

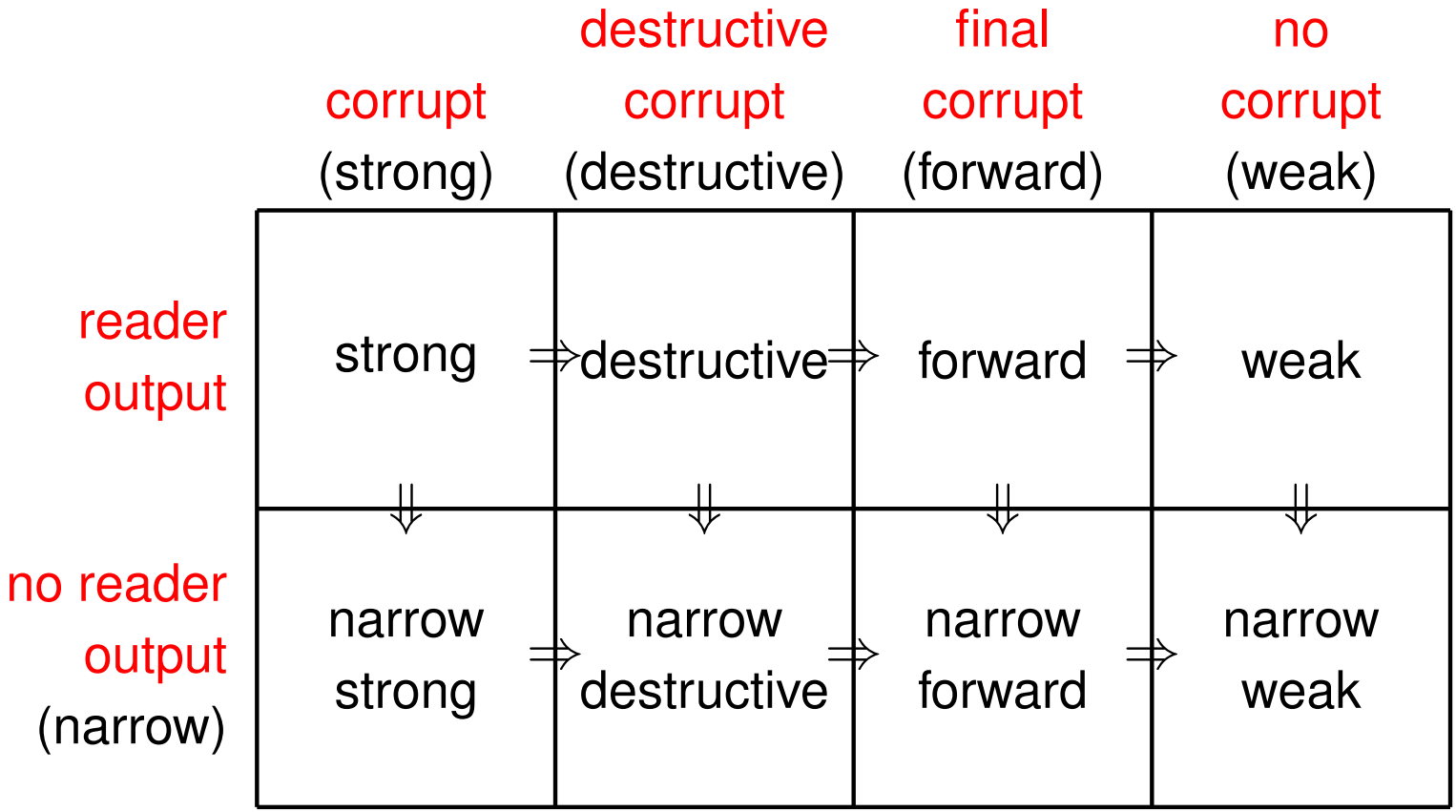
Privacy



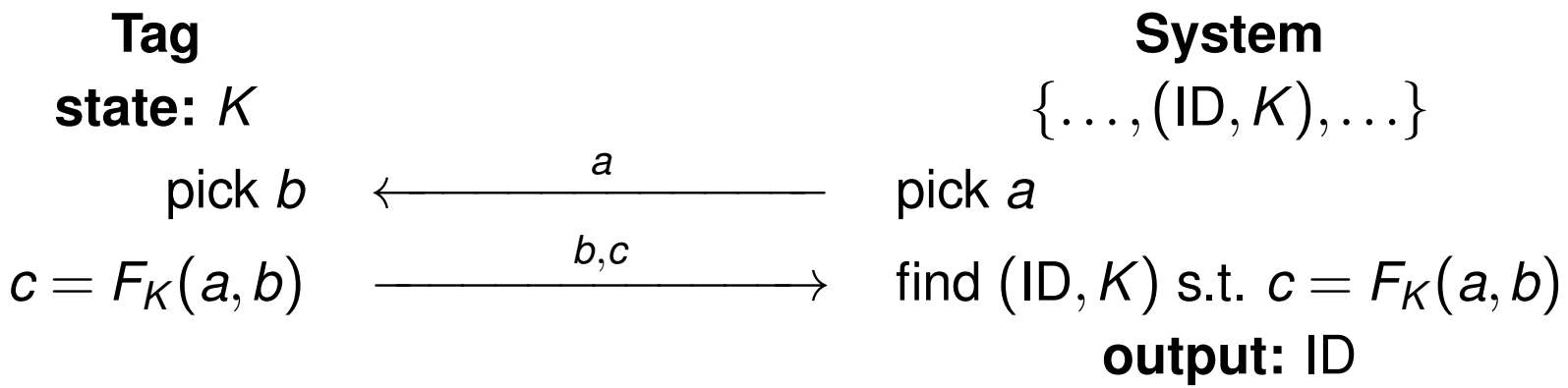
Definition

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



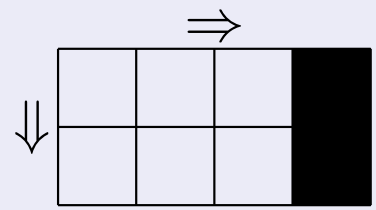
Challenge-Response RFID Scheme



Theorem

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

- *correct*
- *secure*
- ***weak** V07-private*



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

Caveat: Not Even Narrow-Forward Private

1: CreateTag(0), CreateTag(1)
2: vtag $\leftarrow$ DrawTag(0 or 1)
3: $(a, b, c) \leftarrow$ Execute(vtag)
4: Free(vtag)

create two tags, draw one at random, and run the protocol to get a, b, c

5: $\text{vtag}_0 \leftarrow$ DrawTag(0)
6: $K \leftarrow$ Corrupt(vtag_0)

corrupt tag 0 to get K

7: **if** $F_K(a, b) = c$ **then**
8: $\quad x \leftarrow 0$
9: **else**
10: $\quad x \leftarrow 1$
11: **end if**
12: output $1_{\mathcal{T}(\text{vtag})=x}$

test if $F_K(a, b) = c$

We have $\Pr[\mathcal{A} \text{ wins}] \approx 1$. For any blinder B, $\Pr[\mathcal{A}^B \text{ wins}] = \frac{1}{2}$.
Therefore $\Pr[\mathcal{A} \text{ wins}] - \Pr[\mathcal{A}^B \text{ wins}] \approx \frac{1}{2}$.

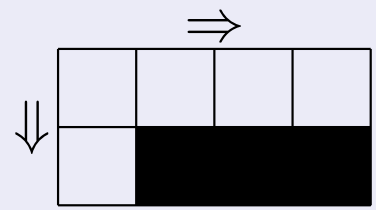
Modified OSK

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** V07-private*



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

Caveat: Not Even Weak Private

(Juels-Weis [JW 2006] attack):

1: CreateTag(0), CreateTag(1)
2: $\text{vtag}_0 \leftarrow \text{DrawTag}(0)$
3: **for** $i = 1$ to $t+1$ **do**
4: pick a random x
5: $\text{SendTag}(\text{vtag}_0, x)$
6: **end for**
7: $\text{Free}(\text{vtag}_0)$
8: $\text{vtag} \leftarrow \text{DrawTag}(0 \text{ or } 1)$
9: $\pi \leftarrow \text{Execute}(\text{vtag})$
10: $x \leftarrow \text{Result}(\pi)$
11: output $1_{\mathcal{T}(\text{vtag})=x}$

play $t+1$ times with tag 0 to desynchronize

draw a tag at random, execute, and see if it is accepted

We have $\Pr[\mathcal{A} \text{ wins}] \approx 1$. For any blinder B, $\Pr[\mathcal{A}^B \text{ wins}] = \frac{1}{2}$.
Therefore $\Pr[\mathcal{A} \text{ wins}] - \Pr[\mathcal{A}^B \text{ wins}] \approx \frac{1}{2}$.

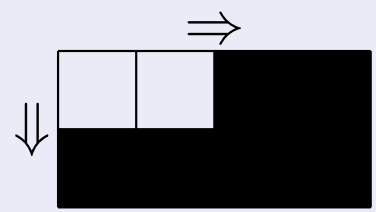
Public-Key-Based RFID Scheme

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*** *V07-private*



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: $(\cdot, S_1) \leftarrow \text{SetupTag}_{K_P}(1)$

create two tags with known keys, one being genuine

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** $x = b$ **then**
10: output true
11: **else**
12: output false
13: **end if**

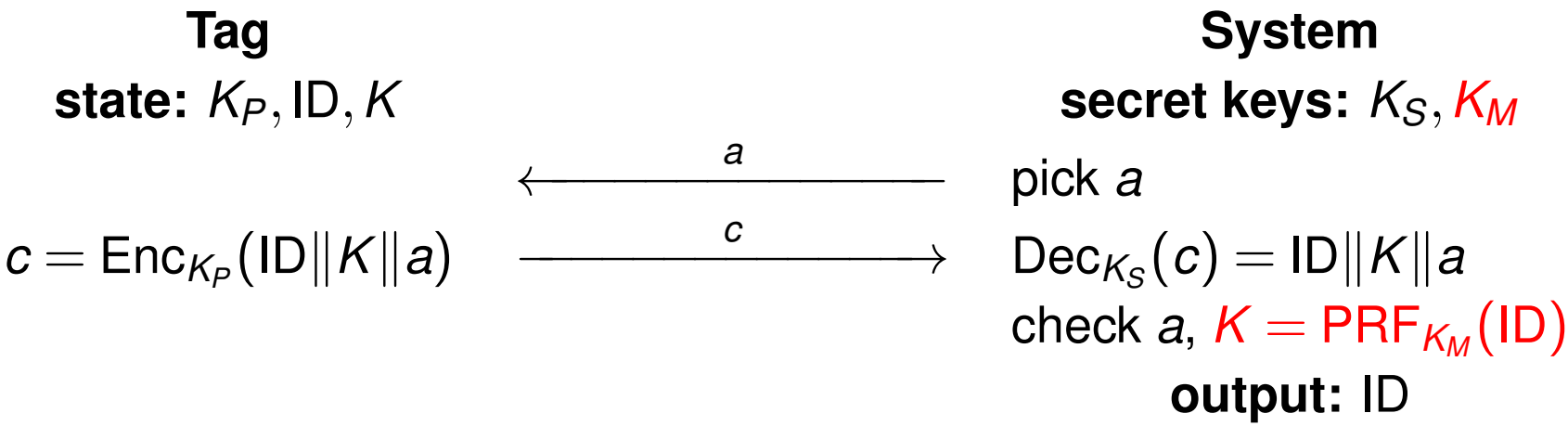
check that reader guessed b

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.

Therefore $\Pr[\mathcal{A} \text{ wins}] - \Pr[\mathcal{A}^B \text{ wins}] \approx \frac{1}{2}$.

Scheme with No Database



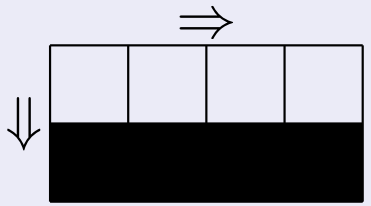
- SetupTag must now use a secret key K_M
- all the theory remains valid if SetupTag produces keys which are indistinguishable from simulated ones

Narrow-Strong Privacy Implies Public-Key Cryptography

Theorem

An RFID scheme that is

- *correct*
- *narrow-strong V07-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

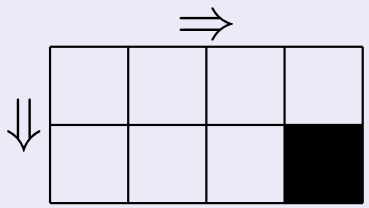
Narrow-Weak Privacy Implies One-Way Function

Theorem

An RFID scheme that is

- *correct*
- *narrow-weak V07-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)

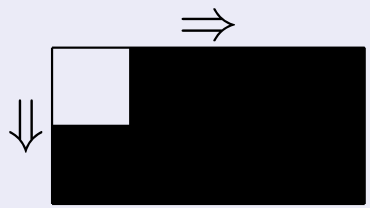
Strong Privacy is Infeasible

Theorem

An RFID scheme cannot be

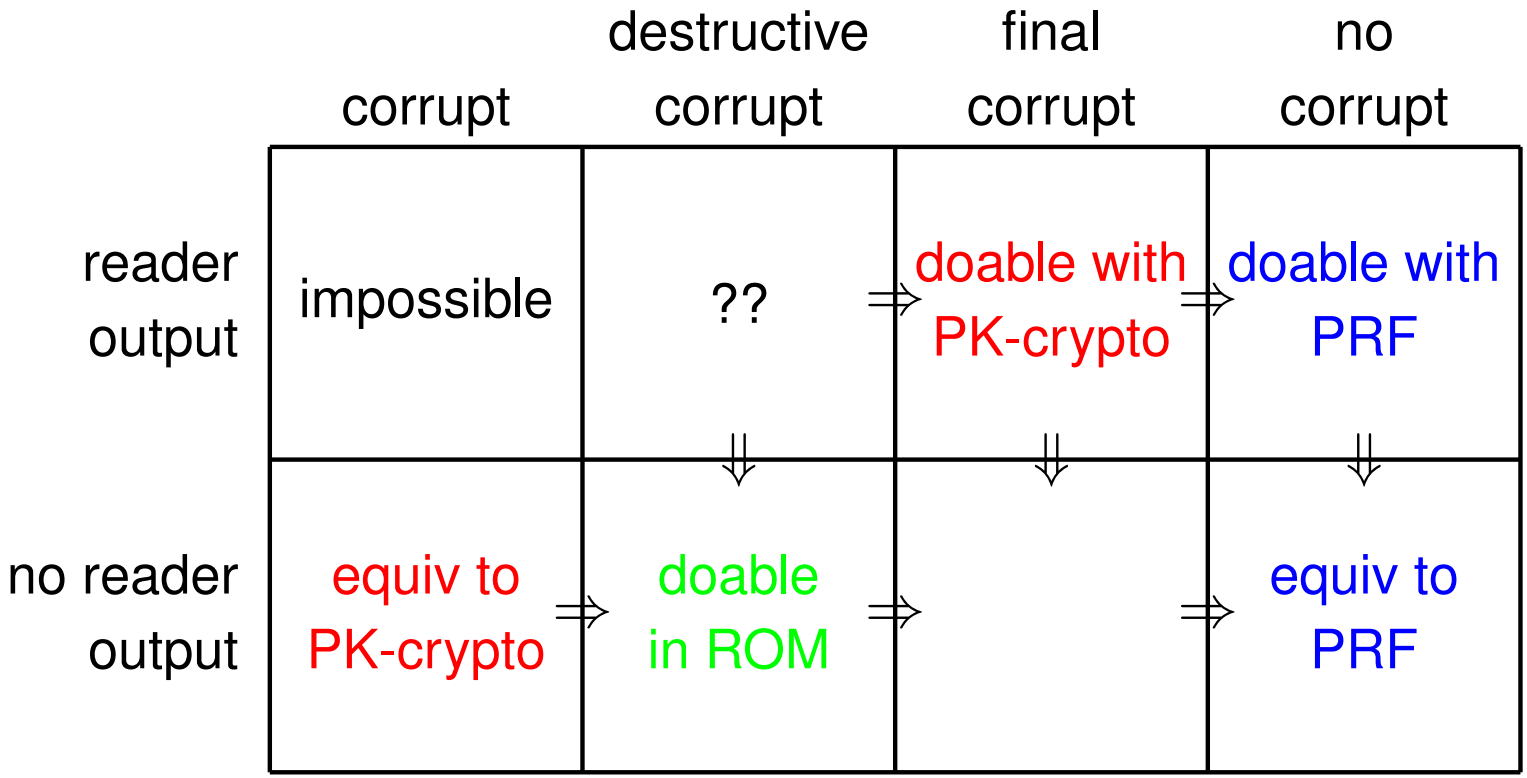
- *correct*
- *narrow-strong and destructive V07-private*

at the same time.

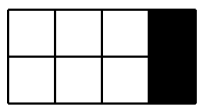


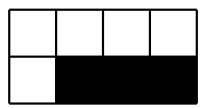
no strong privacy!

Privacy in RFID (V07 Model)



- possible:
- impossible:


(PRF)


(ROM)


(PKC)


(w/o KA)

Reference

Strong Privacy for RFID Systems from Plaintext-Aware Encryption

Khaled Ouafi and Serge Vaudenay

CANS 2012

- new definition of a blinder
- wide-strong privacy using a PA cryptosystem

Impossibility Proof — i

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)

} create two tags with known keys, one being genuine

5: flip a coin $b \in \{0,1\}$
6: $\pi \leftarrow$ Launch
7: simulate tag of state S_b with π

} simulate one at random

8: $x \leftarrow \mathsf{Result}(\pi)$
9: output $1_{x=b}$

} check that reader guessed b

destructive privacy $\Longrightarrow \exists \mathcal{B}$ $\quad \Pr[\mathcal{A} \text{ wins}] \sim \Pr[\mathcal{A}^{\mathcal{B}} \text{ wins}]$

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

Impossibility Proof — ii

take the following adversary (for narrow-strong privacy) defined from $\mathcal{B}$

1: CreateTag(0)
2: CreateTag(1)
3: $\text{vtag}_0 \leftarrow \text{DrawTag}(0)$
4: $\text{vtag}_1 \leftarrow \text{DrawTag}(1)$
5: $S_0 \leftarrow \text{Corrupt}(\text{vtag}_0)$
6: $S_1 \leftarrow \text{Corrupt}(\text{vtag}_1)$
7: $\text{Free}(\text{vtag}_0)$
8: $\text{Free}(\text{vtag}_1)$

} create two tags and get their states

9: vtag $\leftarrow$ DrawTag(0 or 1)
10: $b \leftarrow (\mathcal{B}(K_P, S_1) \leftrightarrow \text{vtag})$

} make $\mathcal{B}$ guess vtag

11: output $1_{\mathcal{T}(\text{vtag})=x}$

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

Any blinder B' must simulate vtag without knowing which one it is, so $\Pr[\mathcal{A}^{B'} \text{ wins}] = \frac{1}{2}$.

Therefore $\Pr[\mathcal{A} \text{ wins}] - \Pr[\mathcal{A}^{B'} \text{ wins}] \approx \frac{1}{2}$.

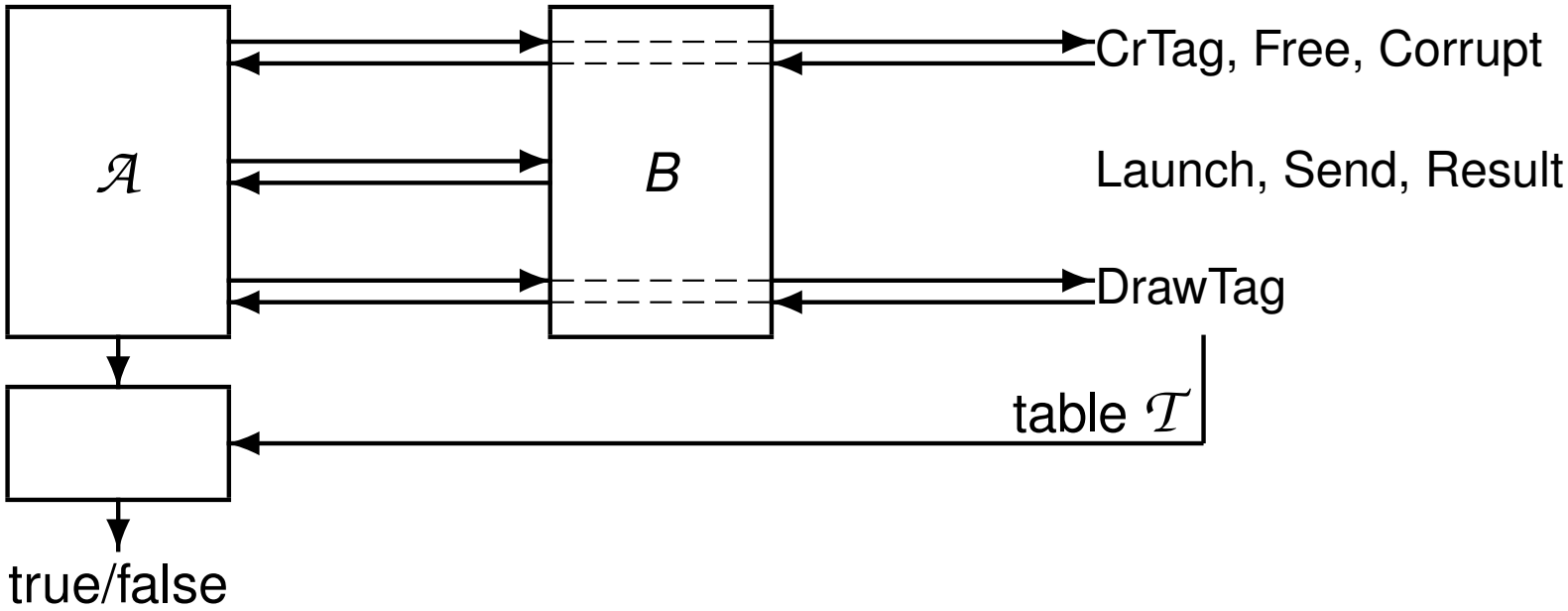
Ng-Susilo-Mu-Safavi-Naini 2008

- 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

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 adversary's random coins

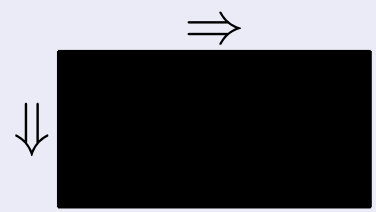
Public-Key-Based RFID Scheme

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*** *OV12-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)

Other Tricky Updates in OV12

- the input distribution for DrawTag is specified by a sampling algorithm Samp
- it must be *inverse-samplable*:
  there must exist Samp^{-1} such that

$$(\rho, \mathsf{Samp}(\rho)) \sim (\mathsf{Samp}^{-1}(x), x)$$

- the table $\mathcal{T}$ must be simulatable:
  there must exist S such that

$$(\mathsf{View}_{\mathcal{A}}, \mathcal{T}) \sim (\mathsf{View}_{\mathcal{A}}, S(\mathsf{View}_{\mathcal{A}}))$$

IND-CCA is Insufficient?? for OV12 — i

- take (G^0, E^0, D^0) an IND-CCA cryptosystem
- take (G^1, E^1, D^1) a homomorphic IND-CPA cryptosystem over bits [GM84]
- define

$$\mathsf{Gen} \to ((\mathsf{sk}_0, \mathsf{sk}_1), (\mathsf{pk}_0, \mathsf{pk}_1, z)) \quad \text{for} \quad \begin{cases} G^0 \to (\mathsf{sk}_0, \mathsf{pk}_0) \\ G^1 \to (\mathsf{sk}_1, \mathsf{pk}_1) \\ \xi \in_U \{0,1\} \\ z = E^1_{\mathsf{pk}_1}(\xi) \end{cases}$$

$$\mathsf{Enc}_{(\mathsf{pk}_0,\mathsf{pk}_1),z}(m_1 \cdots m_n) = E^0_{\mathsf{pk}_0}(E^1_{\mathsf{pk}_1}(m_1) \| \cdots \| E^1_{\mathsf{pk}_1}(m_n))$$

$$\mathsf{Enc}'_{(\mathsf{pk}_0,\mathsf{pk}_1),z}(m_1 \cdots m_n) = E^0_{\mathsf{pk}_0}(z \cdot E^1_{\mathsf{pk}_1}(m_1) \| \cdots \| z \cdot E^1_{\mathsf{pk}_1}(m_n))$$

  where the m_i are bits (note that ξ is only used in z)
- $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is an IND-CCA cryptosystem
- for $e = \mathsf{Enc}'_{\mathsf{pk}}(m)$, we have $\mathsf{Dec}_{\mathsf{sk}}(e) = m \oplus (\xi \cdots \xi)$
- not PA: knowing $\mathsf{Dec}_{\mathsf{sk}}(e)$ is equivalent to breaking (G^1, E^1, D^1)

IND-CCA is Insufficient?? for OV12 — ii

a wide-destructive adversary:

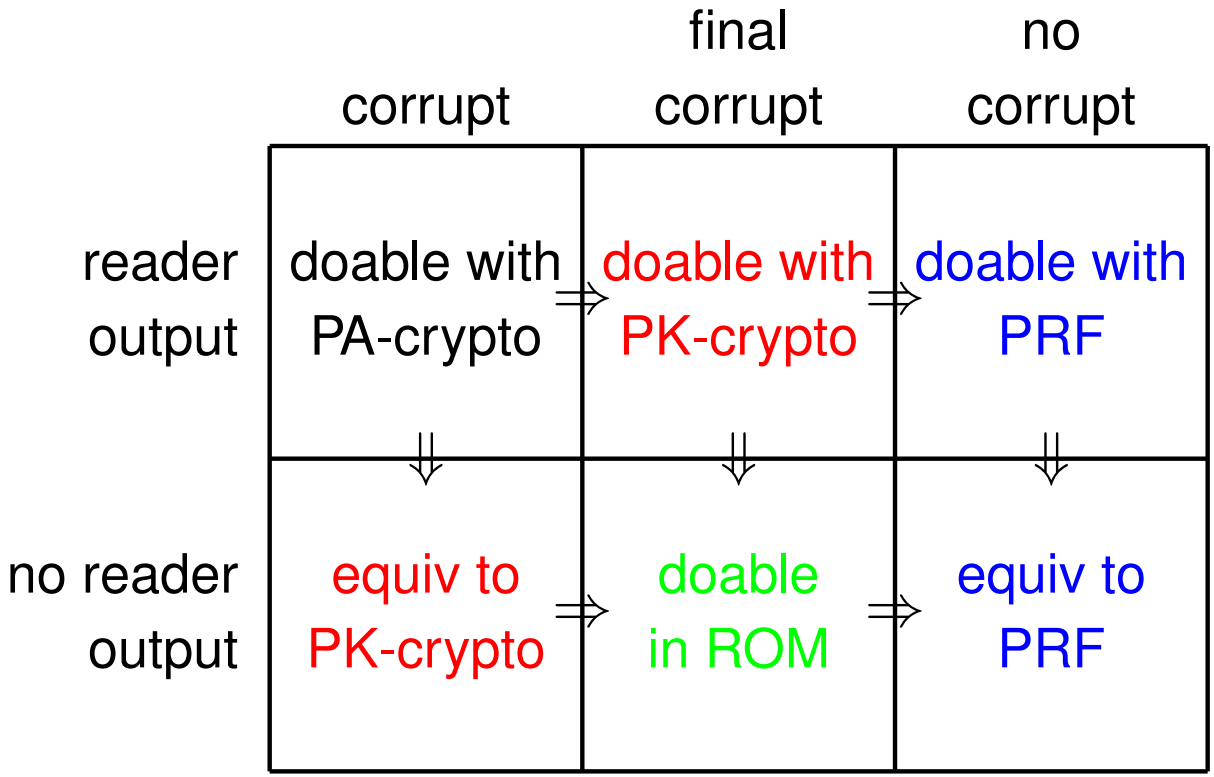
1: CreateTag(0)
2: $\text{vtag}_0 \leftarrow \text{DrawTag}(0)$
3: $S_0 \leftarrow \text{Corrupt}(\text{vtag}_0)$
4: $\pi \leftarrow \text{Launch}$
5: simulate tag 0 to π with Enc'
6: output $\text{Result}(\pi)$

$\text{Result}(\pi) = 1 - \xi$
due to (G^1, E^1, D^1) security no blinder can make the same output

But a blinder could make the result have the same distribution!?!

Privacy in RFID (OV12 Model)

Privacy with respect to adversarial capabilities:



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

1 The V07 Model

2 The OV12 Extension

3 **The HPVP11 Model**

4 Strong Privacy in Distance Bounding

Modifications

- all tags are genuine
- corruption is done on tag ID (not vtag)
- DrawTag has two tag ID as input (left and right)
- all DrawTag draw the left tag or all DrawTag draw the right tag
- the adversary must guess if it is all-left or all-right
- not allowed to use as input an ID which was used before without releasing the vtag

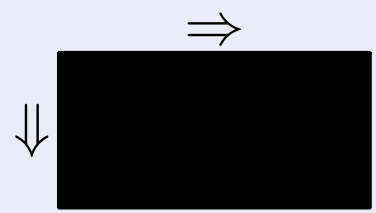
Public-Key-Based RFID Scheme

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 IND-CCA public-key cryptosystem, this RFID scheme is*

- *correct*
- *secure*
- ***strong** HPVP11-private*



1 The V07 Model

2 The OV12 Extension

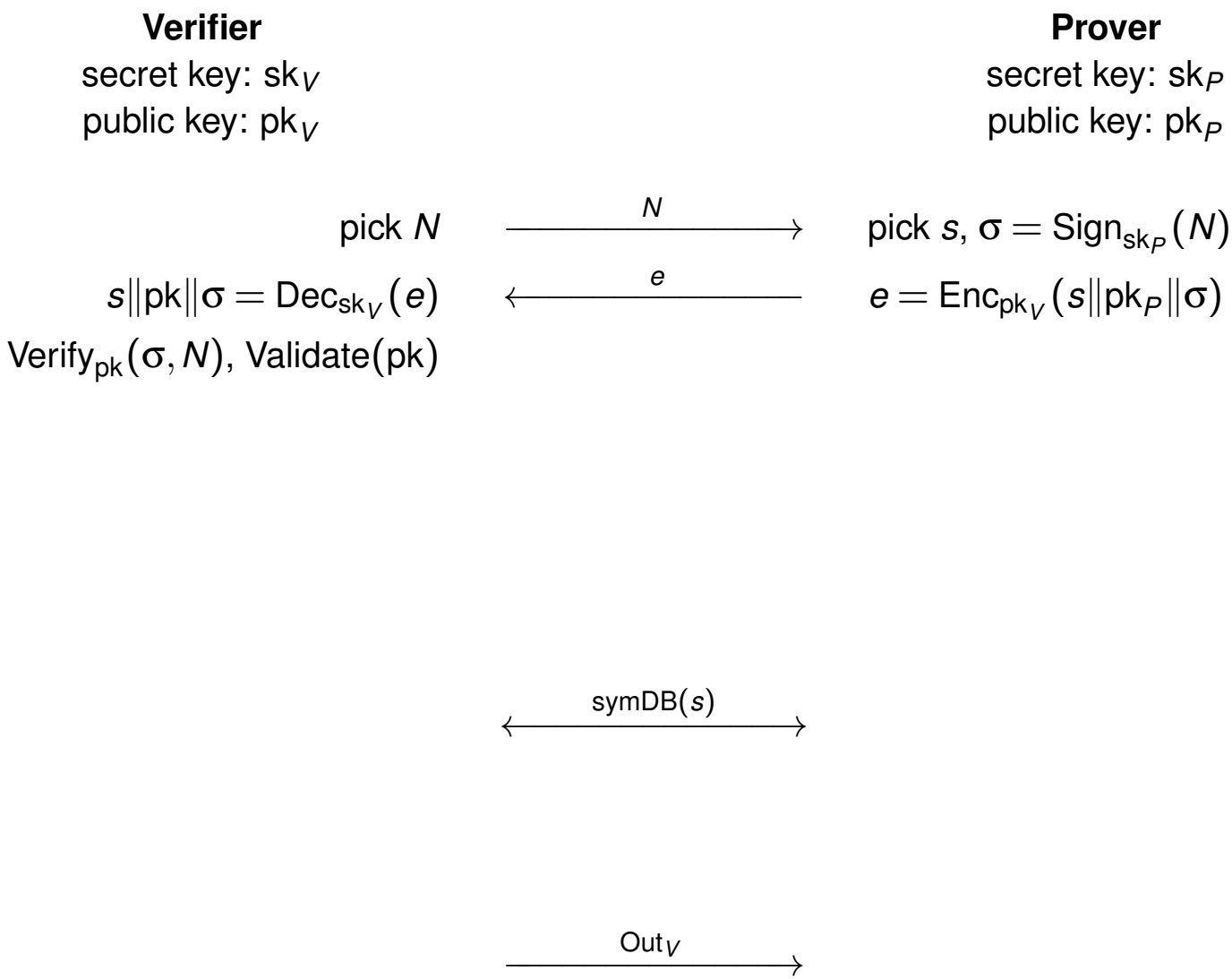
3 The HPVP11 Model

4 **Strong Privacy in Distance Bounding**

Identifying vs Authenticating DB

- in previous definition of DB protocols, the verifier has as input the ID of the prover
  symmetric: he has the secret of the prover
  public-key: he has the public key of the prover
- to address privacy, we must consider the identification process together with the authentication one
- so, we now assume that the verifier does not have the ID of the prover as input but rather produce it as an output
- verifier needs a key pair

privDB


Verifier
secret key: sk_V
public key: pk_V
Prover
secret key: sk_P
public key: pk_P
pick N
N
pick s, $\sigma = \mathrm{Sign}_{sk_P}(N)$
$s\|pk\|\sigma = \mathrm{Dec}_{sk_V}(e)$
e
$e = \mathrm{Enc}_{pk_V}(s\|pk_P\|\sigma)$
$\mathrm{Verify}_{pk}(\sigma, N)$, Validate(pk)
symDB(s)
Out_V
private output: pk

privDB with OTDB

Verifier		**Prover**
secret key: sk_V public key: pk_V		secret key: sk_P public key: pk_P
pick N	$\xrightarrow{N}$	pick s, $\sigma = \mathsf{Sign}_{\mathsf{sk}_P}(N)$
$s\|\|\mathsf{pk}\|\|\sigma = \mathsf{Dec}_{\mathsf{sk}_V}(e)$	$\xleftarrow{e}$	$e = \mathsf{Enc}_{\mathsf{pk}_V}(s\|\|\mathsf{pk}_P\|\|\sigma)$
$\mathsf{Verify}_{\mathsf{pk}}(\sigma, N)$, $\mathsf{Validate}(\mathsf{pk})$		
pick $m \in \{0,1\}^{2n}$	$\xrightarrow{m}$	
$a = s \oplus m$		$a = s \oplus m$
	challenge phase for $i = 1$ to n	
pick $c_i \in \{0,1\}$		
start timer_i	$\xrightarrow{c_i}$	
stop timer_i	$\xleftarrow{r_i}$	$r_i = a_{2i+c_i-1}$
	verification phase	
check $\mathsf{timer}_i \leq 2B$, $r_i = a_{2i+c_i-1}$	$\xrightarrow{\mathsf{Out}_V}$	
private output: pk		

Security of privDB with OTDB

Theorem

If

- *we cannot make a key and a valid signature for two different N*
- *the signature is UF-CMA-secure and*
- *the cryptosystem is IND-CCA-secure,*

then the protocol is

1. *DF-secure*
2. *MF-secure*
3. *DH-secure*
4. *wide-strong HPVP11-private*

State of Affair

protocol	Secure	DF	DH	Sound	Privacy	Strong p.	Efficient
Brands-Chaum	☺	☺	☹	☹	☹	☹	☺
DBPK-Log		!☹!		!☹!	☹	☹	☹
HPO	☺	☺	☹	☹	☺	☹	☺
GOR	☺	☺	☹	☹	!☹!	!☹!	☹
privDB	☺	☺	☺	☹	☺	☺	☺
ProProx	☺	☺	☺	☺	☹	☹	☹
eProProx	☺	☺	☺	☺	☺	☺	☹
Eff-pkDB	☺	☺	☺	☹	☹	☹	☺
Eff-pkDB^p	☺	☺	☺	☹	☺	☺	☺

ProProx (Variant I, Noiseless)

Verifier	$\mathsf{pk} = \mathrm{Com}_H(\mathsf{sk})$ $(\mathsf{pk}_j = \mathrm{Com}(\mathsf{sk}_j; H(\mathsf{sk}, j)))$	**Prover**
public: pk		secret: sk
	initialization phase	
	for $i = 1$ to n and $j = 1$ to s	
(b: a vector of weight $\frac{n}{2}$)		pick $a_{i,j} \in \mathbf{Z}_2$, $\rho_{i,j}$
	$\xleftarrow{A_{i,j}}$	$A_{i,j} = \mathrm{Com}(a_{i,j}; \rho_{i,j})$
	challenge phase	
	for $i = 1$ to n and $j = 1$ to s	
pick $c_{i,j} \in \mathbf{Z}_2$		
start $\mathrm{timer}_{i,j}$	$\xrightarrow{c_{i,j}}$	receive $c'_{i,j}$
receive $r_{i,j}$, stop $\mathrm{timer}_{i,j}$	$\xleftarrow{r'_{i,j}}$	$r'_{i,j} = a_{i,j} + c'_{i,j} b_i + c'_{i,j} \mathsf{sk}_j$
	verification phase	
check $\mathrm{timer}_{i,j} \leq 2B$		
$z_{i,j} = A_{i,j} \left(\theta^{b_i} \mathsf{pk}_j\right)^{c_{i,j}} \theta^{-r_{i,j}}$	$\xleftrightarrow{ZKP_\kappa(z_{i,j}:\zeta_{i,j};i,j)}$	$\zeta_{i,j} = \rho_{i,j} H(\mathsf{sk}, j)^{c'_{i,j}}$
	$\xrightarrow{\mathrm{Out}_V}$	

eProProx (Variant I, Noiseless)

Verifier	$\mathsf{pk} = \mathrm{Com}_H(\mathsf{sk})$ $(\mathsf{pk}_j = \mathrm{Com}(\mathsf{sk}_j; H(\mathsf{sk}, j)))$	**Prover**
input: sk_V		input: $\mathsf{sk}, \mathsf{pk}, \mathsf{pk}_V$
	initialization phase	
	for $i = 1$ to n and $j = 1$ to s	pick $a_{i,j} \in \mathbf{Z}_2$, $\rho_{i,j}, \delta_j$
(b: a vector of weight $\frac{n}{2}$)		$B = \mathrm{Enc}_{\mathsf{pk}_V}(\delta \Vert \mathsf{pk})$
$\delta \Vert \mathsf{pk} = \mathrm{Dec}_{\mathsf{sk}_V}(B)$	$\xleftarrow{A_{i,j}, B}$	$A_{i,j} = \mathrm{Com}(a_{i,j}; \rho_{i,j})$
$\mathsf{pk}'_j = \mathsf{pk}_j \cdot \mathrm{Com}(0; \delta_j)$	$(\mathsf{pk}'_j = \mathrm{Com}(\mathsf{sk}_j; H'(\mathsf{sk}, j)))$	$H'(.,j) = H(.,j) \cdot \delta_j$
	challenge phase	
	for $i = 1$ to n and $j = 1$ to s	
pick $c_{i,j} \in \mathbf{Z}_2$		
start timer$_{i,j}$	$\xrightarrow{c_{i,j}}$	receive $c'_{i,j}$
receive $r_{i,j}$, stop timer$_{i,j}$	$\xleftarrow{r'_{i,j}}$	$r'_{i,j} = a_{i,j} + c'_{i,j} b_i + c'_{i,j} \mathsf{sk}_j$
	verification phase	
check timer$_{i,j} \leq 2B$		
$z_{i,j} = A_{i,j} \left(\theta^{b_i} \mathsf{pk}'_j \right)^{c_{i,j}} \theta^{-r_{i,j}}$	$\xleftrightarrow{ZKP_\kappa(z_{i,j}:\zeta_{i,j};i,j)}$	$\zeta_{i,j} = \rho_{i,j} H'(\mathsf{sk}, j)^{c'_{i,j}}$
output: pk	$\xrightarrow{\mathrm{Out}_V}$	

Privacy in eProProx

Theorem

If

- Com *is a computationally hiding and homomorphic bit commitment,*
- Enc/Dec *is an IND-CCA-secure cryptosystem,*
- ZKP_{κ} *is a computationally zero-knowledge proof of membership,*

then eProProx is ***wide-strong HPVP11-private****.*

Conclusion

- complete privacy models with return channel and/or corruption
- simulation-based or left-or-right definition
- wide-strong privacy is possible with PKC
- wide-weak privacy is possible with PRF
- can be added to distance bounding