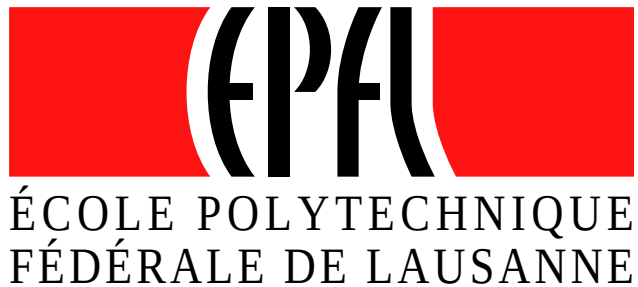
Privacy in Deniable Anonymous Concurrent Authentication with Setup is Impossible

Do we Care?

Serge Vaudenay



http://lasecwww.epfl.ch/

Is Cryptographic Theory Practically Relevant?

1. RC4 Cryptanalysis
2. Deniable Authentication
3. RFID Privacy

1 RC4 Cryptanalysis

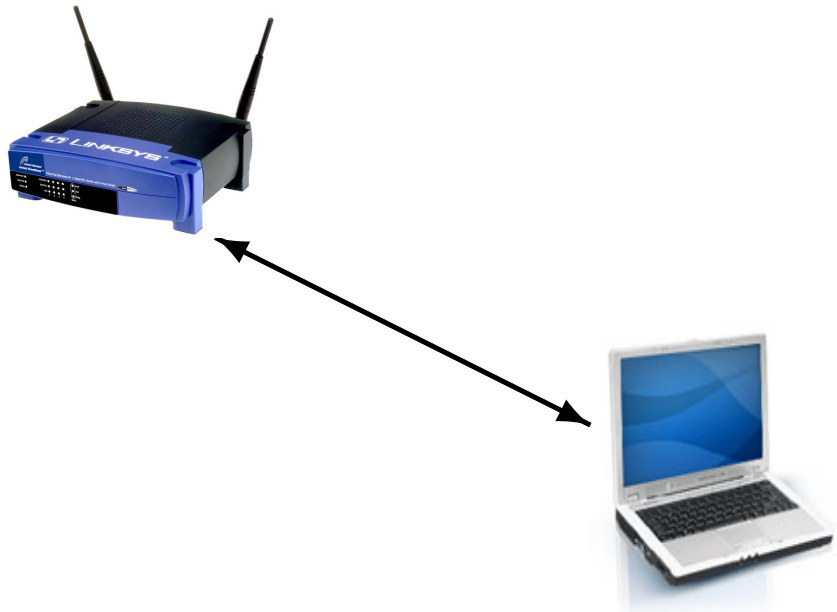
2 Deniable Authentication

3 RFID Privacy

References

- PhD Thesis of **Vuagnoux**.
  Computer Aided Cryptanalysis from Ciphers to Side Channels.
  EPFL, 2010. `http://library.epfl.ch/theses/?nr=4769`
- **Sepehrdad, SV, Vuagnoux**.
  Statistical Attack on RC4: Distinguishing WPA.
  Eurocrypt 2011
- ...and some follow up work to appear in the PhD Thesis of **Sepehrdad**.

WEP Smashing



passive attack: extract the pre-shared key after sniffing a few thousands encrypted packets

Influence of Practice on Theoretical Cryptanalysis

- look for one key byte x
- counter Y_x for the good value and 255 counters Y_y for each $y \neq x$
- assumes all counters are independent, normally distributed, with same variance, all Y_y with same expected value
- not the same variance in practice!
- rank R is the sum of $1_{Y_y > Y_x}$ over all $y \neq x$, assume all $1_{Y_y > Y_x}$ are independent
- not independent in practice!
- assume R to be normally distributed
- does not match practice!
- assume R to be Poisson distributed?
- expected value $\neq$ variance in practice!
- nicely match Pólya distribution in practice! (tornado prediction)
- rebuild the theory with a sound practice-inspired model

Relevance of Practice

- heuristic assumptions must be falsifiable and confirmed by practice
- theoretical cryptanalysis not relevant otherwise
- in theory, we can break *anything*
- as for cryptanalysis:

practical support is necessary to make theory relevant

Is Practical Cryptography Relevant for Theory?

1 RC4 Cryptanalysis

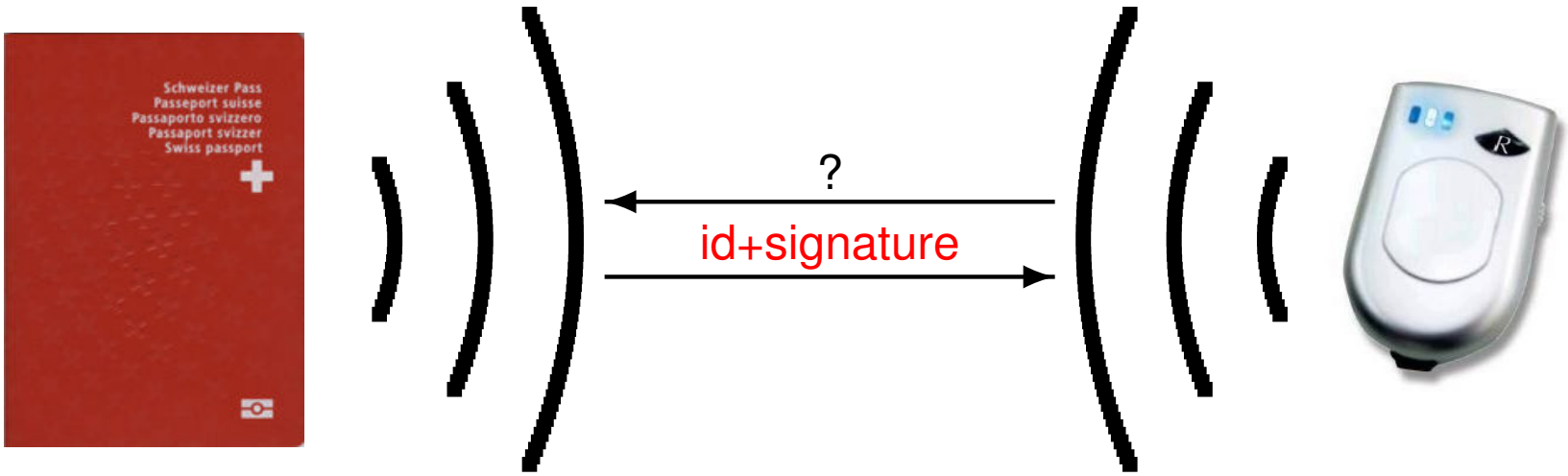
2 **Deniable Authentication**

3 RFID Privacy

References

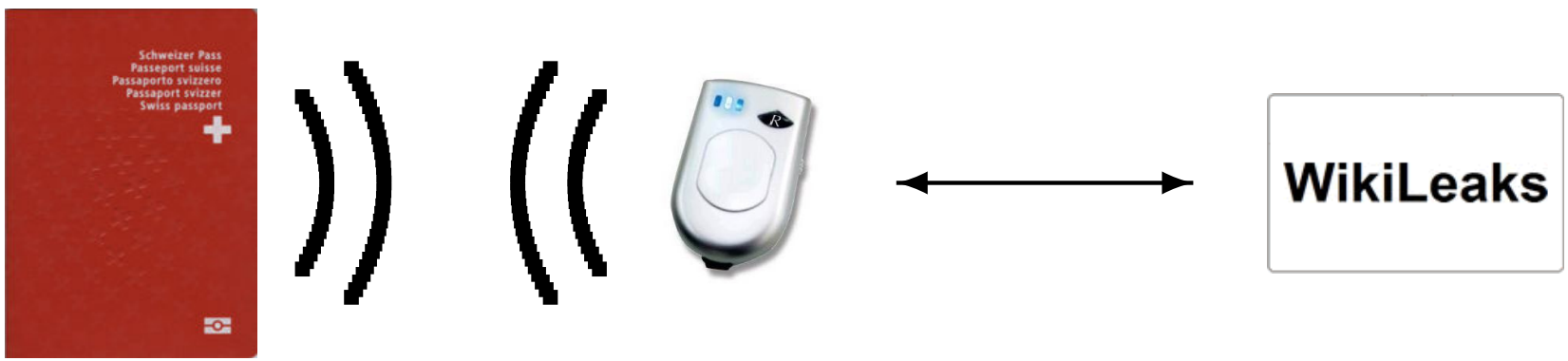
- **Monnerat, SV, Vuagnoux**.
  About Machine-Readable Travel Documents: Privacy Enhancement Using (Weakly) Non-Transferable Data Authentication.
  RFID Security 2007
- **Monnerat, Pasini, SV**.
  Efficient Deniable Authentication for Signatures: Application to Machine-Readable Travel Document.
  ACNS 2009
- **Mateus, SV**.
  On Tamper-Resistance from a Theoretical Viewpoint: The Power of Seals.
  CHES 2009
- **SV**.
  Deniable RSA Signature: The Raise and Fall of Ali Baba.
  Quisquater Festschrift, LNCS 6805 to appear.

Biometric Passport



Mafia Fraud

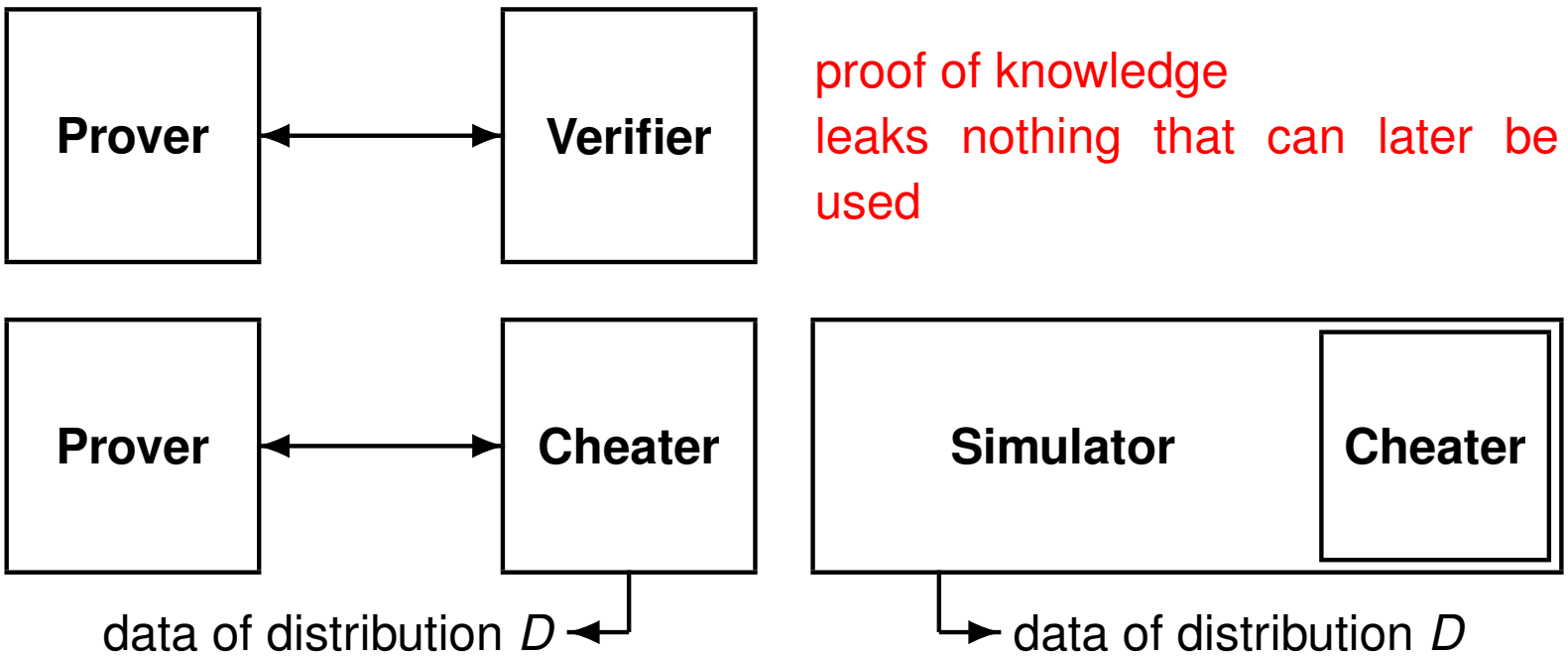
leakage of digital evidence



Problem

- want to prove possession of a valid signature for id
- want to make the proof deniable
- sounds like zero-knowledge!

Zero-Knowledge



HVZK Proof of RSA Signature Knowledge

Guillou-Quisquater

Prover		**Verifier**
formated message: X **private signature**: x	**public key**: N, e	**formated message**: X
pick $y \in \mathbf{Z}_N^*$		pick $c \in \{0,1\}^\ell$
$Y \leftarrow y^e \bmod N$	$\xrightarrow{Y}$	
	$\xleftarrow{c}$	
$z \leftarrow yx^c \bmod N$	$\xrightarrow{z}$	$z^e \stackrel{?}{\equiv} YX^c \pmod N$

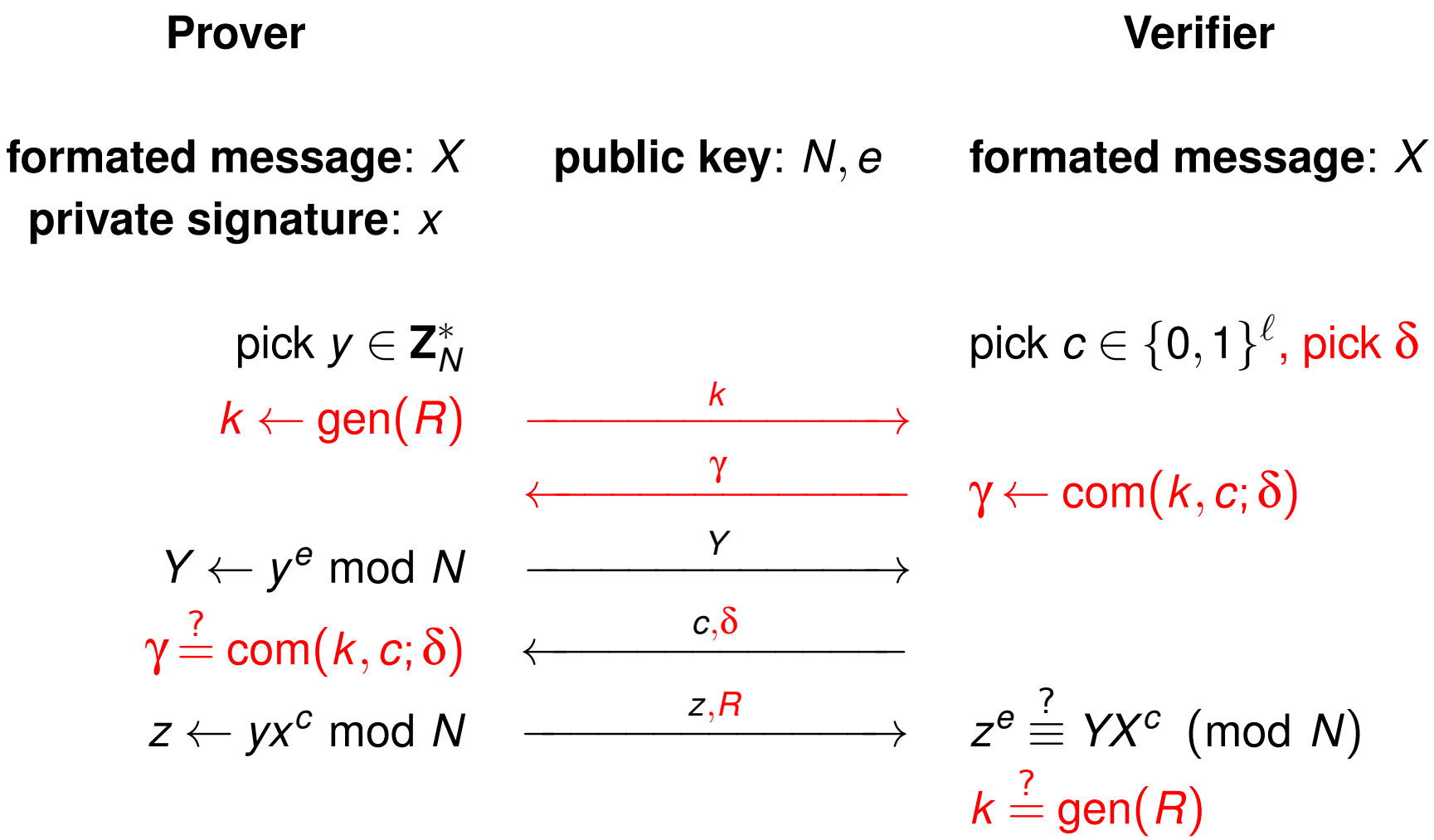
HVZK can Make Non-Repudiable Proofs: not Deniable

Fiat-Shamir Paradigm

Prover		Verifier
x st $x^e \bmod N = X$	(N, e, X)	
pick $y \in \mathbf{Z}_N^*$		pick $c \in \{0,1\}^\ell$
$Y = y^e \bmod N$	$\xrightarrow{Y}$	
	$\xleftarrow{c}$	
$z = yx^c \bmod N$	$\xrightarrow{z}$	$z^e \stackrel{?}{\equiv} YX^c \pmod N$

- domain parameter: N, e
- public key: X
- secret key: x such that $x^e \bmod N = X$
- signature: pick y, set $Y = y^e \bmod N$, $c = H(\text{message} \| Y)$, $z = yx^c \bmod N$, signature is (Y, z)
- verification: $z^e \stackrel{?}{\equiv} YX^{H(\text{message} \| Y)} \pmod N$

Proof of Signature Knowledge based on GQ



full ZK with a prior commitment round (**trapdoor** commitment)

Why a “Trapdoor” Commitment?

- the trapdoor functionality is never used!
- we need it to construct an extractor:
  the extractor runs a protocol with P, gets trapdoor at the end, restart with the protocol with same commitment but opening it to a different challenge, then use the Σ extractor
- trapdoor needed for theory, not practice!
- why don’t we try to get rid of this useless trapdoor in practice?

More Efficient Commitment with CRS

Prover		**Verifier**
formated message: X **private signature**: x	**public key**: N, e $\mathrm{crs} = \mathrm{gen}(R)$	**formated message**: X
pick $y \in \mathbf{Z}_N^*$		pick $c \in \{0,1\}^\ell$, pick δ
	$\xleftarrow{\gamma}$	$\gamma \leftarrow \mathrm{com}(\mathrm{crs}, c; \delta)$
$Y \leftarrow y^e \bmod N$	$\xrightarrow{Y}$	
$\gamma \stackrel{?}{=} \mathrm{com}(\mathrm{crs}, c; \delta)$	$\xleftarrow{c,\delta}$	
$z \leftarrow yx^c \bmod N$	$\xrightarrow{z}$	$z^e \stackrel{?}{\equiv} YX^c \pmod N$

full ZK with a prior commitment round (CRS-based)

Even More Efficient Commitment with Random Oracle

Prover		**Verifier**
formated message: X **private signature**: x	**public key**: N, e	**formated message**: X
pick $y \in \mathbf{Z}_N^*$		pick $c \in \{0,1\}^\ell$, pick δ
	$\xleftarrow{\gamma}$	$\gamma \leftarrow H(c, \delta)$
$Y \leftarrow y^e \bmod N$	$\xrightarrow{Y}$	
$\gamma \stackrel{?}{=} H(c, \delta)$	$\xleftarrow{c,\delta}$	
$z \leftarrow yx^c \bmod N$	$\xrightarrow{z}$	$z^e \stackrel{?}{\equiv} YX^c \pmod N$

full ZK with a prior commitment round (RO-based)

Caveat

Deniable Zero-Knowledge

- ZK is deniable in the plain model only
- ZK in CRS or ROM not always deniable
- how could we have a good protocol in a plain model which becomes bad by adding setup assumptions?
- failure of the deniability theory in the plain model
- theory rescues: can remain deniable if careful (Pass theory)

Setup Assumptions

- OK, we are done with CRS and ROM, but how about other setups?
- no CRS or random oracles in the real world
- can't we think of other setup assumptions?
- tamper resistance?

A Practical (?) Setup

Trusted Agent: a Model for Tamper Resistance

- we add a special participant (tamper-resistant device)
- includes 1- a trusted boot loader, 2- a display, 3- an input port
- first input: a boot code (OS) C
- after boot complete: $h(C)$ displayed in every message

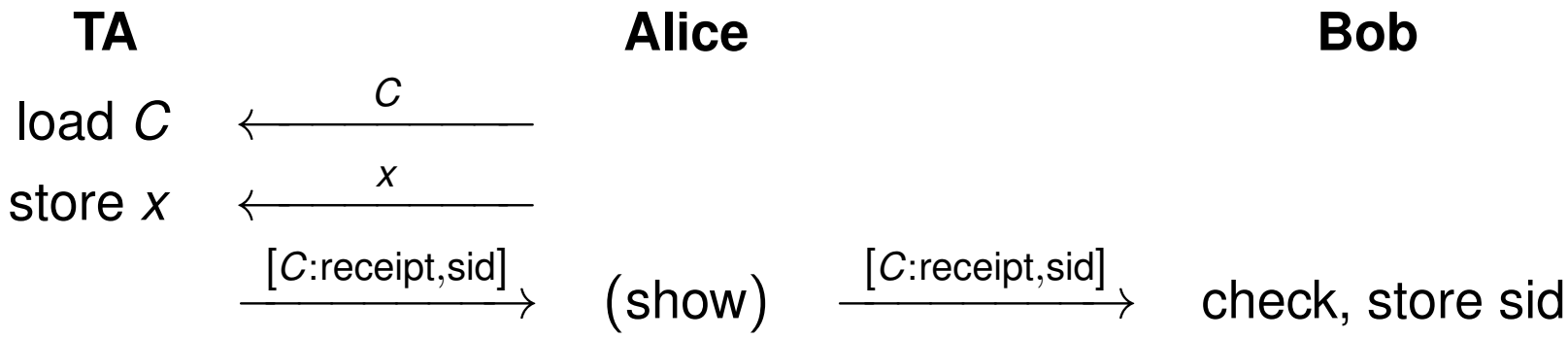
Commitment using a Trusted Agent — i

define code C:

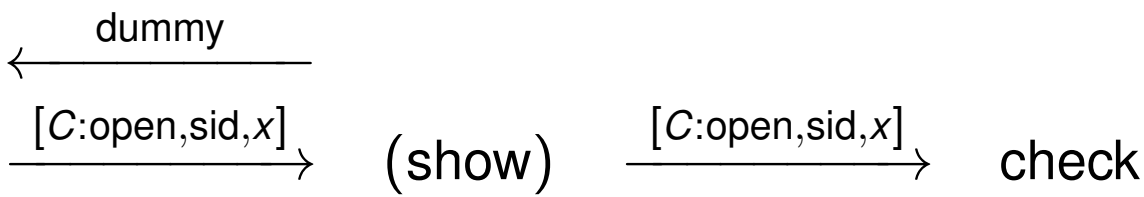
1: receive x
2: pick a random sid
3: output "receipt, sid"
4: wait for new input
5: output "open, sid, x"

Commitment using a Trusted Agent — ii

commit protocol:



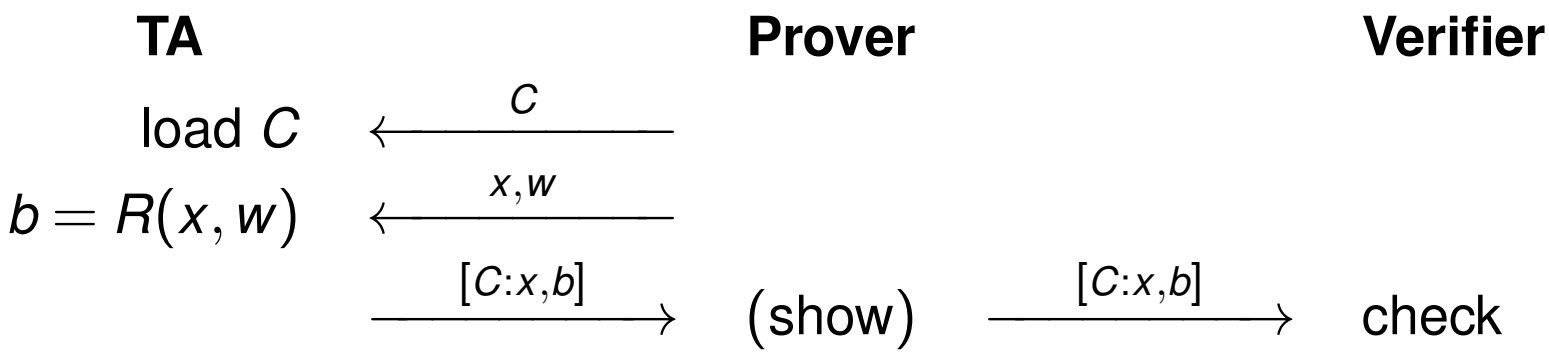
opening protocol:



check means:

- check message comes from a TA
- check code C is as expected by the commitment protocol
- check sid is the same

Trivial Zero-Knowledge for Relation R

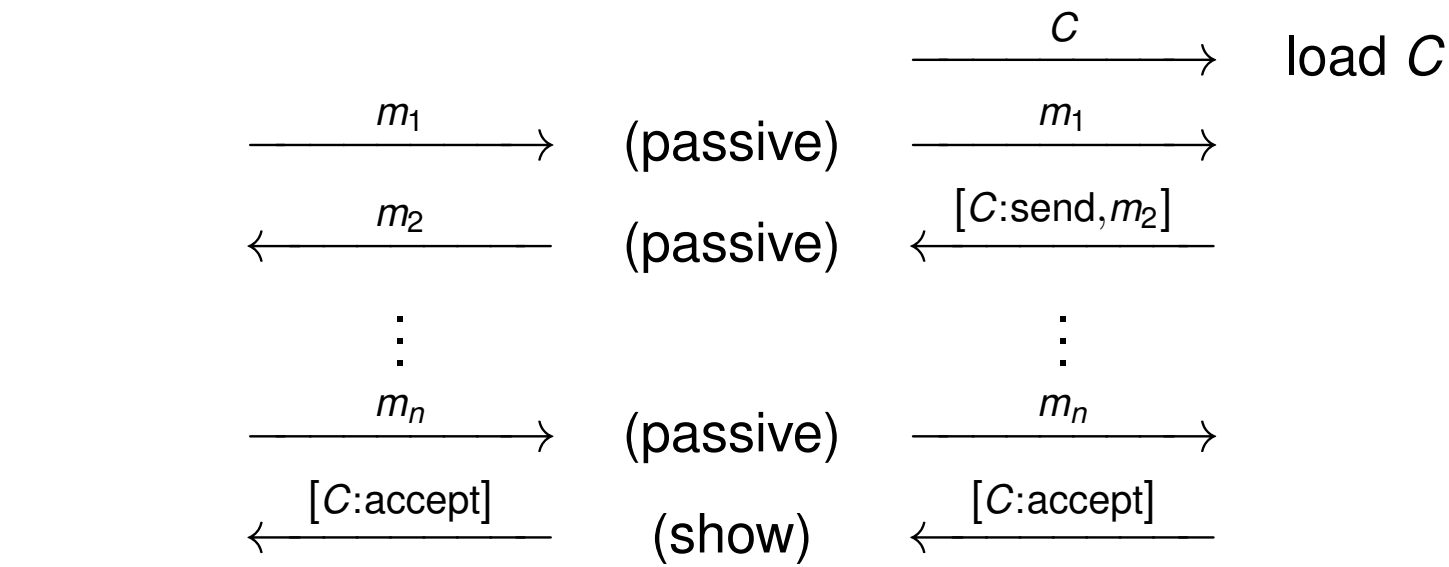


check means:

- check message comes from a TA
- check code C is as expected by the ZK protocol
- check x is as expected and $b = \text{true}$

Deniability Loss in Regular ZK Protocols

C: code to simulate the verifier algorithm



final message cannot be simulated because it comes from a TA!
(TAs cannot be rewinded)

proof is no longer deniable

Conclusion

- an inspiring theory to make cute protocols
- many odd things in protocols playing no practical role
- deniability is too fragile
- may collapse due to setup assumptions
- same with: anonymity, undeniable signatures, receipt-freeness
- nice theory, but helpless in practice

1 RC4 Cryptanalysis

2 Deniable Authentication

3 **RFID Privacy**

References

- Prior work in the PhD Thesis of **Avoine**.
  Cryptography in Radio Frequency Identification and Fair Exchange Protocols.
  EPFL, 2005. `http://library.epfl.ch/theses/?nr=3407`
- **SV**. On Privacy Models for RFID. *Asiacrypt 2007*
- **Radu-Ioan Paise, SV**.
  Mutual Authentication in RFID: Security and Privacy.
  Asiacrypt 2008
- ...and some follow up work to appear in the PhD Thesis of **Ouafi**.
  Security and Privacy in RFID Systems.
  2012

HB Protocol

Prover		**Verifier**
secret key: x		**secret key**: x
pick $\nu \leftarrow \text{Binomial}(r, \eta)$	$\xleftarrow{A}$	pick $A \in \{0,1\}^{k \times r}$
$z \leftarrow xA + \nu$	$\xrightarrow{z}$	$\text{HW}(z + xA) \overset{?}{\leq} t$

- secure against passive adversary who then tries to impersonate (LPN problem)
- insecure against an active adversary: query A several times and make statistics on z to get rid of ν, then solve a linear system

HB+ Protocol

Prover		**Verifier**
secret key: x, y		**secret key**: x, y
pick $B \in \{0,1\}^{k_y \times r}$	$\xrightarrow{B}$	
pick $\nu \leftarrow \text{Binomial}(r, \eta)$	$\xleftarrow{A}$	pick $A \in \{0,1\}^{k_x \times r}$
$z \leftarrow xA + yB + \nu$	$\xrightarrow{z}$	$\text{HW}(z + xA + yB) \stackrel{?}{\leq} t$

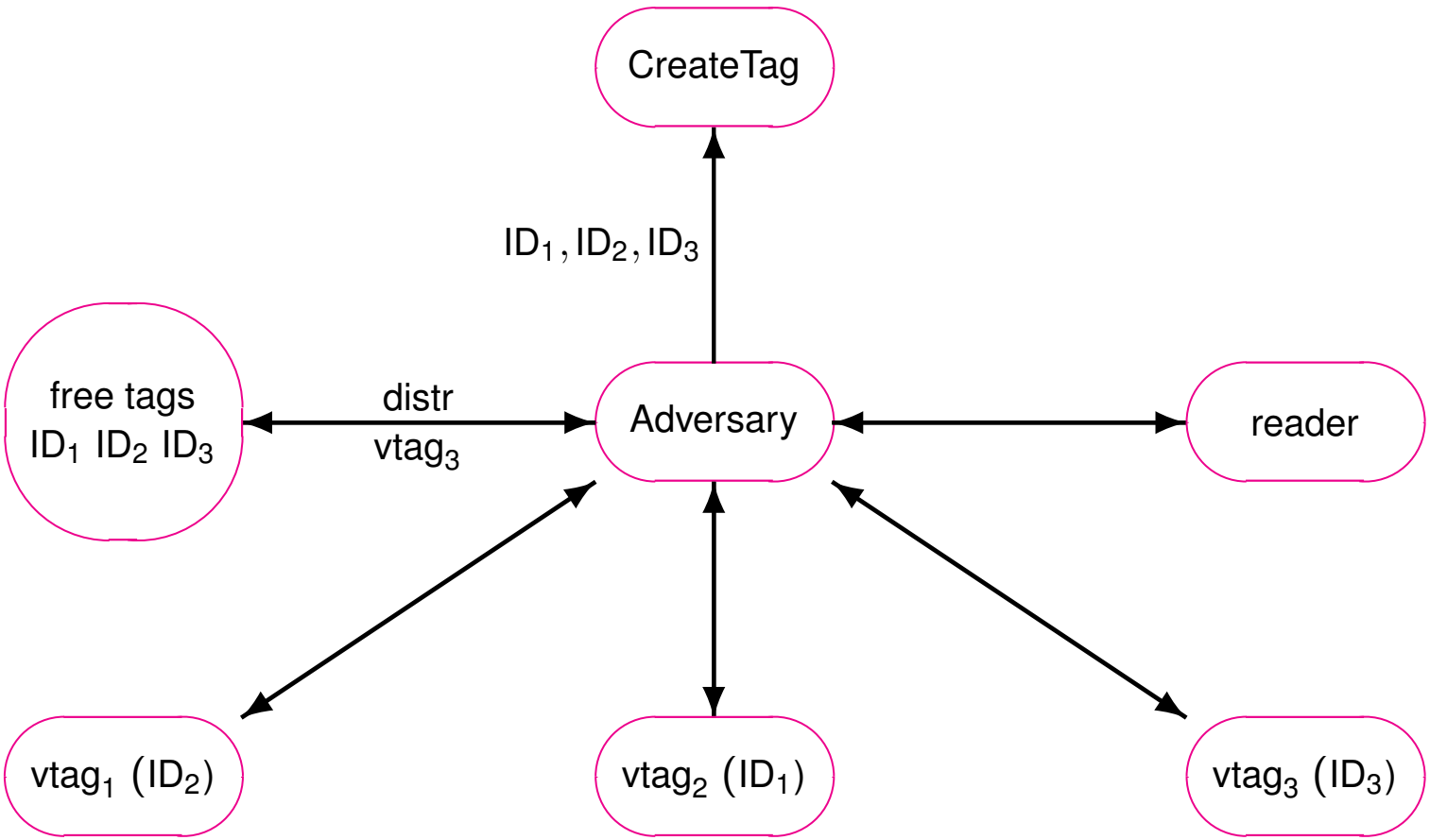
- secure against active adversary who plays first with Prover then once with Verifier
- insecure against MiM adversary with return channel: replace A by $A + (\delta^{\perp}\delta^{\perp}\cdots\delta^{\perp})$, Verifier accepts iff $x \cdot \delta = 0$ which is a linear equation

Random-HB# Protocol

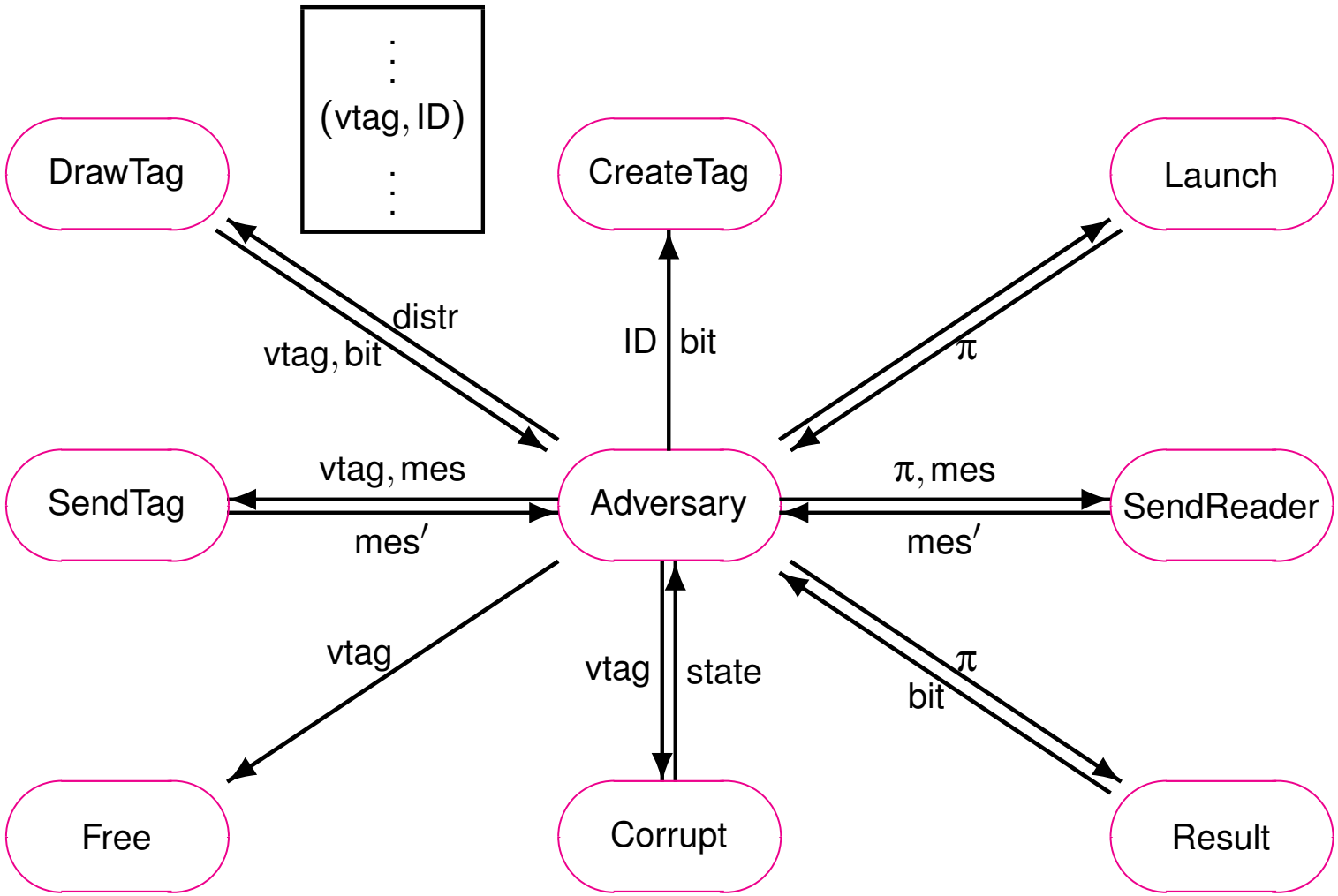
Prover		**Verifier**
secret key: X, Y		**secret key**: X, Y
pick $b \in \{0,1\}^{k_y}$	$\xrightarrow{\quad b \quad}$	
pick $\nu \leftarrow \text{Binomial}(r, \eta)$	$\xleftarrow{\quad a \quad}$	pick $a \in \{0,1\}^{k_x}$
$z \leftarrow aX + bY + \nu$	$\xrightarrow{\quad z \quad}$	$\text{HW}(z + aX + bY) \overset{?}{\leq} t$

- secure against MiM adversary who only corrupt messages from Verifier to Prover
- insecure against full MiM adversary: given $\bar{\nu} = \bar{z} + \bar{a}X + \bar{b}Y$, replace (b, a, z) by $(b + \bar{b}, a + \bar{a}, z + \bar{z})$, Verifier accepts iff $\text{HW}(\nu + \bar{\nu}) \leq t$ on which we can make statistics to get $\text{HW}(\bar{nu})$, then iterate to lower it and get linear relations

Adversarial Model



Oracle Accesses



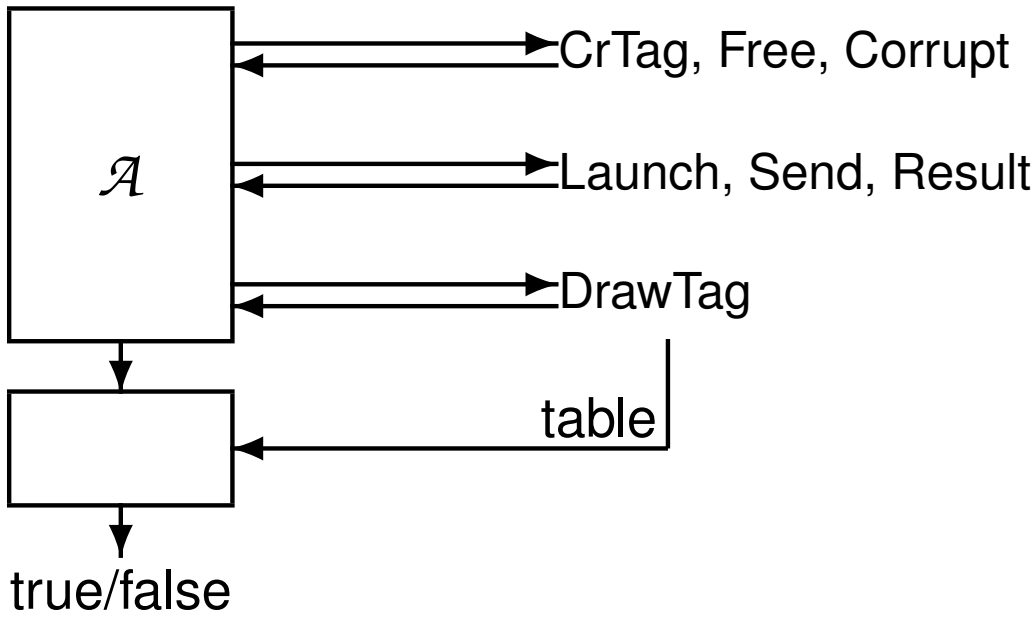
Security

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

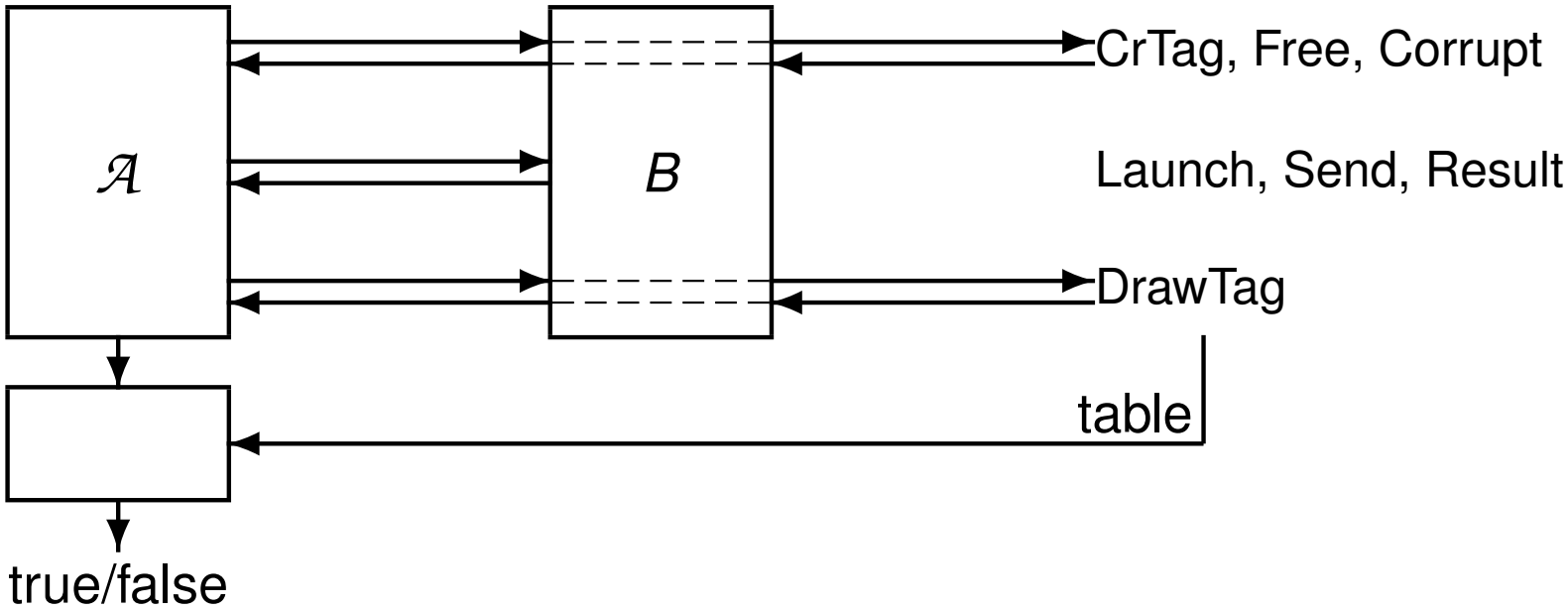
An RFID scheme is secure if for any polynomially bounded adversary the probability of success is negligible.

Privacy Adversary



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

Blinders

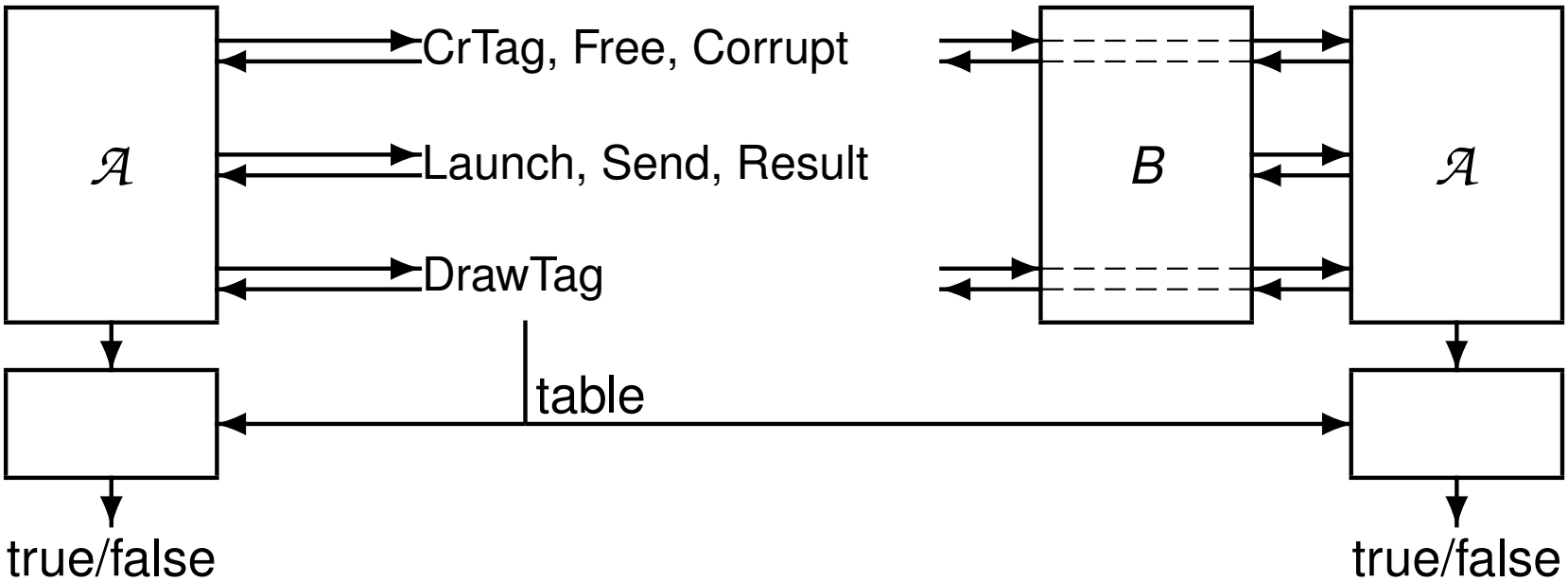


Definition

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

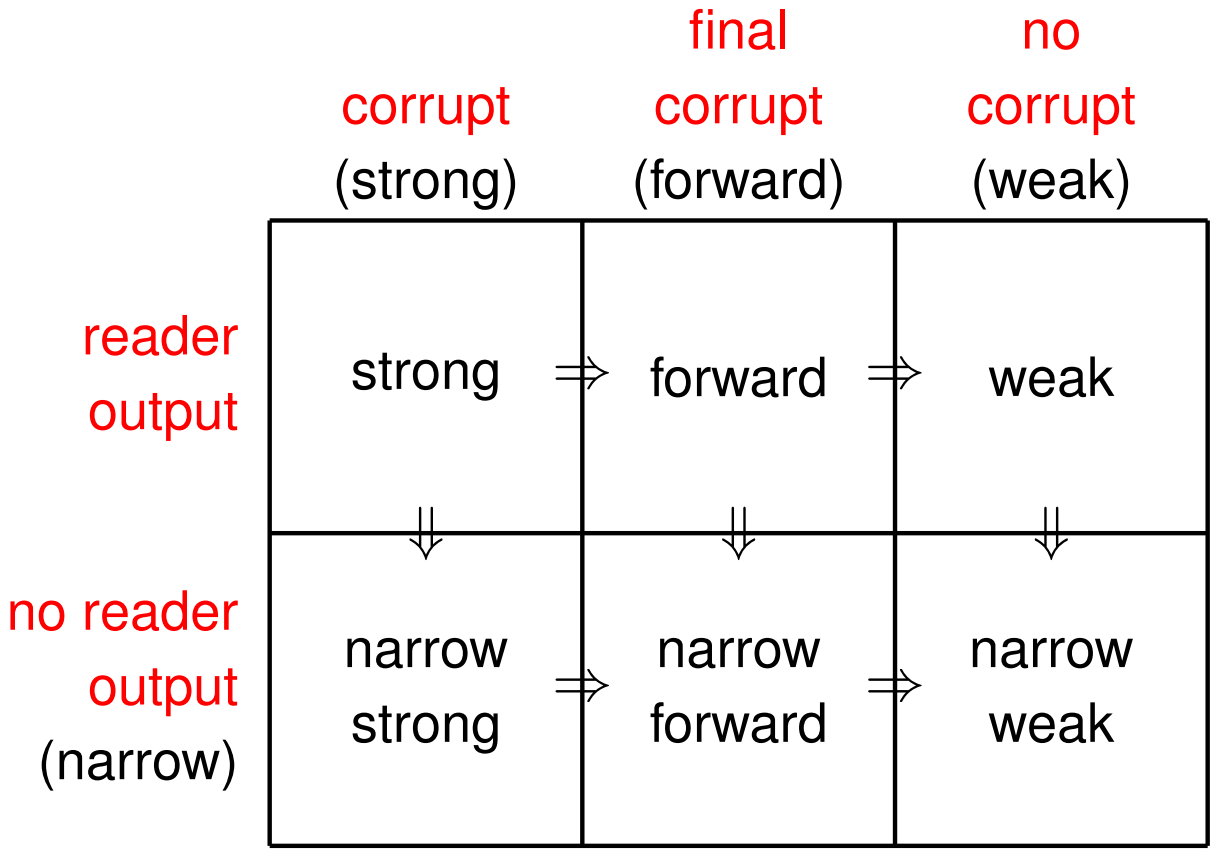
Privacy



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



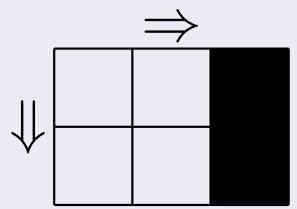
Challenge-Response RFID Scheme

Tag		**System**
state: K		$\{\ldots,(\mathrm{ID},K),\ldots\}$
pick b	$\xleftarrow{a}$	pick a
$c = F_K(a,b)$	$\xrightarrow{b,c}$	find (ID,K) s.t. $c = F_K(a,b)$
		output: ID

Theorem

If F is a PRF, this scheme is

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



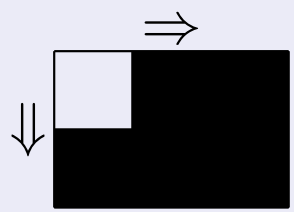
Public-Key-Based RFID Scheme

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

Theorem

If Enc/Dec *is an IND-CCA PKC, this scheme is*

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

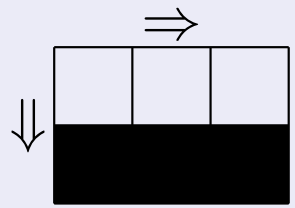


Narrow-Strong Privacy Implies Public-Key Cryptography

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!

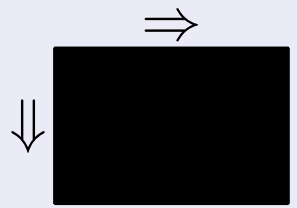
Strong Privacy is Infeasible

Theorem

An RFID scheme cannot be

- *correct*
- *strong private*

at the same time.



no strong privacy!

Recap

- we have a nice model for RFID security and privacy
- several levels of privacy
- nice protocol based on PRF for low level privacy
- protocol based on PKC for nearly-highest level
- theorem saying that PKC is necessary for that level
- impossibility result for highest level
- well done theory, let's go for holidays!

Impossibility Proof

take the following adversary (strong privacy)

1. simulate the creation of a tag 0, get its state S_0
2. create a tag 1, draw it, corrupt it, get its state S_1
3. flip a coin b
4. launch a protocol with the reader and simulate tag with state S_b
5. output the protocol outcome (Result)

a blinder $\mathcal{B}$ for this advesary gets K_P, S_1, interacts with a tag of state S_b, and guesses b

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

1. create a tag 0 and 1, draw them, corrupt them, get their state S_0 and S_1
2. free the tags, then draw one of the two vtag
3. run $\mathcal{B}(K_P, S_1, \text{vtag}) \rightarrow x$
4. output 1 iff $\mathcal{T}(\text{vtag}) = x$

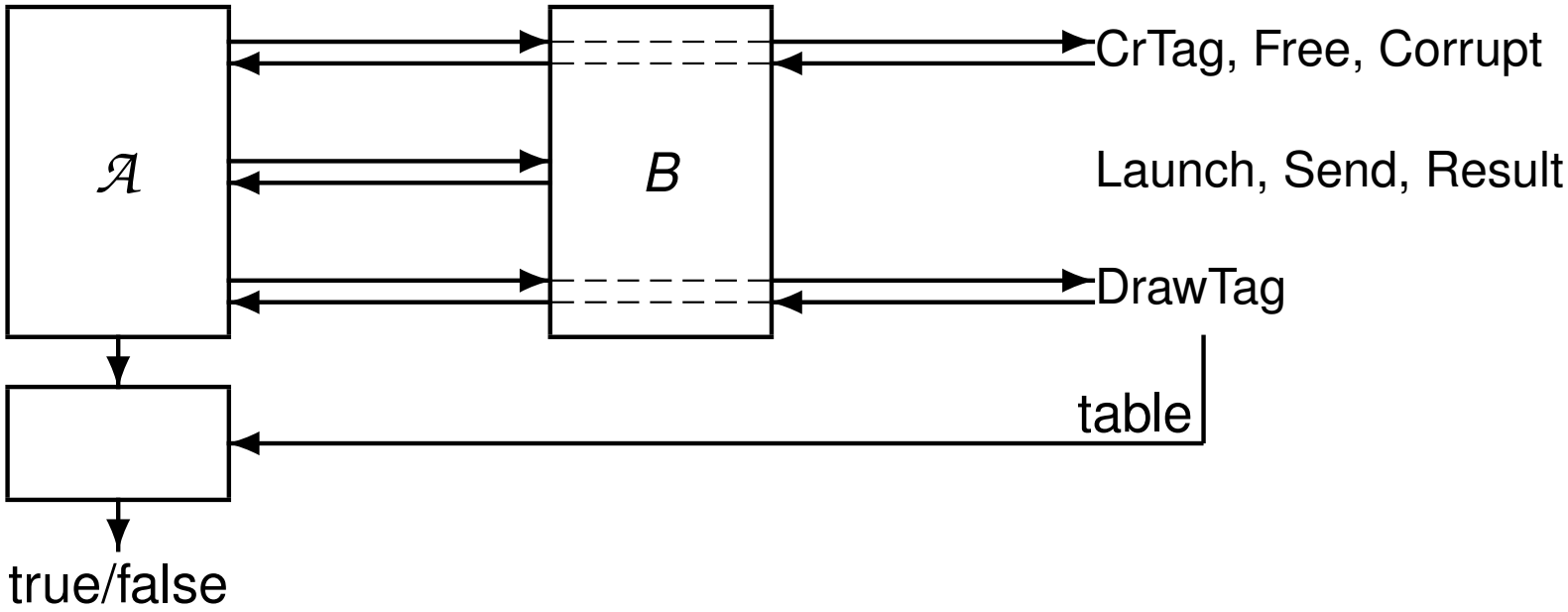
a blinder for this adversary receives no information about the drawn tag and has to guess it!

is this really an attack?!?

Problem with this Proof

- the adversary is querying the system to test if it behaves correctly
- no blinder can simulate the system coherently
- but this does not mean any attack in practice
- morality: to reconciliate theory and practice, the blinder should be able to read the adversary's mind
- need for an update in the definition of the blinder

Telepathic 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

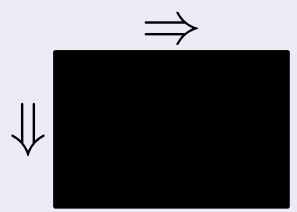
Public-Key-Based RFID Scheme

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

Theorem

If Enc/Dec *is a PA2+IND-CPA PKC, this scheme is*

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

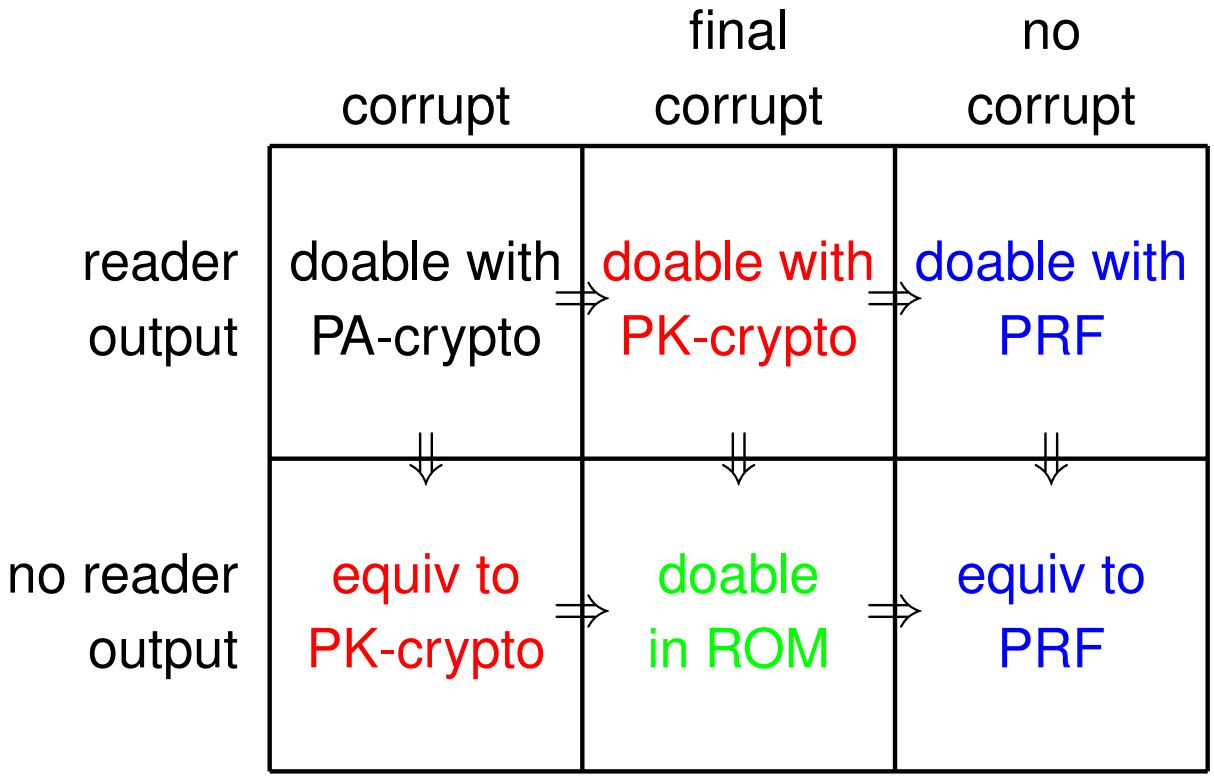


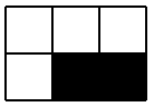
PA2 Trick

- PA2 means that all valid ciphertexts produced by the adversary must either be a reused one that the adversary got or a ciphertext for which the adversary knows how it decrypts (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)

Privacy in RFID

Privacy with respect to adversarial capabilities:



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

Conclusion

- theory helped to identify good protocols here
- the one based on PKC was the good one, except that the model to prove it was ill-designed to begin with
- needs the theoretical notion of PA
  (by the way, is there any practical gap between IND-CCA and PA+IND-CCA?)
- we had to fight with the theory to prove it
- except strengthening our confidence, no impact on practice!

Conclusion

- theory needs supporting experiments (e.g. for cryptanalysis)
- theory helps to strengthen confidence in protocols
- does not seem to have any other significant impact in real world