Privacy in RFID

Strong Privacy needs Public-Key Cryptography

Serge Vaudenay

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

http://lasecwww.epfl.ch/

1. The Bluetooth Case
2. The Passport RFID Case
3. Some RFID Schemes
4. Strong Privacy in RFID

The Bluetooth Principles

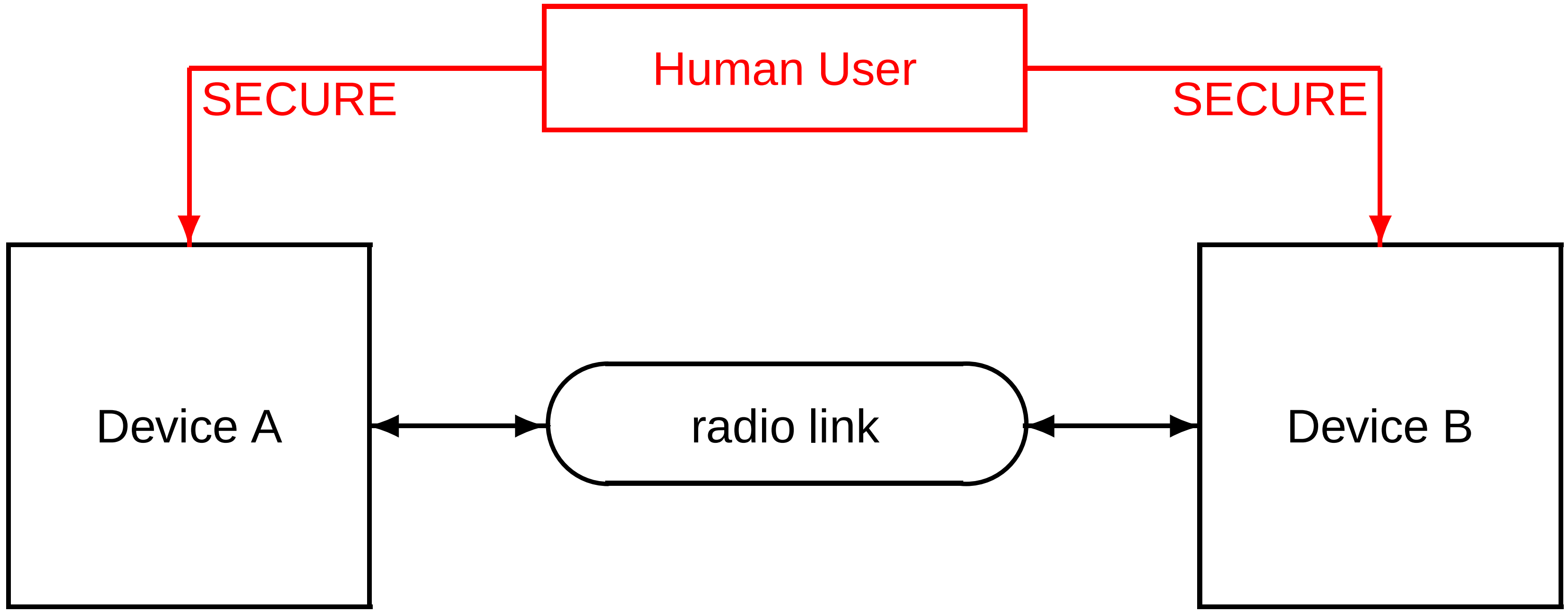
- short-range wireless technology
- designed to transmit voice and data
- for a variety of mobile devices (computing, communicating, ...)
- bring together various markets





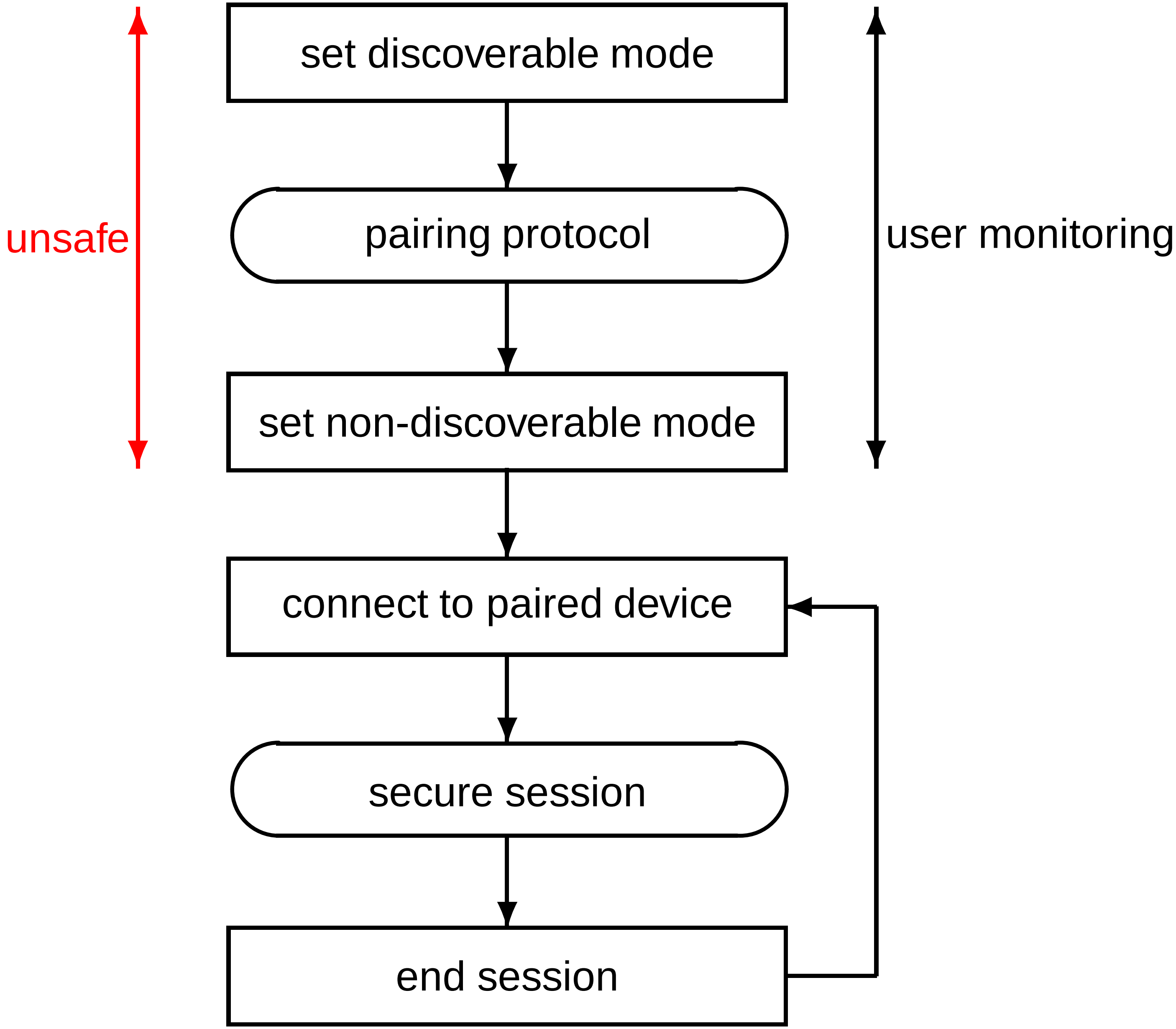
- 1Mbit/sec up to 10 meters over the 2.4-GHz radio fequency
- robustness, low complexity, low power, low cost

Bluetooth Channels



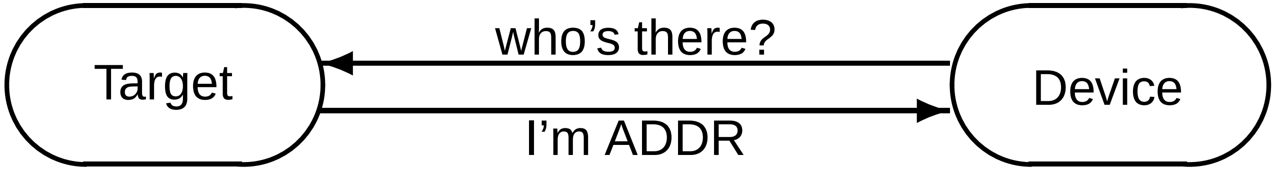
- secure channel for a PIN only
- security based on an ephemeral PIN

Privacy in Bluetooth

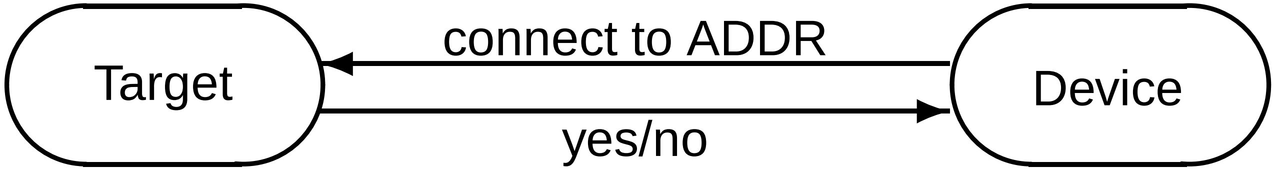


Discovery and Connection Protocols

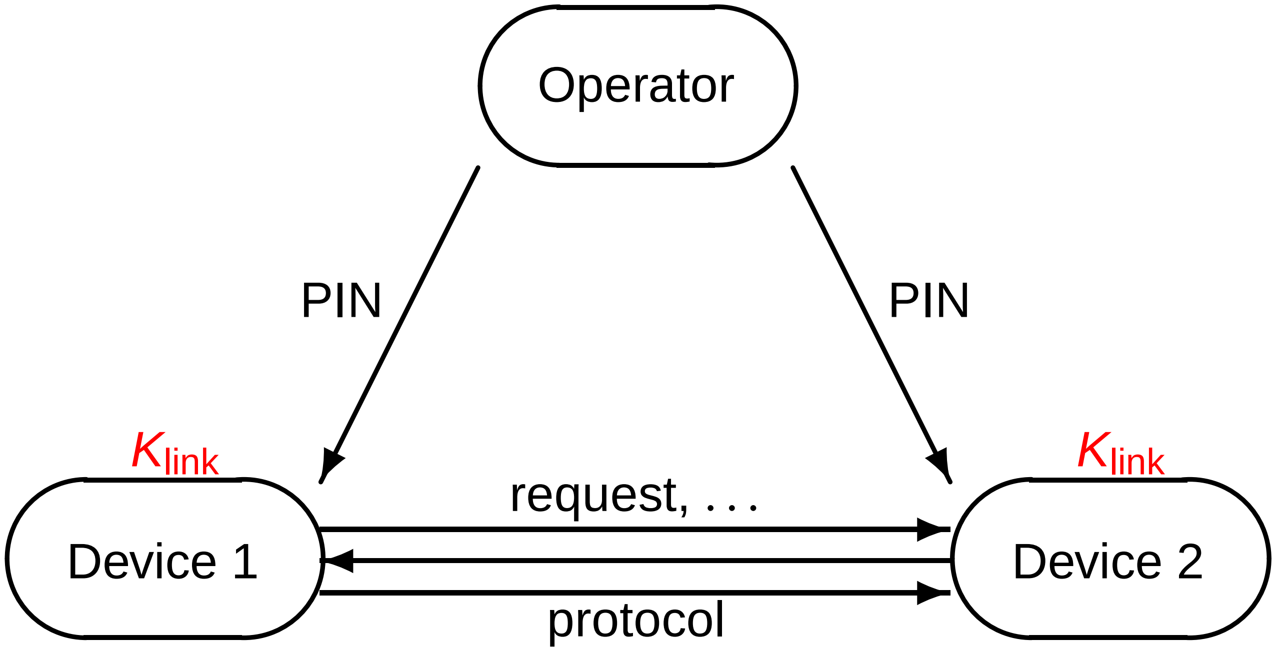
- Discovery protocol:



- Connection protocol:



Device Pairing



Peer Authentication

Master A		Slave B
pick challenge	challenge $\longrightarrow$	
check	response $\longleftarrow$	compute response
	challenge $\longleftarrow$	pick challenge
compute response	response $\longrightarrow$	check

$$\text{response} = \text{MAC}(\text{challenge})$$

Key Establishment (In)security

Theorem

Under some “reasonable assumptions”, the pairing protocol is secure if either PIN *has large entropy or the protocol is run through a private channel.*

- ☺ a cheap pragmatic security
- ☹ pretty weak security

devastating sniffing attacks in other cases! (Jakobsson-Wetzel 2001 [JW 2001])

Bluetooth (In)security

Current (mode 3) security is rather poor:

- confidentiality ☺ (attacks still academic so far)
- authentication ☺ (not academic though: by encryption)
- integrity ☹
- freshness ☺
- liveliness ☹
- key establishment ☹ (yes, but...)
- sequentiality ☺/☹ (message loss)
- privacy ☹

Machine Readable Travel Documents Offering ICC Read-Only Access

- standard by ICAO (International Civil Aviation Organization)
- purpose: put radio readable IC chip in travel documents (passport) that contain biometric (privacy-sensitive) information
- version 1.1 published in 2004 (`http://www.icao.int/mrtd`)

Objectives

- to enable inspecting authorities of receiving States to verify the authenticity and integrity of the data stored in the MRTD
- use contactless IC chip devices
- add digitally stored fingerprint and/or iris images in MRTD
- treat those data as privacy-sensitive
- have no centralized private key
- maintained by ICAO

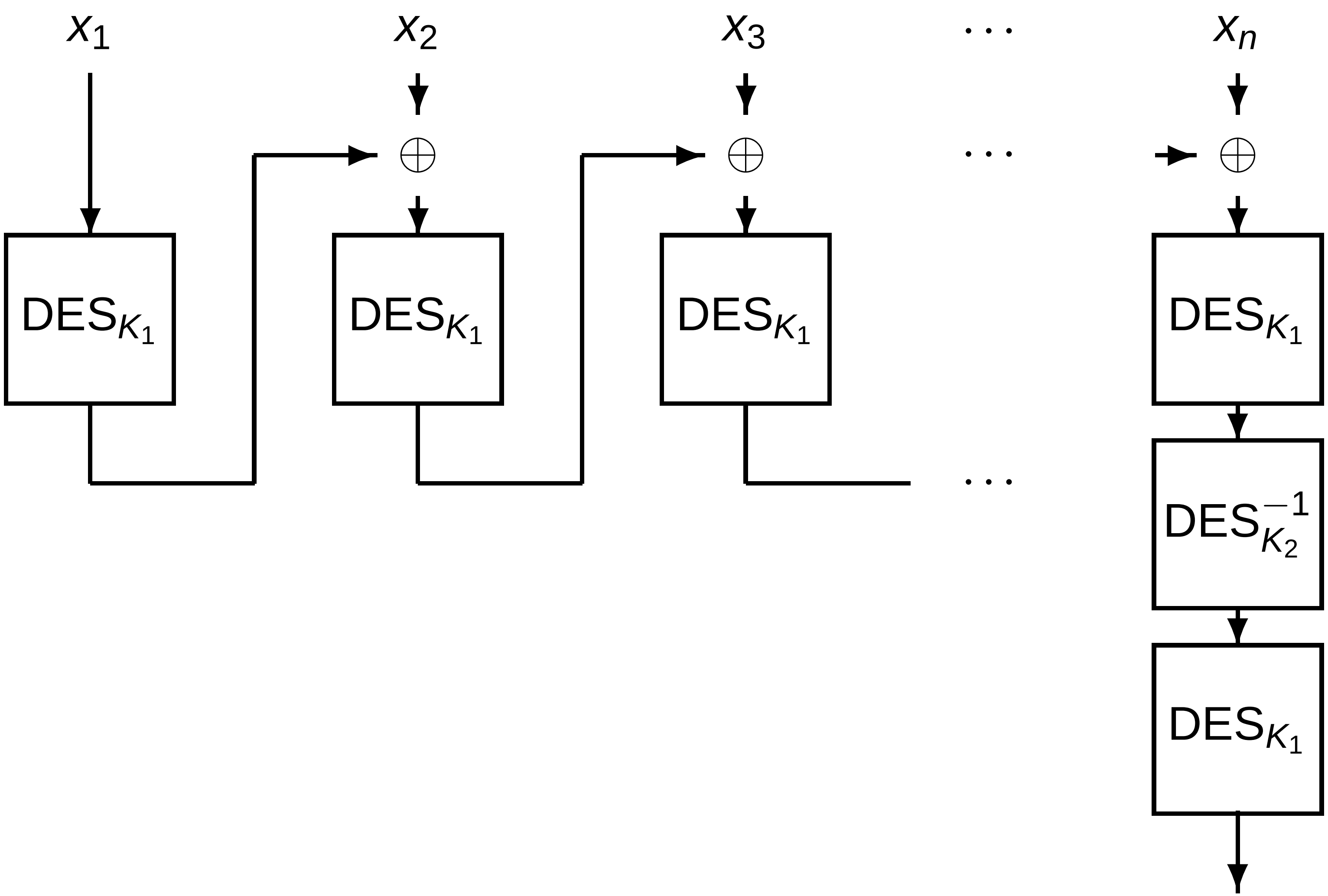
Underlying Cryptography

- SHA1 and sisters
- DES, triple-DES, CBC encryption mode
- one of the ISO/IEC 9797-1 MAC (next slide)
- RSA signatures (ISO/IEC 9796, PKCS#1), DSA, ECDSA
- X.509

ISO/IEC 9797-1

(MAC algorithm 3 based on DES with padding method 2)

(concatenate message with bit 1 and enough 0 to reach a length multiple of the block size)



PKI

- each country has a certificate authority CSCA (Country Signing Certificate Authority)
- public key of CSCA KPu_{CSCA} is self-signed into C_{CSCA}
- C_{CSCA} is distributed to other countries and ICAO by diplomatic means
- each DS (Document Signer) has a public key KPu_{DS}, a secret key KPr_{DS}, and a certificate C_{DS} signed by CSCA
- revocation lists are frequently released

Traveling Document

MRTD (Machine Readable Travel Document) with ICC read-only access contain

- a logical data structure LDS (e.g. fingerprint images)
- document security object SO_D, containing the hash of LDS, signed by DS, that may contain the certificate C_{DS} by CSCA
- (for active authentication only) a public key KPu_{AA} and secret key KPr_{AA} (the hash of KPu_{AA} is also in SO_D for authentication purpose)
- an optically readable MRZ, the hash of which being also contained in SO_D for authentication purpose

Access Control Options

- none: anyone can query the ICC, communication in clear
- basic: uses secure channel with authenticated key establishment from MRZ
- extended: up to bilateral agreements (no standard)

Passive Authentication (No Access Control)

- inspection authority loads SO_D, extract the DS, gets C_{DS}, verifies it, check the signature of SO_D
- inspection authority loads LDS and check its hash in SO_D

pro requires no processing capabilities on the MRTD side

con no privacy protection

Basic Access Control

- inspection authority reads MRZ, takes the 16 first bytes of its SHA1 hash and uses it as a key seed to derivate symmetric keys
- inspection authority and ICC mutually authenticate and derive session keys
- inspection authority can now talk to ICC through a secure channel

pro privacy protection

con requires processing capabilities on the MRTD side

Key Derivation from MRZ (Basic Access Control)

used to derivate Enc and MAC keys at two places

1. to talk to ICC (K_{ENC} and K_{MAC})
2. to generate session keys (KS_{ENC} and KS_{MAC})

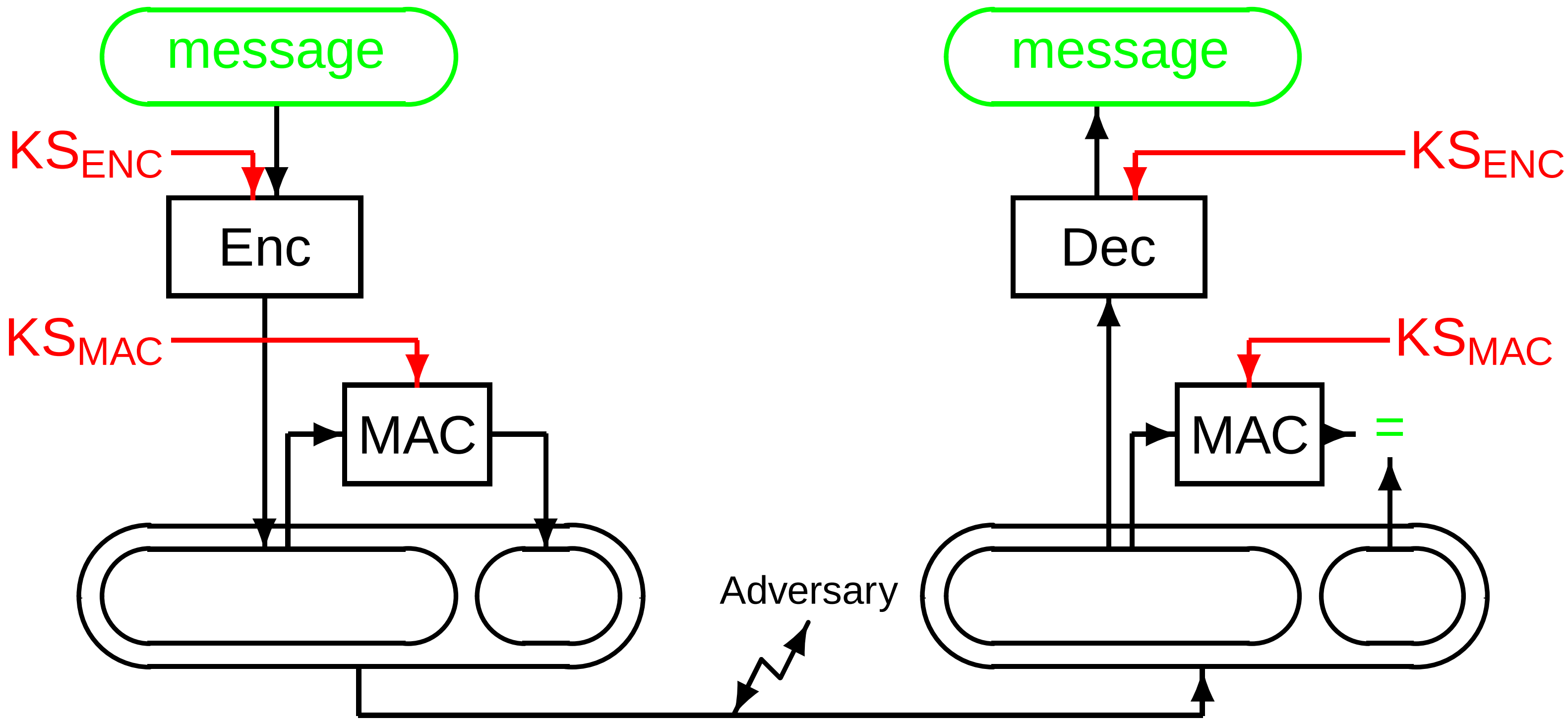
- set $D = K_{\text{seed}} || c$ where $c = 00\,00\,00\,01$ for the encryption key and $c = 00\,00\,00\,02$ for the MAC key
- compute $H = \text{SHA1}(D)$
- the first 8 bytes and the next 8 bytes of H are set to the 2-key triple-DES
- adjust the parity bits of the two DES keys

Authentication and Key Estab. (Basic Access Control)

IFD		ICC
	GET CHALLENGE $\longrightarrow$	
pick RND.IFD, K.IFD	$\longleftarrow$ RND.ICC	pick RND.ICC, K.ICC
$S \leftarrow \text{RND.IFD} \| \text{RND.ICC} \| \text{K.IFD}$		
$\text{E\_IFD} \leftarrow \text{Enc}_{K_{\text{ENC}}}(S)$		
$\text{M\_IFD} \leftarrow \text{MAC}_{K_{\text{MAC}}}(\text{E\_IFD})$	E_IFD,M_IFD $\longrightarrow$	check, decrypt
		$R \leftarrow \text{RND.ICC} \| \text{RND.IFD} \| \text{K.ICC}$
		$\text{E\_ICC} \leftarrow \text{Enc}_{K_{\text{ENC}}}(R)$
check, decrypt	$\longleftarrow$ E_ICC,M_ICC	$\text{M\_ICC} \leftarrow \text{MAC}_{K_{\text{MAC}}}(\text{E\_ICC})$
get $\text{KS}_{\text{ENC}}, \text{KS}_{\text{MAC}}$		get $\text{KS}_{\text{ENC}}, \text{KS}_{\text{MAC}}$

(derive KS_{ENC} and KS_{MAC} from $K_{\text{seed}} = \text{K.ICC} \oplus \text{K.IFD}$)

Secure Channel (Basic Access Control)



Active Authentication

- authenticate ICC knows some secret key KPr_{AA} by a challenge-response protocol

pro prevents chip substitution

con processing demanding

Active Authentication Protocol

IFD		ICC
pick RND.IFD	$\xrightarrow{\text{RND.IFD}}$	$F \leftarrow \text{nonce} \| \text{RND.IFD}$
check	$\xleftarrow{\Sigma}$	$\Sigma \leftarrow \text{Sign}_{\text{KPr}_{\text{AA}}}(F)$

Comments (Personal Opinion)

- privacy protection is rather small
  - we can check whether an MRZ is equal to a target value
    Example: continuously try the MRZ of M. Leueuberger in the street until one MRTD answers
  - MRZ entropy is less than 48 bits
    By evesdropping RND.ICC and E_IFD of existing session we can do exhaustive search on MRZ and either decrypt the session or later ask the MRTD for privacy-sensitive information
- ICC will eventually be reverse engineered and copied
- old technology:
  - DES standard is no longer supported
  - SHA1 hash function is half broken
  - home-made secure channel
  - random key establishment based on low-entropy MRZ

  we can use much better cryptographic schemes (e.g. password-based authenticated key agreement)

Authentication and Identification Protocols

- System init: generate key materials + reset a database
- Tag init: Tag is given an initial state and System is updated with a new tag $(\mathrm{ID}, \mathrm{key})$ entry in database

Authentication

Tag		System
	$\longleftarrow$	
	$\longrightarrow$	output

output: *whether tag belongs to system*

Identification

Tag		System
	$\longleftarrow$	
	$\longrightarrow$	output

output: *tag ID (if belongs to system)*

- security: completeness, soundness, privacy
- side channel: authentication output is public or not

Weis-Sarma-Rivest-Engel 2003 [WSRE 2003]: The Hash-Lock Paradigm

Tag		**System**
state: S	$(S = H(K))$	$\{\ldots,(\mathrm{ID},K),\ldots\}$
	$\xleftarrow{\text{request}}$	
	$\xrightarrow{S}$	find (ID,K) s.t. $S = H(K)$
if $S = H(K)$, unlock	$\xleftarrow{K}$	

- use one-time unlock keys and update it after unlocking

pro simple, efficient

con man-in-the-middle

con privacy threat (linkability)

The Randomized Hash-Lock Paradigm

Tag		**System**
state: K		$\{\ldots,(\text{ID},K),\ldots\}$
	$\xleftarrow{\text{request}}$	
pick b, $c = H(K,b)$	$\xrightarrow{b,c}$	find (ID,K) s.t. $c = H(K,b)$
if correct, unlock	$\xleftarrow{K}$	

- use one-time unlock keys and update it after unlocking

pro simple, efficient

con man-in-the-middle for one-time keys

con replay attack if key is not one-time

Randomized Hash-Lock Identification

Tag		System
state: K		$\{\ldots,(\text{ID},K),\ldots\}$
	request $\longleftarrow$	
pick b, $c = H(K,b)$	b,c $\longrightarrow$	find (ID,K) s.t. $c = H(K,b)$
		output: ID

pro simple, efficient

con replay attack $\longrightarrow$ tag impersonation

con tag corruption $\longrightarrow$ tag cloning, tag traceability

Feldhofer-Dominikus-Wolkerstorfer 2004 [FDW 2004]

- block ciphers are more efficient than hash functions in RFID tags
- use ISO/IEC 9798-2 unilateral authentication
- use ISO/IEC 9798-2 mutual authentication

ISO/IEC 9798-2 2-Pass Unilateral Authentication

Tag		**System**
state: K		$\{\ldots,(\mathsf{ID},K),\ldots\}$
	$\xleftarrow{\quad a \quad}$	pick a
$c = \mathsf{Enc}_K(a)$	$\xrightarrow{\quad c \quad}$	find (ID,K) s.t. $c = \mathsf{Enc}_K(a)$
		output: ID

pro simple, efficient

con replay attack $\longrightarrow$ tag traceability

con tag corruption $\longrightarrow$ tag cloning

ISO/IEC 9798-2 3-Pass Mutual Authentication

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

pro simple, efficient

pro pretty good soundness and privacy

con tag corruption $\longrightarrow$ tag cloning

Molnar-Wagner 2004 [MW 2004]

Tag		System
state: $K_{d_1}, \ldots, K_{d_1,\ldots,d_n}$		**keys:** $K_{.,\ldots,.}$ $\{\ldots, (\text{ID}, (d_1, \ldots, d_n)), \ldots\}$
pick b	$\xleftarrow{\;a\;}$	pick a
$c = \text{Enc}_{K_{d_1}}(a, b)$	$\xrightarrow{\;b,c\;}$	find d_1 s.t. $c = \text{Enc}_{K_{d_1}}(a, b)$
pick b	$\xleftarrow{\;a\;}$	pick a
$c = \text{Enc}_{K_{d_1,d_2}}(a, b)$	$\xrightarrow{\;b,c\;}$	find d_2 s.t. $c = \text{Enc}_{K_{d_1,d_2}}(a, b)$
$\vdots$	$\vdots$	$\vdots$
		output: ID

pro improved the search complexity on the system side

con privacy leakage

Attack by Avoine-Dysli-Oechslin 2005 [ADO 2005]

1: pick two tags at random associated to $d_1^1, \ldots, d_n^1$ and $d_1^2, \ldots, d_n^2$
2: listen to one protocol communication between one random tag T out of T^1 and T^2 and the system
3: get one random tag T^0, **corrupt** it, get $K_{d_1^0}, \ldots, K_{d_1^0,\ldots,d_n^0}$
4: let i be the maximum s.t. $\forall j = 1, \ldots, i-1$, $d_j^0 = d_j^1 = d_j^2$
5: if $d_i^0 \notin \{d_i^1, d_i^2\}$ then fail
6: if the ith key in the protocol transcript matches $K_{d_1^0,\ldots,d_i^0}$, declare that $T = T^b$ s.t. $d_i^0 = d_i^b$ otherwise, declare that $T = T^b$ s.t. $d_i^0 \neq d_i^b$

The lower the branch number, the higher the success probability

The higher the branch number, the higher the complexity

Ohkubo-Suzuki-Kinoshita 2003 [OSK 2003]

Tag		**System**
state: S		$\{\ldots,(\mathsf{ID},K),\ldots\}$
	request $\longleftarrow$	
$c = F(S)$	$\xrightarrow{c}$	find (ID,K) s.t. $c = F(H^i(K))$
replace S by $H(S)$		replace K by $H^i(K)$
		output: ID

pro pretty good soundness and *forward* privacy

con no complexity upper bound

con man-in-the-middle attack

Modified Ohkubo-Suzuki-Kinoshita

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

pro simple, efficient

pro pretty good soundness and *forward* privacy

con privacy leakage from side channel

Attack by Juels-Weis 2006 [JW 2006]

pick one tag T at random
simulate t times a reader that sends a random challenge a
get one tag which is T with probability $\frac{1}{2}$
execute a complete protocol between this tag and the reader
get the reader result success or failure
if the result is failure, declare that the tag is T

Previous Work

Challenge-response protocols: Hash Locks [WSRE 2003],
using ISO/IEC 9798-2 [FDW 2004],
with optimized database search [MW 2004]

Forward privacy: Ohkubo-Suzuki-Kinoshita [OSK 2003],
with optimized database search [ADO 2005],
Dimitriou [Dim 2005]

Privacy with corruption: Avoine-Dysli-Oechslin [ADO 2005], Avoine [Avo 2005],

Privacy with side-channels: Ohkubo-Suzuki 2005 [OS 2005],
Juels-Weis [JW 2006],
Burmester-van Le-Medeiros 2006 [BLM 2006]

RFID Scheme Definition

Definition

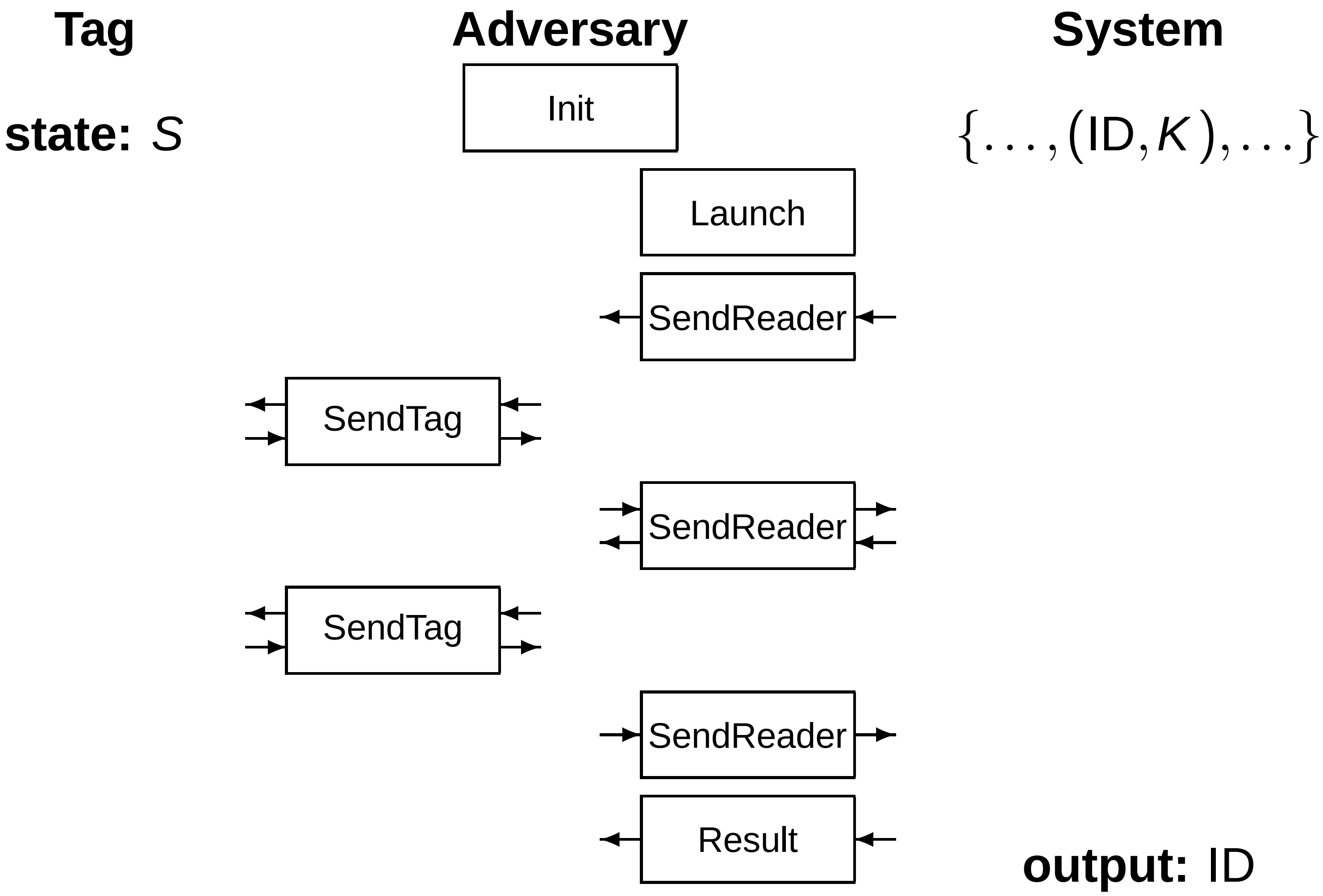
An RFID scheme consists of

Reader setup algorithm $\mathrm{Setup}(1^s) \longrightarrow (K_S, K_P)$ where K_S is safely stored in the system and K_P is publicly released;

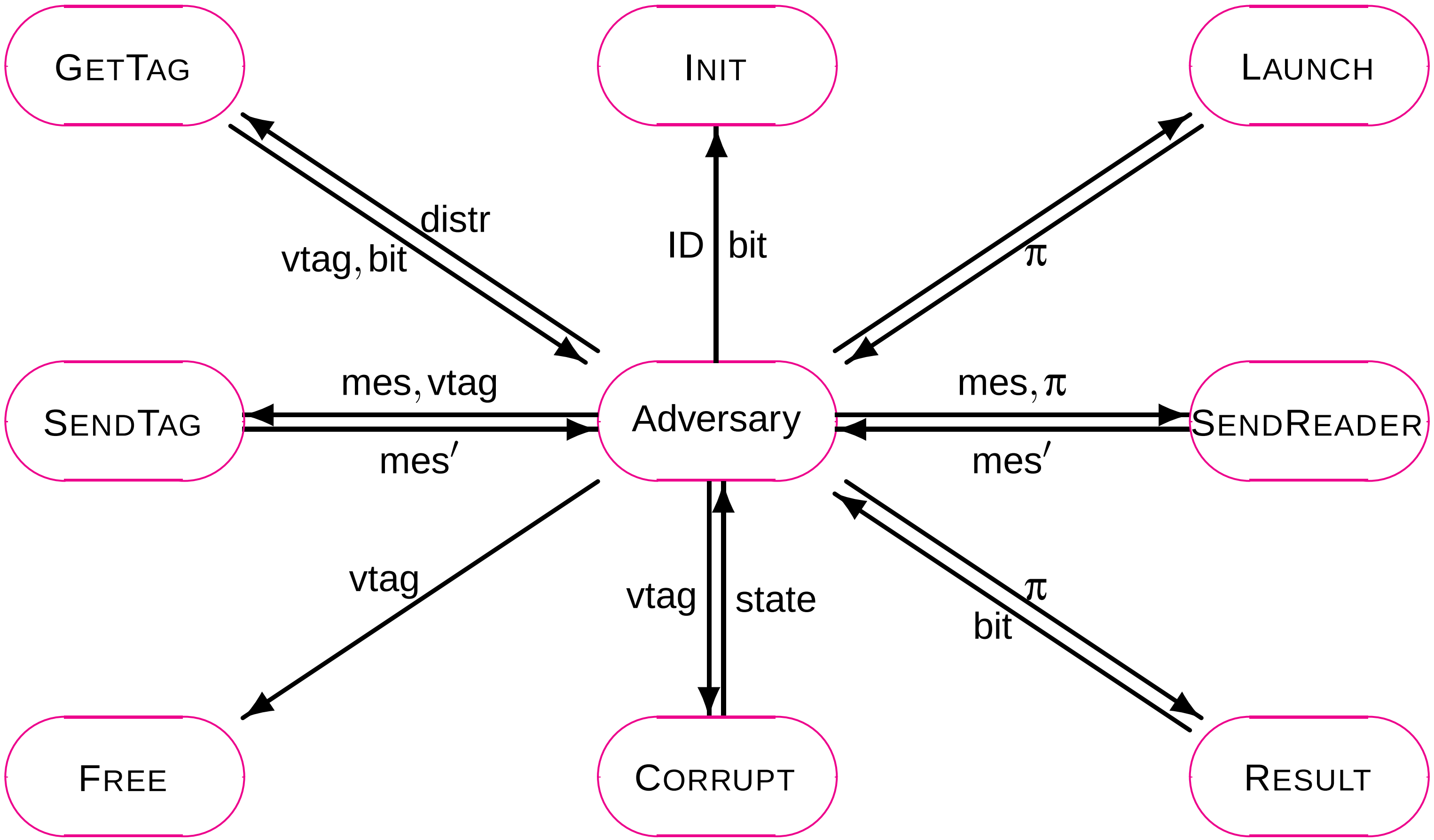
Tag setup algorithm $\mathrm{Gen}_{K_S,K_P}(\mathrm{ID}) \longrightarrow (K, S)$ where S is the initial state of the tag and (ID, K) is a new entry to be inserted in the reader database;

Identification protocol between a tag with state S and a reader with database of (ID, K) and key pair (K_S, K_P). The protocol output on the reader side should be ID is the tag was identified in the database or $\perp$ otherwise.

Adversarial Model



Oracle Accesses



Corruption Models

Weak adversary: no CORRUPT query

Forward adversary: CORRUPT queries at the end only

Destructive adversary: CORRUPT(vtag) queries followed by no queries using vtag

Strong adversary: no restriction for using CORRUPT queries

Side Channel Models

Narrow adversary: no RESULT query

(default): no restriction for using RESULT queries

Completeness

1: $\textsc{Init}(1,\ldots,r;r+1,\ldots,n)$
2: pick $i \in \{1,\ldots,n\}$ at random
3: $(\text{vtag},\cdot) \leftarrow \textsc{GetTag}(i)$
4: $\textsc{Execute}(\text{vtag})$

Definition

An RFID scheme is complete if for any polynomially bounded n and any $r \leq n$ the above adversary induces an unexpected output with negligible probability.

Soundness

for $i = 1$ to n **do**
  INIT$(i;)$
  $(\text{vtag}_i, \cdot) \leftarrow$ GETTAG(i)
end for
(training phase) do any LAUNCH, SENDREADER, SENDTAG, RESULT
$\pi \leftarrow$ LAUNCH
(attack phase) do any LAUNCH, SENDREADER, SENDTAG, RESULT

Wining condition: π outputs $\text{Out} = \text{ID} \neq \perp$ for some ID value, tag with this ID was not corrupted, and tag with this ID did not complete a protocol run during the attack phase.

Definition

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

Soundness Models

- CORRUPT queries followed by nothing are useless
  (forward and weak adversaries are equivalent for soundness)
- once a tag is corrupted, we can fully simulate it thus assume it is never used again
  (strong and destructive adversaries are equivalent for soundness)

$$\begin{array}{ccc} \text{strong sound} & \Rightarrow & \text{weak sound} \\ \Downarrow & & \Downarrow \\ \text{narrow-strong sound} & \Rightarrow & \text{narrow-weak sound} \end{array}$$

Privacy

Wining condition: the adversary output a predicate using equalities on vtag's and/or constant ID values such that replacing the vtag's by their identities satisfies the predicate.

Definition

An adversary $\mathcal{A}$ for privacy is significant if there exists no blinder B such that $\Pr[\mathcal{A}\text{ succeed}] - \Pr[\mathcal{A}^B\text{ succeed}]$ is negligible.

Blinders

Definition

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

- passively looks at communications to INIT, GETTAG, FREE, and CORRUPT queries
- impersonate the oracles LAUNCH, SENDREADER, SENDTAG, and RESULT to simulate the queries.

Privacy Models

strong p.	$\Rightarrow$	destructive p.	$\Rightarrow$	forward p.	$\Rightarrow$	weak p.
$\Downarrow$		$\Downarrow$		$\Downarrow$		$\Downarrow$
narrow-strong p.	$\Rightarrow$	narrow-destr. p.	$\Rightarrow$	narrow-forward p.	$\Rightarrow$	narrow-weak p.

The Ohkubo-Suzuki 2005 Model [OS 2005]

- single tag
- single corruption (at the end)
- adversary can travel through the tag or reader time
  (suitable when state transition is deterministic)
- last interaction (for the adversary time) is either real or simulated

$\longrightarrow$ this can reduce to a forward adversary

The Juels-Weis 2006 Model [JW 2006]

for $i = 1$ to n **do**
  $\textsc{Init}(i;)$
  $(\text{vtag}_i, \cdot) \leftarrow \textsc{GetTag}(i)$
end for
do any Launch, SendReader, SendTag, Result, Corrupt (at least two virtual tags should be left incorrupted)
select T_0, T_1, the ID of two uncorrupted tags
$\textsc{Free}(\text{vtag}_{T_0}, \text{vtag}_{T_1})$
$(\text{vtag}, \cdot) \leftarrow \textsc{GetTag}(\Pr[T_0] = \Pr[T_1] = \frac{1}{2})$
do any Launch, SendReader, SendTag, Result
(forward model only) $S \leftarrow \textsc{Corrupt}(\text{vtag})$
select $b \in \{0, 1\}$
output $\text{vtag} \equiv T_b$

$\longrightarrow$ model weaker than destructive privacy

The Burmester-van Le-Medeiros 2006 Model [BLM 2006]

- destructive model
- adversaries are not allowed to produce an output involving a corrupted vtag

$\longrightarrow$ model weaker than destructive privacy
$\longrightarrow$ some protocol private in this model may be not even narrow-forward private

Challenge-Response RFID Scheme

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

Theorem

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

- *complete*
- *strong sound*
- *weak private*

Caveat: Not Even Narrow-Forward Private

$\textsc{Init}(0,1)$
$(\text{vtag},\cdot) \leftarrow \textsc{GetTag}(\Pr[0] = \Pr[1] = \frac{1}{2})$
$(\cdot,(a,b,c)) \leftarrow \textsc{Execute}(\text{vtag})$
$\textsc{Free}(\text{vtag})$
$(\text{vtag}_0,\cdot) \leftarrow \textsc{GetTag}(0)$
$K \leftarrow \textsc{Corrupt}(\text{vtag}_0)$
if $F_K(a,b) = c$ **then**
    $x \leftarrow 0$
else
    $x \leftarrow 1$
end if
output vtag $\equiv x$

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

Modified Ohkubo-Suzuki-Kinoshita

Tag		**System**
state: S		$\{\ldots,(\mathrm{ID},K),\ldots\}$
	$\xleftarrow{\quad a \quad}$	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

- *complete*
- *strong sound*
- *narrow-destructive private*

Caveat: Not Even Weak Private

(Juels-Weis [JW 2006] attack):

$\textsc{Init}(0,1)$
$(\text{vtag}_0,\cdot) \leftarrow \textsc{GetTag}(0)$
for $i = 1$ to $t+1$ **do**
    pick a random x
    $\textsc{SendTag}(x, \text{vtag}_0)$
end for
$\textsc{Free}(\text{vtag}_0)$
$(\text{vtag},\cdot) \leftarrow \textsc{GetTag}(\Pr[0] = \Pr[1] = \frac{1}{2})$
$(\pi,\cdot) \leftarrow \textsc{Execute}(\text{vtag})$
$x \leftarrow \textsc{Result}(\pi)$
output $\text{vtag} \equiv x$

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

Public-Key-Based RFID Scheme

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

Theorem

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

- *complete*
- *strong sound*
- *narrow-strong and forward private*

Caveat: Not Destructive Private

$\textsc{Init}(0;1)$
$(\text{vtag}_0, \cdot) \leftarrow \textsc{GetTag}(0)$
$S_0 \leftarrow \textsc{Corrupt}(\text{vtag}_0)$
$(\text{vtag}_1, \cdot) \leftarrow \textsc{GetTag}(1)$
$S_1 \leftarrow \textsc{Corrupt}(\text{vtag}_1)$
flip a coin $b \in \{0,1\}$
$\pi \leftarrow \textsc{Launch}$
simulate a tag of state S_b with reader instance π
$x \leftarrow \textsc{Result}(\pi)$
if $x = b$ **then**
    output true
else
    output false
end if

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

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

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

Separation Results

Theorem

- *A complete RFID scheme that is narrow-destructive private cannot be destructive private.*
  $\longrightarrow$ *strong privacy is impossible for complete schemes*
- *A complete and narrow-strong RFID scheme can be transformed into a secure key agreement protocol*
  $\longrightarrow$ *narrow-strong privacy needs public-key cryptography techniques*
- *A complete and narrow-forward stateless RFID scheme can be transformed into a secure key agreement protocol*
  $\longrightarrow$ *narrow-forward privacy without public-key cryptography must be stateful*

Conclusion

- We have a strong framework to treat RFID schemes
- We have several levels of privacy
- The strongest possible require public-key cryptography
  (an application for TCHo [FV 2006]?)
- We identified optimal solutions

Further Readings

- **M. Jakobsson, S. Wetzel**.
  Security Weaknesses in Bluetooth.
  In *Topics in Cryptology (CT–RSA'01)*, LNCS vol. 2020,
  pp. 176–191, 2001.
- **A. Juels, D. Molnar, D. Wagner**.
  Security and Privacy Issues in E-Passports.
  In *Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm*. IEEE. 2005.
- **A. Juels, S. Weis**.
  Defining Strong Privacy for RFID.
  Cryptology ePrint Archive 2006-137.
  `http://eprint.iacr.org/2006/137`
- **G. Avoine**.
  Cryptography in Radio Frequency Identification and Fair Exchange Protocols.
  PhD Thesis no. 3407. EPFL. 2005.
  `http://library.epfl.ch/theses/?nr=3407`

Q & A

References

- Avoine 2005: PhD Thesis
  `http://library.epfl.ch/theses/?nr=3407`
- Avoine-Dysli-Oechslin 2005: SAC 2005
- Burmester-van Le-Medeiros 2006: SecureComm 2006
- Dimitriou 2005: SecureComm 2005
- Feldhofer-Dominikus-Wolkerstrofer 2004: CHES 2004
- Finiasz-Vaudenay 2006: SAC 2006
- Jakobsson-Wetzel 2001: CT-RSA 2001
- Juels-Molnar-Wagner 2005: SecureComm 2005
- Juels-Weis 2006: `http://eprint.iacr.org/2006/137`
- Molnar-Wagner 2004: ACM CCS 2004
- Ohkubo-Suzuki 2005: Communications of the ACM 2005
- Ohkubo-Suzuki-Kinoshita 2003: RFID Privacy Workshop 2003
- Vaudenay 2006: ICISC 2006
- Weis-Sarma-Rivest-Engel 2003: SPC 2003