An excursion through RFID
Security & Privacy

Some material gathered from:

- MIT (Goldwasser)
- RSA (Juels)
- Berkeley (Wagner)

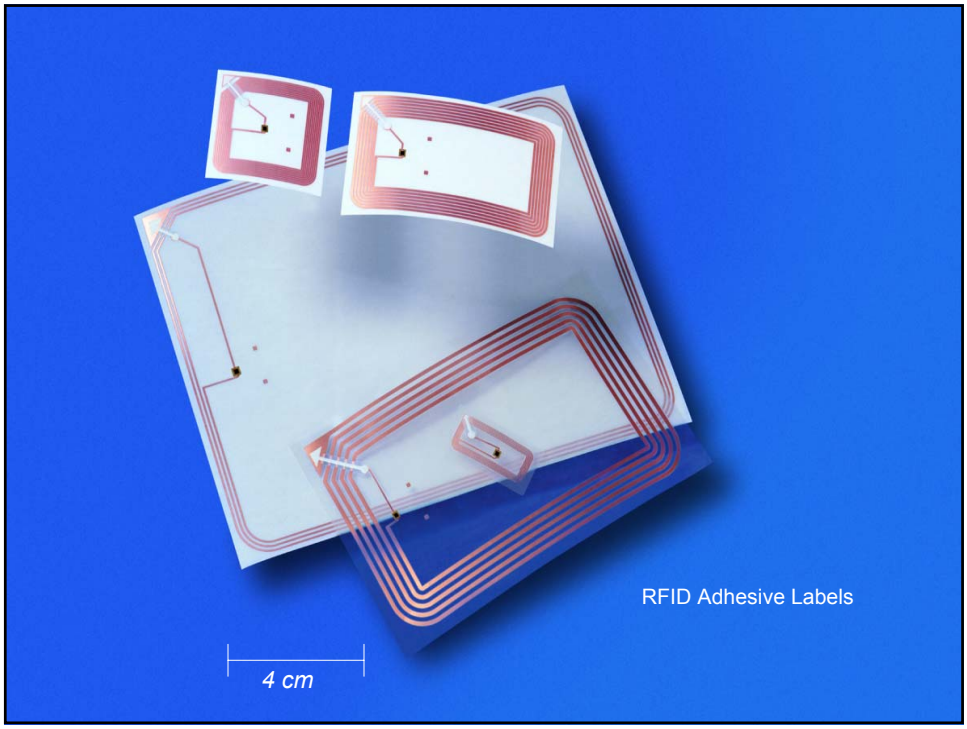
1

RFID Introduction

3 Main Components:

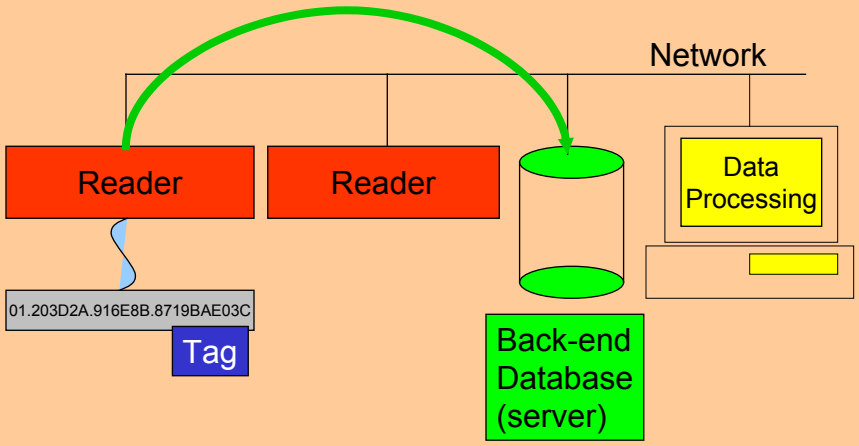
- Tags, or *transponders:*
  - affixed to objects and carry identifying data.
- Readers, or *transceivers*:
  - read or write tag data and interface with back-end databases.
- Back-end databases (servers):
  - correlate data stored on tags with physical objects.

2



An RFID “Smart Shelf” Reader

System Interface



5

RFID History

- Earliest Patent: John Logie Baird (1926)
- “Identify Friend or Foe” (IFF) systems developed by the British RAF to identify friendly aircraft.
- Both sides secretly tracked their enemy’s IFF.
- How do you identify yourself only to your friends?

6

Related Military Applications

- IFF still used today for aircraft and missiles.
  Technology is obviously classified.
- Could envision an IFF system for soldiers.
- Lots of military interest in pervasive networks of cheap, RFID-like sensors.
- Monitoring pipelines, detecting biological agents, tracking munitions, etc.

7

Commercial Applications

- Early Applications:
  - Tracking boxcars and shipping containers.
  - Cows: RFID ear tags.
  - Bulky, rugged, and expensive devices.
- The RFID Killer Appl?
  - Replace bar codes!

8

Supply-Chain Management

- First Universal Product Code (UPC) scanned: a pack of Juicy Fruit gum in 1976.
- Every day, over 5,000,000,000 barcodes are scanned around the world.
- Barcodes are slow, need line of sight, physical alignment, and take up packaging "real estate"
- Over one billion RFID tags on the market.

9

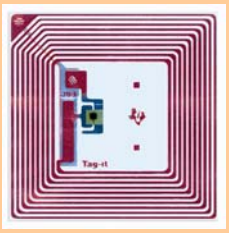
Modern RFID Applications

- Supply-Chain Management
  - Inventory Control
  - Logistics
  - Retail Check-Out
- Access Control: Facility Access Proximity Cards (contactless badges / smartcards)
- Payment Systems: Mobil SpeedPass.
- Medical Records
- Pet tracking chips

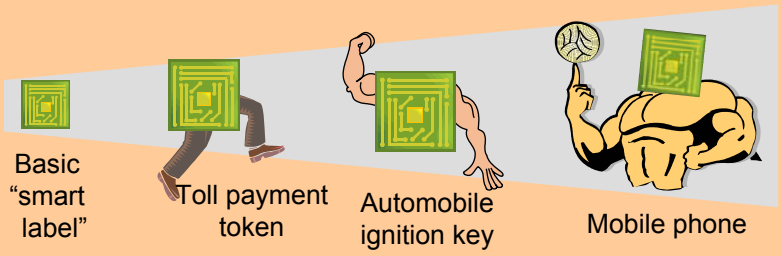
10

RFID devices take many forms

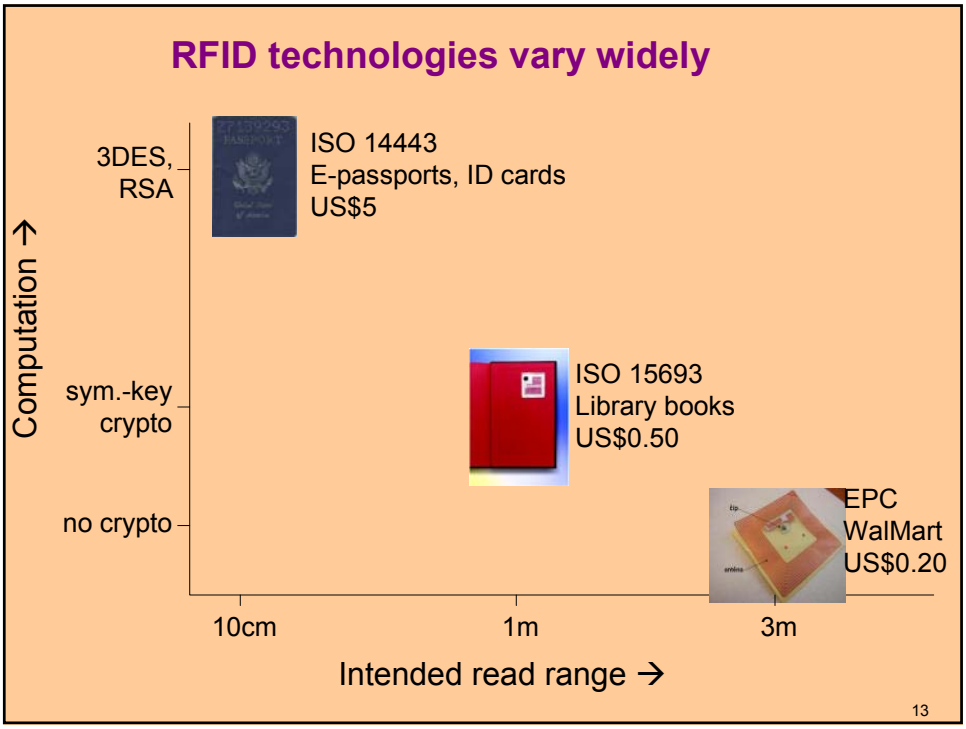




"RFID" really denotes a spectrum of devices

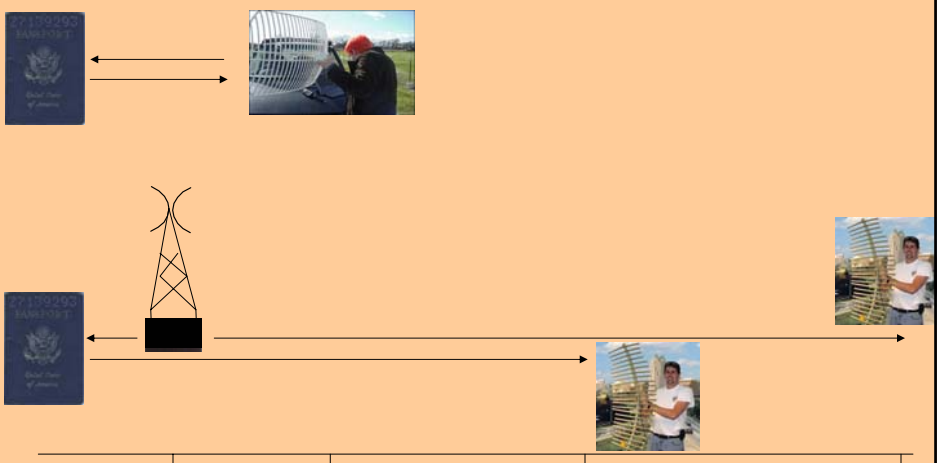


RFID technologies vary widely



13

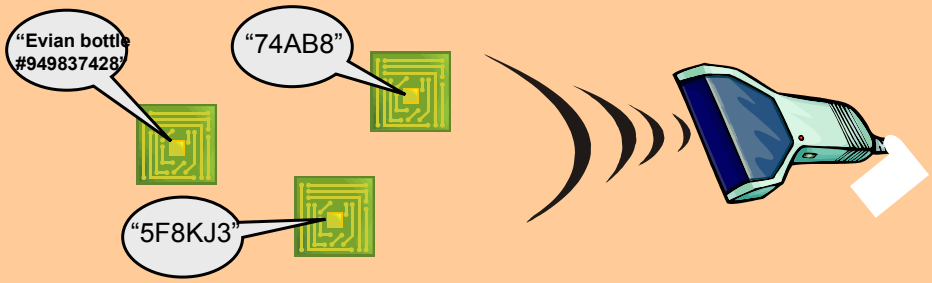
Read range?



14

“Smart label” RFID tag

- Passive device – receives power from reader
- Range of up to several meters
- Simply calls out (unique) name and static data



15

Capabilities of “smart label” RFID tag

- Very little memory
  - Static 96-bit+ identifier in current ultra-cheap tags
  - Hundreds of bits soon
- Little computational power
  - Several thousand gates (mostly for basic functionality)
  - ***No* real cryptographic functions possible**
  - Pricing pressure may keep it this way for a while

16

What the future has "in store" for us: EPC (Electronic Product Code) tags

Barcode

EPC tag

Fast, automated scanning

Line-of-sight | **Radio contact**

Specifies object type | **Uniquely specifies object**

Provides pointer to database entry for every object, i.e., unique, detailed history

Not just object type/class!

17

Other applications of RFID

- Automobile immobilizers

- Payment devices
  - Currency?

18

Other applications of RFID

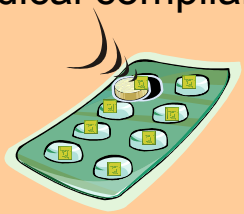
- Tracking cattle

- Passports

19

Other applications of RFID

- Medical compliance



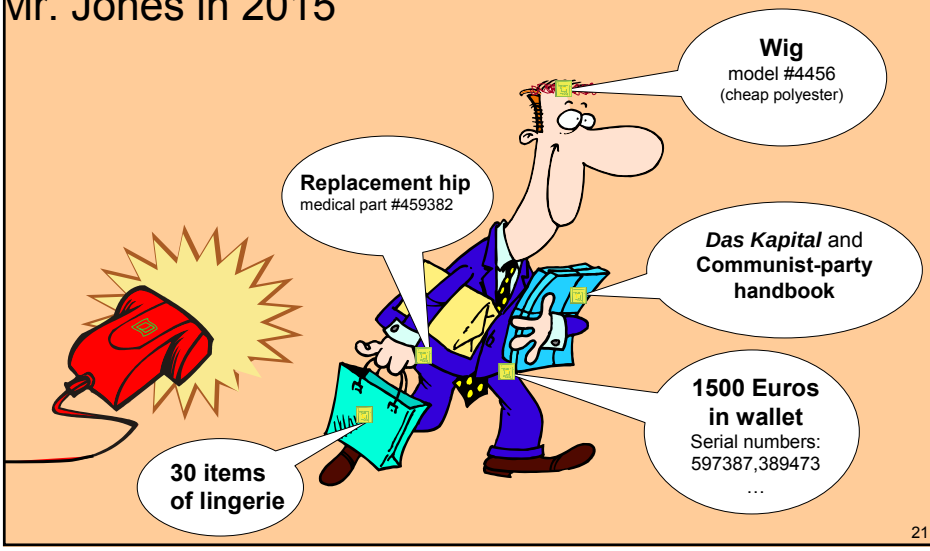
- RFID readers in mobile handsets

20

The privacy problem

Bad readers, good tags

Mr. Jones in 2015

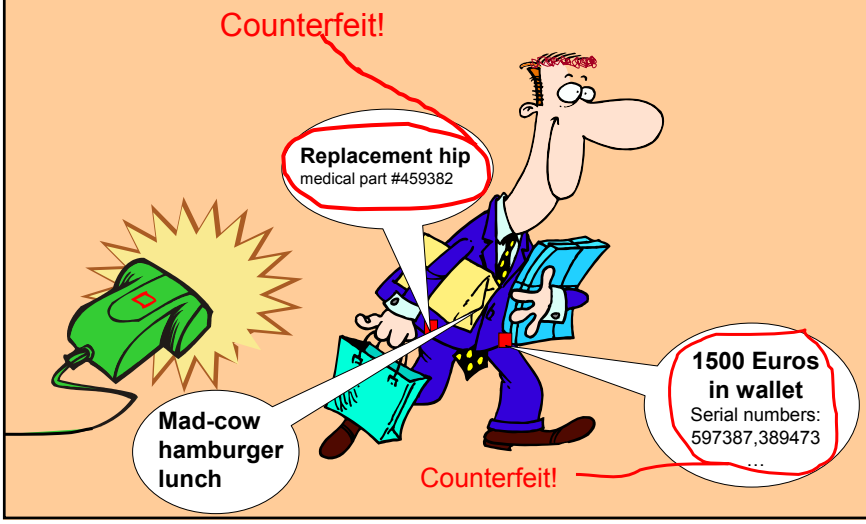


21

The authentication problem

Good readers, bad tags

Mr. Jones in 2015



22

Tag Power Source

- Passive (true RFID):
  - All power comes from a reader's interrogation signal
  - Tag is inactive unless a reader activates it
  - Passive powering is the cheapest; but short range
- Semi-Passive (more like a sensor) :
  - Tags have an on-board power source (battery).
  - Cannot initiate communications, but can be sensors.
  - Longer read range, more cost for battery.
- Active (more like a "fancy" sensor or PDA):
  - On-board power and can initiate communications.

23

Functionality Classes

Class	Nickname	Memory	Power Source	Features
0	Anti-Shoplift Tags	None	Passive	Article Surveillance
1	Electronic Product Code	Read-Only	Passive	Identification Only
2	Electronic Product Code	Read/Write	Passive	Data Logging
3	Sensor Tags	Read/Write	Semi-Passive	Environmental Sensors
4	Smart Dust	Read/Write	Active	Ad Hoc Networking

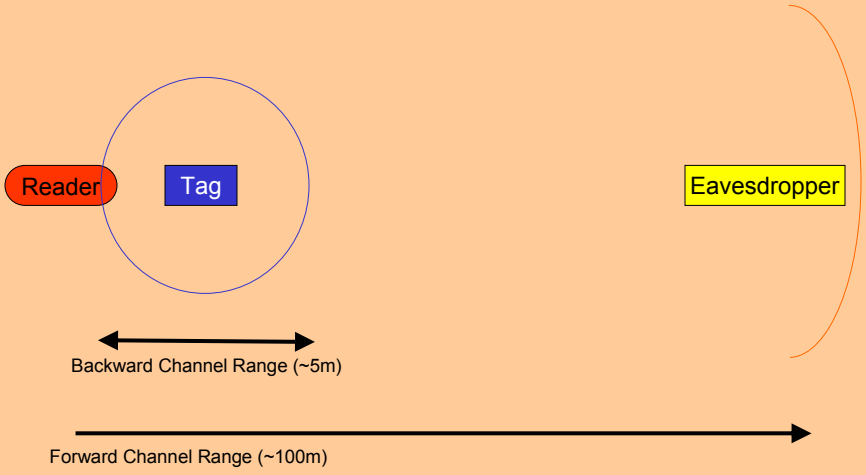
24

Operating Frequencies

Range Class	LF	HF	UHF
Frequency Range	120-140 MHz	13.56 MHz	868-956 MHz
Maximum Range?	3 meters	3 meters	10 meters
Typical Range	10-20 centimeters	10-20 centimeters	3 meters

25

Asymmetric Channels



26

Security Risks: Espionage/Privacy

- Espionage:
  - Identify Valuable Items to Steal
  - Monitor Changes in Inventory
- Personal Privacy
  - Leakage of personal information (prescriptions, brand/size of underwear, etc.).
  - Location privacy: Tracking the physical location of individuals by their RFID tags.

27

Espionage Case Study

- The US Food and Drug Administration (FDA) recently recommended tagging prescription drugs with RFID “pedigrees”.
- Problems:
  - “I’m Morphine. Steal me.”
  - “Bob’s Viagra use is really up this month.”
  - “Hi. I’m Alice’s anti-herpes cream.”

28

Security Risks: Forgery

- RFID casino chips, Mobil SpeedPass, EZ-Pass, FasTrak, prox cards, €500 banknotes, designer clothing.
- Skimming: Read your tag, make my own.
- Swapping: Replace real tags with decoys.
- Producing a basic RFID device is simple.
- A “hobbyist” hacker can probably spoof most RFID devices in a weekend for under $50.

29

Security Risks: Sabotage

- If we can’t eavesdrop or forge valid tags, can simply attack the RFID infrastructure.
- Wiping out inventory data.
- Vandalizing – “killing” tags
- Interrupting supply chains.
- Seeding fake tags – difficult to remove.

30

Adversarial Model

- Can classify adversaries by their access.
- Three levels of read or write access:
  - Physical: Direct access to physical bits.
  - Logical: Send or receive coherent messages.
  - Signal: Detect traffic or broadcast noise.
- Can further break down into Forward-only or Backward-only access.

31

Adversarial Model: Attacks

- Long-Range Passive Eavesdropper:
  - Forward-Only Logical Read Access.
  - No Write Access.
- Tag Manufacture/Cloning:
  - No Read Access/Physical Read Access.
  - Physical Write Access.
- Traffic Analysis: Signal Read Access.
- Jamming: Signal Write Access.
- Short-Range Reader Impersonator:
  - Forward/Backward Logical Read/Write Access
  - Signal Read/Write

32

Adversarial Model: Countermeasures

- Countermeasures will degrade adversary's access:
  - Encryption degrades logical read access to signal read access.
  - Authentication degrades logical write to signal write access.
  - Tamper resistance degrades physical read to logical read access.

33

Is the problem really so terrible?

- Maybe Not.
- Tags can only be read from a few meters
- Will be mostly used in closed systems like warehouses or shipping terminals.
- Can already track many consumer purchases through credit cards.
- Difficult to read some tags near liquids or metals.
- Can already track people by cell phones, wireless MAC addresses, CCTV cameras, etc.

34

But…the customer is always right.

- The public perception of a security risk, whether valid or not, could limit adoption and success.
- Similar to Pentium III's unique ID numbers.
- Successful boycott of Benetton.
- Privacy advocates have latched on and lashed out
  - *"…e-mails sent to the RFID Journal…hint at some of the concerns. 'I'll grow a beard and f--k Gillette,' wrote one reader",* Economist Magazine, June 2003.
  - *"Auto-ID: The worst thing that ever happened to consumer privacy",* CASPIAN website.

35

RFID Public Relations

- The industry never misses a chance to shoot itself in the foot.
- *"Track anything, anywhere".*
- *"Wal-Mart Caught Conducting Secret Human Trials Using Alien Technology!"*
- Lesson: If you don't want people to negatively spin your technology, don't make their jobs easier.

36

Security Challenge

- Resources, resources, resources.
- EPC tags ~ 5 cents. 1000 gates ~ 1 cent.
- Main security challenges come from resource constraints.
- Gate count, memory, storage, power, time, bandwidth, performance, die space, and physical size are all tightly constrained.
- Pervasiveness also makes security hard.

37

Example Tag Specification

Storage	128-512 bits of read-only storage.
Memory	32-128 bits of volatile read-write memory.
Gate Count	1000-10000 gates
Security Gate Budget	200-2000 gates.
Operating Frequency	UHF 868-956 MHz.
Forward Range	100 meters.
Backward Range	3 meters.
Read Performance	100 read operations per second.
Cycles per Read	10,000 clock cycles.
Tag Power Source	Passively powered via RF signal.
Power Consumption per Read	10 µWatts
Features	Anti-Collision Support Random Number Generator (from outside)

38

Resource Constraints

- With these constraints, modular-math-based public-key algorithms like RSA or ElGamal are **much** too expensive.
- Alternative public-key cryptosystems like ECC, NTRU, or XTR are too expensive.
- Symmetric encryption is also too costly. Can't fit DES, AES, or SHA-1 in 2000 gates.
- *(Recent progress made with AES.)*

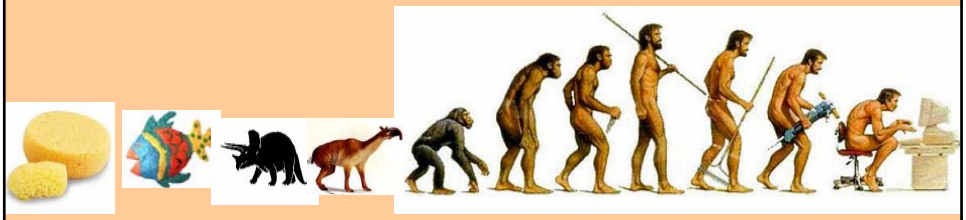
39

The RFID security challenge

How to obtain maximum security with almost no resources?

40

A brief history: (d)evolution

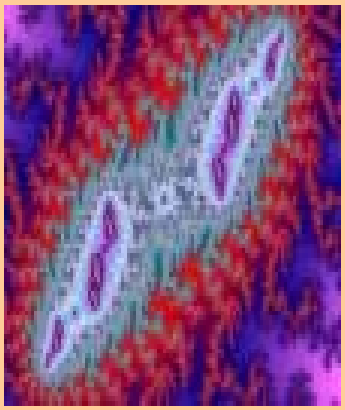


TIME

41

Dumb and Dumberer…

- Can sponges and amoebae perform crypto operations?
- Can Sponge Bob do hash chains?
- Can it do public key crypto?
- Can it remember stuff? How much can it retain?



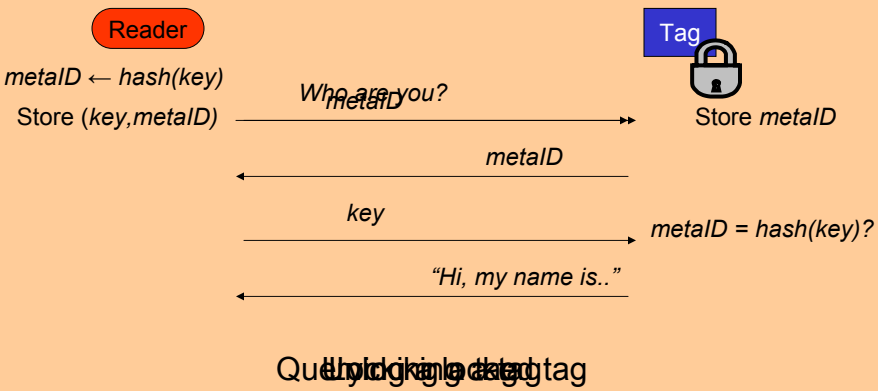
42

Hash Locks

- Rivest, Weis, Sarma, Engels (2003).
- Access control mechanism:
  - Authenticates readers to tags.
- "Only" requires OW hash function on tag.
- Lock tags with a one-way hash output.
- Unlock tags with the hash pre-image.
- Old idea, new application.

43

Hash Lock Access Control



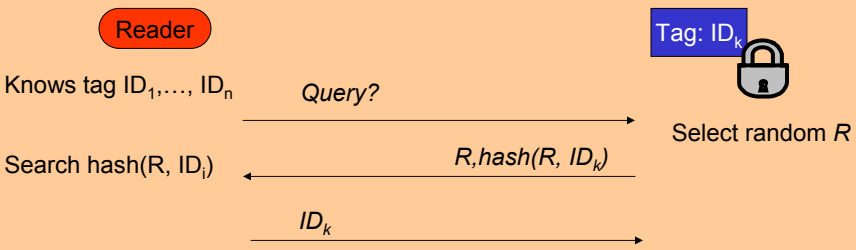
44

Hash Lock Analysis

+ Cheap to implement on tags:
  A hash function and storage for *metaID*.
+ Security based on hardness of hash.
+ Hash output has nice random properties.
+ Low key look-up overhead.
- Tags respond predictably; allows tracking.
  Motivates randomization.
- Too many messages/rounds
- Requires reader to know all keys

45

Randomized Hash Lock



Unlocking a tag

46

Randomized Hash Lock Analysis

+ Implementation requires hash and random number generator
  - Low-cost PRNG.
  - Physical randomness.
+ Randomized response prevents tracking.
- Inefficient brute force key look-up.
- Hash only guaranteed to be one-way. Might leak information about the ID.

  (Essentially end up with a block cipher?)

47

Blocker Tags

- Juels, Rivest, Szydlo (2003).
- Consumer Privacy Protecting Device:
  - Hides your tag data from strangers.
- Users carry a “blocker tag” device.
- Blocker tag injects itself into the tag’s anti-collision protocol.
- Effectively spoofs non-existent tags.
- *(Only exists on paper.)*

48

The Digital Signature Transponder (DST)

A. Juels, S. Bono, M. Green, A. Stubblefield, A. Rubin, and M. Szydlo
USENIX Security '05

"I'm tag #123"

40-bit challenge C

24-bit response $R = f_K(C)$

(simplified)

- Helps secure tens of millions of automobiles
  - Philips claims more than 90% reduction in car theft thanks to RFID! (TI did at one point.)
- Also used in millions of payment transponders

49

The Digital Signature Transponder (DST)

"I'm tag #123"

40-bit challenge C

24-bit response $R = f_K(C)$

(simplified)

- The key K is only 40 bits in length!

50

The Digital Signature Transponder (DST)

"I'm tag #123"

40-bit challenge C

24-bit response $R = f_K(C)$

(simplified)

Goal: Demonstrate security vulnerability by cloning real DST keys

51

The Digital Signature Transponder (DST)

"I'm tag #123"

40-bit challenge C

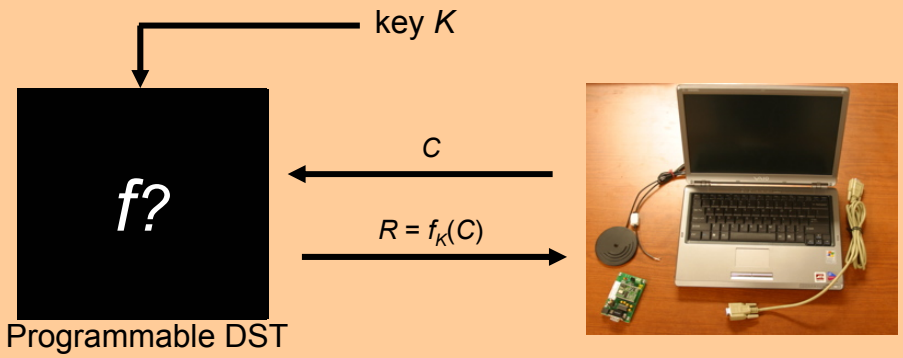
24-bit response $R = f_K(C)$

(simplified)

- The key K is only 40 bits in length!
- But what is the cryptographic function f?

52

Black-box cryptanalysis



53

The full cloning process

1. Skimming
2. Key cracking
3. Simulation

54

The full cloning process

Step 1: Skimming

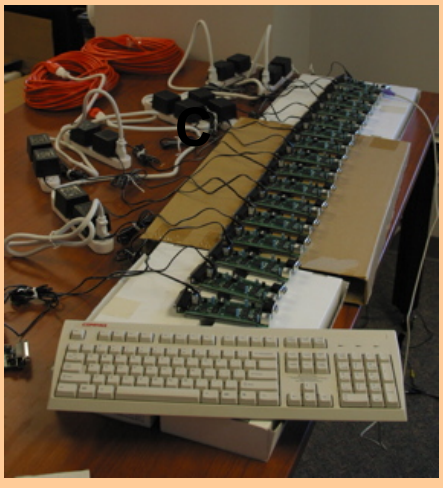
Obtain responses r_1, r_2 to two challenges, c_1, c_2

(1/4 second)

55

The full cloning process

Step 2: Key cracking



Find secret key k such that $r_1 = f_k(c_1)$ and $r_2 = f_k(c_2)$

(30 mins. on 16-way parallel cracker)

56

The full cloning process
Step 3: Simulation

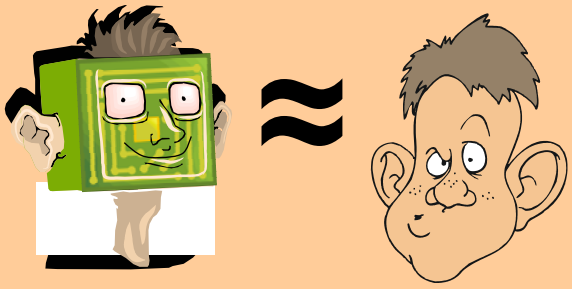
Simulate radio protocols with computation of f_k

57

Human-like authentication for extremely cheap RFID tags

A. Juels and S. Weis, Crypto '05

RFID tags are a little like people



- Very limited memory for numbers
- Very limited ability for arithmetic computation

58

Hopper-Blum (HB)
Human Identification Protocol

59

Hopper-Blum (HB)
Human Identification Protocol

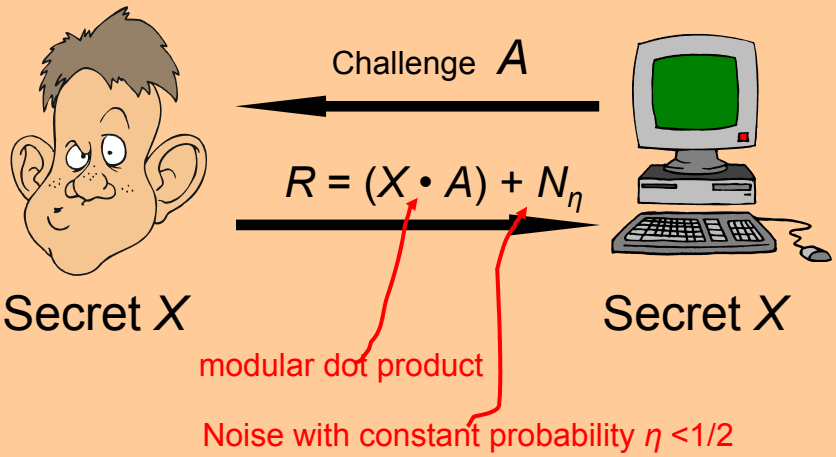
Challenge A

Response $f(X,A)$

Secret X Secret X

60

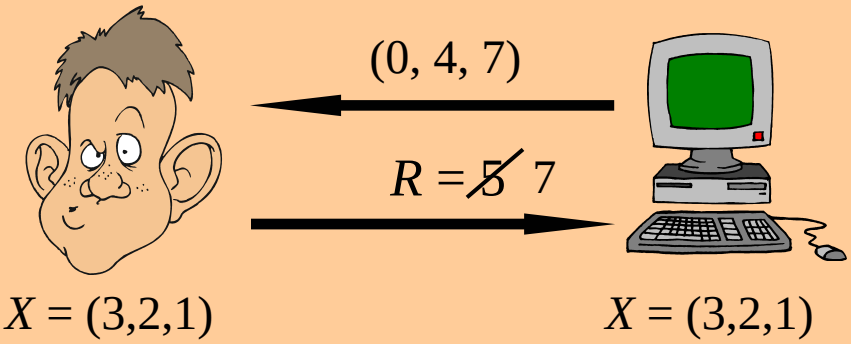
Hopper-Blum (HB)
Human Identification Protocol



61

HB Protocol

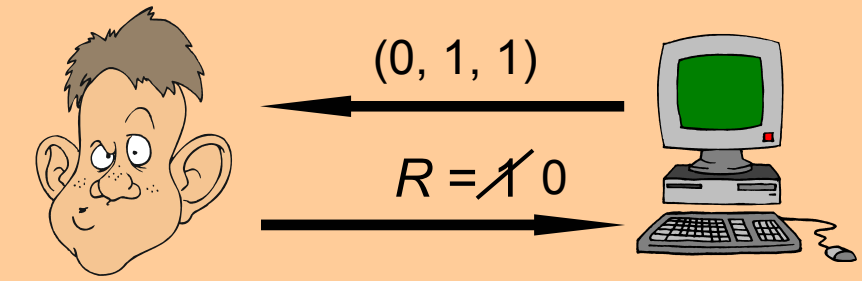
Example, mod 10



62

HB Protocol

Example round, mod 2



$X = (1,0,1)$ $X = (1,0,1)$

63

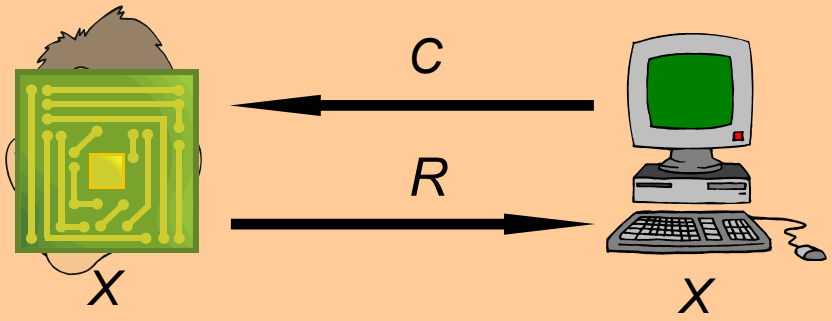
Learning Parity in the presence of Noise (LPN)

- Given multiple rounds of protocol, find X
  Given q challenge-response pairs $(A_1,R_1)\ldots(A_q,R_q)$, find X' such that $R_i = X' \bullet A_i$ on at most ηq instances, for constant $\eta > 0$
  - ***Binary values***
- Note that noise is critical – else, Gaussian elimination can be used to compute X

- LPN is NP-hard – even within approx. of 2
- Theoretical and empirical evidence of average-case hardness
- Poly. adversarial advantage in HB protocol → LPN

64

HB Protocol

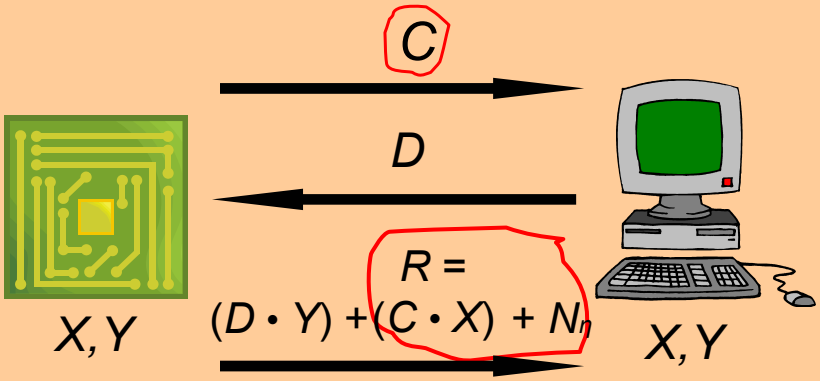


Problem: Not secure against active adversaries!

Malicious reader can supply non-random C-s

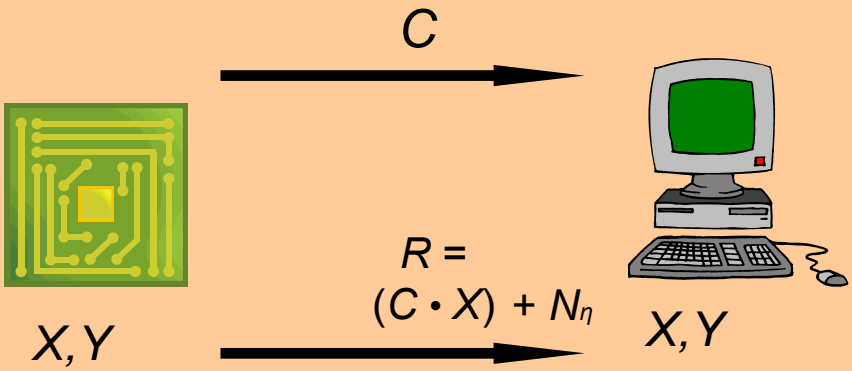
65

HB⁺ Protocol



66

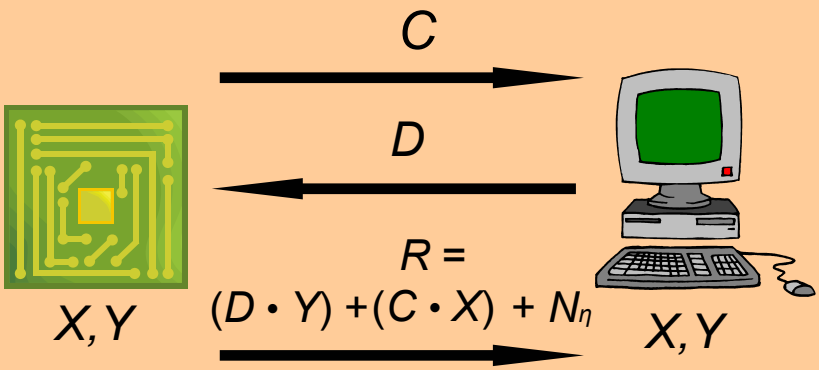
HB+ Protocol



Intuition: Looks just like HB protocol, except tag outputs C

67

HB+ Protocol



Intuition:

- Looks just like HB protocol, except tag outputs C
- Tag initiates "passive" HB protocol to conceal value $(D \cdot Y)$ of "active" challenge-response protocol

68

See paper for details:

- Paper elaborates on security reduction from HB^+ to LPN
- Implementation of algorithm seems very practical – just linear number of ANDs and XORs and a little noise!
  - Looks like EPC might be amenable, but…

BUT:

- Not clear how C is generated? PRNG?
- Requires q protocol rounds
- Each round: 3 (or is it 4?) messages

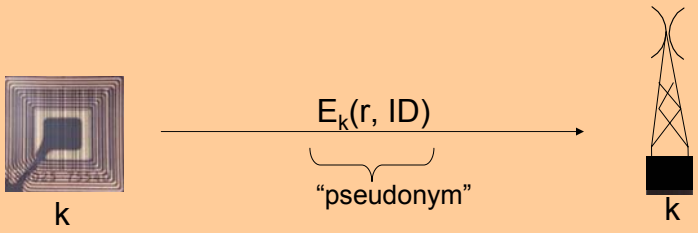
69

Two recent papers by Molnar, Sappera and Wagner

- Privacy For RFID Through Trusted Computing, WPES 2005.
- A Scalable, Delegatable Pseudonym Protocol Enabling Ownership Transfer of RFID Tags, SAC 2005.

70

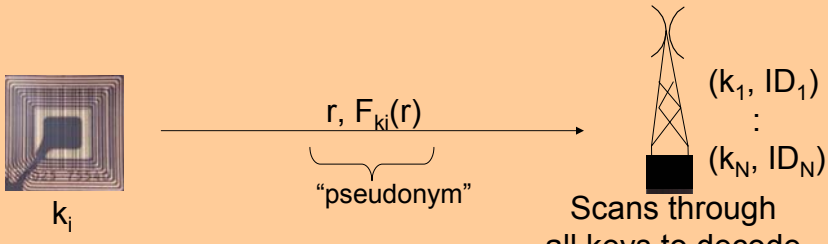
A first attempt at defeating eavesdropping and unauthorized tag-reading



Problem:
- All tags and readers share the same key k
- If any tag is compromised, all security is lost
- If any reader is compromised, all security is lost

71

Another extreme: uniquely-keyed tags



Problem:
- Doesn't scale
- Takes O(N) work to decode each pseudonym

72

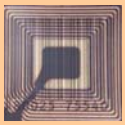
Private identification protocols

Goal: a tag <-> reader protocol, providing:
- Identification: Authorized reader learns tag's identity
- Privacy: Unauthorized readers learn nothing
  - Attacker cannot even link two sightings of same tag
- Authentication: Tag identity cannot be spoofed
- Scalability: Can be used with many tags

A real technical challenge

73

Hierarchical private tag identification



k_i, k_{ij}

$r, F_{k_i}(r), F_{k_{ij}}(r)$

pseudonym

:
(k_i, i)
:
(i, k_{ij}, ID_{ij})
:

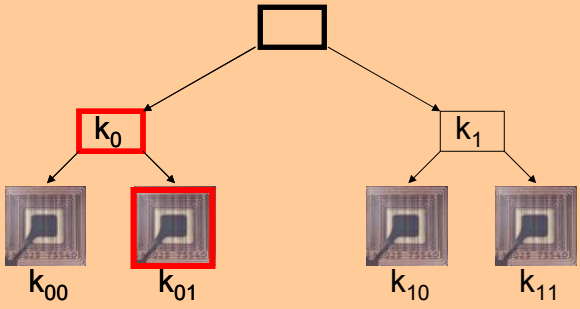
Decodes i, then j

More scalable: $O(\sqrt{N})$ work to decode each pseudonym
- First, scan all k_i to learn i
- Then, scan all k_{ij} to learn j and thus tag identity

BUT:
- Learning k_i allows tracking the entire "family" of tags

74

Another way: tree of secrets (LKH?)



Tag ≡ leaf of the tree.
Each tag receives the keys on path from leaf to the root.
Tag ij generates pseudonyms as $(r, F_{k_i}(r), F_{k_{ij}}(r))$.
Reader can decode pseudonym using a depth-first search.

75

Analysis: tree of secrets

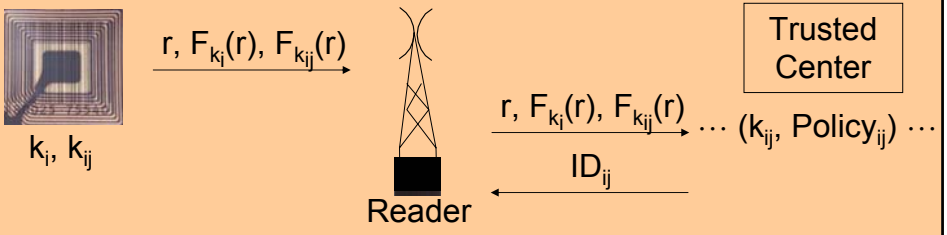
Generalizations:
- Use any depth tree (e.g., lg N)
- Use any branching factor (e.g., 2^{10})
- Use any other identification scheme (e.g., mutual auth)

	Theory	A concrete example
Number of tags:	N	2^{20} tags
Tag storage:	O(lg N)	128 bits
Tag work:	O(lg N)	2 PRF invocations
Communications:	O(lg N)	138 bits
Reader work:	O(lg N)	2×2^{10} PRF invocations

Privacy degrades "gracefully" if tags are compromised

76

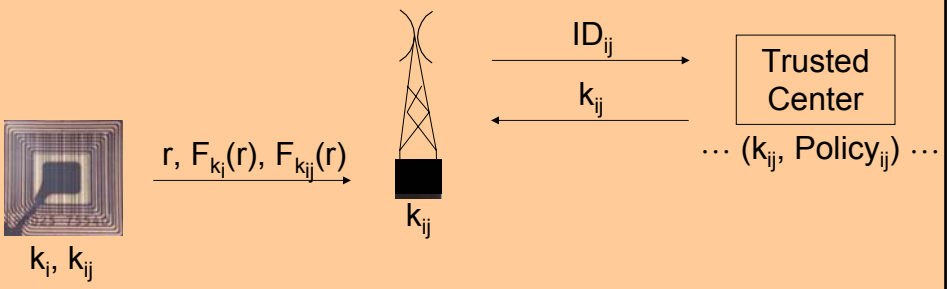
Reducing trust in readers



If readers are online, Trusted Center can do decoding for them, and enforce a privacy policy for each tag.
No keys stored at reader => less chance of privacy spills.

77

Reducing trust: Delegation

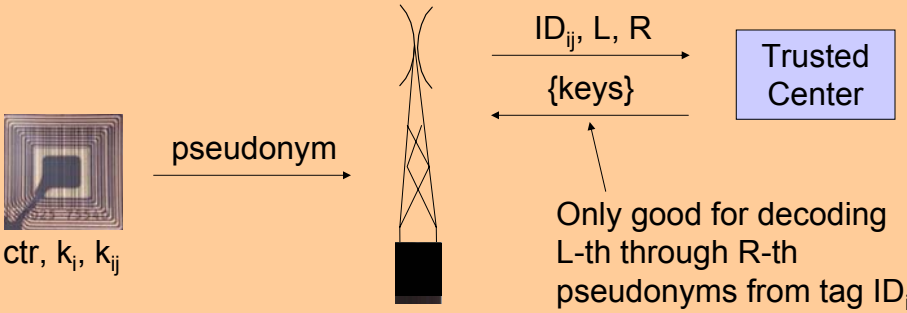


For offline or partially disconnected readers, can delegate power to decode pseudonyms for a single tag to designated readers.

Reader workload: O(D) per pseudonym,
where D = # of tags delegated to this reader.

78

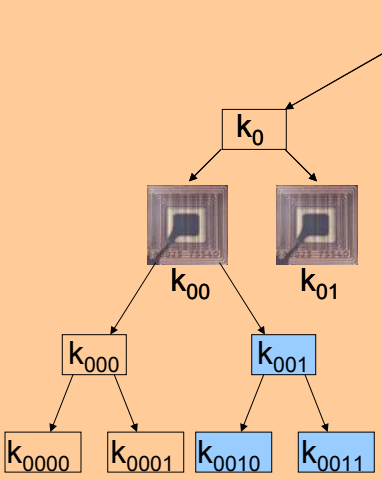
Time-limited delegation



Even less trust: Reader gets access to the next 100 pseudonyms from this tag and nothing more.

79

Enabling time-limited delegation



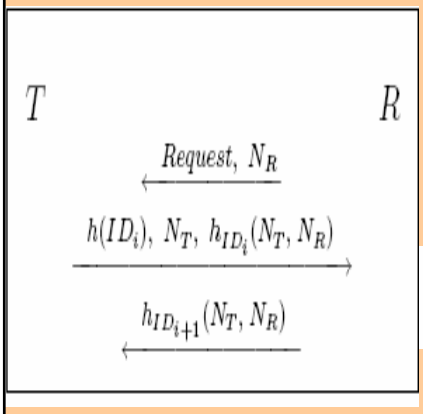
Use GGM technique at lower levels:
$(k_{s0}, k_{s1}) = G(k_s)$
Tag uses leaves sequentially

Reader gets keys for a subset

80

A Lightweight RFID Protocol to protect against Traceability and Cloning attacks

T. Dimitriou, Securecomm 2005



Trusted Center

$h(ID_i),\ N_T,\ h_{ID_i}(N_T, N_R)$

$h_{ID_{i+1}}(N_T, N_R)$

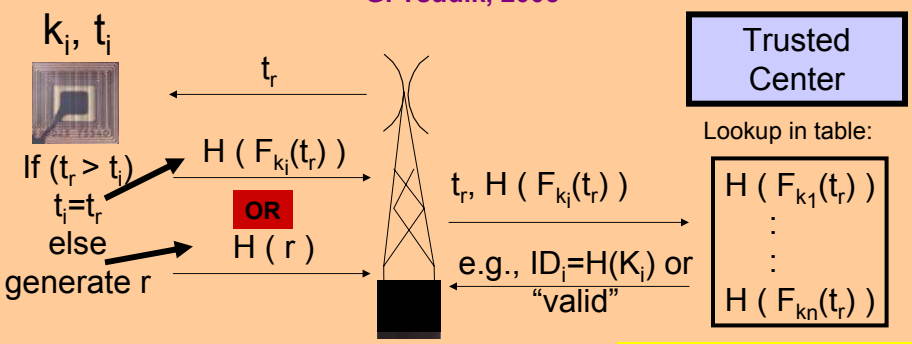
Lookup in table, verify and update ID_i to ID_{i+1}

- simple, forward-secure
- 3 messages: undesirable → tag must keep transient state
- need PRNG
- robustness is a problem: 3rd message might not arrive…or arrive a year later!
- what if malicious reader wants to track tags?
- cannot batch communication with center

81

Using Monotonically Increasing Timestamps

G. Tsudik, 2005



- Table recomputed periodically, not on-demand!
- Only "timely" requests accepted

- Only 2 messages
- Adversary can't differentiate between two replies
- Resistant to "narrowing" attacks
- Need PRNG on tag, but no clock
- DoS by rogue reader → kills tag dead ☺
- Tag eventually expires/dies
- Can be combined with hierarchical/tree-based approach
- Can be combined with forward-secure techniques

82

To learn more:

- Limited Bibliography:
  - crypto.csail.mit.edu/~sweis/rfid
- Primers and current RFID news:
  - www.rfidjournal.com
- RSA Labs RFID Web site:
  - www.rsasecurity.com/go/rfid
  - www.rfid-security.com
- JHU/RSA RFID Web site:
  - www.rfidanalysis.org
- David Wagner's Web site:
  - www.cs.berkeley.edu/~daw/papers

83