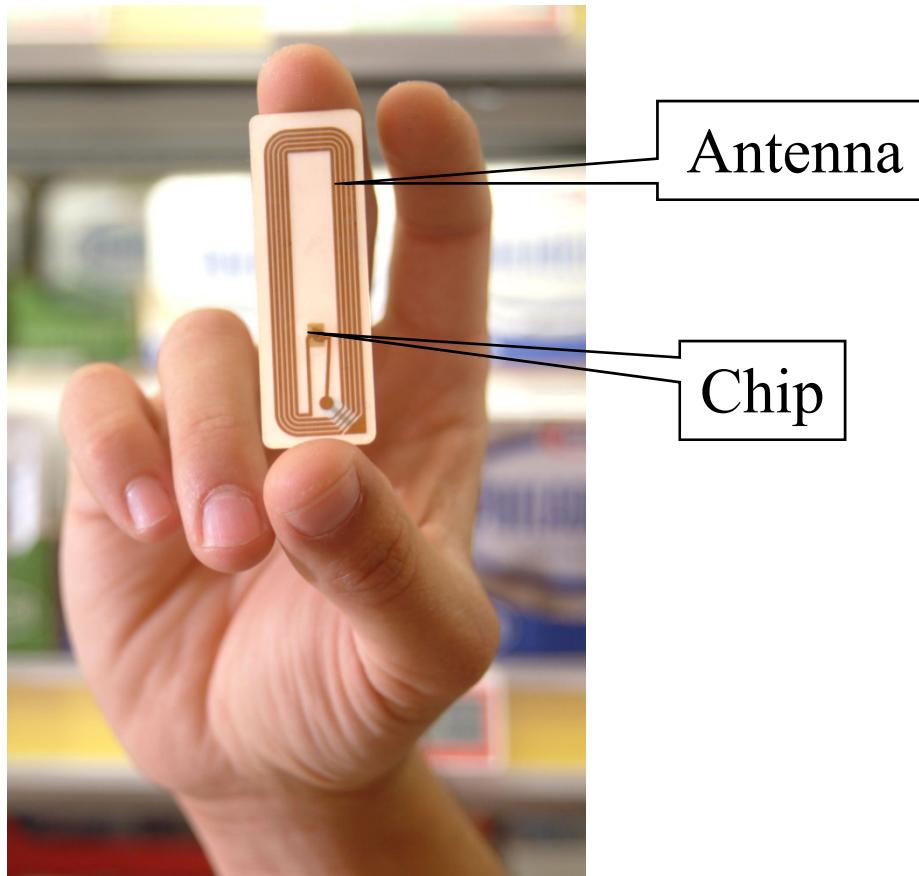


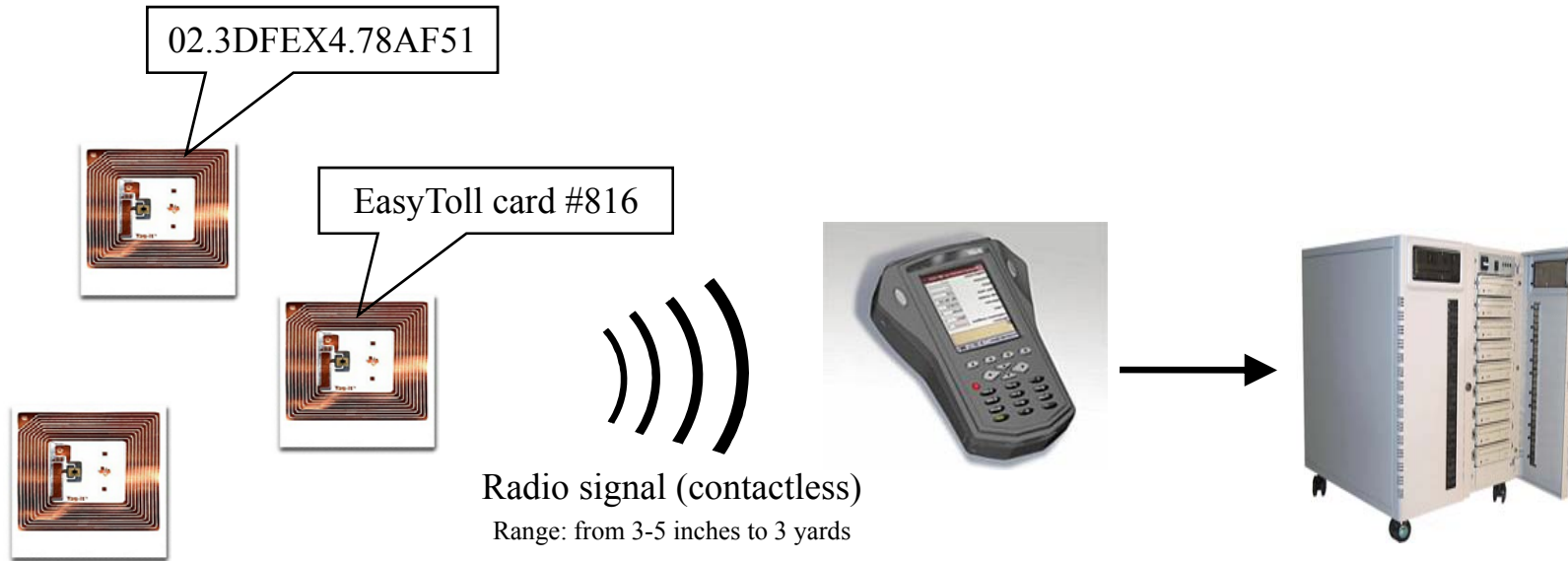
RFID Security and Privacy

What is RFID?

- Radio-Frequency Identification Tag



How Does RFID Work?



Tags (transponders)

Attached to objects,
“call out” identifying data
on a special radio frequency

Reader (transceiver)

Reads data off the tags
without direct contact

Database

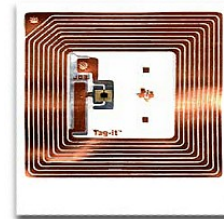
Matches tag IDs to
physical objects

“The Barcode of the Future”

Barcode



RFID



Fast, automated scanning
(object doesn't have to leave
pocket, shelf or container)

Line-of-sight reading

- Reader must be looking at the barcode

Reading by radio contact

- Reader can be anywhere within range

Specifies object type

- E.g., “I am a pack of Juicy Fruit”

Specifies unique object id

- E.g., “I am a pack of Juicy Fruit #86715-A”

Can look up this object
in the database

Where Are RFID Used?

- Physical-access cards
- Inventory control
 - Gillette Mach3 razor blades, ear tags on cows, kid bracelets in waterparks, pet tracking
- Logistics and supply-chain management
 - Track a product from manufacturing through shipping to the retail shelf
- Gas station and highway toll payment
 - Mobil SpeedPass
- European Central Bank rumored to plan implanting RFID tags in banknotes
 - Anti-counterfeiting
 - Tracking of illicit monetary flows



Commercial Applications of RFID

- RFID cost is dropping dramatically, making it possible to tag even low-value objects
 - Around 5c per tag, \$100 for a reader
- Logistics and supply-chain management is the killer application for RFID
 - Shipping, inventory tracking, shelf stocking, anti-counterfeiting, anti-shoplifting
- Massive deployment of RFID is in the works
 - Wal-Mart pushing suppliers to use RFID at pallet level, Gillette has ordered 500,000,000 RFID tags

Futuristic Applications

- Prada store in New York City already uses RFID to display matching accessories on in-store screens
- Refrigerator shelves that tell when milk expires
- Airline tickets with RFIDs on them that help direct travelers through the airport
- Microwave ovens that read cooking directions from RFID tags on food packages
- RFID tags on postage stamps
- Businesses may attach RFID tags to invoices, coupons, and return envelopes

Privacy Issues (slide: Ari Juels)

RFID tags will be *everywhere*...



Risks

- Personal privacy
 - FDA recommended tagging drugs with RFID “pedigrees”; ECB planned to add RFID tags to euro banknotes...
 - I’ll furtively scan your briefcase and learn how much cash you are carrying and which prescription medications you are taking

- Skimming: read your tag and make my own
 - In February 2005, JHU-RSA Labs team skimmed and cloned Texas Instruments’ RFID device used in car anti-theft protection and SpeedPass gas station tokens

- Corporate espionage
 - Track your competitor’s inventory

Consumer Backlash



Is Big Brother in **your** grocery cart?

RFID Tag Power Sources

- Passive (this is what mostly used now)
 - Tags are inactive until the reader's interrogation signal “wakes” them up
 - Cheap, but short range only

- Semi-passive
 - On-board battery, but cannot initiate communication
 - Can serve as sensors, collect information from environment: for example, “smart dust” for military applications
 - More expensive, longer range

- Active
 - On-board battery, can initiate communication

RFID Capabilities

- No or very limited power
- Little memory
 - Static 64- or 128-bit identifier in current 5-cent tags
- Little computational power
 - A few thousand gates at most
 - Static keys for read/write access control
- Not enough resources to support public- or symmetric-key cryptography
 - Cannot support modular arithmetic (RSA, DSS), elliptic curves, DES, AES; hash functions are barely feasible
 - Recent progress on putting AES on RFID tags

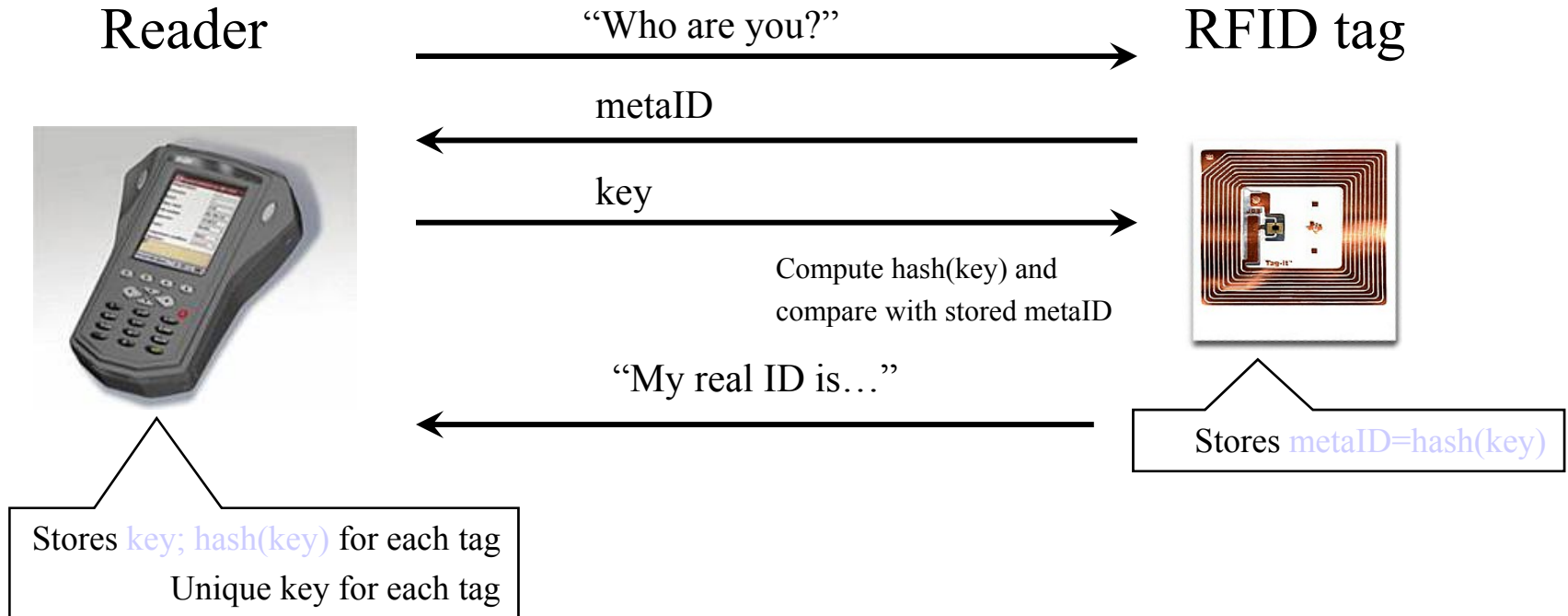
Blocking Unwanted Scanning

- Kill tag after purchase
 - Special command permanently de-activates tag after the product is purchased
 - Disables many futuristic applications
- Faraday cage
 - Container made of foil or metal mesh, impenetrable by radio signals of certain frequencies
 - Shoplifters are already known to use foil-lined bags
 - Maybe works for a wallet, but huge hassle in general
- Active jamming
 - Disables all RFID, including legitimate applications

Hash Locks

[Rivest, Weis, Sharma, Engels]

Goal: authenticate reader to the RFID tag



Why is this not a perfect solution?

Analysis of Hash Locks

- Relatively cheap to implement
 - Tag has to store hash implementation and metaID
- Security based on weak collision-resistance of hash function
- metaID looks random
- Problem: tag always responds with the same value
 - Attacker can track the same tag from place to place even if he cannot learn its real ID
- Another problem: an attacker can receive the key sent from the reader even in long distance.

Randomized Hash Locks [Weis et al.]

Goal: authenticate reader to the RFID tag

Reader



Stores all IDs:
 ID_1, \dots, ID_n

“Who are you?”

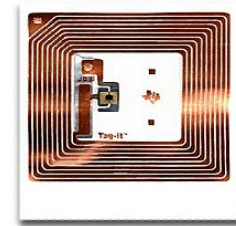
Generate random R

$R, \text{hash}(R, ID_k)$

Compute $\text{hash}(R, ID_i)$ for every
known ID_i and compare

“You must be ID_k ”

RFID tag



Stores its own ID_k

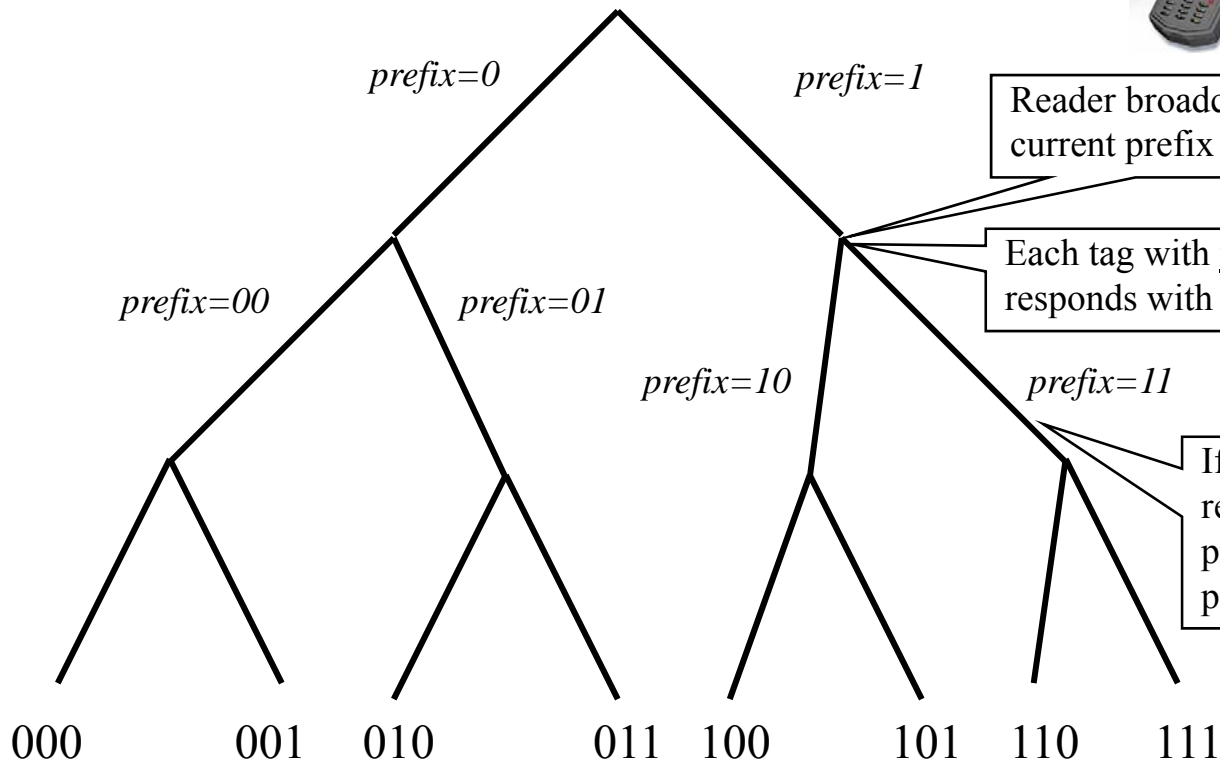
Analysis of Randomized Hash Locks

- Tag must store hash implementation and pseudo-random number generator
 - Low-cost PRNGs exist; can use physical randomness
- Secure against tracking because tag response is different each time
- Reader must perform brute-force ID search
 - Effectively, reader must stage a mini-dictionary attack to unlock the tag
- Alternative: use a block cipher
 - Need a very efficient implementation of AES

How Does the Reader Read a Tag?

- When the reader sends a signal, more than one RFID tag may respond: this is a **collision**
 - Reader cannot accurately read information from more than one tag at a time
 - Example: every tagged item in a supermarket cart responds to the cashier's RFID reader
- Reader must engage in a special **singulation** protocol to talk to each tag separately
- **Tree-walking** is a common singulation method
 - Used by 915 Mhz tags, expected to be the most common type in the U.S.

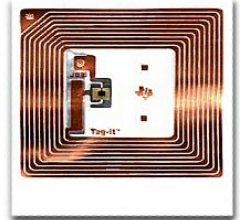
Tree Walking



Reader broadcasts current prefix

Each tag with **this** prefix responds with its next bit

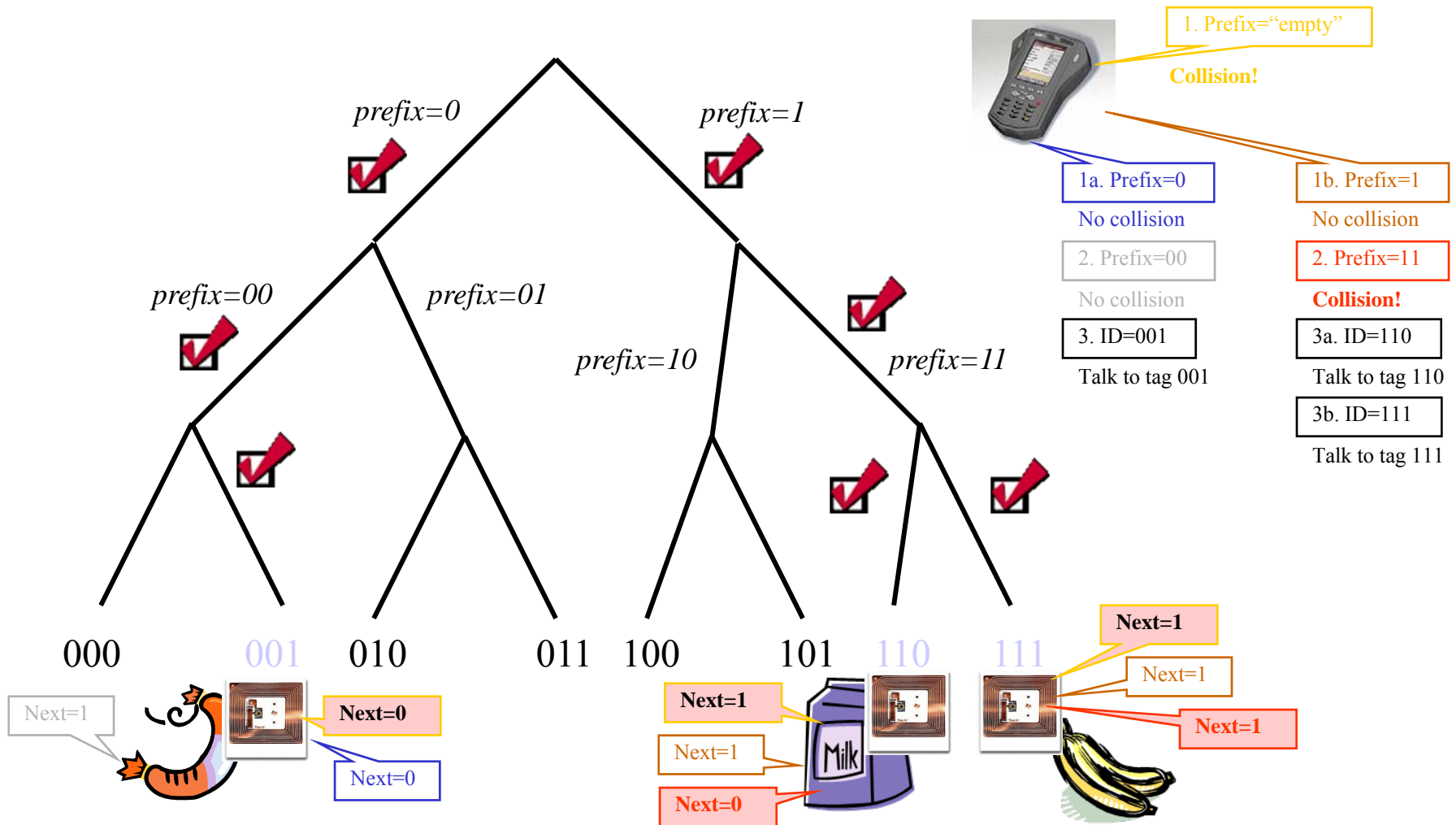
If responses don't collide, reader adds 1 bit to current prefix, otherwise tries both possibilities



Every tag has a k-bit identifier

This takes $O(k \cdot \text{number of tags})$

Example: Supermarket Cart

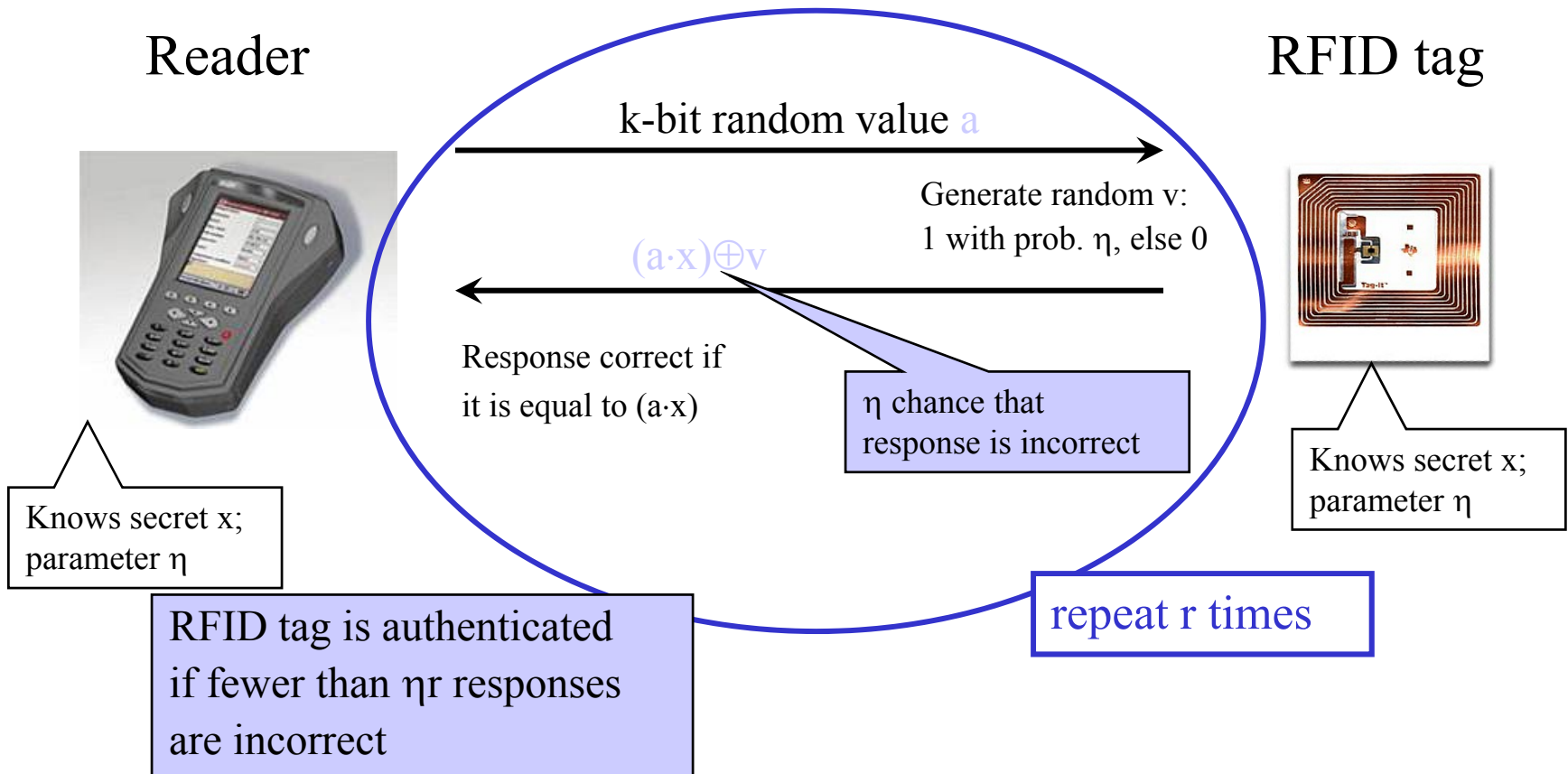


Blocker Tag [Rivest, Juels, Szydlo]

- A form of jamming: broadcast both “0” and “1” in response to any request from an RFID reader
 - Guarantees collision no matter what tags are present
 - To talk to a tag, reader must traverse every tree path
 - With 128-bit IDs, reader must try 2^{128} values – infeasible!
- To prevent illegitimate blocking, make blocker tag selective (block only certain ID ranges)
 - E.g., blocker tag blocks all IDs with first bit=1
 - Items on supermarket shelves have first bit=0
 - Can’t block tags on unpurchased items (anti-shoplifting)
 - After purchase, flip first bit on the tag from 0 to 1

HB Protocol [Juels and Weis, based on Hopper and Blum]

Goal: authenticate RFID tag to the reader



Active Adversary



non-random value a



Generate random v :
1 with prob. η , else 0

$$(a \cdot x) \oplus v$$



non-random value a



Generate random v :
1 with prob. η , else 0

$$(a \cdot x) \oplus v$$

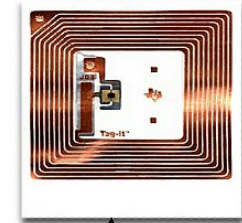


non-random value a



...

RFID tag



Knows secret x ;
parameter η

What does
attacker learn?

HB+ Protocol

[Juels and Weis]

Goal: authenticate RFID tag to the reader

