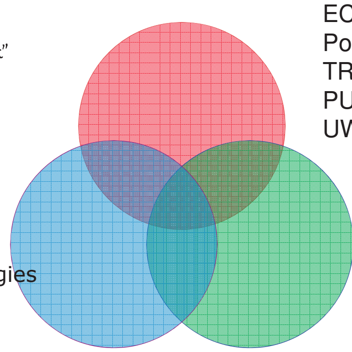
## Hardware security = lightweight, embedded, EE

"Securing the Perimeter of the Internet"

Crypto Implementations:
- Block and Stream Ciphers
- ECC
- Post-Quantum Crypto
- TRNG
- PUF
- UWB



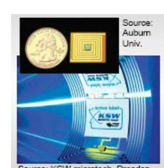
Applications:
- Transportation
- Commerce
- Assistive Technologies
- Supply Chain
- Pharmaceutical
- Medical Devices

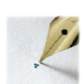
Threat Models:
- Side-channels:
  - Power
  - Electromagnetics
  - Fault Injection
- Eavesdropping
- Jamming/DoS
- Power Depletion
- Thermal Virus
- Trojans

"Interaction of Physical and Virtual Worlds"

## What is RFID?

- Passively powered integrated circuits
  - LF (125 – 148.5 kHz)
    - Automobile immobilizers, Exxon Mobile SpeedPass™
  - HF (13.56 MHz)
    - Credit Cards, MIFARE, E-Passports
  - UHF (902-928 MHz)
    - Inventory tracking
- Cheap
- Abundant



Secure Systems Part 4 4

# RFID tags will soon be *everywhere*…

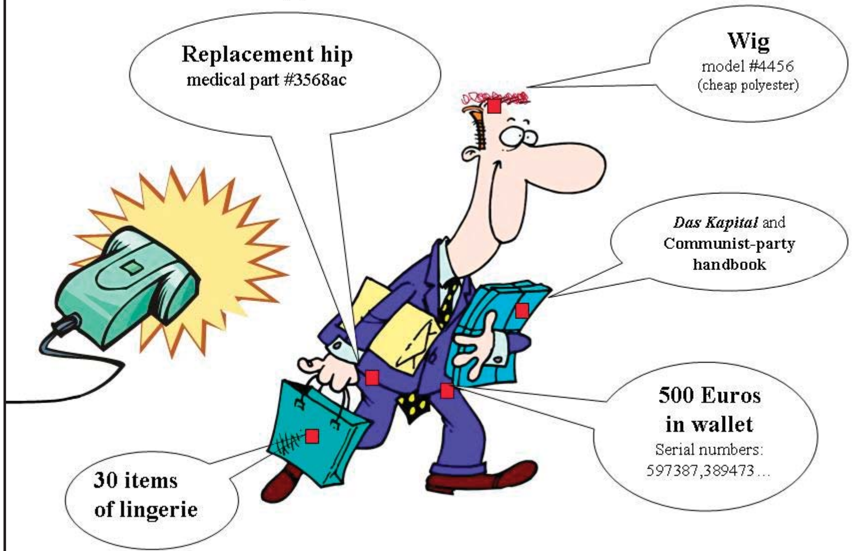



Image courtesy Ari Juels



# RFID Circuits

- Older technologies (0.25µm/0.18µm)
- Low power (1-10µW)
  - Subthreshold logic
  - Energy efficiency over performance
- Low area (0.5mm$^2$)
  - Digital logic
    - 4,000 – 8,000 gates in EPC tags
    - 200 – 2,000 gates for security
  - Other
    - Power rectification
    - Storage capacitors
    - Signal modulation
    - ID

## RFID Security and Privacy (Juels 2006)

- RFID is ubiquitous in space and time
- RFID is very limited in terms of power (uW) and processing (<5K gates)

- RFID Privacy involves bad (snooping) readers and good tags
- RFID Counterfeiting involves good readers and bad (cloned) tags
- Lightweight cryptography can help solve both problems
- But we must assume a limited attacker model



## Why are RFIDs trackable?

- Simple static identifiers are the most naïve
- How about encrypting ID?
  - Creates new static identifier, i.e., “meta-ID”
- How about a law-enforcement access key?
  - Tag-specific keys require initial release of identity
  - Universal keys subject to interception / reverse-engineering
- Tags readable only at short range, e.g., 1 cm?
  - Protects privacy, but is RFID cost effective?
- Anti-counterfeiting?

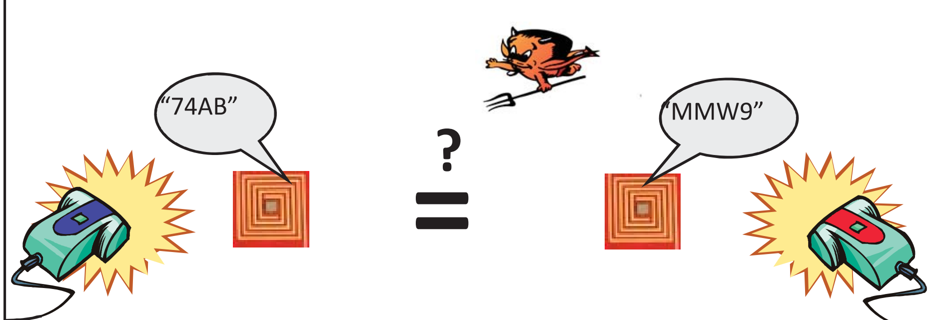
# Read Ranges of Tags

- **Nominal read range:** RFID standards and product specifications generally indicate the read ranges at which they intend tags to operate. These ranges represent the maximum distances at which a normally operating reader, with an ordinary antenna and power output, can reliably scan tag data. ISO 14443, for example, specifies a nominal range of 10cm for contactless smartcards.
- **Rogue scanning range:** The range of a sensitive reader equipped with a powerful antenna – or antenna array – can exceed the nominal read range. High power output further amplifies read ranges. A rogue reader may even output power exceeding legal limits. For example, Kfir and Wool [65] suggest that a battery-powered reading device can potentially scan ISO 14443 tags at a range of as much as 50cm, i.e., five times the nominal range. The rogue scanning range is the maximum range at which a reader can power and read a tag.
- **Tag-to-reader eavesdropping range:** Read-range limitations for passive RFID result primarily from the requirement that the reader power the tag. Once a reader has powered a tag, a second reader can monitor resulting tag emissions without itself outputting a signal, i.e., it can eavesdrop. The maximum distance of such a second, eavesdropping reader may be larger than its rogue scanning range.
- **Reader-to-tag eavesdropping range:** In some RFID protocols, a reader transmits tag-specific information to the tag. Because readers transmit at much higher power than tags, they are subject to eavesdropping at much greater distances than tag-to-reader communications – perhaps even kilometers away.



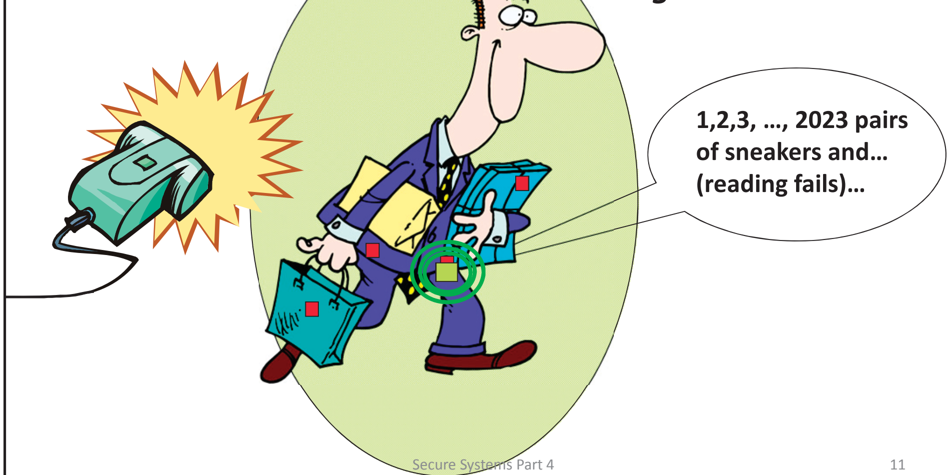
# Pseudonym rotation

- Set of cryptographically unlinkable pseudonyms *computed externally* by trusted verifier
- Pseudonyms stored on tag
    - Limited storage means at most, e.g., 10 pseudonyms
- Tag cycles through pseudonyms



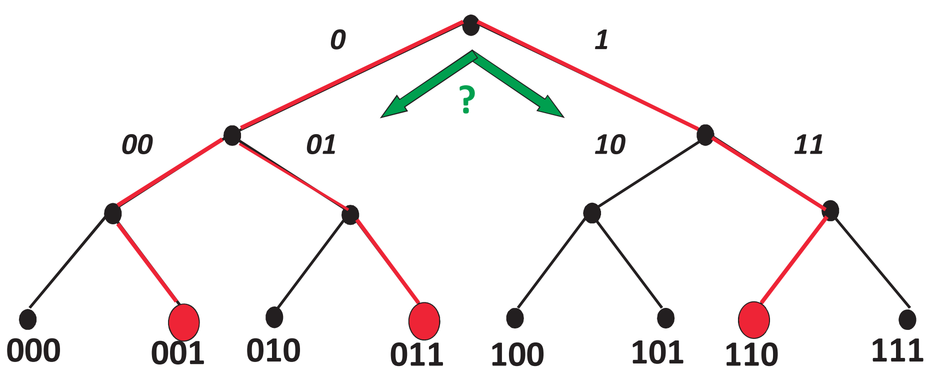
# "Blocker" Tag [Juels:03]

***Blocker simulates all** (billions of) **possible tag serial numbers!!***






# "Tree-walking" anti-collision protocol



# In a nutshell

- “Tree-walking” protocol for identifying tags recursively asks question:
  - “What is your next bit?”
- Blocker tag always says ***both ‘0’ and ‘1’***!
  - Makes it seem like *all* possible tags are present
  - Reader cannot figure out which tags are actually present
  - Number of possible tags is *huge* (at least a billion billion), so reader stalls

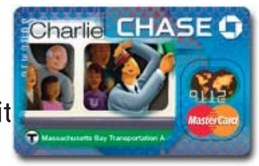


## Privateway Supermarkets


**Blocker tag system should protect privacy but still avoid blocking unpurchased items**

# RFID Privacy for Public Transportation

- Hong Kong Octopus has 12 million card holders
- 9 billion unlinked trips/yr on US public transit
- Atlanta, Seattle, Chicago, DC, San Francisco
- Boston MBTA in pilot program
  - 50,000 Mifare 1K cards issued
  - $200 million upgrade of fare system
- Boston MBTA issues
  - How to securely share tag storage space wit
  - No more issuing transit cards (PKI?)
  - Real-time information and resource provisioning?
- Ongoing project with Umass/EPFL on location-privacy preserving payment system based on e-cash and pseudonyms






# Privacy for Public Transportation