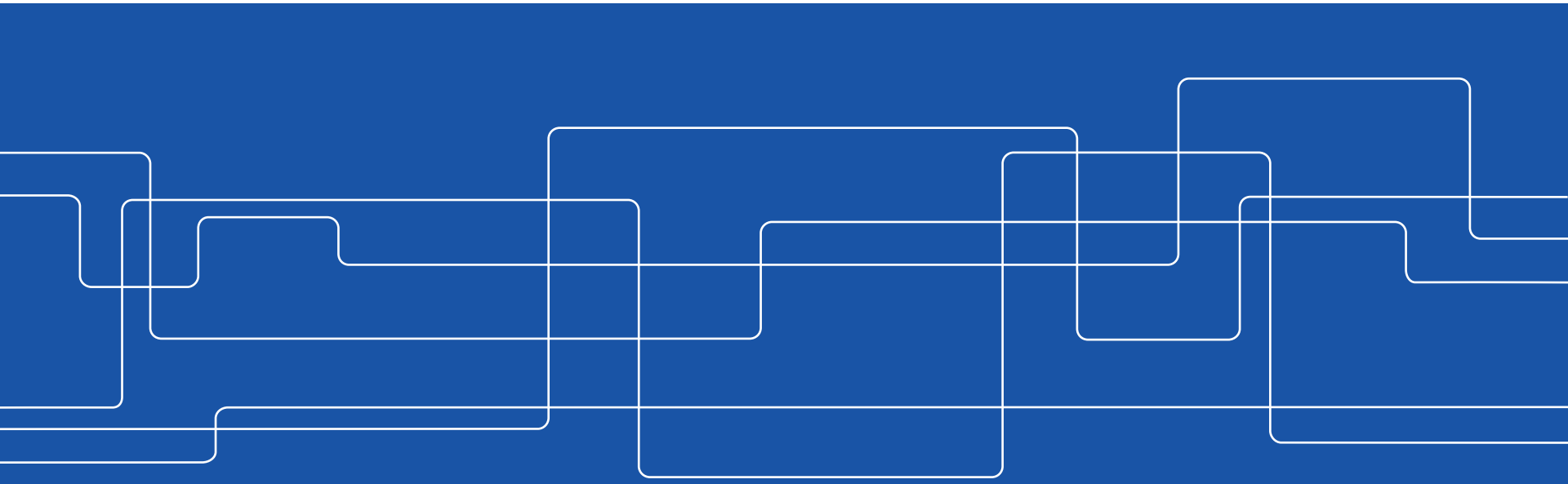
KTH ROYAL INSTITUTE
OF TECHNOLOGY

INTRODUCTION TO RFID SECURITY

Sha Tao

Postdoc at Department of ESY/ICT
KTH Royal Institute of Technology

October 3, 2016



Outline

Part I

- Background
- Vulnerabilities and Treats
- Protection Mechanisms

Part II

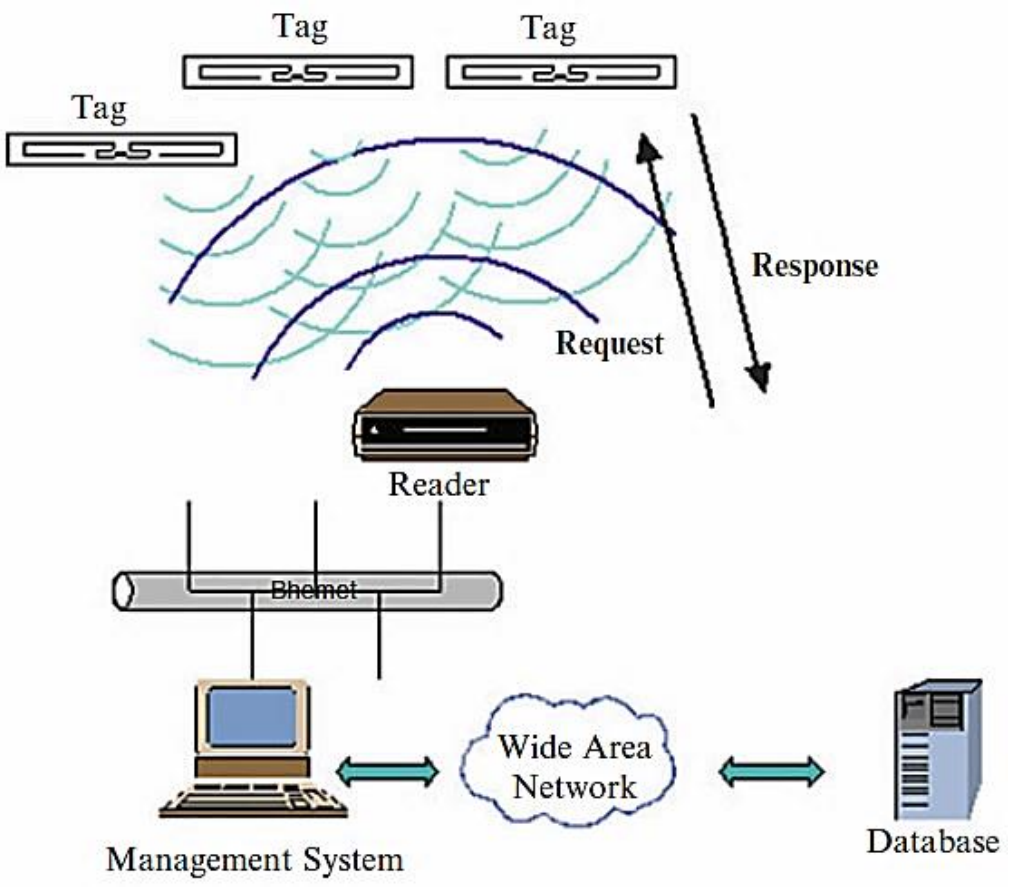
- Case Study
  - An “Unclonable” RFID IC for Anti-Counterfeiting Applications

Security & Privacy – *does it matter?*

Source: https://www.ibiblio.org/Dave/Dr-Fun/df200601/df20060116.jpg.

Low-Cost RFID Systems: A Revisit

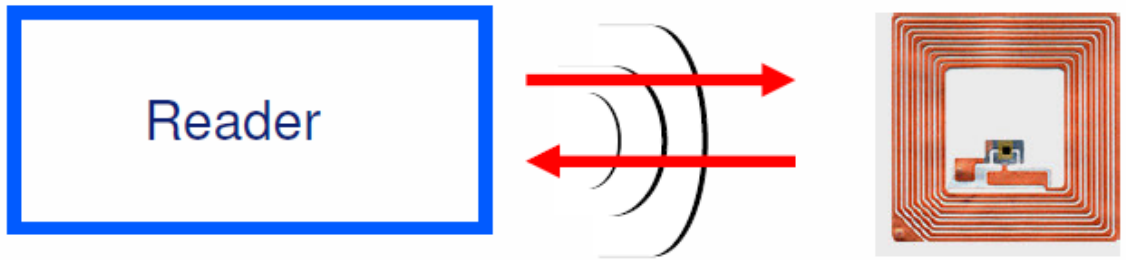
- Reader emits RF signals and keeping observing
- Passive tags harvest energy from received RF signal
- Tag reflects a modified RF signal back to the reader
- Reader demodulates the received signals and decodes it for further processing



Source: M. Tehranipoor and C. Wang, Introduction to Hardware Security and Trust, Springer, 2012.

Passive RFID Tags: A Revisit

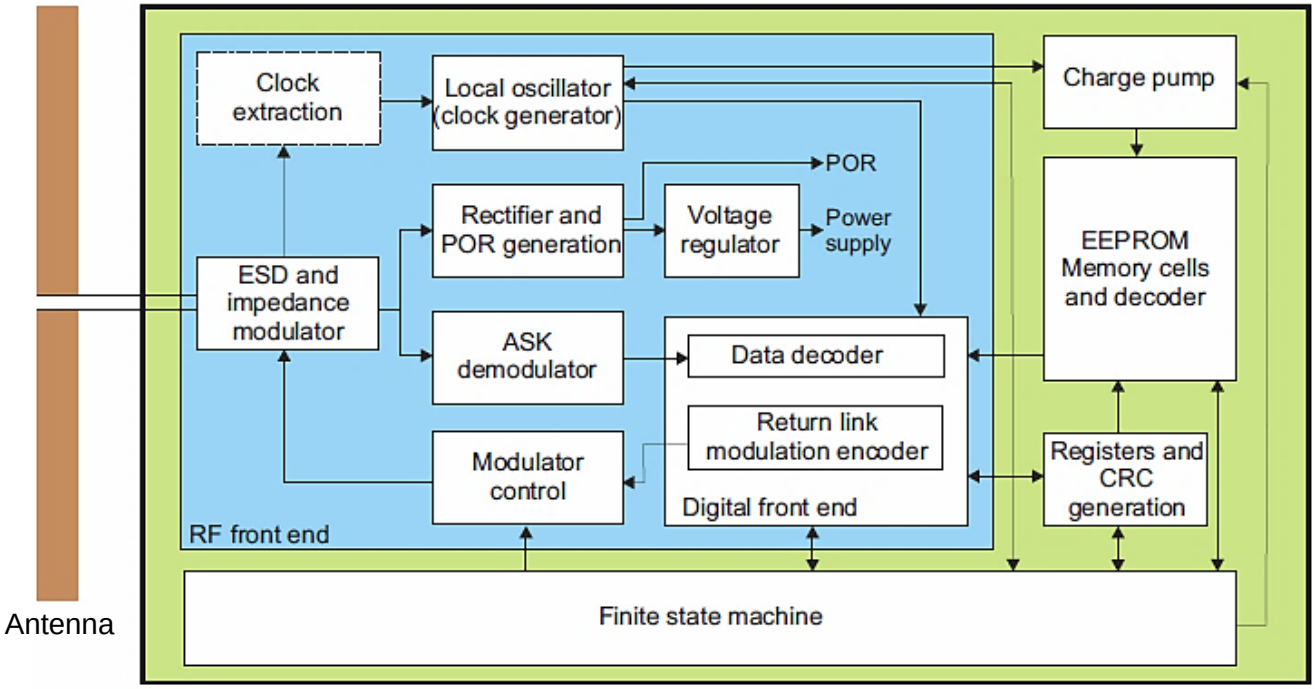
- Antenna connected to a micro-chip
- No battery, power is obtained from EM-field of the reader
- Low-cost identification of goods
  - If no chip 1-2cents (billions pieces/year)
  - With chip 5 cents (billions pieces/year)
  - Small: < $1mm^2$
- Range: up to several meters (depends on the frequency)



Source: P. Tuyls, RFID-Tags: Privacy and Security Issues, Philips Research, 2006.

Passive RFID Tags: A Revisit

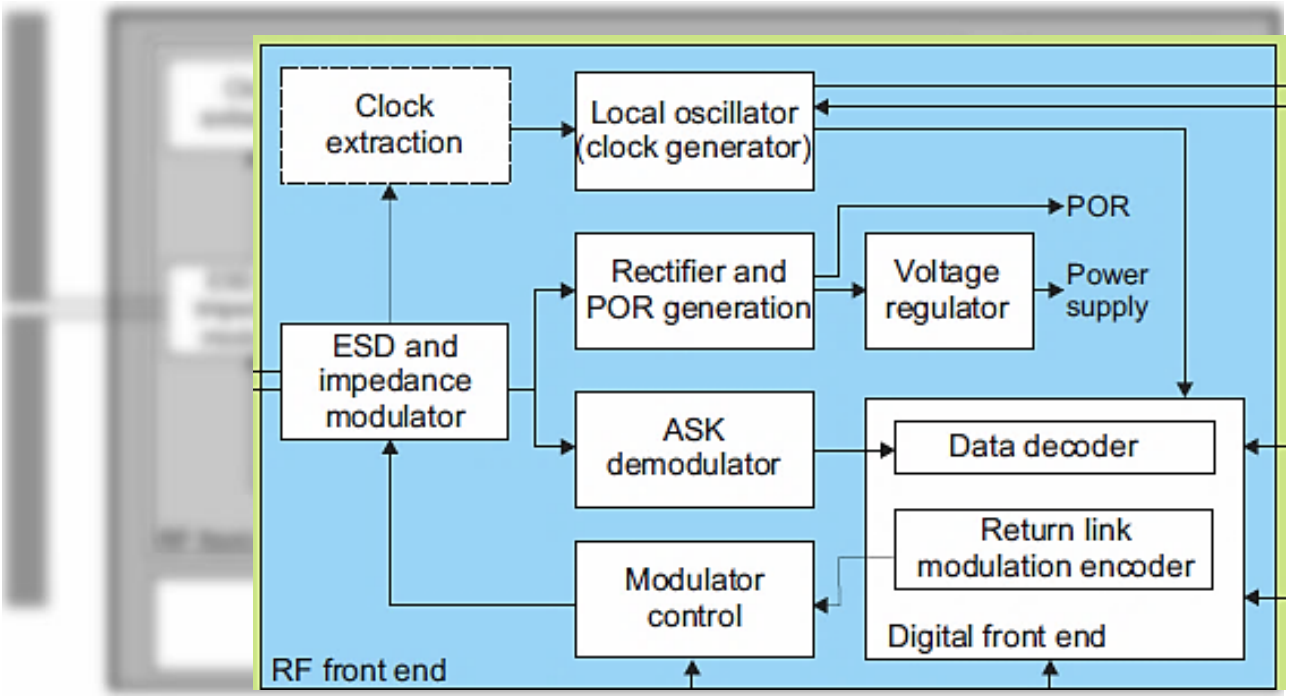
- Block Diagram of a Passive RFID Tag[1]



- RF Front End (Demodulation, modulation and energy harvesting)
- Memory Circuitry (EEPROM stores the EPC number)
- Finite State Machine (Logic Circuitry)

Passive RFID Tags: A Revisit

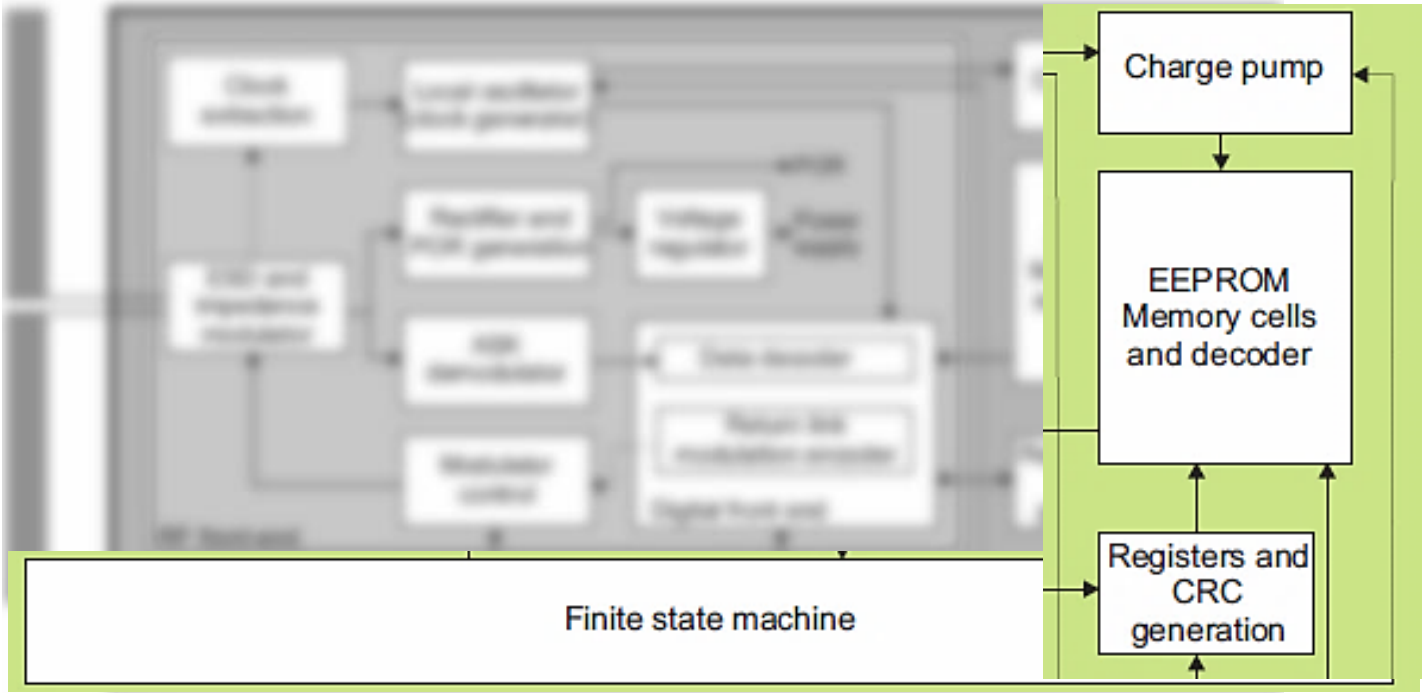
- Block Diagram of a Passive RFID Tag[1]



- RF Front End (Demodulation, modulation and energy harvesting)
- Memory Circuitry (EEPROM stores the EPC number)
- Finite State Machine (Logic Circuitry)

Passive RFID Tags: A Revisit

- Block Diagram of a Passive RFID Tag[1]



  - RF Front End (Demodulation, modulation and energy harvesting)
  - Memory Circuitry (EEPROM stores the EPC number)
  - Finite State Machine (Logic Circuitry)

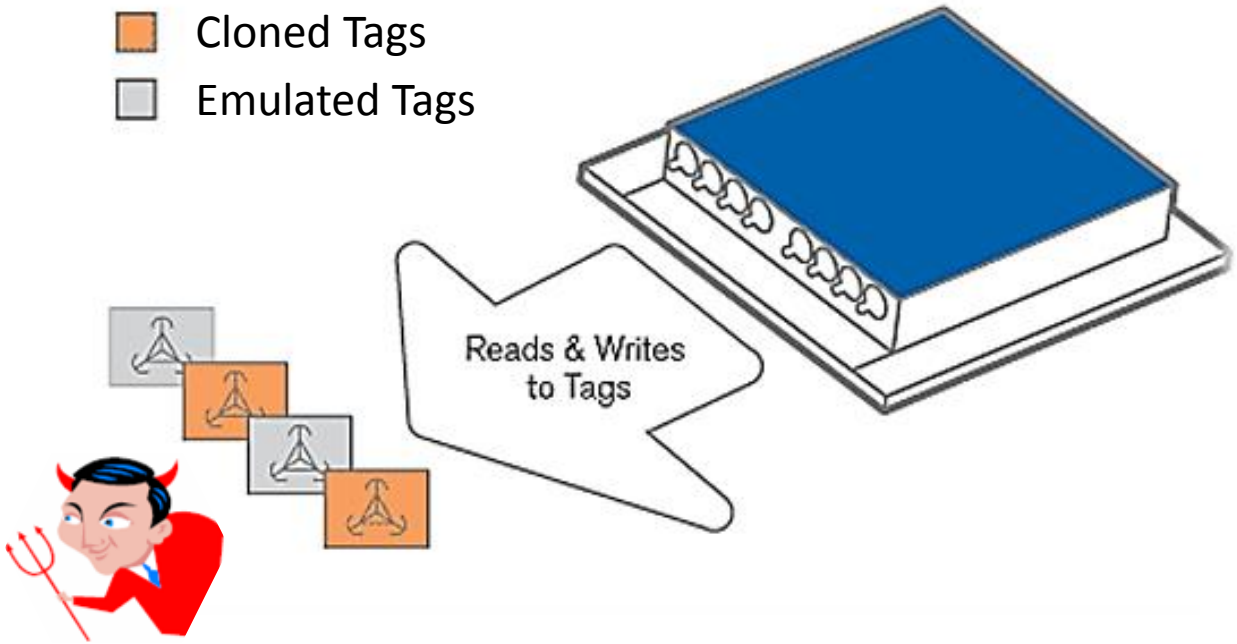
Treats and Attacks to RFID Tags[2,3]

- Attacks for Impersonation
  - Tag cloning, tag emulation, etc.
- Attacks for Information Leakage
  - Unauthorized tag reading
  - Side-channel attacks
- Attacks through Physical Manipulation
  - Physical tampering
  - Tag removal
  - Tag destruction

Source: Google Image.

Treats and Attacks to RFID Tags

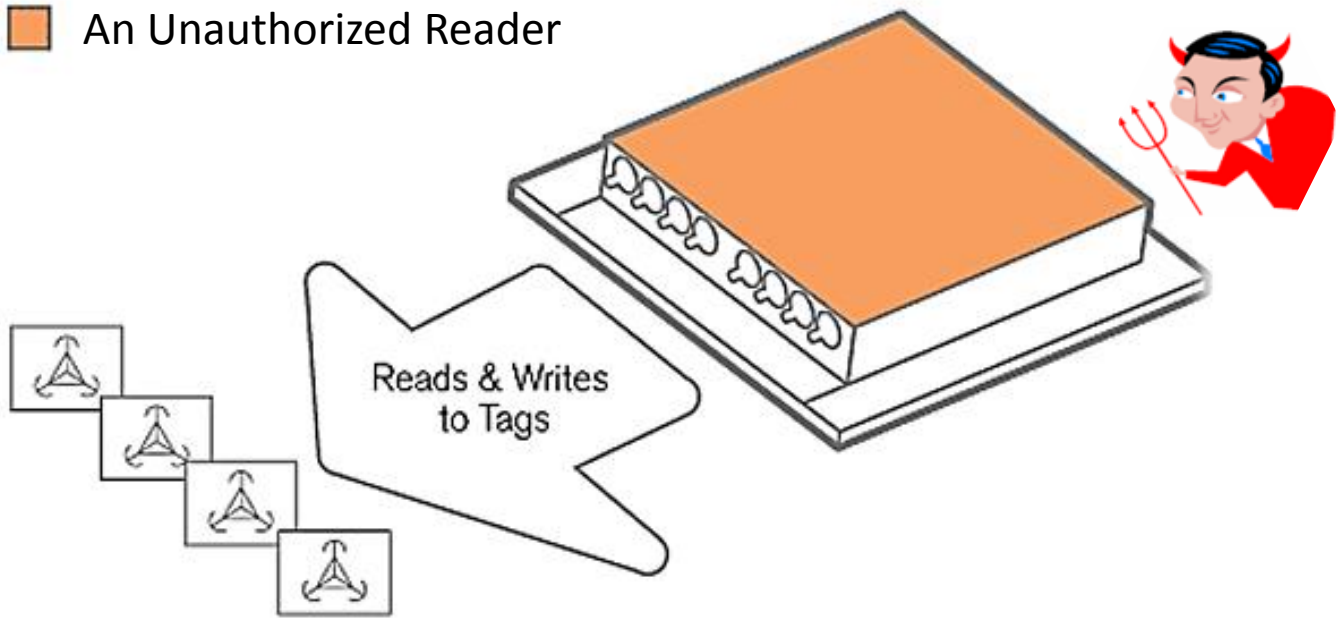
- Scenario 1: Tag Cloning and Emulation



Source: http://www.thingmagic.com/index.php/rfid-security-issues.

Treats and Attacks to RFID Tags

- Scenario 2: Unauthorized Access to Tags

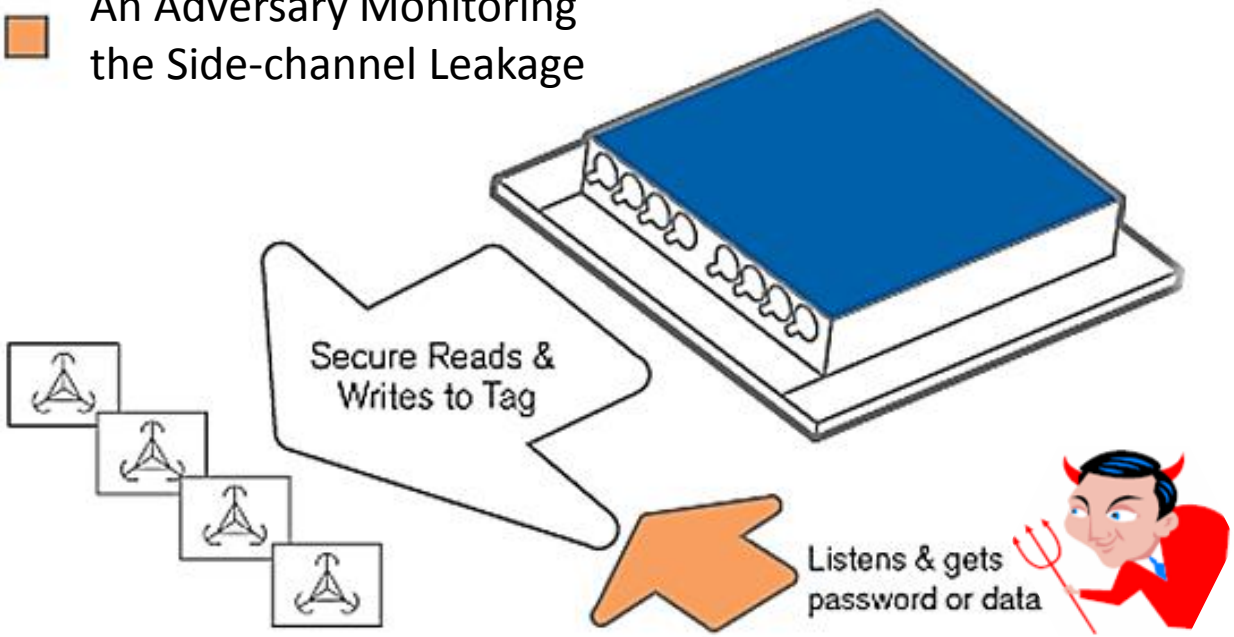


Source: http://www.thingmagic.com/index.php/rfid-security-issues.

Treats and Attacks to RFID Tags

- Scenario 3: Side Channel Attacks

An Adversary Monitoring the Side-channel Leakage



Source: http://www.thingmagic.com/index.php/rfid-security-issues.

Existing Protections for RFID Tags[3]

- Attacks through Physical Manipulation
  - Tamper-resistance Techniques
- Attacks for Information Leakage
  - Countermeasures to unauthorized tag reading
    - Break the communication when the tag is not accessed
    - Apply access control mechanism to the tag (e.g., KILL command)
  - Countermeasures to side-channel attacks
    - Decouple power consumption from data being processed: achieved by 1) power balancing or 2) power randomization

Existing Protections for RFID Tags[3]

- Attacks through Physical Manipulation
  - Tamper-resistance Techniques
- Attacks for Information Leakage
  - Countermeasures to unauthorized tag reading
    - Break the communication when the tag is not accessed
    - Apply access control mechanism to the tag (e.g., KILL command)
  - Countermeasures to side-channel attacks
    - Power Analysis: decouple power consumption from data, achieved by 1) power balancing or 2) power randomization
    - EM Analysis: 1) shielding by a Faraday Cage, 2) low power design

Existing Protections for RFID Tags[3]

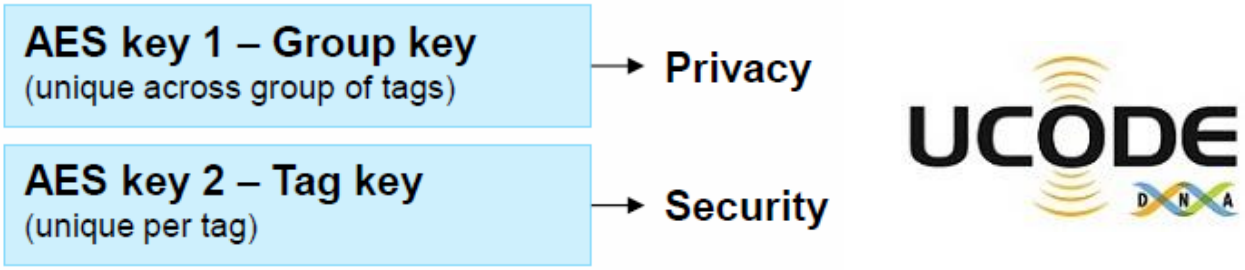
- Attacks for Impersonation
  - Countermeasures to tag cloning and tag emulation
    - Conventional cryptography: 1) hardware overhead, 2) limited on-tag resources may lead to weak authentication protocols
    - Novel methods: Watermarking & physical unclonable function
  - **Watermarking**: generates a watermark using a pseudo random number generator using data stored on tags
  - **Physical unclonable function (PUF)**: creates challenge-response pairs with additional low-cost circuitry on tags

Existing Protections for RFID Tags[3]

- Attacks for Impersonation
  - Countermeasures to tag cloning and tag emulation
    - Conventional cryptography: 1) hardware overhead, 2) limited on-tag resources may lead to weak authentication protocols
    - Novel methods: Watermarking & physical unclonable function
  - **Watermarking**: generates a watermark using a pseudo random number generator using data stored on tags
  - **Physical unclonable function (PUF)**: creates challenge-response pairs with additional low-cost circuitry on tags

Existing Protections for RFID Tags

- UCODE® DNA Tag IC from NXP Semiconductors
  - In accordance with GS1™ **UHF EPC Gen2 v2.0**
  - Innovative functionality: integrates *Advanced Encryption Standard* (AES) implementation into passive RFID tags
  - Privacy protection and cryptographic authentication
    - Tag authentication via 128-bit AES+ unique crypto key
    - Privacy protection via 128-bit AES+ group crypto key

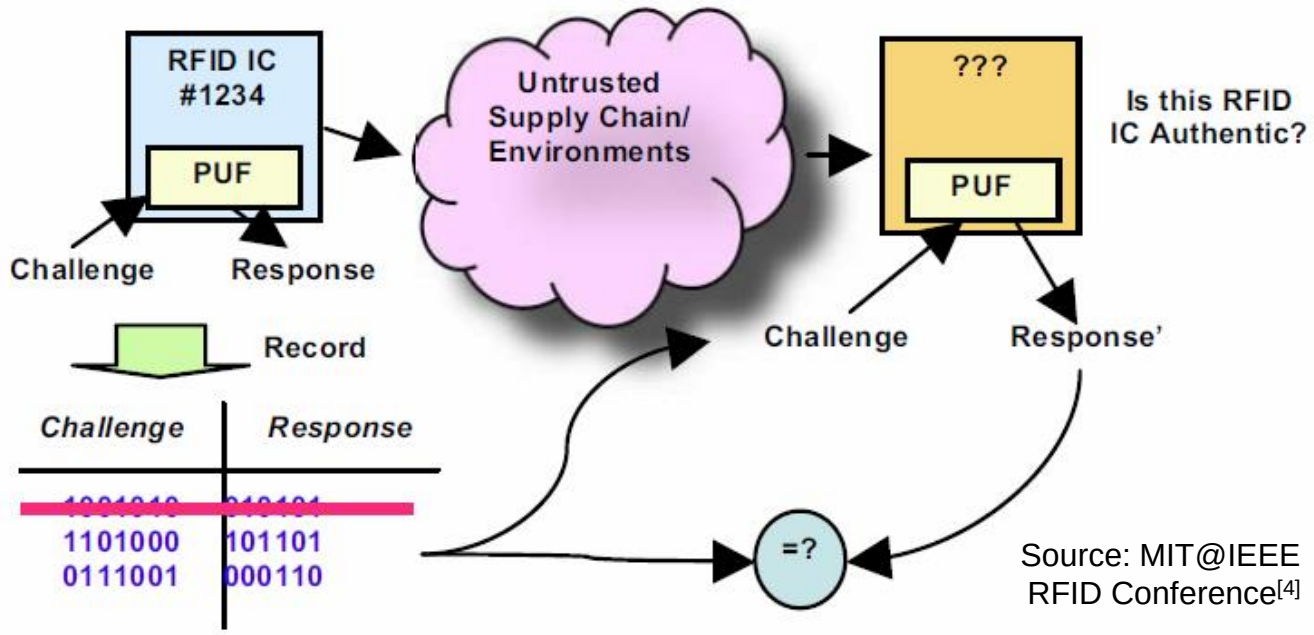


+ 128-bit AES refers to the AES-*128* standardized in ISO/IEC DIS 29167-10.

Source: http://www.nxp.com/products/identification-and-security/smart-label-and-tag-ics/ucode-dna.

Case Study

- PUF-based authentication for RFID IC
  - A lightweight PUF circuit is embedded in each RFID chip
  - Each RFID chip has its unique secrets, *i.e., an exponential number of challenge-response pairs*, derived from silicon

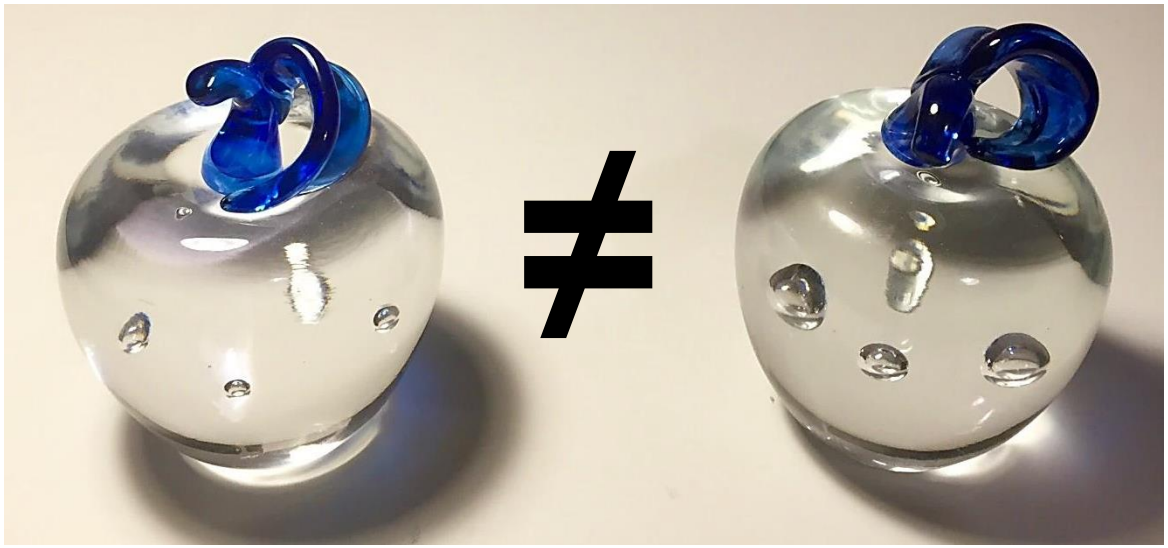


Source: MIT@IEEE RFID Conference[4]

Case Study

Physical Unclonable Apples

- Due to manufacturing process variations, every “apple” is slightly different[+]

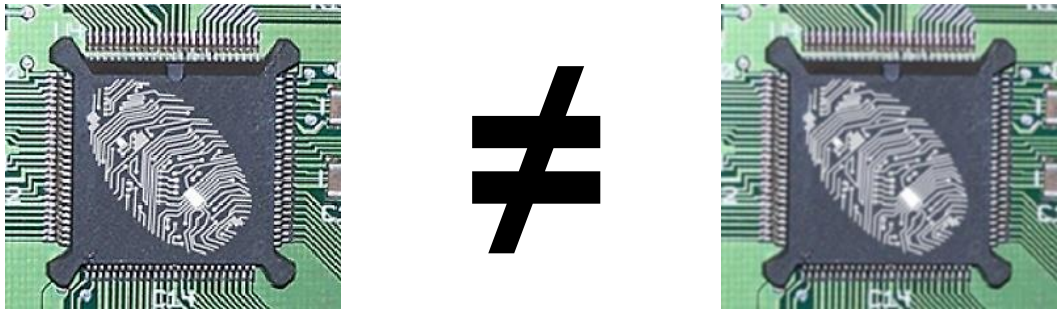


[+] Quoted from: Georg T. Becker, Physical Unclonable Functions in theory and practice, Trudevice 2016.

Case Study

Physical Unclonable Functions

- Due to manufacturing process variations, every chip is slightly different



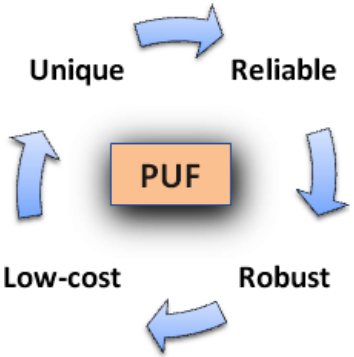
- Exploit this fact to give every chip a unique “fingerprint”
- These unique characteristics are similar to the secret keys
- Authenticate each RFID chip by observing the PUF response

Case Study

- (Silicon) Physical Unclonable Functions

  Secrets Derived from the Embedded Silicon PUF are

  - intrinsic to the silicon itself
  - extremely difficult to predict or “control” before manufacture
  - almost impossible to duplicate or “clone” from one to another



Source: google image.

Case Study

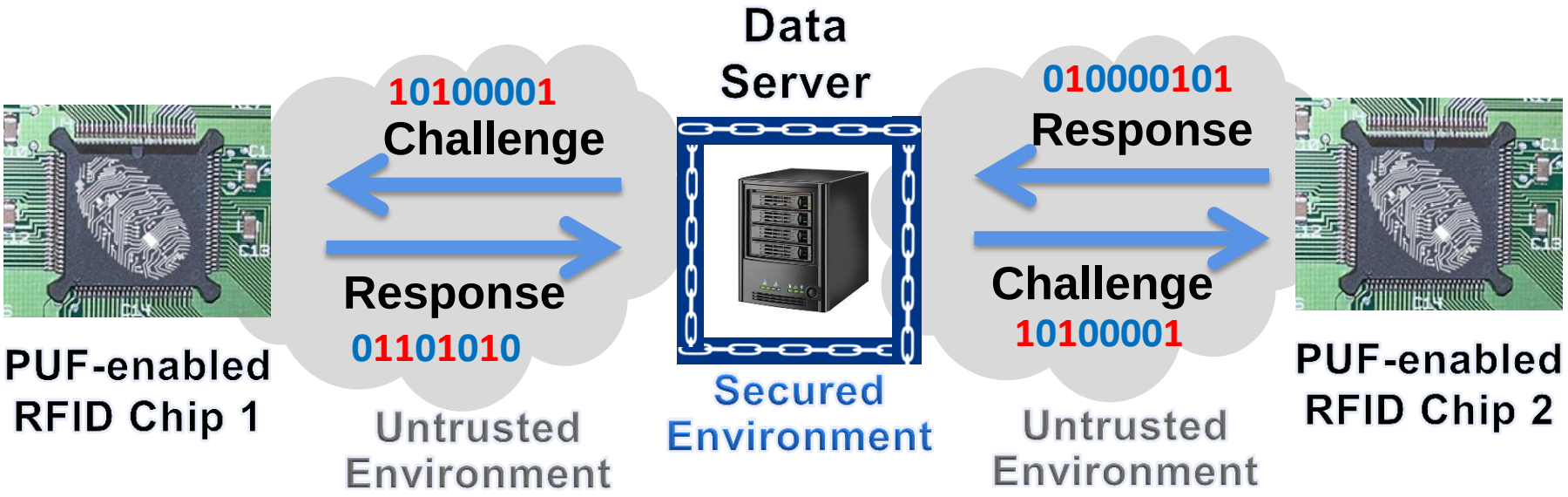
- (Silicon) Physical Unclonable Functions

  Advantages over Conventional Approach of Storing Secrets[4]

  1. Increase physical security by generating volatile secrets
     - Rather than read stored secret, an adversary needs to apply an attack while the chip is running and using the secret
  2. Even the IC manufacturer cannot clone a PUF-enabled chip
     - Randomness in process variation cannot be controlled or programmed by the manufacturer in any conventional way
  3. PUFs also simplify and secure key provisioning process
     - Manufacturers do not have to program the IC with secrets

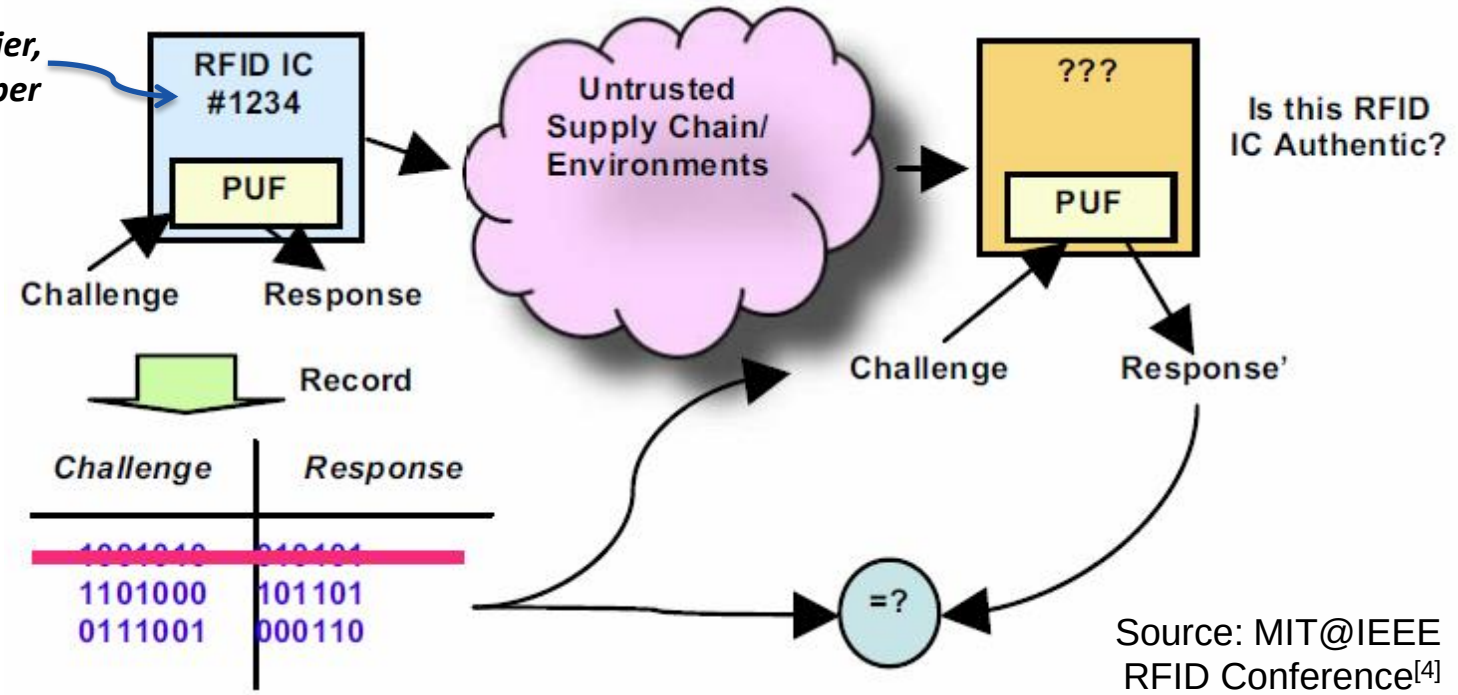
Case Study

- PUF-based Authentication
  - Given a challenge, each RFID chip has its unique responses
  - The response is calculated based on PUF characteristics
  - Only an authentic IC can produce an expected response



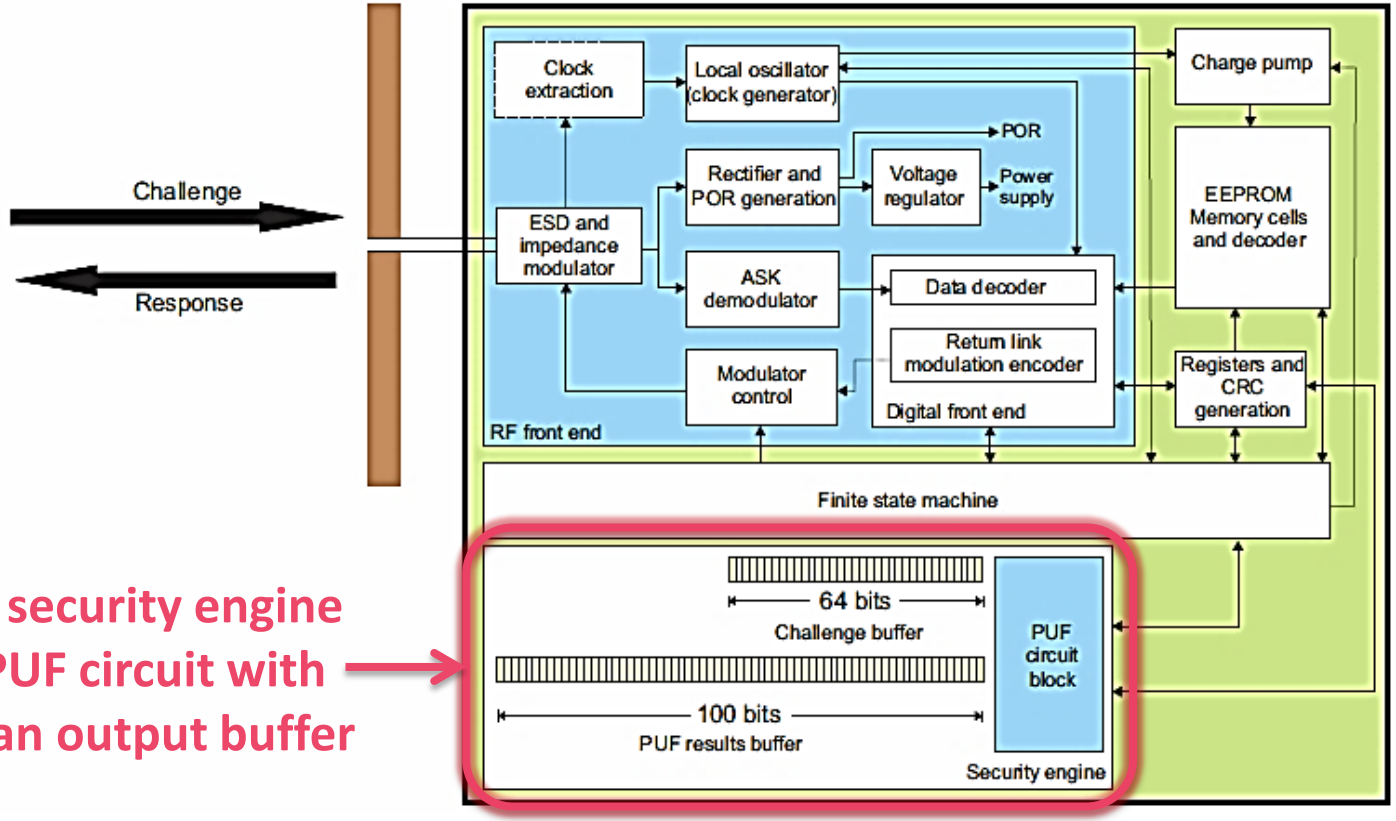
Case Study

- PUF-based Authentication for Anti-Counterfeiting



Case Study

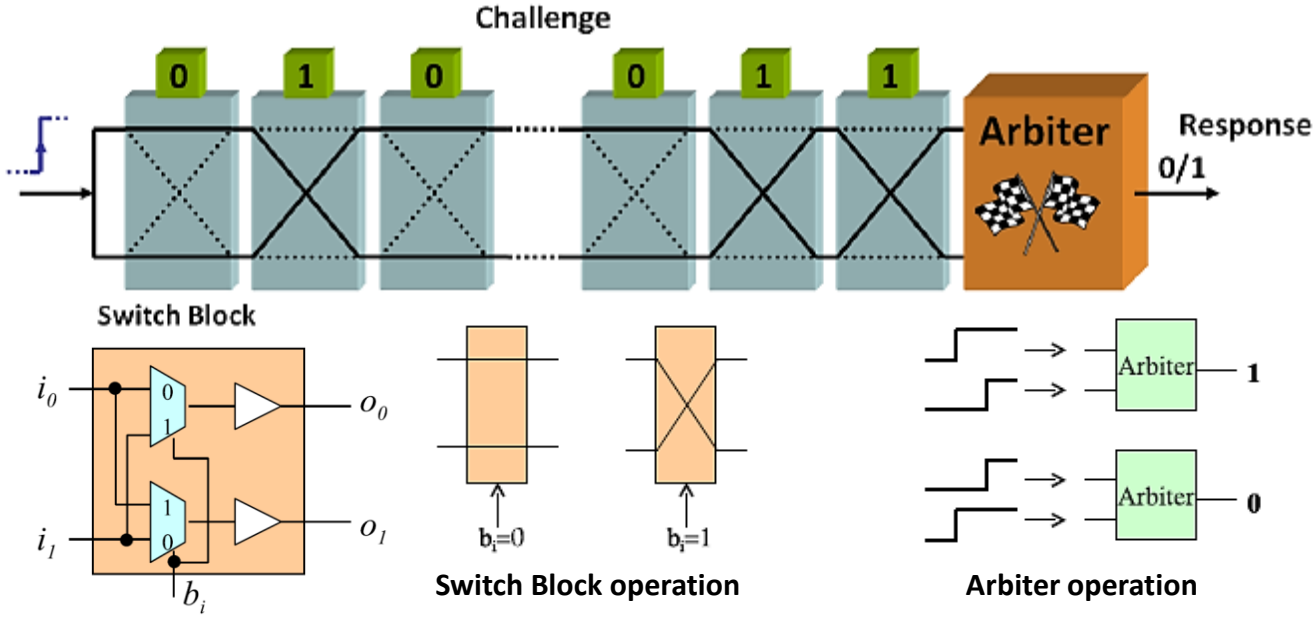
- A PUF-enabled RFID Chip
  - Block Diagram[1,5]



An additional security engine consists of a PUF circuit with an input and an output buffer

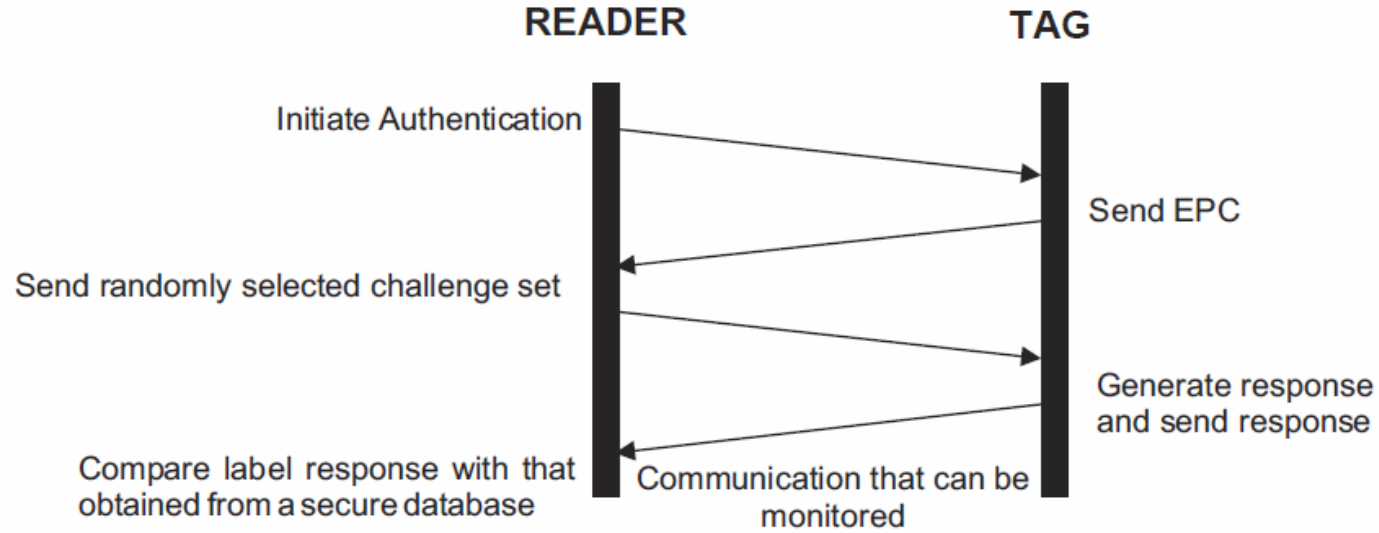
Case Study

- A PUF-enabled RFID Chip
  - Arbiter-based PUF Circuit [1,4,6]
    - create a race between two identically designed delay paths
    - process variations result in unpredictable response on each tag
    - switch blocks used to create challenge-response pairs (CRPs)



Case Study

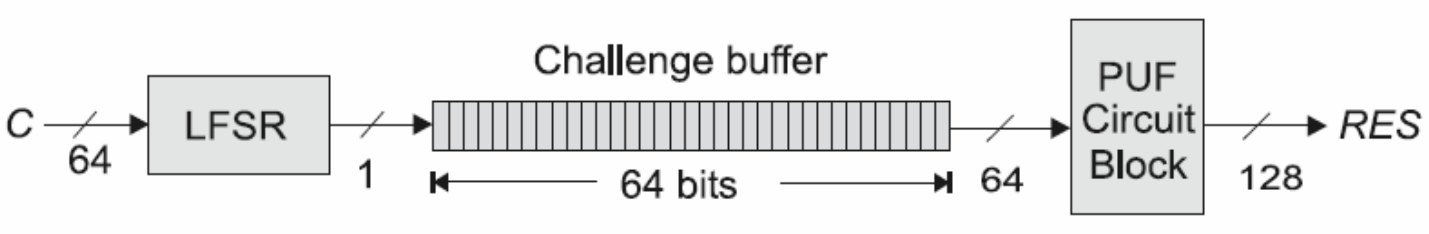
- A PUF-enabled RFID Chip
  - Message exchange protocol between a **READER** and a **TAG** during a Tag Authentication Process[1]



  - A Tag and Reader Mutual Authentication Protocol[5]
  - A Hash based Tag Authentication Protocol[5]

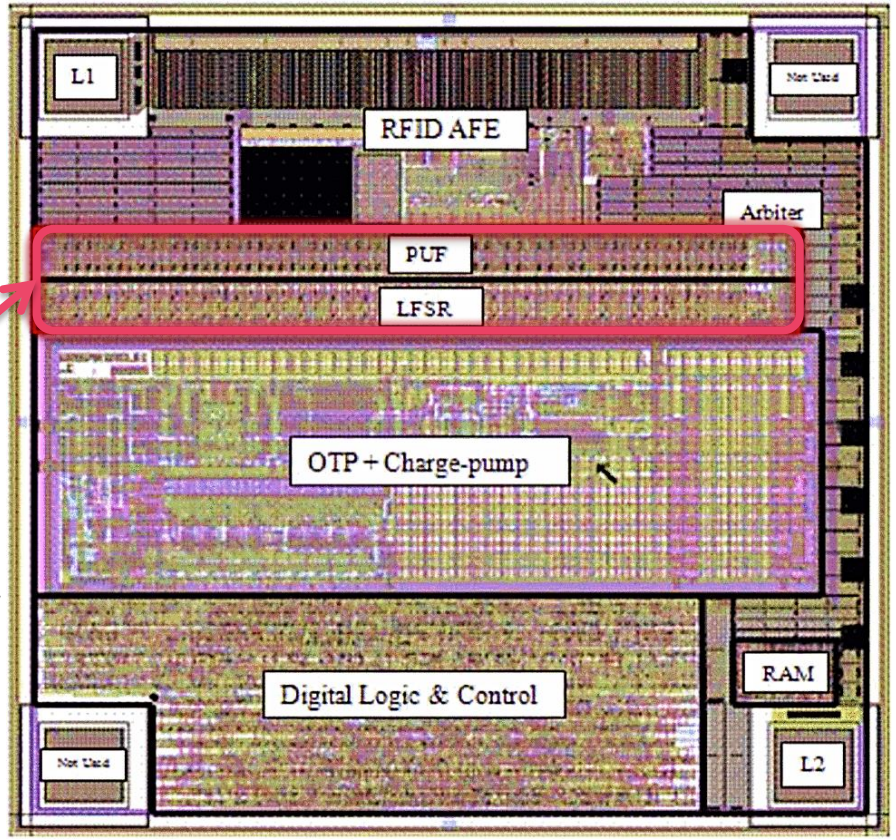
Case Study

- A PUF-enabled RFID Chip
  - The primary performance obstacle
    - The excessive overhead of transmitting a large number of challenges where each challenge consisted of 64 bits
    - Max. transmission speed specified in EPC C1G2 is 126 kbps
  - An improved approach to overcome the obstacle[5]
    - Use a linear feedback shift register (LFSR) to generate the challenges once initialized with a seed
    - Then, only the seed to the LFSR needs to be sent to a tag as a challenge C, from a reader



Case Study

- A PUF-based RFID Chip[4]
  - The PUF-enabled RFID IC was designed and fabricated
  - The approach is area-efficient
    - Majority of silicon area consumed by standard RFID components
    - PUF and LFSR use small area ca. 0.02mm^2 in a 180 nm CMOS
  - The approach is power-efficient
    - PUF consumes dynamic power only during evaluation which is small
    - In most of the time, only leakage current is consumed



Case Study

- Advantages of PUF-enabled RFID Approach[4] over basic passive RFIDs and cryptographic RFIDs
  1. Highly Secure
     - The RFID chip can hardly be cloned
     - Responses are generated dynamically and are volatile
  2. Low Cost and Low Power
     - A PUF is a fairly lightweight addition to the RFID IC
  3. Simple and Robust Authentication
     - PUFs provide strong authentication for passive RFID tags
     - These tags can be authenticated by simply comparison

References

[1] D. C. Ranasinghe, D. Lim, P. H. Cole, and S. Devadas, A Low Cost Solution to Authentication in Passive RFID Systems, Auto-ID Labs White Paper, 2006.

[2] M. Tehranipoor and C. Wang, Eds., Introduction to Hardware Security and Trust. New York, NY: Springer New York, 2012.

[3] A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, "Classifying RFID attacks and defenses," Information Systems Frontiers, vol. 12, no. 5, pp. 491-505, 2010.

[4] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, "Design and Implementation of PUF-Based 'Unclonable' RFID ICs for Anti-Counterfeiting and Security Applications," in IEEE International Conference on RFID, 2008, pp. 58-64.

[5] P. H. Cole and D. C. Ranasinghe, Eds., Networked RFID Systems and Lightweight Cryptography: Raising Barriers to Product Counterfeiting. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008.

[6] A.-R. Sadeghi and D. Naccache, Eds., Towards Hardware-Intrinsic Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010.

Thanks for your attention !