UBICOMP

Episode 14: RFID

Hannes Frey and Peter Sturm
University of Trier

Outline

- Introduction
- Applications
- Communication Principles
- Data Integrity and Security

References

[1] K. Finkenzeller, “RFID-Handbuch”, Hanser Verlag, 2002
[2] R. Want *et al.*, Bridging Physical and Virtual Worlds with electronic Tags, Proc. Of CHI, 1999

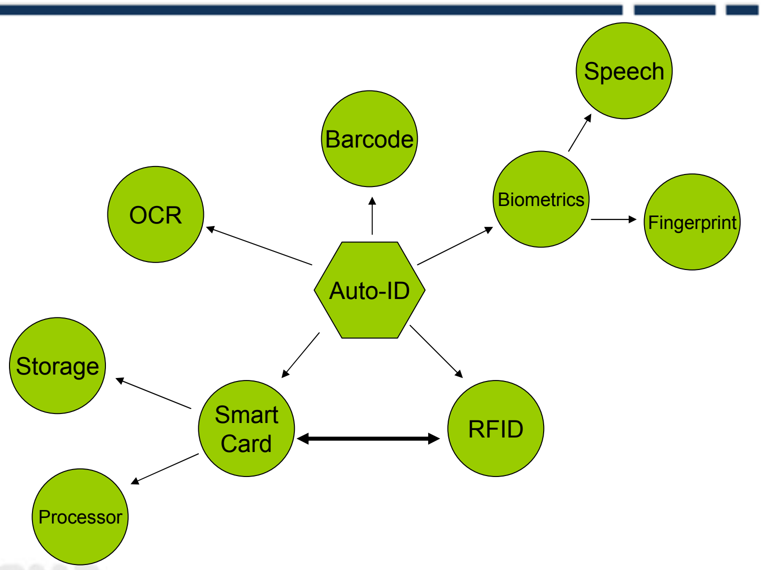
UBICOMP

Introduction

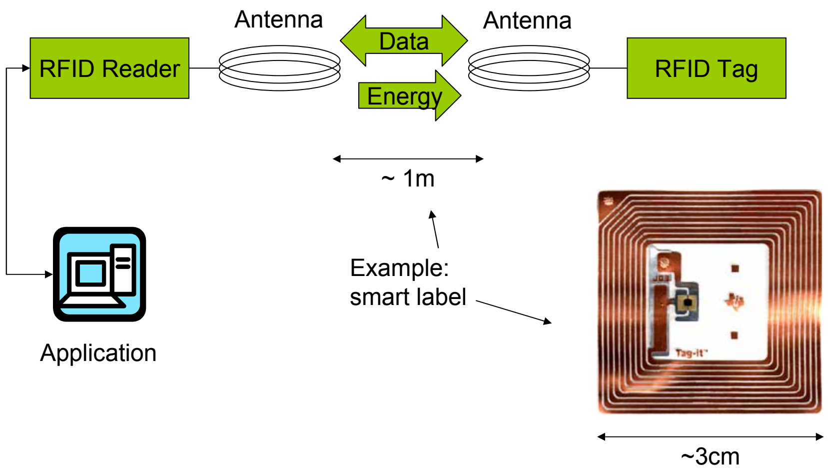
Smart Identification and UbiComp?

- Identify Objects
  - Typically: from distance
  - Or: in a secure way
- Purpose
  - Associate specific actions, attributes etc. with an object
  - Authenticate an object, person
  - …
- What techniques do we know?

Automatic Identification Systems



Components of an RFID System



RFID Systems (1)

- Communication principles
  - Full-duplex and half-duplex
    - Transponder sends during energy transmission
    - Techniques needed to detect weak signals from tag
  - Sequential
    - Turn off field of the reader; tag sends during reader is idle
    - Tag needs a capacitor or battery supply
- Data volume
  - From a few bytes to several Kbytes
  - Special 1-bit transponders
    - Only two states: Transponder in field or not
    - Possible applications? → anti-theft system

RFID Systems (2)

- Read/Write and Read-Only transponders
  - EEPROM: writing has a high energy consumption, max. 100000 reads possible
  - FRAM: writing consumes only a fraction of energy and is 1000 times faster compared to EEPROMs, difficult to produce
  - SRAM: fast write cycles, needs battery supply
- Control of Read-Write and Authorization
  - State Machine: Inflexible to function changes
  - Micro processor architecture (smart-card OS)
- Energy Supply
  - Passive: Energy supply by the magnetic/electric field of the reader
  - Active: Battery supply needed

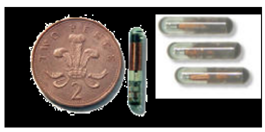
RFID Systems (3)

- Range
  - Close coupling: ~1cm
  - Remote coupling: ~1m
  - Long-range system: >1m
- Techniques to read data from tag
  - Backscatter 1:1
  - Load modulation: 1:1
  - Subharmonic: 1:n
  - Harmonic: n

Tag Styles (1)

- Disks and coins
  - Few millimeter to 10cm

- Glass Transponder
  - Identification of animals
  - Length: 12-32mm



- Plastic Package Transponder
  - Car industry
  - Very robust

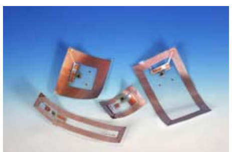
Tag Styles (2)

- Tool- and Bottle-identification
  - Designed to work even on metallic surfaces
  - Mechanic stability, Vibrations, Heat
- Coil-on-Chip
  - Smallest tag technology: 3x3mm^2
- Key fob
  - Anti-theft device
  - Access systems
- Watches, Wristbands

Tag Styles (3)

- ID-1 Cards
  - Large coil surface → increased communication range
  - Sometimes used: micro-wave transponder cards → same dimensions but width sometimes > 0,8mm

- Smart Labels
  - Transponder coil on 0,1mm plastic foil
  - Flexible enough to be placed on each item
  - Maybe a replacement of barcodes
    - New applications possible



UBICOMP

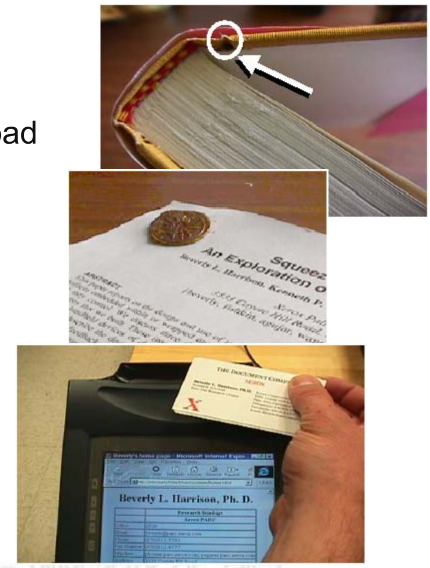
Applications

Common Applications

- Public Transport and Ticketing
- Access Control
- Logistics
- Animal identification
- Anti-theft system
- Real time measurements in sports
- Inventory Control in supermarkets
- Electronic payments
- Waste Collection
- Industry automation
- Medicine
- Future Applications?

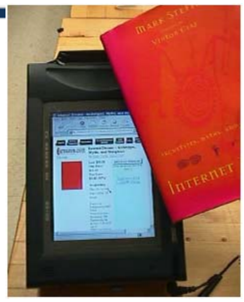
Bridging the Physical and Virtual World (1)

- Augmenting Books and documents
- Computational device may load virtual document
  - Related Web Content
  - New Versions
  - Link to an order form
- Business Cards
  - Present users website
  - Open empty mail with filled address field



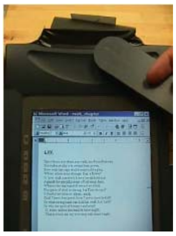
Bridging the Physical and Virtual World (2)

- Extending a documents functionality
  - E.g. dictionary invokes language translation program on currently selected document (context awareness)
  - More general office tools invoke electronic services upon documents
- User identification
  - Apply user preferences to the current context
- Augmenting the environment
  - Tags: Computer sensing the location
  - Reader: Location sensing the computer
  - E.g. display document only in certain locations, show last document opened here, …



Bridging the Physical and Virtual World (3)

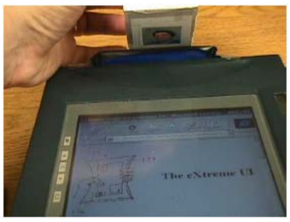
- Augmenting bookmarks
  - Physical bookmark referencing a particular page
  - Write remarks on physical object
  - How to store the current link? → additional tag for both operations (simple user interface mechanism)



- The wristwatch
  - Extend functionality of every day objects unambiguously
  - E.g. Striking the clock on top of the tablet PC opens a calendar application

Bridging the Physical and Virtual World (4)

- More experimental: The Photo Cube
  - 3D augmented object
  - Container with six related information sets



RFID Chef

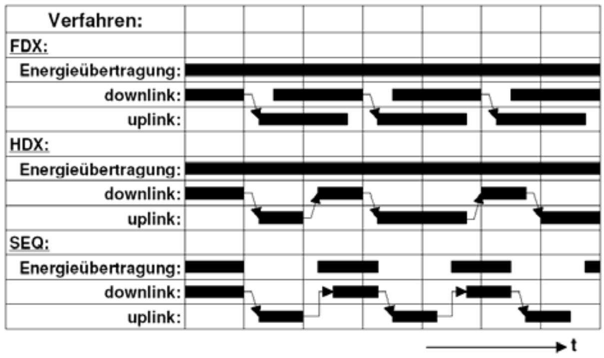
- Smart Kitchen Appliances
- Distributed Systems Group ETH Zurich

Play Demo (5min)

UBICOMP

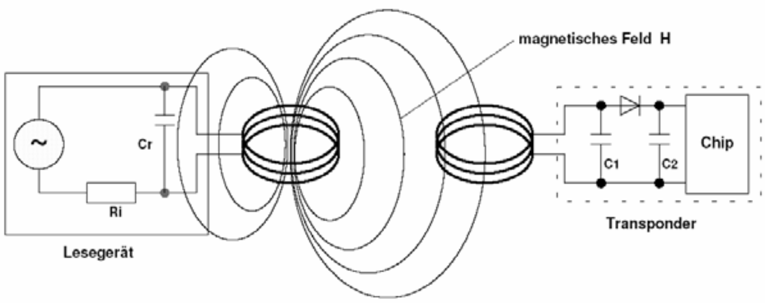
Communication Principles

Communication Principles



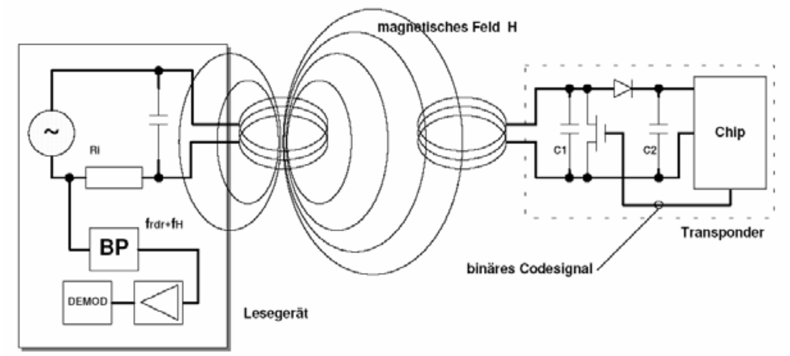
- Communication reader → tag performed easy (enough energy at the reader)
- Energy supply and Communication tag → reader?

Inductive Coupling: Energy Supply



- Magnetic field of reader induces voltage in tag coil
  - Can be interpreted as transformer
- Capacitor for oscillating circuit can be made of 10µm foil
- Typically 10mW at 1cm (close coupling), 100µW at 10cm
  - More powerful processors possible for close coupling (e.g. strong security demands)

Inductive Coupling: Communication

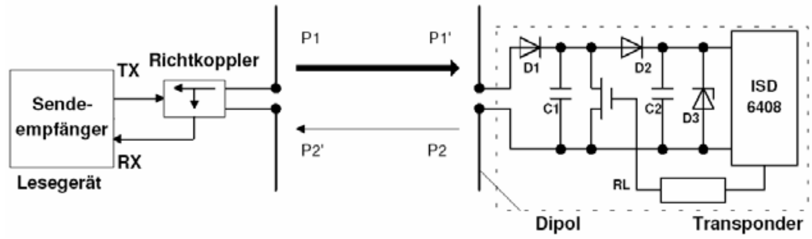


- Tag coil absorbs energy from the magnetic field
- Resistor at the tag antenna results in changing voltage at reader antenna
- Use inductive coupling to modulate data

Backscatter Coupling

- Magnetic field substituted by electromagnetic field at ~λ/2π (λ wavelength in m)
  - → Inductive coupling only used within a few meters
- Energy supply degrades significantly if electromagnetic coupling is used
- Backscatter systems have their own power supply
- Use received energy to switch power states
  - When leaving the electromagnetic field → stand-by
- Battery power used for processing only
- Communication via Backscatter modulation

Backscatter Modulation



- Electro magnetic waves are partly reflected by antenna
- Reflection properties can be changed by a resistor
- Receiver filters received electromagnetic signal received from tag
- (Harmonic, subharmonic)

UBICOMP

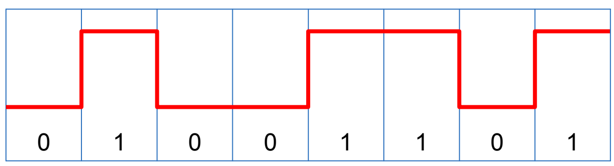
Data Integrity and Security

Commonly used Coding and Modulation Schemes

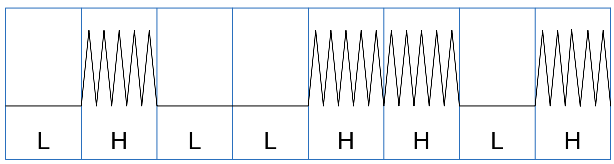
- Coding: map sequence of bits to a signal which is optimized to the characteristics of the transmission media in use
- Coding schemes
  - Non-return-to-zero (NRZ)
  - Manchester
  - *Unipolar*
  - *Differential bi-phase (DBP)*
  - *Miller*
  - *Differential*
  - *Pulse pause (PP)*
- Modulation: modify parameters of a high frequency carrier signal used to transmit binary information
- Modulation Schemes
  - Amplitude Shift Keying (ASK)
  - *Frequency Shift Keying (FSK)*
  - *Phase Shift Keying (PSK)*

An Example for Coding and Modulation

- NRZ-coding of a bit string

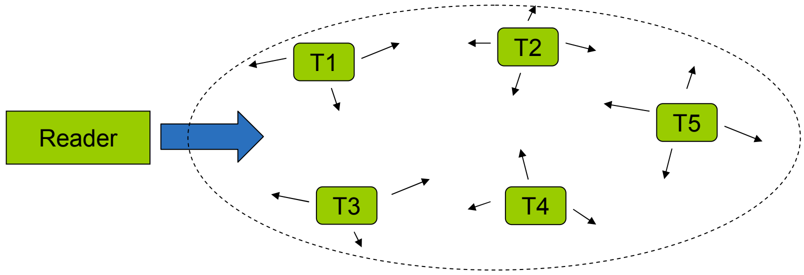


- ASK-modulation of the NRZ-code



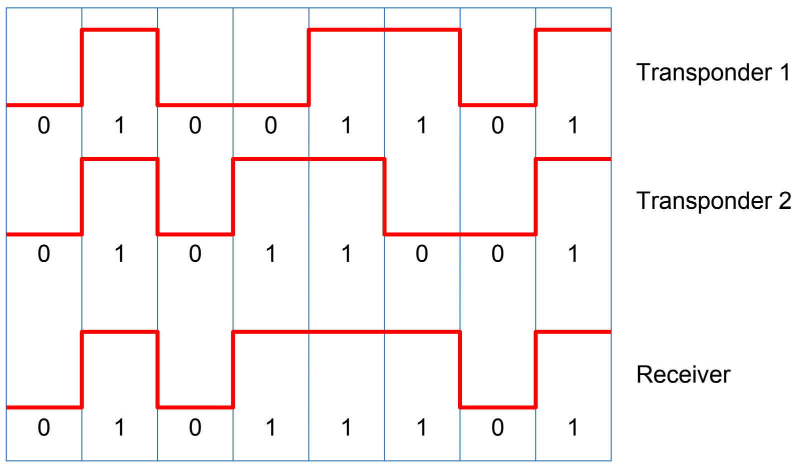
The Collision Problem

- Sender broadcasts signal to all transponders in vicinity



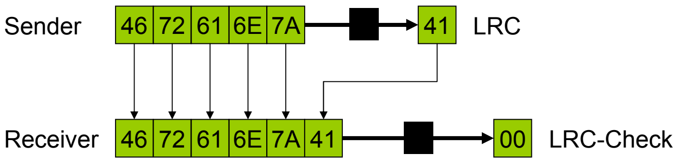
- All Transponders may answer simultaneously
  – Interference in a single shared medium
  – Can we apply CSMA/CD or CSMA/CA?

NRZ+ASK and Collisions



Parity Check and LRC

- Parity Check
  - Produce always an even/uneven number of bits
  - E.g. 0010 → 0010-1
- Longitudinal Redundancy Check LRC



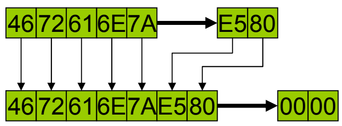
- Simple to implement by using XOR elements
- Weak error detection method
  - Parity: even number of inverted bits
  - LRC: blocks may mutually affect each other, block permutations

Cyclic Redundancy Check

- Divide by generator polynomial

```
             F7   Start
        111101110000
XOR     10011
        011011
XOR      10011
         010001
XOR       10011
          00010100
XOR          10011
             0011100
XOR            10011
Result          1111
```

- Use Result as start value for next calculation
- CRC-calculation with Data and CRC results in CRC value 0

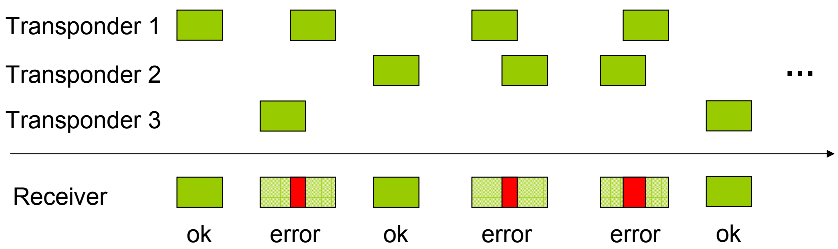


- Simple Error check
- May detect multiple errors
- Implementation with linear feedback register and XOR elements

Does PC, LRC, and CRC Solve Multiple Access?

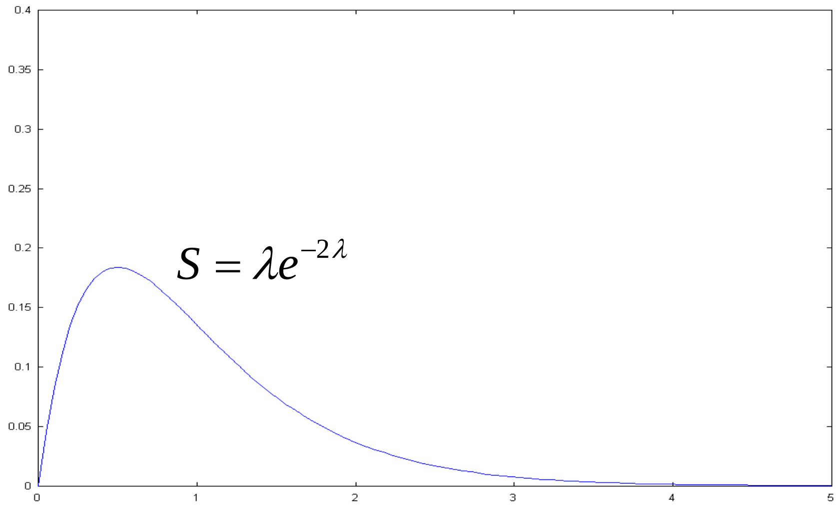
The ALOHA Principle

- Periodically send data packet with random quiet periods



- If collisions happen occasionally, the data of each transponder eventually gets through
- How good is this solution?

Throughput of ALOHA

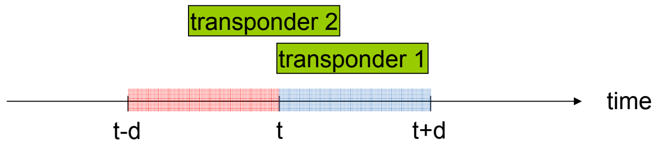


The Time Needed to Read all Transponders

# transponders	average	99%	99.9%
2	150ms	350ms	500ms
4	300ms	750ms	1.0s
6	500ms	1.2s	1.6s
8	800ms	1.8s	2.7s

Improving ALOHA

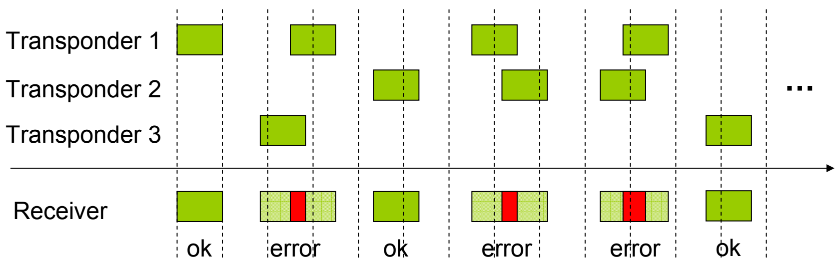
- Suppose unique data packet size d
- Packet transmission start at time t
- Collision in ALOHA ⇔ another transponders willing to send within time interval [t-d,t+d] (T<=2*d)



- How can we improve throughput?

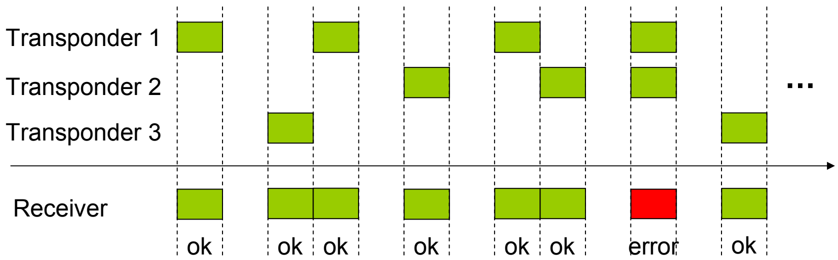
Slotted ALOHA

- Reader introduces timeslots



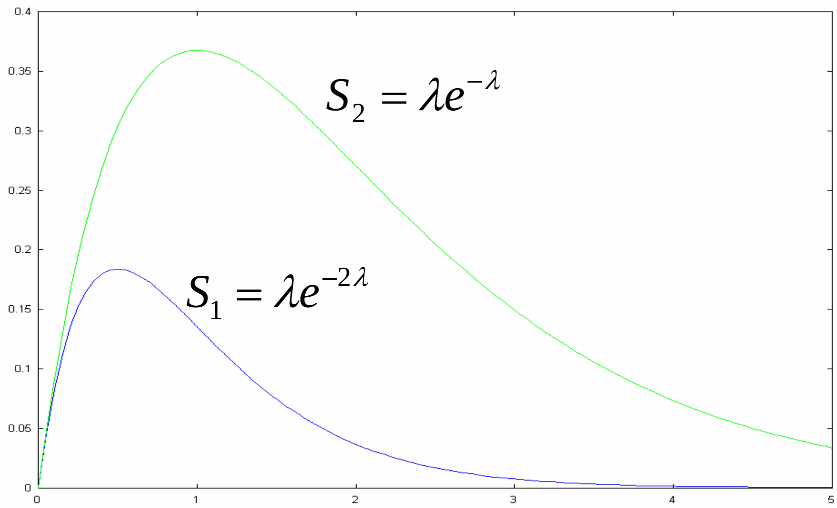
Slotted ALOHA

- Transponders restrict transmission to time slot intervals



- Collision in slotted ALOHA ⇔ another transponders willing to send within time interval T <= d

Throughput of slotted ALOHA

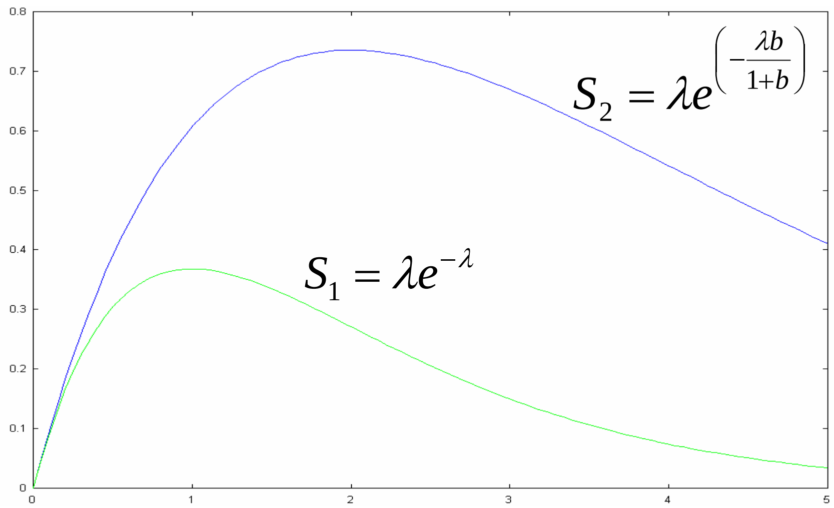


Further Improving ALOHA

- Signal strength depends on distance between tag an reader

- Data packet may dominate others in the same slot → Capture Effect
- Success depends on bias b
- Throughput increases with decreasing bias
- E.g. b=1 on next slide

Throughput of slotted ALOHA with Capture



Applying the ALOHA principle to RFIDs

READER:

```
Loop n times {
    provide k time slots;
    for each time slot {
        if received id and
            no collision {
            store id;
        }
    }
    for each new id {
        read/send data from tag;
    }
}
```

TAG:

```
On id request with k slots {
    randomly select slot i;
    send id in slot i;
}

On data provided/requested {
    store/send data;
}
```


Dynamic Slotted ALOHA

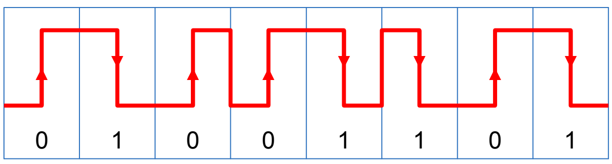
- How many time slots have to be reserved
  - Optimum: #time slots = #tags
  - To less: frequent collisions
  - To much: long waiting time
- Reader may dynamically increase number of slots if collision occurred: 1,2,4,8,16,…
- Break requesting ID when first ID is received correctly
- (Currently mute all tags which have been handled)

Deterministic Anti-Collision Schemes

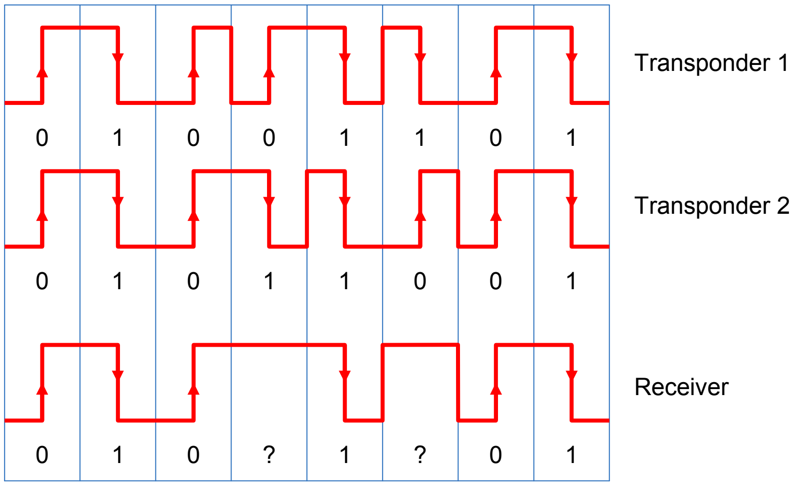
- ALOHA and its improvements are stochastic solutions
  - It remains a probability that tag are not found
- Are there deterministic solutions?
  - E.g. successively address each possible tag and wait for reply
    - Simple to implement
    - Scalability?
  - Binary tree search algorithm
  - Algorithms may reach 100% in theory

Manchester Code

- Deterministic algorithm described subsequently needs exact bit position of a collision
- Not possible with NRZ
- What about Manchester encoding?
  - Constant signal during a bit period not allowed



Manchester Coding and Collisions



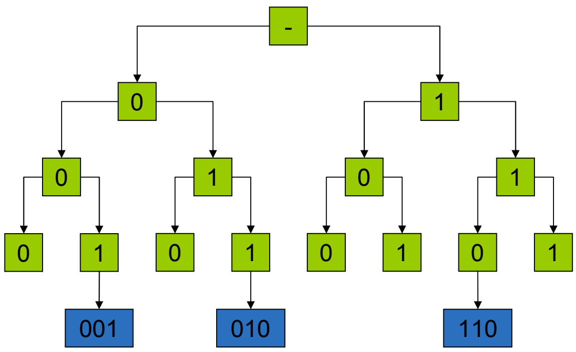
The Idea of the Binary Search Algortihm

- Simultaneously request IDs of all transponders
- Inspect bitwise collisions, e.g. 1X0X
- Set of all possible IDs {1000, 1001, 1100, 1101}
- At least one transponder ID is within {1000, 1001}
- Mute all transponders with ID >= 1100
- Request IDs of remaining transponders
- Suppose again collision 100X
- Remaining possible IDs {1000, 1001}
- Read data by explicitly addressing transponder 1000

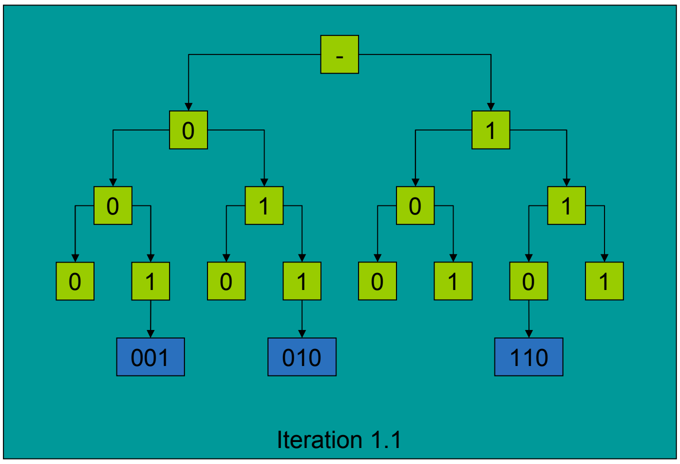
The Binary Search Algorithm

```
turn on all transponders;
request serial number x from all transponders;
while at least one transponder replied {
    while collision detected {
        determine leftmost collision bit in x;
        mute all transponders with that bit set to 1;
        request serial number x from remaining transponders;
    }
    request data from unique transponder x;
    turn off transponder x from further use;
    activate all muted transponder;
    request serial number from all transponders not turned off;
}
```

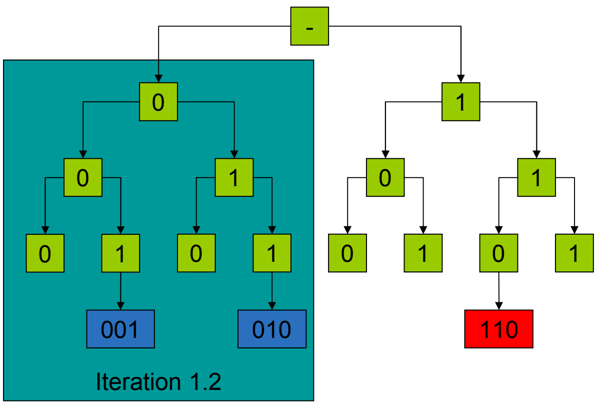

An Example of the Binary Search Algorithm



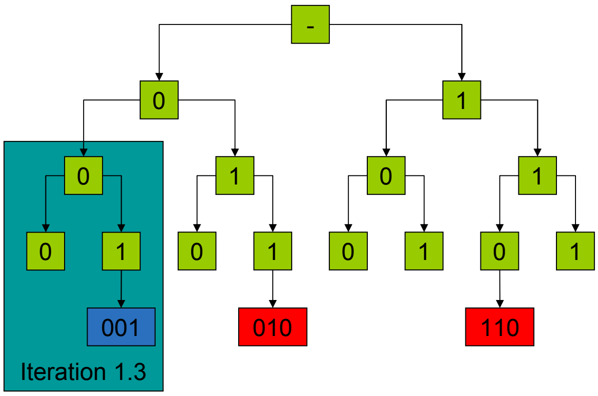
An Example of the Binary Search Algorithm



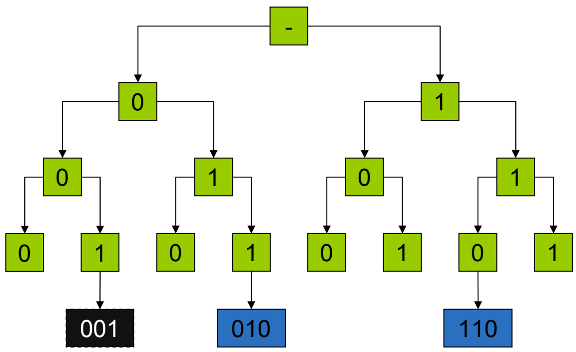
An Example of the Binary Search Algorithm



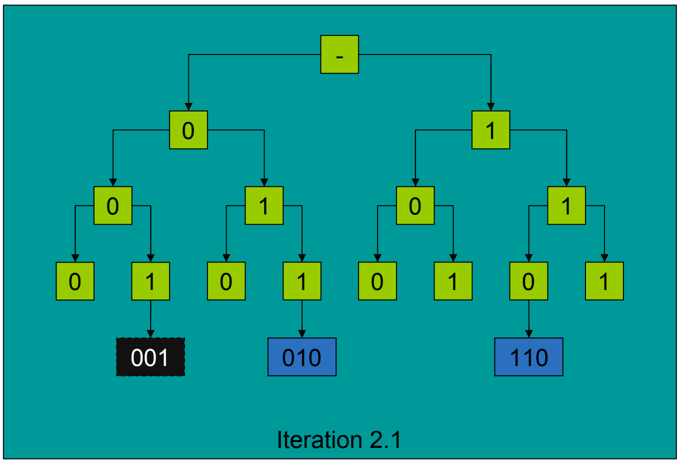
An Example of the Binary Search Algorithm



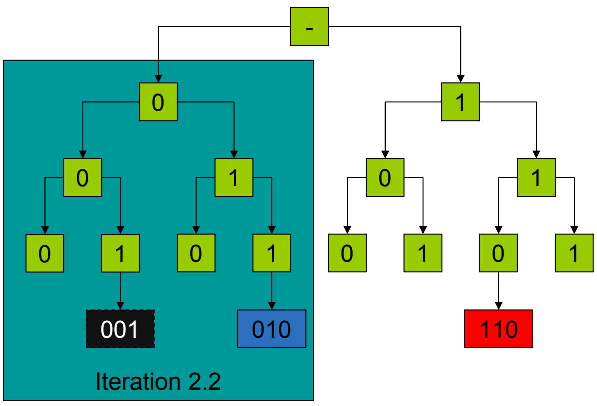
An Example of the Binary Search Algorithm



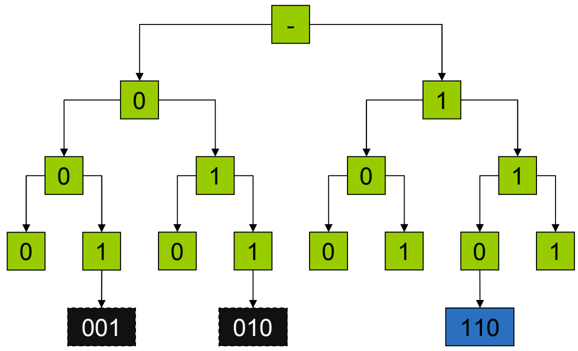
An Example of the Binary Search Algorithm



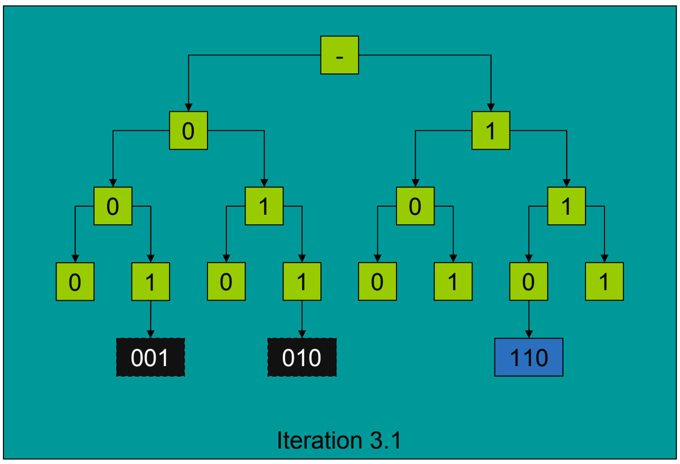
An Example of the Binary Search Algorithm



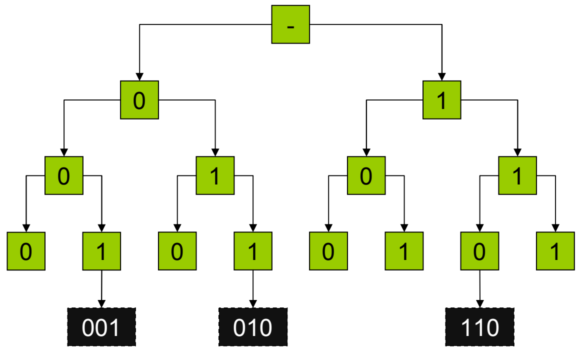
An Example of the Binary Search Algorithm



An Example of the Binary Search Algorithm



An Example of the Binary Search Algorithm



Dynamic Binary Search by Example

reader → transponder

- Iteration 1.1: request →
  - ← 10110010
  - ← 10100011
  - ← 10110011
  - ← 11100011
- Iteration 1.2: request | 10 →
  - ← 110010
  - ← 100011
  - ← 110011
- Iteration 1.3: request | 1010 →
  - ← 0011
- …

Possible Threats to RFID-Systems

- Unauthorized read out of data
  - In order to duplicate
  - Or modify data
- Using a faked tag in order to get unauthorized access
- Eavesdropping of a communication and replay of the sequence of signals

- Complexity of cryptographic functions increases production cost and communication cost
  - Not all applications need security (e.g. Industry automation)
  - Inversely forgoing security concerns may be critical in other applications (e.g. ticketing, wireless payment)

Mutual Symmetric Authentication

- Three Pass Mutual Authentication (challenge-response)
  - All tags and readers share the same common key K
    - Reader protects application of faked data
    - Tag protects its data for unauthorized read out

```
READER: send GET_CHALLENGE to TAG;
TAG:    create random number A;
        send A to READER;
READER: create random number B;
        encipher token T=(A,B,DATA) with K and send it to TAG;
TAG:    decipher received token T' with K;
        if A and received A' are not equal then break;
        create random number C;
        encipher token S=(C,B) with K and send it to READER;
READER: decipher received token S' with K;
        if B and received B' are not equal then break;
```

Properties of the Challenge-Response Protocol

- Shared Key is never transmitted
- Transmission of two random number avoids retransformation of tokens in order to get the key is not possible
- Any encryption algorithm may be used
- Replay attack is not possible due to creation of random number at both tag and reader
- Random numbers may be used as session key in subsequent communication

- Unfortunately, all devices share the same key

Solution: Derived Keys

- Each tag should use a different key
- During production of tag create key out of master key and transponder ID

- Reader asks for tag ID
- Reader calculates specific key from tag ID and master key
- Authentication as described above but using derived key

- Master key only stored in reader device!

Secure data transmission

- RFID technology uses private key cryptography
  - Streamcipher, Blockchiffre
- Streamcipher frequently used
  - One-time-pad would be the best
  - Pseudo-random generator used in practice to create the key
    - Session key as seed
  - Linear feedback register
  - Encipher by simple XOR calculation