Lightweight Cryptography for RFID Systems

Guang Gong

Department of Electrical and Computer Engineering
University of Waterloo
CANADA
<http://comsec.uwaterloo.ca/~ggong>

Outline of Tutorials

- Part I. Introduction to Security and Privacy of **Radio Frequency Identification** (RFID) Systems
- Part II. Design of **Lightweight** Crypto primitives
- Part III. **Design** of Authentication Protocols

Part I. Introduction to Security and Privacy of **Radio Frequency Identification** (RFID) Systems

- **RFID** Technology Overview
- **Physical** Layer of EPC Tags
- **Security** Threats in RFID System

RFID Technology Overview

RFID

Radio Frequency IDentification (**RFID**) is a method of remotely **identifying** objects or subjects using transponders (**tags**) queried through a **radio frequency** channel.

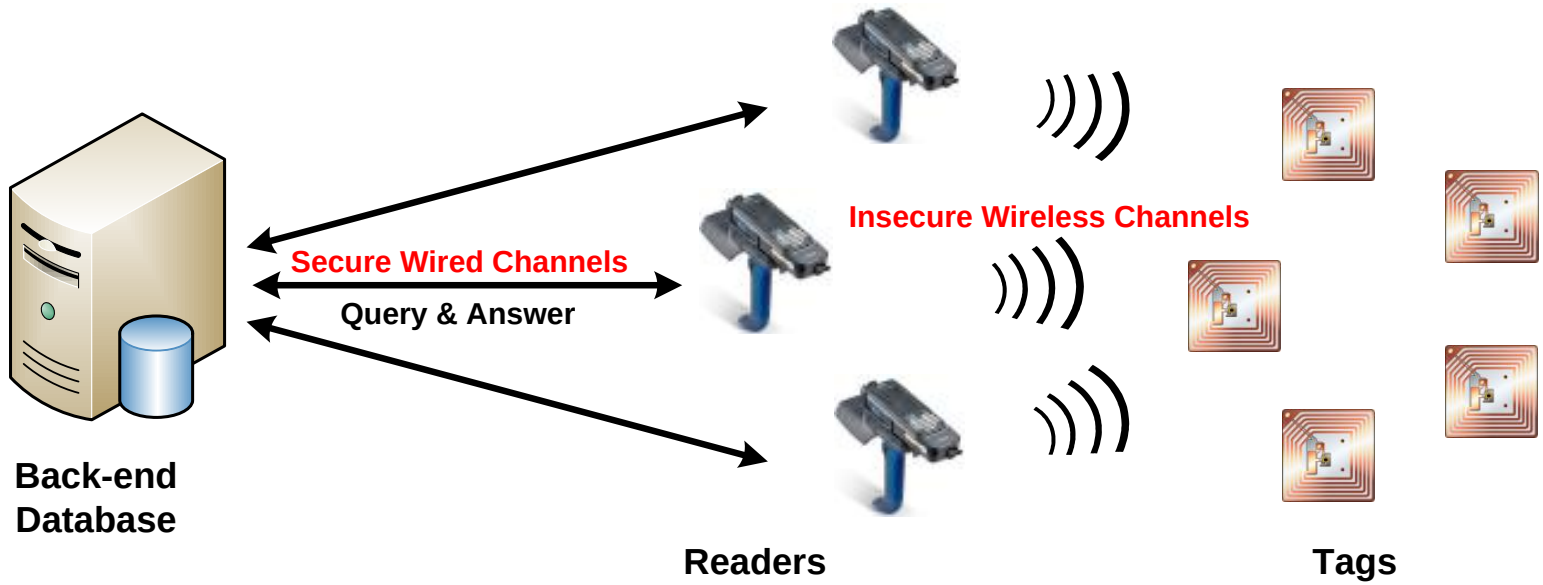


Figure: Radio Frequency Identification Architecture

Characteristics of RFID Systems

- The channels between the reader and the back-end database might be **wired channels** that are usually assumed to be secure.
- Both reader and back-end server are powerful enough to handle the overhead introduced by performing **strong** cryptographic protocols.
- The channels between the tags and the reader are **wireless links** and are therefore vulnerable to a variety of attacks.
- RFID tags usually have **constrained capabilities** in every aspect of computation, communication and storage due to the extremely low production cost.
- Each tag has a rewritable memory that might be susceptible to **compromise**.

Worldwide Adoption of RFID Technologies

Wal-Mart announced that they would require their top 100 suppliers to provide RFID tags on pallets and cases by 2006

Intel recently launched a pilot to track tagged cases of microchips as it packed and shipped them to an OEM customer

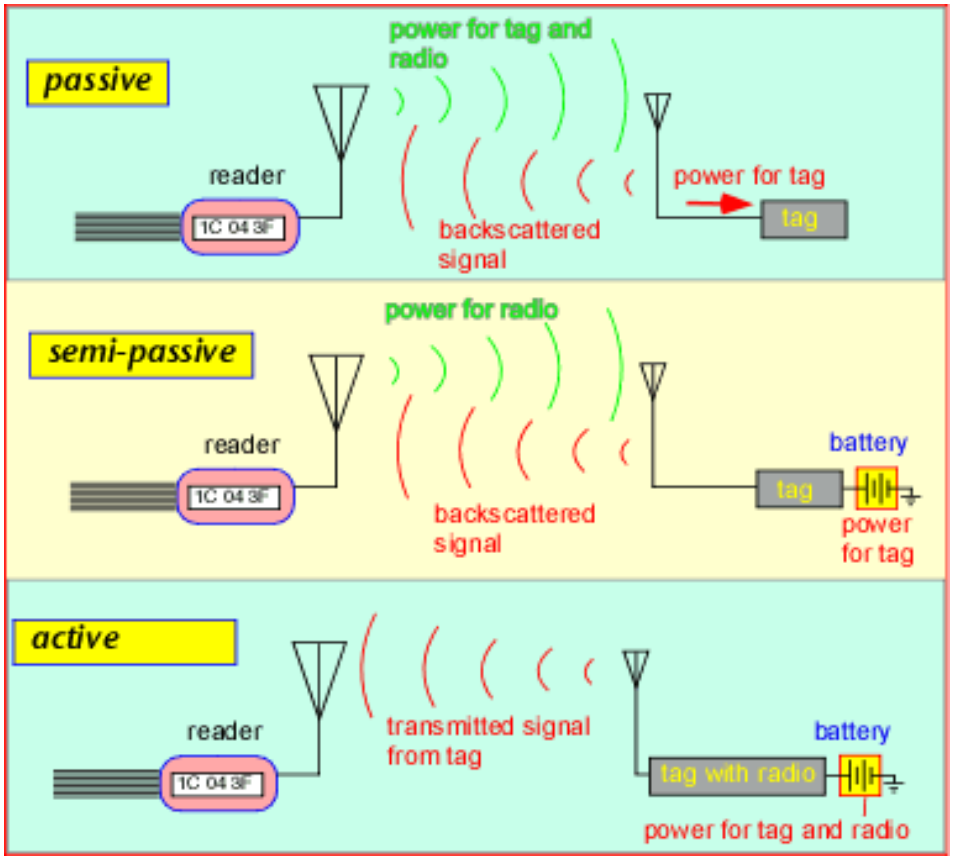
Air Canada used an innovative RFID system from Scanpak to slash unexplained losses and improve food cart utilization globally

Toll collection and contactless payment, i.e., **Oyster cards** in UK, i.e., **Electronic Road Pricing System** on Highway 407, Canada. E-Tickets used in **Olympic 2008** and **EXPO 2010**

Lucile Packard Children's Hospital uses RFID to track the location of its patients

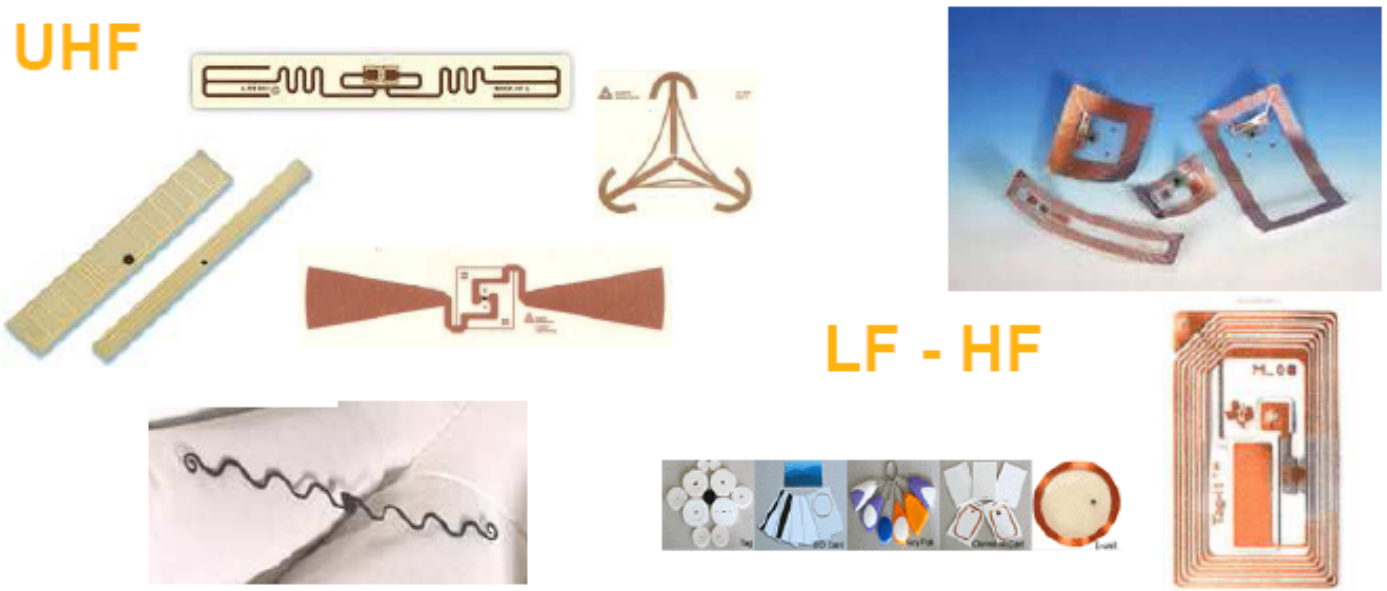
Tag Types (1)

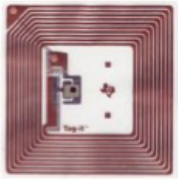
- **Passive Tags**
  - All power comes from a reader's signal
  - Tags are inactive unless a reader activates them
  - Cheaper and smaller, but short range
- **Semi-passive Tags**
  - On-board battery, but cannot initiate communication
  - More expensive, longer range
- **Active Tags**
  - On-board battery, can initiate communication
  - Very expensive, long range

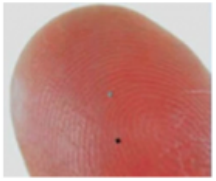


Tag Types (2)

	Low Frequency (LF) Tags	High Frequency (HF) Tags	Ultra High Frequency (UHF) Tags
Frequency Range	125 - 134 KHz	13.56 MHz	866 - 915 MHz
Read Range	10 cm	1 m	2 - 7 m
Applications	Smart Cards, Ticketing Animal tagging Access Control	Small item management Supply chain Anti-theft, library Transportation	Transportation vehicle ID Access/Security Large item management Supply chain



Active Tags

Semi-active Tags

Passive Tags

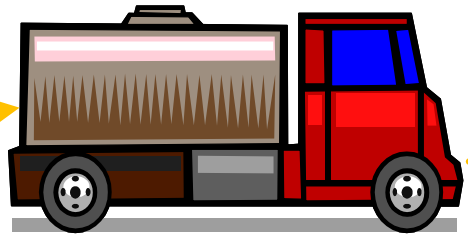
Our research focus on this!

A Typical Application – Supply Chain Management

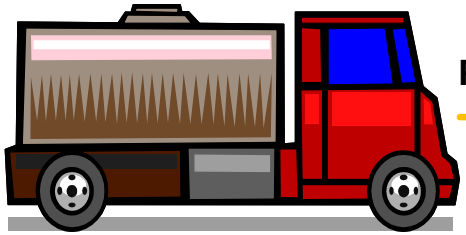
Order received, then released for picking

Pick & packed into a cargo container. RFID tag applied

The tagged cargo is detected as it passes through the shipping dock & ship confirmation is processed



Shipping



Receiving

The tagged cargo is detected as it passes through the receiving dock & Receipt is processed

EPC Tags (1)

- EPCglobal class-1 generation-2 (**EPC Gen2** in brief) was approved as **ISO 18000-6C** in July 2006.
- It is widely believed that Gen2 tags will be the mainstream for RFID application due to the large effective reading range.
- Four types of memory in EPC tags:
  - **Reserved memory**: Store passwords (32-bit) for access to other parts of the memory or to kill a tag.
  - **EPC memory**: Store EPC code (96-bit) which identifies the tag. This memory is locked.
  - **TID memory**: Store information that identifies the tag and its functionality (64-bit).
  - **User memory**: This is optional memory for extending functionalities of tags.

EPC Tags (2)

- The EPC standard specifies a restricted number of mandatory commands for the basic functionality of an RFID-enabled application:
  - **Select**: This command is used by the reader to select a subset of the tag population.
  - **Inventory**: These commands are used to establish communications between different tags and the reader.
  - **Access**: This set of commands allow the reader to functionally interact with a tag (see below).
    - Req_RN: Request the tag to return a 16-bit random number
    - Read: Read the memory on the tag
    - Write: Write to the memory on the tag
    - Kill: Permanently disable the tag
    - Lock: Lock the memory

Class 1 Generation 2 UHF Air Interface Protocol Standard

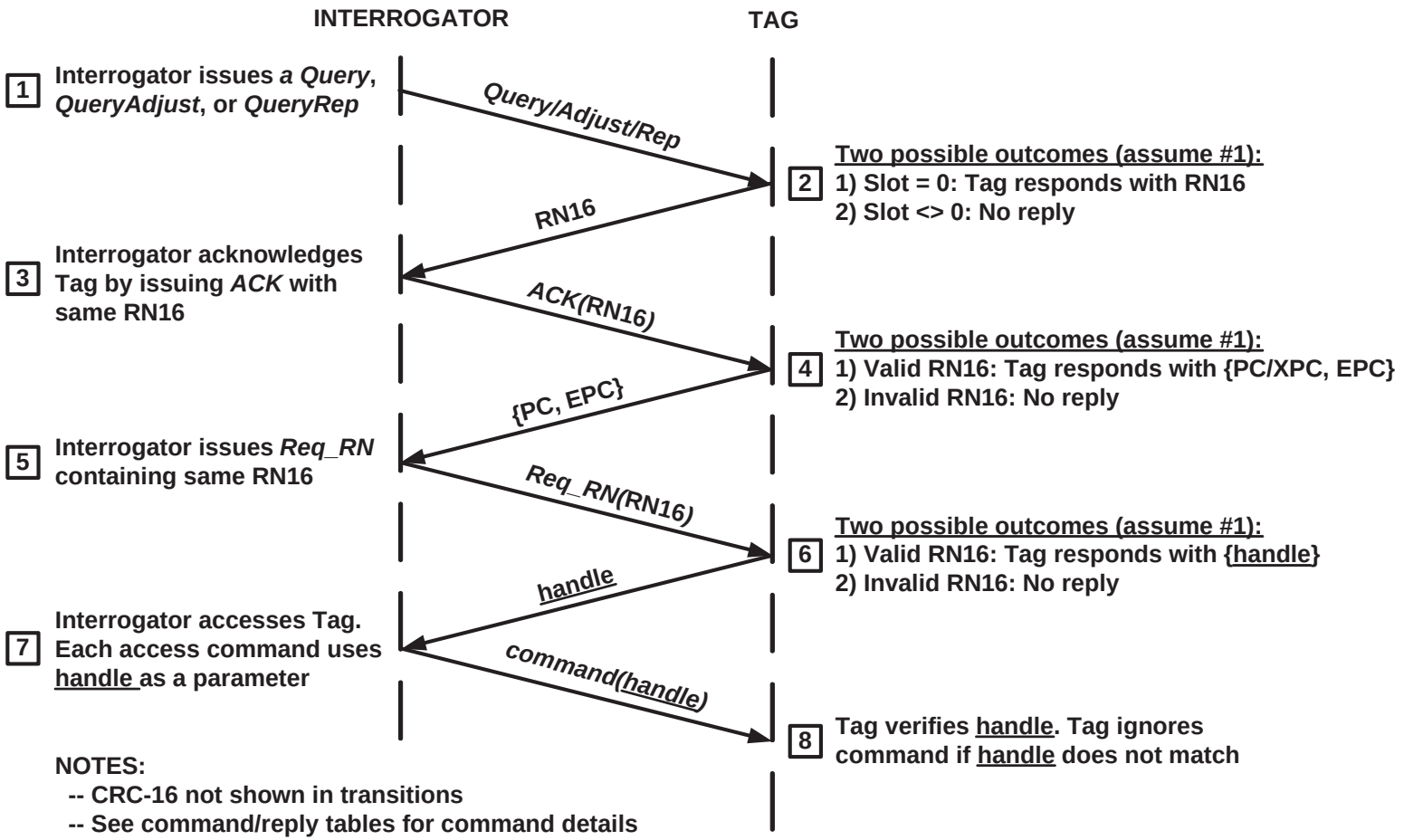
Take Class 1 Generation 2 UHF Air Interface Protocol Standard as an example

- It is a de facto standard for UHF passive RFID systems.
- It is developed by EPCglobal, which is the successor organization to the MIT Auto-ID Center.

This standard specifies:

- An air interface: the complete communication link between an reader and a tag.
- Two roles: the reader and the tag.
- Physical layer:
  - signal design
  - data-coding methodology
  - command-response structure

How a Reader interrogates a Tag?



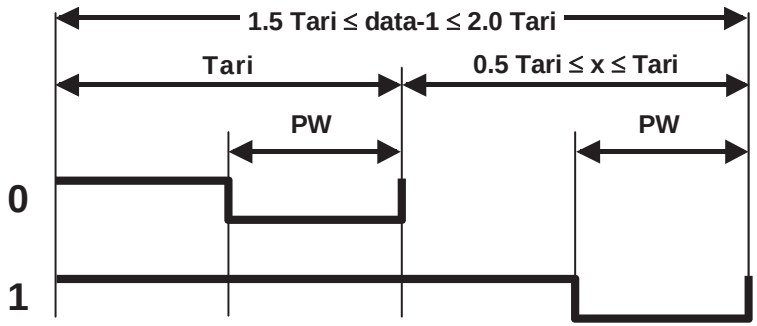
- Note that security and privacy are not considered!

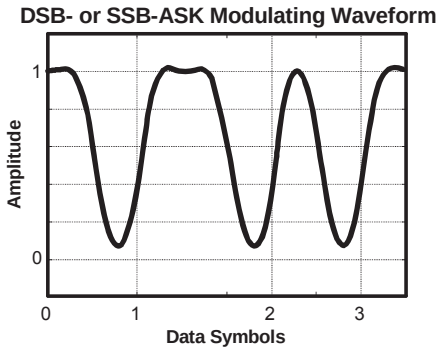
Physical Layer of EPC Gen2 Standard

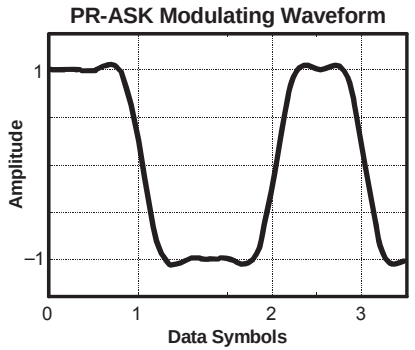
Reader⇒Tag Coding and Modulation

Reader⇒Tag

- Pulse-Interval Encoding: in the right plot, Tari is in 6.25μs to 25μs. e.g., a message “010" is encoded as “10 1110 10".
- The encoded data is modulated by DSB/SSB-ASK, or PR-ASK modulation, e.g., given “10 1110 10" as the baseband signal, the modulated signal is shown in the left plot.



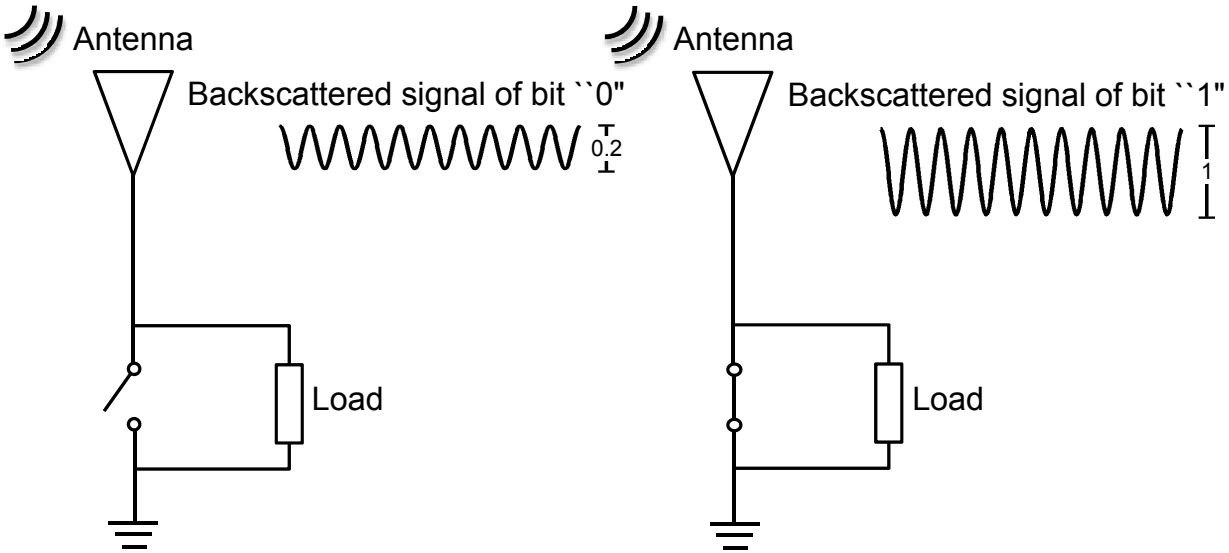




Tag⇒Reader: Backscatter Modulation

Tag⇒Reader

Tag switches the reflection coefficient of its antenna between two states in accordance with the data being sent. The backscattered signal is modulated by Amplitude Shift Keying (ASK), which allows the establishment of a communication.



Tag⇒Reader: Manchester-like Coding

FM0 or Miller is employed in order for the reader to detect collision when multiple tags response simultaneously. e.g.,

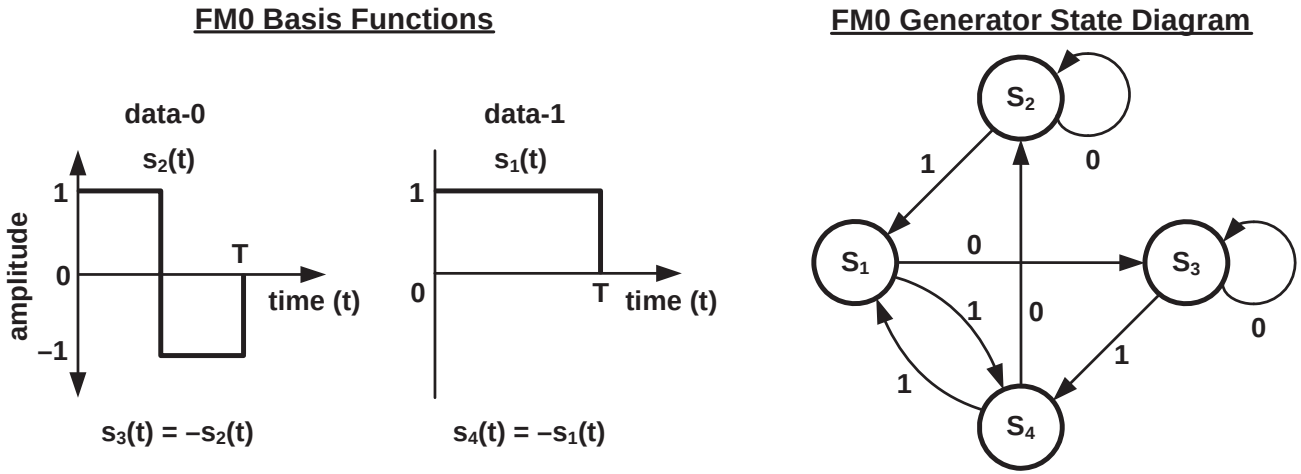
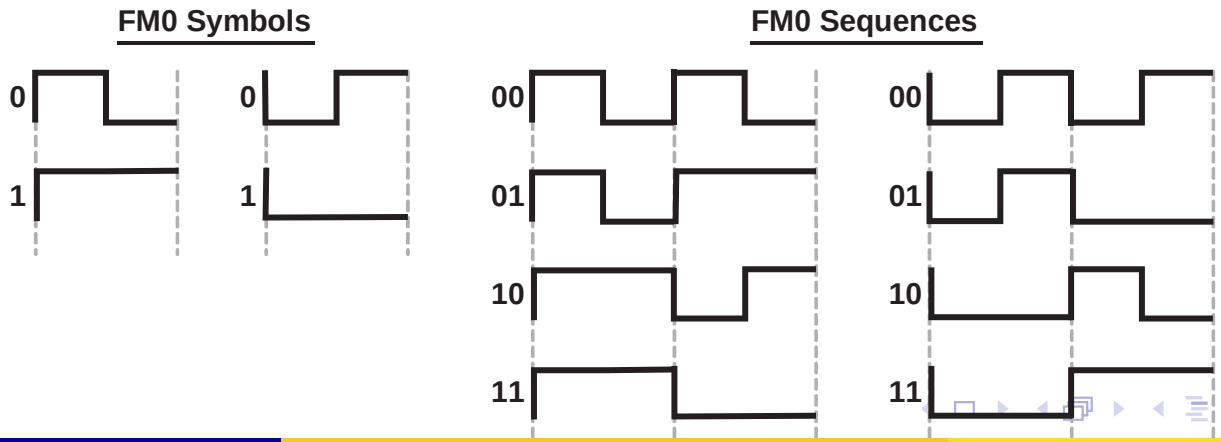


Figure 6.8 – FM0 basis functions and generator state diagram

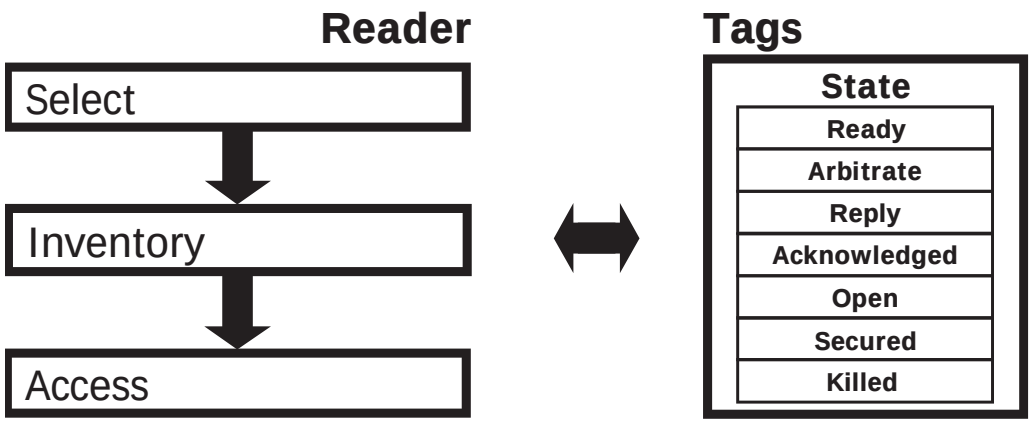


Tag Identification Layer of EPC Gen2 Standard

Operations, Commands, States

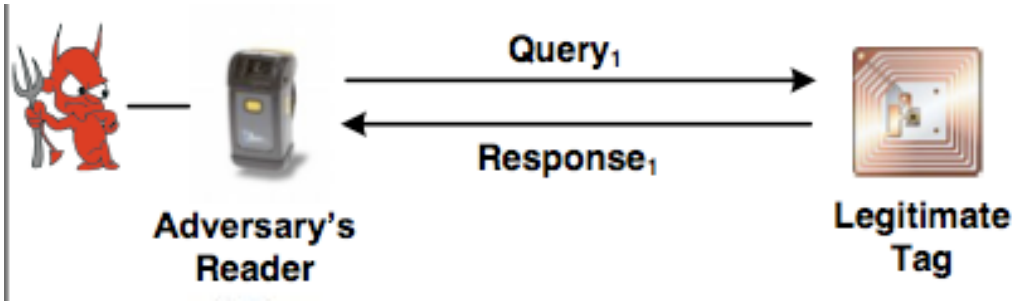
Readers manage tags using three basic operations:

- Select: Reader selects individual tags from the population.
- Inventory: Reader identifies tags.
- Access: Reader transacts with individual tags, e.g., read their memories.
- Tags can be viewed as a finite state machine.



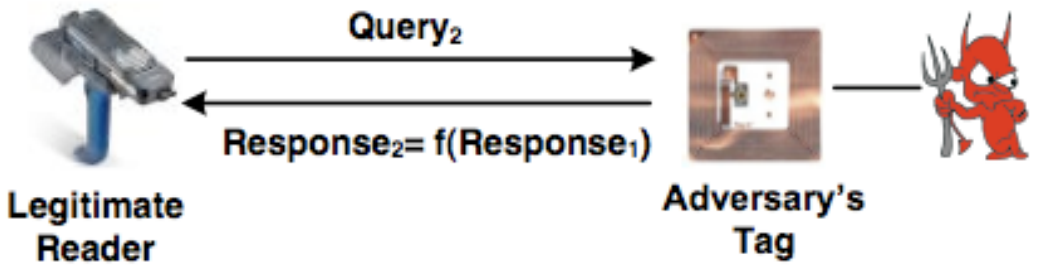
Attacks on Tags: Privacy Violation

- RFID technology raises two main **privacy concerns** for users: clandestine physical tracking of tags and inventorying of tags.
- Misbehaving readers harvest information from well-behaved RFID tags.
- **Since RFID tags** automatically respond to the interrogation from the reader without alerting the bearer/owner, a person carrying an RFID tag is prone to clandestine physical tracking.
- **Consequently**, an adversary equipped with commodity RFID readers can effectively trace a person carrying a tagged item by linking different sightings of the same RFID tag.
- In addition, in **supply chain** applications, individually tagged objects in stores allow competitors to learn about stock turnover rates (inventorying).



Attacks on Tags: Authentication Problem

- **RFID authentication** focuses on the problem of well-behaved readers receiving information from misbehaving tags (e.g., counterfeit tags).
- **Basic RFID tags** (e.g., Gen2 type) are vulnerable to simple counterfeiting attacks or cloning attacks. An attacker can skim the electronic product code (EPC) from a target tag and then program it into a counterfeit tag.
- **Authentication** is an important issue when RFID tags are used for access control or as security devices to detect counterfeit products such as medicines, electronics accessories, and other high-value items.
- **In general**, today's RFID systems do not conduct mutual authentication between RFID readers and tags, so it is easy for an adversary to impersonate a tag to obtain all of its secret information and then clone new tags.



Communication Attacks

- **Many possible** security threats arise from unprotected wireless communication between RFID readers and tags.
- **Examples** include
  - Spoofing and replay
  - Eavesdropping
  - Jamming
  - Traffic analysis

Countermeasures

Physical Protection	Distance measurement, Faraday cage approach
Deactivation	Killing, sleeping, hash lock
Re-naming	Relabeling or effacing, minimalist cryptography, re-encryption
User-Oriented	Light Crypto based approaches
Proxy Or Filter	Watchdog tag, RFID guardian
Jamming	Blocking, soft-blocking tag
Entity authentication	PRG-based, hash-based, private authentication

Performance Requirements

- **Low Computational Cost**: The computational overhead of authentication protocols in the tag side should be small due to the limited power available to RFID tags.
- **Low Communication Cost**: The message transmitted in the authentication phase should be minimized because of the limited bandwidth available to RFID tags.
- **Low Storage Requirement**: The data stored in a RFID tag should be kept as small as possible since the tag memory is extremely constrained.
- **Scalability**: The back-end database should be able to efficiently identify an individual tag even though the tag population is huge.