TECHNICAL UNIVERSITY OF CRETE

DEPT. OF ELECTRONIC AND COMPUTER ENGINEERING

ELECTRIC CIRCUITS AND RENEWABLE ENERGY SOURCES LAB.

SECURITY AND PRIVACY OF PASSIVE LOW-COST RFID SYSTEMS

Athanasios Andrianakis

CHANIA 2012

ΠΟΛΥΤΕΧΝΕΙΟ ΚΡΗΤΗΣ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΕΡΓΑΣΤΗΡΙΟ ΗΛΕΚΤΡΙΚΩΝ ΚΥΚΛΩΜΑΤΩΝ ΚΑΙ ΑΝΑΝΕΩΣΙΜΩΝ ΠΗΓΩΝ ΕΝΕΡΓΕΙΑΣ

ΑΣΦΑΛΕΙΑ ΚΑΙ ΙΔΙΩΤΙΚΟΤΗΤΑ ΣΕ ΠΑΘΗΤΙΚΑ ΣΥΣΤΗΜΑΤΑ RFID ΧΑΜΗΛΟΥ ΚΟΣΤΟΥΣ

Αθανάσιος Ανδριανάκης

Επιτροπή: Κωνσταντίνος Καλαϊτζάκης (Επιβλέπων)
Διονύσιος Πνευματικάτος
Ευτύχιος Κουτρούλης

ΧΑΝΙΑ 2012

Abstract

In 2012, we are in a decade where Radio Frequency Identification (RFID) systems are becoming ubiquitous, slowly but surely replacing its old ancestor: the Barcode. With the RFID come many advantages such as faster and continuous control of retailing or along the supply chain, as well as better localization and monitoring of items. However, all these benefits require increased security of the systems, especially in applications where information is quite sensitive, such as pharmaceutics and military. Furthermore, the privacy aspect involved with this technology could become a major issue in the perspective of a global adoption. In the past few years, an increasing number of researchers concentrate their efforts into improving the security for RFID systems. Implementing high-security cryptographic primitives in such systems require increase of the tag's cost, which makes it prohibitive for wide-scale use.

In this work, we focus on the security and privacy of low-cost RFID systems working on the UHF frequency band. An initial study and analysis of the state of the art identifies the need for lightweight cryptographic solutions suitable for such constrained devices. From a theoretical point of view, standard cryptographic solutions (hash functions, message authentication codes, block/stream ciphers, etc.) may be a correct approach. However, they are quite demanding in terms of circuit size, power consumption and memory size, so they make costly solutions for low-cost RFID tags. Lightweight cryptography is therefore a pressing need.

This work is organized as follows: In chapter 1, we analyze the basic principles of an RFID system and things to consider when building such a system. In chapter 2, we summarize related works on security threat classification, as well as proposals over security and privacy of UHF RFID systems. In chapter 3, we present our experiments' results on the evaluation of a commercial RFID system. In chapter 4 we present the proposals of our work, first on the simple classification of RFID security and privacy threats and the proposals over them, and second, a software which enables faster, automated and more detailed evaluation of an RFID system. In chapter 5 we present some results of the evaluation using our software, some of which are related to the security mechanisms currently available on commercial RFID system. Finally, in chapter 6 we conclude that the research for improving security of RFID systems still has some nice days ahead, and remains an open research topic, and we refer possible future work in order to extend our current work.

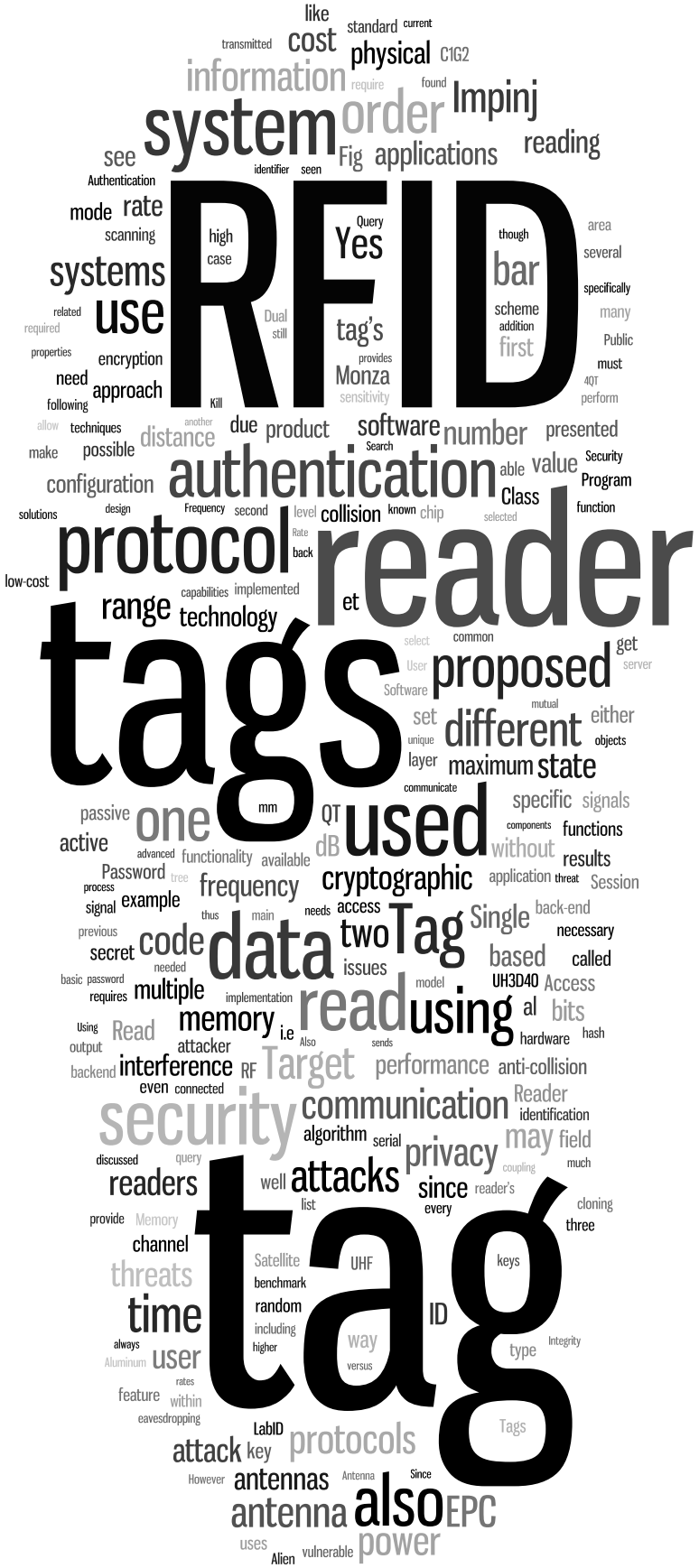
like
standard
current
transmitted
cost
physical
C1G2
information
require
found
Impinj
system
order
reading
see
Fig
applications
identifier
seen
Authentication
RFID
mode
rate
Query
Yes
though
area
scanning
high
case
several
systems
bar
specifically
use
Dual
still
tag's
scheme
addition
many
related
required
first
Public
properties
encryption
provides
must
need
Monza
4QT
approach
sensitivity
perform
following
Kill
another
allow
techniques
due
product
software
number
presented
distance
make
possible
Search
authentication
able
value
Security
configuration
Class
Program
solutions
design
Frequency
second
level
collision
known
chip
selected
function
protocol
reader
Rate
back
low-cost
capabilities
implemented
et
range
technology
tags
select
common
get
User
proposed
server
Software
mutual
set
different
either
unique
objects
layer
maximum
state
communicate
specific
signals
passive
one
mm
QT
used
components
functions
active
dB
without
advanced
functionality
available
results
Password
tree
cryptographic
application
threat
Session
process
frequency
signal
example
thus
main
needs
access
Tag
Single
back-end
previous
two
necessary
secret
code
data
based
called
needed
issues
basic
password
model
UH3D40
Access
requires
multiple
implementation
read
using
al
bits
Using
Read
memory
i.e
hardware
hash
output
attacker
Also
sends
backend
interference
RF
Target
performance
anti-collision
even
connected
Reader
security
communication
identification
algorithm
serial
may
field
discussed
query
privacy
coupling
much
readers
well
attacks
since
reader's
list
every
cloning
provide
Memory
three
channel
Satellite
UHF
keys
threats
benchmark
random
ID
time
including
way
always
higher
type
Integrity
Aluminum
user
versus
rates
feature
within
eavesdropping
Tags
LabID
attack
key
protocols
However
antennas
Antenna
Since
antenna
also
EPC
uses
Alien
vulnerable
power

Table of Contents

1 Radio Frequency Identification 1

1.1 Applications 1
1.2 RFID components 3
1.2.1 Tags 3
1.2.2 Interrogators 4
1.2.3 Backend System 4
1.3 Technical Principles 5
1.3.1 Frequency 5
1.3.2 Coupling 7
1.3.3 Field Propagation 8
1.3.4 OSI Model 8
1.3.5 Standardization 9
1.3.6 Anti-Collision 10
1.4 Optical Identification: Barcode 13
1.4.1 What is a Barcode? 13
1.4.2 RFID versus Barcode 14
1.4.3 RFID as the Barcode successor 15

2 Related work 17

2.1 Classification of the RFID Security and Privacy threats 17
2.2 Proposals over RFID Security and Privacy 19
2.2.1 Serial Numbering 19
2.2.2 Hash Lock 20
2.2.3 Challenge-Response Protocols 22
2.2.4 Ultralightweight Cryptography 24
2.2.5 Binary Tree-Walking 25

3 Evaluation 27

3.1 Antenna Mapping 28
3.2 Read Rate versus Tag-Antenna Distance 33
3.3 Tag performance on objects of different materials 34
3.4 Tag interference 35
3.4.1 Stack of Tags 36
3.4.2 Array of Tags 36
3.5 Read range versus Antenna Output Power 38
3.6 Tag reading sequence 41
3.7 Antenna Power Output versus Power Consumption 42

4 Security & Privacy 43

4.1 Components of networking security 43
4.2 Security Threats 44
4.2.1 Hardware Components 45
4.2.2 Communication 47
4.3 Maximum security mechanisms commercially available 49
4.3.1 EPC Class-1 Generation-2 Protocol 49
4.3.2 Impinj QT Technology 50

4.4 The Competing Objectives 52
4.5 Improving Security & Privacy 53
4.5.1 RFID tags without Cryptographic capabilities 53
4.5.2 RFID tags with Cryptographic capabilities 56
4.6 Evaluation Software 60
4.6.1 Query Reader State 62
4.6.2 Query Tags 62
4.6.3 Query Tag Access/Kill Password 64
4.6.4 Program Reader Settings 65
4.6.5 Program Tag EPC 65
4.6.6 Program Tag Public EPC 66
4.6.7 Program Tag Access/Kill Password 67
4.6.8 Program Tag User Memory 67
4.6.9 Program Tag QT Profile 68
4.6.10 Lock/Unlock Memory bank 69
4.6.11 Benchmarks 69

5 Results 71

5.1 Tag Shielding 71
5.2 Randomized (Re)Encryption 71
5.3 Password Lock 73
5.4 Ultralightweight Mutual Authentication Protocols 74
5.5 Tag read rate 75

6 Conclusions 83

References 85

Table of Figures 89

1 Radio Frequency Identification

Radio Frequency Identification (RFID) is a well-known AIDC (Automatic Identification and Data Capture) technology to provide the benefits including contactless read, long transmission range and transaction time saving. Since World War II, it is being used in automatic identification and tracking of almost anything, from objects to humans and animals. Back in 1940s, it was used in detecting friendly aircrafts (known as Identification Friend or Foe, IFF [1], [2]), while during the latest years it is being used in order to identify almost any kind of –moving or not– physical object.

RFID technology works well in harsh or dirty environment, and requires neither physical, nor visual contact between the antenna and the object to be identified. This gives it many advantages over existing machine-readable identification techniques, such as barcodes. However, unlike barcodes and other consumer labeling techniques, RFID tags record a sufficiently long bit-string to uniquely identify specific product units, such as the bottle of a medicine sold to a particular patient. Another important feature of RFID tags is that they can be read efficiently at a distance of a few inches to several feet (depending on the technology). Both of the above-mentioned features present potential benefits to consumers, retailers and manufacturers. For instance, RFID tags can be read faster than barcode tags since unlike the latter, they do not require precise reader-tag alignment, making inventory management more efficient. Similarly, the unit-specific feature of RFID tags allows for finer inventory control by, for instance, supporting automated verification of expiration dates.

The motivation behind the pervasive use of RFID systems is the need to fully automate remote tracking and identification of objects by embedding cheap and low power RFID tags in the objects.

1.1 Applications

The flexibility of RFID technology holds great promise for novel applications, and increasingly RFID tags are being deployed in situations where their proper operation must be assured to a medium or high level of confidence.

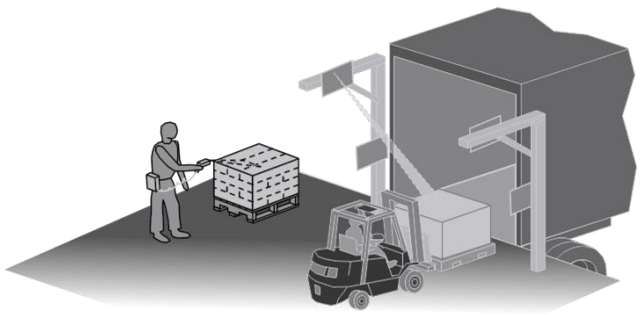

Figure 1.1 – Typical RFID Application

Currently, RFID systems are being used in a variety of application areas, such as Access Control, Retailing and Tracking, while with the upcoming of *NFC technology*, which allows embedding RFID readers in commercial mobile phones, the number of RFID based systems will increase dramatically.

- **Access Control**

  Truly hands-free and unencumbered access to places like controlled parking lots and offices. One of the most famous uses of RFID access control during the latest years is the widely-known anti-theft system in automotive industry, known as *immobilizer*. Popular Access Control applications of RFID include:
  - Vehicle Immobilizer
  - Automation
  - Security
  - Transportation
  - Surveillance

- **Retailing**

  Inventory management is the most widely used application of RFID technology since 2005 (see Wal-Mart [1]). Industry and retailers save money by enhanced automation of fabrication and warehousing. Popular Retailing applications of RFID include:
  - Transactions
  - Inventory Management
  - Stock Management
  - Supply Chain
  - Warehouses
  - Manufacturing

- **Tracking**

  Consumers can also take advantage from goods being able to communicate their environment (e.g. washing machine communicates with clothes, milk packs communicate with refrigerator). Popular Tracking applications of RFID include:
  - Baggage Handling
  - Wildlife Monitoring
  - Livestock
  - Timing
  - Asset Tracking
  - People tracking
  - Athletics
  - Medical

1.2 RFID components

The main components of a basic RFID system are the tag (transponder), the interrogator (transceiver), and the backend system/database (Fig. 1.2).

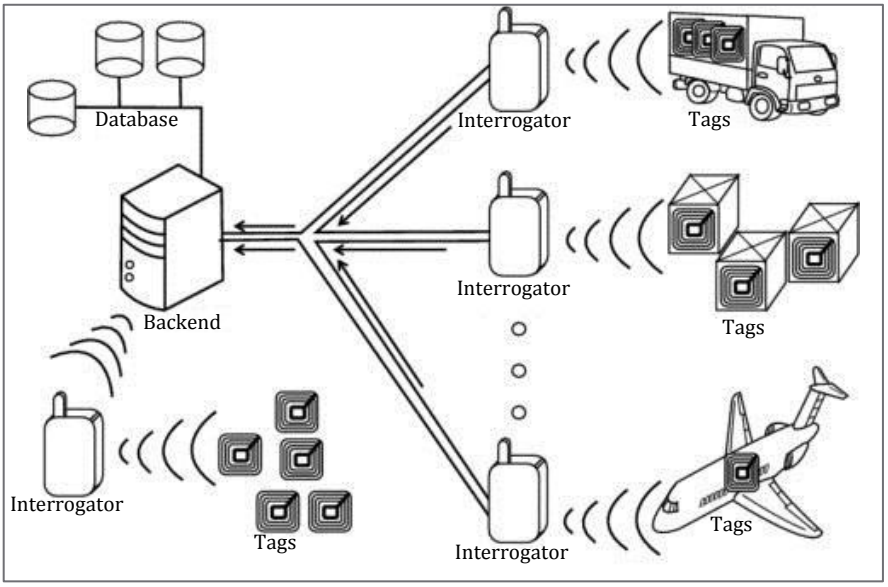

Figure 1.2 – RFID System Components

1.2.1 Tags

RFID tags are used to identify any object. They consist of the integrated circuit, the antenna, and the printed circuit board. The antenna is responsible for receiving and sending signals from/to the interrogator whether these are translated into energy in order to power up the tag, or they are used for exchanging information with the interrogator (described below). The Integrated Circuit (IC) is responsible for storing the tag's data, including its unique tag ID, and for processing the signals received/sent. The printed circuit board is used to hold the tag's components together, as well as any additional tag circuitry/components such as battery and sensors; thus, circuitry is only available in more advanced tags. RFID tags are classified into four main categories: passive tags, active tags, semi-passive tags and semi-active tags. They are also classified depending on the read/write capabilities of their IC (Table 1.1).

Class	Function	Features	Memory	Range
Class 0	Passive	Read Only	-	< 25m
Class 1	Passive	Write Once	-	< 25m
Class 2	Passive	Read, Write	< 64kb	< 25m
Class 3	Semi-Passive	Read, Write	< 64kb	< 100m
Class 4	Active	Read, Write	> 64kb	< 1000m
Class 5	Active-Reader	Read, Write	> 64kb	< 1000m

Table 1.1 – RFID tag classification

- **Passive tags**

  Passive tags are the most widely used ones, because of their low cost and reduced size. They are passively powered by the interrogator's radio frequency waves, which also leads to reduced range (only when compared to active tags, since currently there exist passive tags with read range of over 20 meters) and reduced processing power.

- **Active tags**

  Active tags are battery powered, which makes them much more expensive than passive ones, and they have range of several hundred feet. Their basic disadvantages are their increased size, weight and cost, and the need of maintenance (such as replacing the battery). Also, since active tags aren't powered by RF signals, they send signals at a fixed rate (called beacon rate) which ranges from sub-second to several minutes according to application or battery life needs.

- **Semi-passive tags**

  Semi-passive tags are a combination of active and passive tags. Their RF circuit is powered by the interrogator's RF signals, while they integrate a battery which is used to power the rest of their circuitry, most likely sensors. Semi-passive tags are cheaper than active ones, but still more expensive than passive ones. Their cost and size are also in between then ones of passive and active tags. Since this kind of tags use the power absorbed from RF signals only for transmissions and not for data processing, their range is higher than passive ones. Also, the battery is used to power their circuitry only when they receive RF signals, which leads to extended battery life when compared to active tags.

- **Semi-active tags**

  Semi-active tags behave like active tags, with the difference that they only transmit when they are in range of an RFID antenna. This means that semi-active tags do not have a beacon rate, which also leads to extended battery life when compared to active tags. In every other way, they work just like active tags.

1.2.2 Interrogators

RFID interrogators (also known as readers) are used to send energy to RFID tags and exchange data with them, all by transmitting RF waves at a specified frequency. First, the radio waves are used to power on the tag (except when using active tags), which then responds with its data. Then the communication proceeds according to the protocol used. Factors that affect the interrogator's range include: output power (or antenna gain), receiving sensitivity, frequency, and orientation/polarization of both interrogator and tag antennas. Multiple interrogators can be connected on the same system to improve coverage if necessary. Interrogators may also provide initial data processing before forwarding them to the backend system.

1.2.3 Backend System

The backend system is the part of the RFID system that receives and processes data received from the interrogators according to the application. It usually consists of one or more computers, connected on the same network so that they can share their data with each other. Interrogators are usually connected to the backend system either directly via serial RS232 or USB, or via Ethernet. When an RFID tag is in range of an interrogator, it can be read multiple times within a second, which is most of the times useless. The backend system is responsible for controlling how many times a unique tag will be processed within a limited time frame.

1.3 Technical Principles

This chapter discusses the technical principles that readers and transponders utilize to couple and exchange energy and data. These relay on the frequency, coupling method, field propagation and the standard that will be used. This also discusses the communication scheme behind RFID as well as the handling methods when multiple tags are scanned simultaneously.

1.3.1 Frequency

Most RFID systems operate in the Industrial Scientific Medical (ISM) bands, which are freely available to low-power, short-range systems. These bands are defined by the International Telecommunications Union (ITU). In Europe, they are defined by the European Telecommunications Standards Institute (ETSI), while in the United States of America they are defined by the Federal Communications Commission (FCC) (Table 1.2) [3].

Band	Europe	USA	Range
Low Frequency (LF)	125 - 135 kHz		< 0.5m
High Frequency (HF)	13.56 MHz		< 1.5m
Ultra High Frequency (UHF)	865 - 868 MHz	902 - 928 MHz	< 1km
Microwave (µW) (Low)	2.4 GHz		< 1km
Microwave (µW) (High)	5.8 GHz		< 1km

Table 1.2 – RFID Frequency Bands

Figure 1.3 displays the influence characteristics along each frequency band.

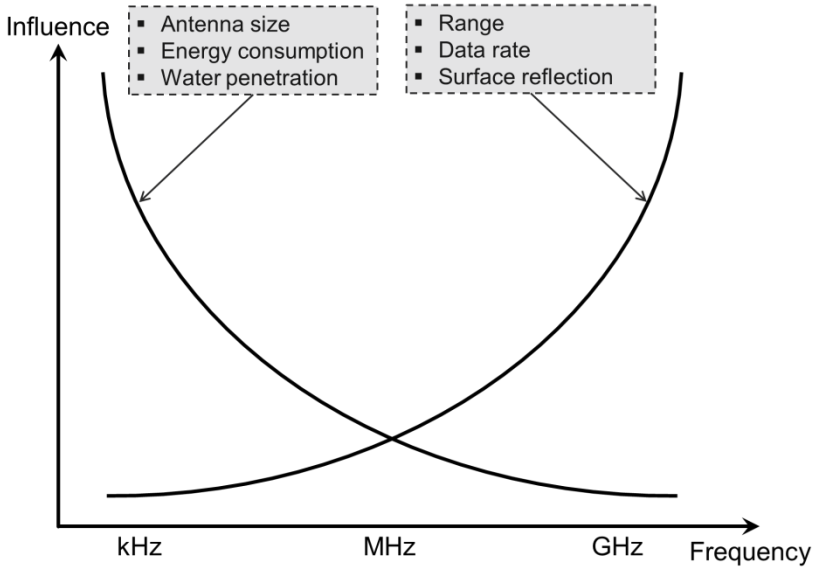

Figure 1.3 – Frequency Influence

Devices operating in each band are subject to different power and bandwidth regulations. For example, systems operating in the HF band are limited to a bandwidth of 14 kHz in the forward channel. The backward channel may use a greater bandwidth, since it has much lower power. In contrast, the 915 MHz ISM band is less restricted and several options are available for reader-to-tag communications. The option that provides the longest read range requires the reader to "hop" among 50 channels every 400ms, each with up to 260kHz of bandwidth (Fig 1.4), thus providing a maximum read rate of 1200 reads/second currently. In Europe these numbers drop

down to 15 channels (5 of which are limited to only 25mW, thus usable only for the backward channel), each with up to 100kHz of bandwidth (Fig. 1.5), thus capable of only 600 reads/second. This is a trade-off, since tags cannot be guaranteed continuous communication across a frequency hop. As a result, reader/tag communications must be limited to 400ms. Transactions must be completed within this period; otherwise they will be interrupted by a frequency hop [3].

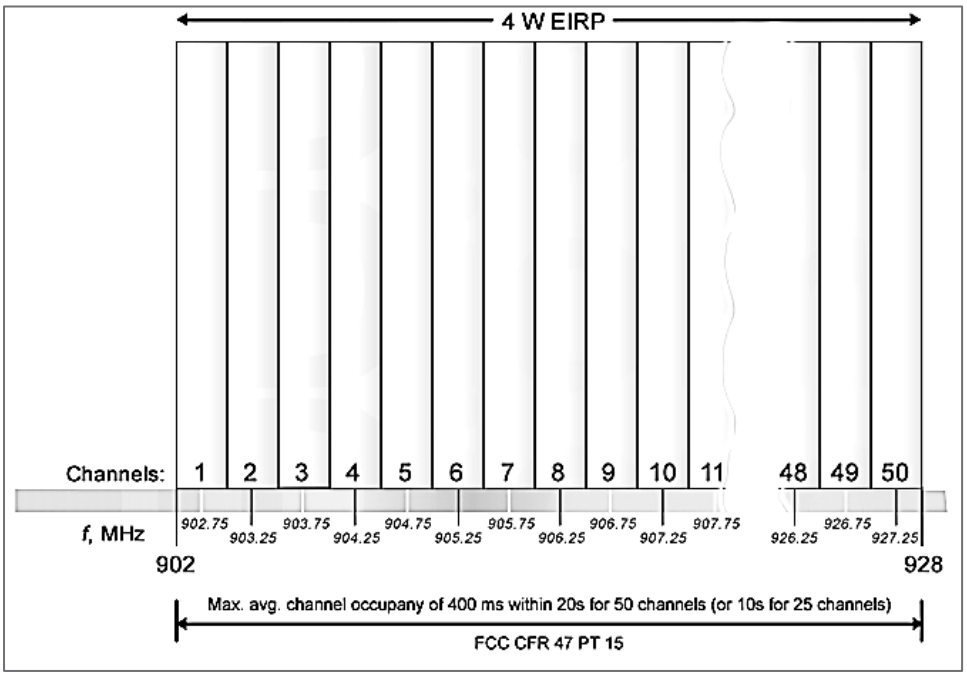

Figure 1.4 – FCC Channels & Power limits

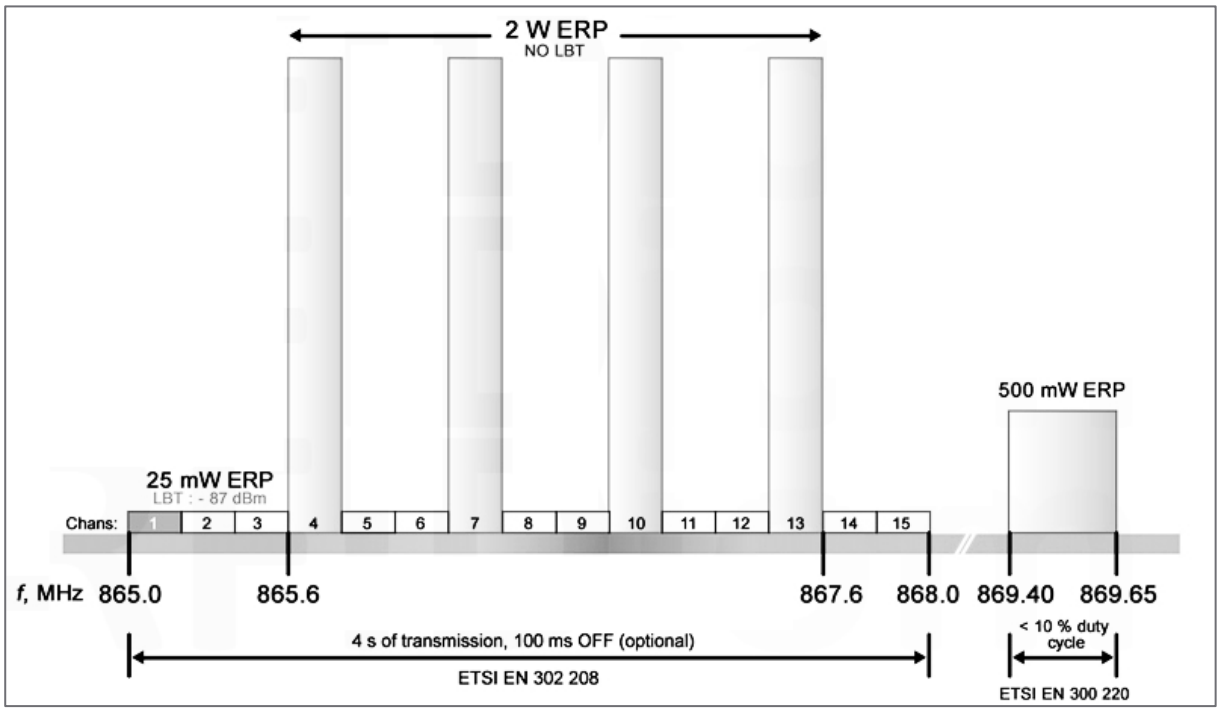

Figure 1.5 – ETSI Channels & Power limits

1.3.2 Coupling

Depending on the tag type, there are two coupling mechanisms between the tag and the interrogator [1]:

- **Inductive coupling**

  Inductive coupling is based on electromagnetic induction, mostly used in the LF and HF frequency bands (Fig. 1.6). The distance between the coils must be kept within the range of the effect - normally this is taken to be about 0.15 wavelength of the frequency in use. Inductively coupled tags are almost always operated passively, which means that the interrogator provides all the energy needed for the operation of the tag's IC.

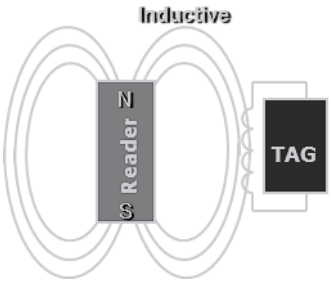

Figure 1.6 – Inductive coupling

- **Modulated backscatter coupling**

  Backscatter coupling uses the RF power transmitter by the reader to energize the tag. Essentially it "reflects" back some of the power transmitted by the reader, but changes some of the properties, and in this way it sends back information to the reader. Backscatter coupling operates outside the near field region so it is mostly used in UHF and μW frequency bands (Fig. 1.7). Over short ranges, the amount of power reaching the tag from the reader is sufficient to allow operation of small low current circuits within the tag. In order to allow transmission and reception of a signal at the same time, a directional coupler is often used to allow the received signal to be separated from the transmitted on. Additionally the reader must be able to detect the modulation in the presence of a host of other reflections, although these will normally be stable and not modulated in any way. Backscatter coupling subdivides into two more types: transmitter and transponder.

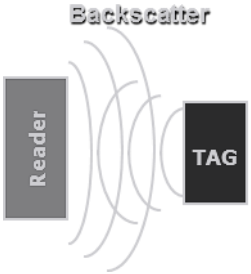

Figure 1.7 – Backscatter coupling

- **Transmitter (beacon) type**: This type of coupling is used in active RFID tags, in which a beacon transmits a signal with its unique identification number at predefined intervals (beacon rate). The query time could be done at many different times and could be as frequent as every two seconds or once a day, depending on the application. At least three reader antennas positioned around the perimeter of the area where

assets are being tracked detect the beacon's signal, so that the exact location of the asset can be found.

- **Transponder type**: In this type of modulation, transponders are awakened when they receive a signal from a reader. This type of tags is usually called semi-active, because of the lack of beacon rate (see 1.2.1). These RFID tags are used, for instance, in toll payment collection, checkpoint control and port security systems. This leads to extended battery life, since the tag communicates only when it is within the read range of a reader.

1.3.3 Field Propagation

Currently, RFID systems on the market fall into two main categories: Near-Field systems that employ inductive coupling of the transponder tag to the reactive energy circulating around the reader antenna, and Far-Field systems that couple to the real power contained in free space propagating electromagnetic plane waves. Whether or not a tag is in the near or far field depends on how close it is to the field creation system and the operating frequency or wavelength. There is a distance, commonly known as the radian sphere, inside which one is said to be in the near field and outside of which one is said to be in the far field. Because changed in electromagnetic fields occur gradually, the boundary is not exactly defined; the primary magnetic field begins at the antenna and induces electric field lines in space (the near field) [4].

The zone where the electromagnetic field separates from the antenna and propagates into free space as a plane wave is called the Far Field. The approximate distance where this transition zone happens is given as follows:

$$r = \frac{\lambda}{2\pi}$$

It is important to notice that this expression is valid for small antennas where $D<<\lambda$. It has been estimated that the far-field distance for the case in which $D>\lambda$ is given as follows:

$$r = \frac{2D^2}{\lambda},$$

where D is the maximum dimension of the radiating structure (antenna) and r is the distance from the antenna. Note that this is only an estimate, and the transition from near field to far field is not abrupt. Typically, D for reader antennas is 0.3m. The far-field distance in the UHF band in Europe (866.5 MHz, λ = 34.6 cm) is estimated to be 52 cm, while in the United States (915 MHz, λ = 32.8 cm) it is estimated to be 54.9 cm.

Near-field communication is generally applied in the LF and HF frequency bands, with relatively short reading distances, while Far-field communication is applicable to the potentially longer reading ranges of UHF and μW RFID systems.

1.3.4 OSI Model

The whole communication scheme used in RFID systems is related to the OSI (Open Systems Interconnection) model. The OSI model is a conceptual illustration for data communication. The module is hierarchical in structure and is constructed of seven (7) layers that define the requirements of communication between two end users (in our case, an RFID tag and an RFID reader) (Fig. 1.8).

- **Physical Layer**: Manages physical interface between tag and reader and defines data rate, encoding and modulation schemes.
- **Data-Link Layer**: Transmission of data blocks and manages addressing, error detection and correction.
- **Network Layer**: Routing and flow control
- **Transport Layer**: Controls the reliability of data transfer between end users
- **Session Layer**: Manages and terminates connection between transmitting and receiving ends
- **Presentation Layer**: Data representation and encryption
- **Application Layer**: Sends or retrieves applications to or from tags

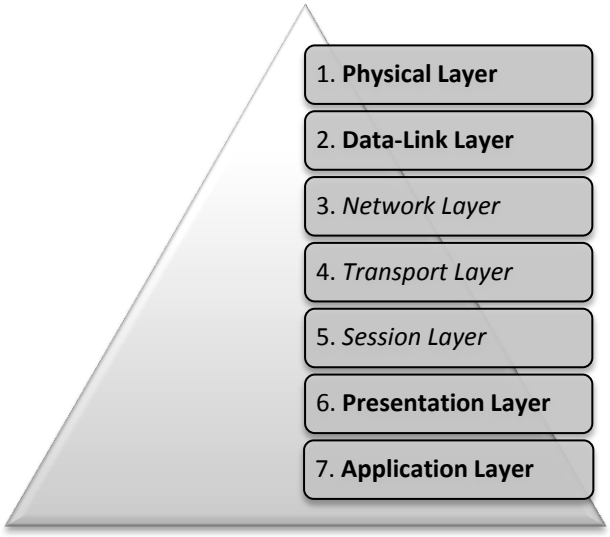

Figure 1.8 – The OSI model

In RFID, only layers 1, 2, 6 and 7 are used. The Network layer (3) is not applicable in RFID, since all links are point to point, as well as the Transport layer (4), since there are no complex links involved. The Session layer (5) is also not used, since neither restart nor termination of operation is applied [1].

1.3.5 Standardization

RFID standardization is one of the most challenging tasks, and that's because it deals with all the four layers of the -RFID related- OSI model we discussed in the previous section. Developing international standards for RFID technology can bring up three major benefits [5,6]:

- An international standard will make sure that **interoperability** among RFID readers and tags manufactured by different venders and improve interoperation across national boundaries.
- Having an international standard will decrease the **cost** due to compatibility and exchangeability.
- An international standard will help dramatically on **proliferation** of RFID technology worldwide.

Currently, there are four major organizations involving in development of standards for the RFID technology:

- **EPCglobal Inc.**

EPCglobal is a joint venture between Uniform Code Council (UCC) and EAN International. The organization carries the mission of the former Auto-ID Center at MIT. It's primarily goal is to make the final EPC standard an official global standard. The current Electronic Product Code (EPC) structure is presented bellow (Fig. 1.9). Currently, the latest protocol is the EPC Class-1 Generation 2 (C1G2) protocol for UHF RFID systems.

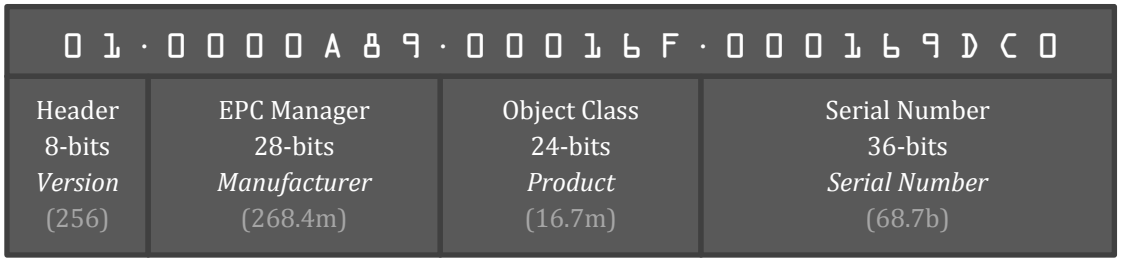

Figure 1.9 – 96-bit EPC structure

The way C1G2 operates is described below. There are eight steps:

1. A query is sent by the reader to the tag.
2. The tag generates a 16-bit random value (RN16), puts it into a slot counter and starts the counter. The tag only sends the RN16 to the reader when the RN16 in the slot counter decreases to zero.
3. The reader responds to the tag with an ACK and the same RN16.
4. The tag first compares the two RN16 and transmits the PC (Protocol-Control), EPC (Electronic Product Code), and CRC (Cyclic Redundancy Check) to the reader only when the two RN16s are matched. The reading process is done up to this point.

If the reader wants to access the tag, the following additional steps are required:

5. The reader sends ReqRN (containing RN16) to the tag.
6. The tag gives the handle to the reader only if the RN16 in ReqRN is the same as RN16 in the tag.
7. When the reader gets the handle of the tag, it XORs the PIN with RN16 and sends the result to the tag.
8. The tag executes the command if the PIN received from reader matches the PIN stored in the tag.

- **International Standard Organization (ISO)**

  ISO has been working on RFID applications in several areas, such as proximity cards, RFID air interface, animal identification, supply chain, etc. ISO protocols are widely used in HF RFID systems.

- **European Telecommunication Standards Institute (ETSI)**
- **Federal Communication Commission (FCC)**

Among these, EPCglobal and ISO have done an incredible job over the past few years. In fact, ISO approved EPCglobal Class 1 Generation 2 as an 18000-6C extension in 2006. This event has opened the way to a single UHF global protocol [7].

1.3.6 Anti-Collision

If many tags are present within the interrogator's scanning area, then they will all reply at the same time, which –at the reader end– is seen as a signal collision and an indication of multiple tags (Fig. 1.10).

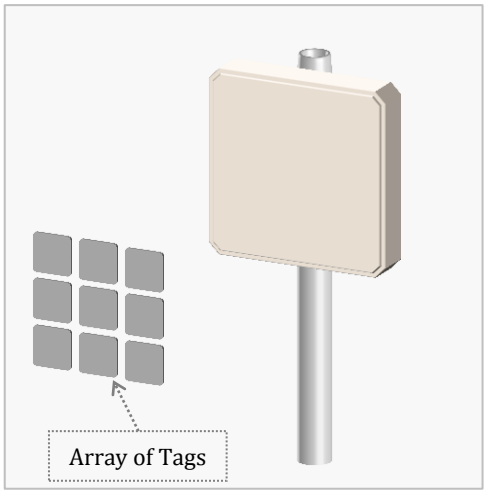

Figure 1.10 – RFID collision

The reader manages this problem by using an anti-collision algorithm designed to allow tags to be sorted and individually selected. The many different types of algorithms (Binary Tree, Aloha, and so on) are defined as part of the protocol standards. The number of tags that can be identified depends on the frequency and protocol used, and can typically range from 50 tags per second for HF up to 1500 tags per second for UHF. Once a tag is selected, the reader is able to perform a number of operations, such as reading the tag's identifier number or, in the case of a read/write tag, writing information to it. After finishing its dialogue with the tag, the reader can then either remove it from the list, or put it on standby until a later time. This process continues under control of the anti-collision algorithm until all tags have been selected [4].

Many RFID applications require the use of multiple tags simultaneously. For example, consider a shipping truck that contains hundreds of boxes, each with an RFID tag. When the truck enters a warehouse, it would be ideal for the tags on all the boxes to be read at the same time to avoid the time-consuming task of reading one box at a time. Without proper management, the multiple uses of tags could lead to a failure in communication between tag and reader called collision. There are two types of collision that can occur with the application of RFID: tag collision and reader collision. Tag collision occurs when two or more RFID tags communicate with one reader at the same time, while reader collision occurs when multiple nearby interrogators interfere with each other due to the concurrent use of the same frequency channel. We will consider tag collision and methods of management. Since a reader can only communicate with one tag at a time, multiple tags communicating with the reader at the same moment can cause confusion to the reader. There are two ways to tackle this problem: reader anti-collision and tag anti-collision algorithms.

- **Reader anti-collision algorithm**

  Using anti-collision algorithms, a reader can communicate with several tags within a very short time frame, such that communication appears simultaneous. This type of communication is referred to as multi-access. For multi-access communication to be realized, a variety of procedures have been developed to separate individual signals from one another and to prevent different tag data from colliding with one another. There are many basic multi-access procedures that are applicable to RFID systems. To mention a few:
  - Space Division Multiple Access (SDMA)
  - Frequency Division Multiple Access (FDMA)
  - Time Division Multiple Access (TDMA)

TDMA is used for reader anti-collision as well as two of the most common tag anti-collision algorithms in RFID systems today: Aloha and Binary Tree Walking. SDMA and FDMA both have restricted usage due to the complexity and the high cost of implementation [1].

- **Tag anti-collision algorithm**

  Like the reader in the reader anti-collision algorithm, the tag could also adopt an anti-collision or singulation protocol that will enable effective communication with the reader without colliding with other tags in the read range. There are two main types of tag anti-collision algorithms in use today: Aloha (mostly HF RFID systems) and Binary Tree-Walking (mostly UHF RFID systems).

  - **Aloha**: Aloha is a basic TDMA protocol mostly used in high frequency (HF) RFID systems (typically 13.56 MHz). A tag begins transmitting as soon as it has data to send, without any form of synchronization. At the start of the communication between reader and tag, the tags in the read range automatically send their tag IDs to the reader upon entering the read range. If one tag has data to send during the same time interval as another tag, the interval during which the two tags transmit overlaps and this results in either complete or partial collision. In the simplest form of a random back-off protocol used by the ALOHA algorithm, an occurrence of a collision forces the tags to stop transmitting. Then the colliding tags are assigned a randomly determined delay (waiting time). Each tag retransmits its data after its allocated delay has expired. Technological advancements permit a version of Aloha, called Slotted Aloha, in which the transmissions of signals are synchronized at the beginning of a slot. Each terminal waits for the available slot and transmits with a random probability. A slot is a time frame with limited number of bits. While pure Aloha has efficiency level of 18%, Slotted Aloha provides double of that, at 36%.
  - **Binary Tree Walking**: For UHF RFID tags, a more deterministic scheme is used to avoid collisions. The reader could sort through tags in its read range based on their tag ID. Singulation is generally the basic method used in this procedure. Singulation is a mean by which an RFID reader identifies a tag with a specific serial tag ID from a number of tags in its field. This identification process is necessary in situations where multiple tags simultaneously communicate with the reader. If each tag is not uniquely identified, the transmission will be disrupted. There are different methods of singulation, but tree walking is the most common method adopted for RFID systems.

    In tree walking, the space of k-bit identifiers is viewed as the leaves in a tree of depth k. A reader traverses the tree, asking subsets of tags to broadcast a single bit at a time. For example, if a reader is seeking a tag with ID 1010, the reader sends out a query requesting that all tags with a serial number that starts with a 1 to respond. If more than one responds, the reader might ask for all tags with a serial number that starts with 10 to respond. Again, if more than one tag responds, the reader again sends out a query for tags with serial number that starts with 101. The reader repeats this querying until it finds the specific tag with serial number 1010. Because of the querying method adopted by this procedure, this protocol is very susceptible to eavesdropping. Any system that can get data from the reader can get all but the last bit of the tag's serial number. Because of this, more advanced tree-walking-based singulation classes have been developed to reduce the susceptibility to eavesdropping. These protocols are Class 0 UHF and Class 1 UHF (Class 1 Generation 1 & 2) [1]:

- **Class-0 UHF**: A tree-walking algorithm that adopts certain changes to reduce the susceptibility to eavesdropping. The interface for Class 0 is based on pulse-width modulation (PWM) for the reader-to-tag link. The reader-to-tag link uses 100 percent amplitude modulation or 20 percent amplitude modulation of the carrier signal for transmission. There are three basic Class 0 reader-to-tag symbols: binary 0, binary 1, and Null. A binary 0 is transmitted by turning the reader off for a brief time, τ, after which the power is turned back on for the remainder of the symbol. A binary 1 is transmitted by turning the reader off for a longer period, for instance, 2τ. The null is a symbol used to inform the tags when to change their state. For the implementation of a Class 0 algorithm, a binary tree anti-collision protocol is usually employed.
- **Class-1 UHF**: A Class 1 tag has a unique identifier that is combined with an error detection/correction code. The error detection/correction code is usually a cyclic redundancy check (CRC). The Class 1 tag data (identifier and CRC) is stored in the identifier tag memory. Class 1 procedure is divided into two different generations for implementation. This is a more advanced technology that uses a filter capability that is built into reader commands. For the Class 1 Gen 1, the same modulation encoding technique as Class 0 is used. However, instead of a binary tree, a query tree walking technique is used. Here, the reader sends a Query command to the tags in its read range by using a group of bits that contain the filter bits and CRC plus identifying bits. The tag for which the query was intended replies with an 8-bit response in one of the eight time slots allocated. For Class 1 Gen 2, the ASK, FSK, or PSK is the modulation scheme used in combination with the PIE for this procedure. In this algorithm, the reader picks the encoding format for the tag-to-reader link. Two distinct sets of tag symbols are used: FM0 encoding and Miller encoding. Variations of the slotted ALOHA random algorithm (called Q Protocol) are used for the anti-collision process.

1.4 Optical Identification: Barcode

Radio Frequency Identification is the next generation of an optical barcode with several major advantages, since line-of-sight between the reader and the tag is not needed, and several tags can be read simultaneously. The media regularly proclaims that the days of bar code are numbered and that RFID will replace bar codes “soon”. In fact, RFID does have some clear-cut advantages over bar code, but bar codes also offer some clear-cut advantages over RFID.

1.4.1 What is a Barcode?

A bar code is a scheme in which printed symbols represent textual information. The printed symbols generally consist of vertical bars, spaces, and squares and dots. A method that encodes alphanumeric characters using these symbol elements to a printed symbol is called symbology. Two symbologies may use the same or different symbol elements to encode the same character string. Some characteristics of a symbology are:

- **Encoding technique**: A symbology with better encoding techniques allows for efficient and error-free encoding.

- **Character density**: A symbology that offers better character density can represent more textual information per unit physical area.
- **Error-checking techniques**: A symbology with better error-checking capability can allow the data to be read correctly even if some of the symbol components are damaged or missing.

Each symbology falls into one of the following three categories:

- **Linear**: They consist of vertical lines with different widths with white space separating two adjacent lines. The maximum number of characters that can be encoded with a linear symbology is 50.
- **2-Dimensional**: Two-dimensional symbologies have the most data-storage capacity. The maximum number of characters that can be encoded with a two-dimensional bar code symbology is 3,750.

Each symbology can be either printed or engraved (also called a bumpy bar code). An engraved symbology is actually a bar code embossed on a surface. This type of bar code is read using the "bumpiness" or the three-dimensional relief of the bar code. A bumpy bar code is thus not dependent on the contrast between the bar code lines and spaces for its reading. This type of bar code can be painted and subject to harsh environmental conditions, whereas a paper bar code in similar scenarios is easily destroyed.

A bar code scanner uses a light beam to scan across the bar code. The direction of scanning, in general, is irrelevant. However, during scanning, the light beam cannot move out of the bar code region. Therefore, in general, an increase in a bar code length also means an increase in scanner height to accommodate for larger deviations of the light beam outside the bar code region during scanning. During the scanning process, the reader measures the intensity of the reflected light by the black and white regions (for example, vertical bars) of this bar code. A dark bar absorbs light, and white space reflects light. An electronic device called a photodiode or a photocell translates this light pattern into an electric current (or analog signal). Electric circuits then decode this generated electrical current into digital data. This data is what was originally encoded by this bar code. The digital data is represented as ASCII characters. (Fig. 1.11)

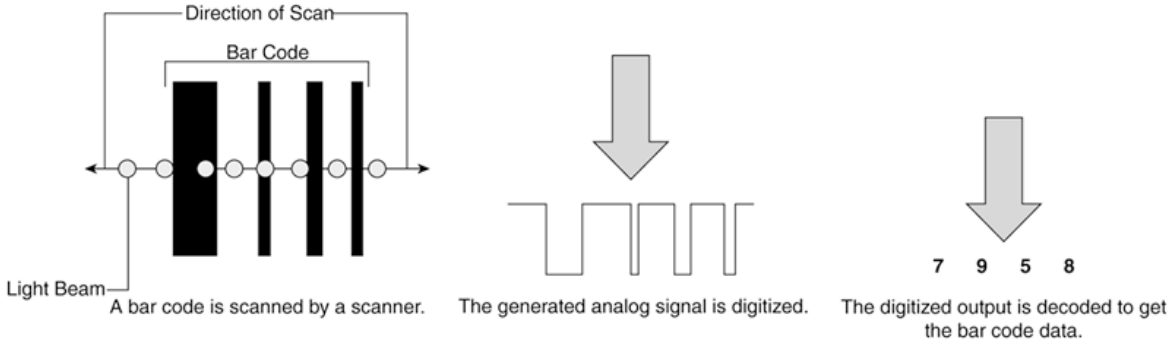

Figure 1.11 – Barcode scanning process

1.4.2 RFID versus Barcode

The advantages of RFID over barcodes are as follows:

- **Support for non-static data**: An RFID tag data can be rewritten many times (assuming, of course, that the RFID tag is an RW tag). The data on a bar code is static and cannot be changed.

- **No need for line of sight**: Generally, an RFID reader does not need a line of sight to read an RFID tag's data. A bar code reader always needs a line of sight to read a bar code.
- **Longer read range**: An RFID tag can have a much longer read range than a bar code. Depending on several factors, this can range from several feet to a few hundred feet
- **Larger data capacity**: An RFID tag can store more data than a bar code.
- **Multiple reads**: A suitable reader can read several RFID tags within a very short period of time, automatically, using a feature called anti-collision. A bar code reader, however, can only scan one bar code at a time.
- **Sustainability**: An RFID tag is generally rugged and resistant to harsh environmental operating conditions (to a fair extent). A bar code is easily damaged (for example, by moisture or dirt).
- **Intelligent behavior**: An RFID tag can be used to do other tasks besides simply being a data carrier and transporter. A bar code, however, does not have any intelligence and is a vehicle for only storing data.
- **Read accuracy**: RFID is far more accurate than bar codes.
- **Item-level tagging**: A bar code does not support item-level tagging.

The advantages of barcodes over RFID are as follows:

- **Lower cost**: The cost of implementing a bar code solution is generally less than that of a comparable RFID solution.
- **Comparable accuracy rates**: In some cases, the accuracy of a bar code solution is about the same, compared to an equivalent RFID solution.
- **Unaffected by the material type**: A bar code system can be used to successfully tag almost every kind of material.
- **Absence of international restrictions**: Bar code systems are used worldwide without any legal limitation on the use of the technology.
- **No social issues**: Today, you can find bar codes on almost every item on the planet, but no privacy rights group object to its use.
- **Mature technology with large installed base**: Bar code technology is probably the most widely deployed technology in the world.

1.4.3 RFID as the Barcode successor

For RFID to “replace barcodes soon”, it must overcome the following hurdles "soon" [8]: Tag any item that a bar code can tag today. Such items include almost every type of physical merchandise in existence in the world economy. To do this at an acceptable cost, the following four hurdles must be overcome:

- Cheap hardware with tags costing less than 5¢. The profit margin of some of industries is razor thin and prone to cutthroat competition. Any extra cost that does not go toward the bottom line is rarely justified.
- No consumer issues. The consumer must accept the use of RFID to tag every item that bar codes can today.
- Technical advancement to satisfactorily tag any possible item. RFID is an emerging technology, so the capabilities of tags, readers, and antennas are all undergoing rapid changes. At this point, the capabilities are not sufficient to tag every item to which a bar code can be affixed.

- Worldwide acceptance of common frequencies of operation. When common frequency bands for RFID operations are standardized, deployment of RFID implementations will definitely speed up. Even if these hurdles are overcome, there is still the following last hurdle, which might be the most daunting of all.

2 Related work

The continuously growing development of RFID systems in sensitive applications like e-passports, e-health, credit cards, and personal devices and products, makes it necessary to consider the related security and privacy issues in great detail. On the other hand, the technical principles of RFID, such as contactless-ness, lack of clear line of sight and the broadcast of signals, bring itself the security vulnerabilities which disturb the reliability of RFID systems and block the deployment progress of RFID techniques. Several works have been published on multiple different areas regarding the enhancement of RFID security and privacy. In this chapter we will discuss some of them by organizing them into two categories:

- **Classification of the RFID Security and Privacy threats**: Proposals that categorize and analyze several issues regarding RFID security and privacy.
- **Proposals over RFID Security and Privacy**: Proposals that attend to improve one or more vulnerabilities of RFID systems

2.1 Classification of the RFID Security and Privacy threats

In [9], a taxonomy model of RFID security threats is presented. This model has two levels. There are three layers in the first level, threats of Application layer, threats of Communication layer, and threats of Physical layer. In the second level, types of system-specific attacks associated with each layer are presented (Fig 2.1).

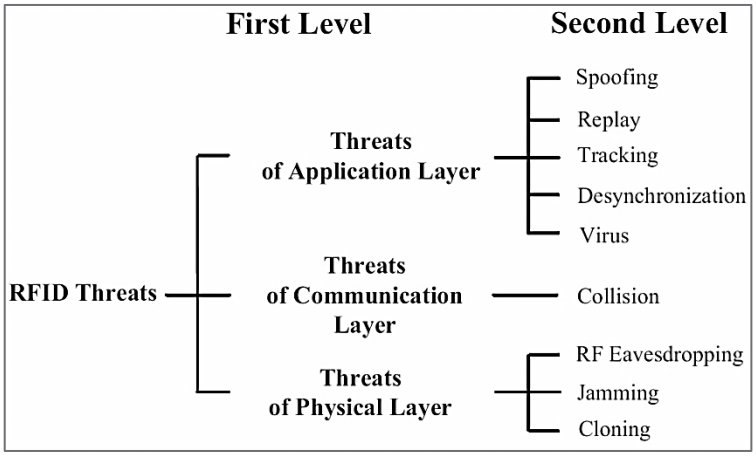

Figure 2.1 – Taxonomy model of RFID threats

- **Physical Layer**: Type of attacks in physical layer included RF eavesdropping, jamming and cloning, generally violate electromagnetic properties (RF signal) in the physical layer. Due to the reason that RFID tags and readers communicate wirelessly, RF eavesdropping can be achieved by simply using an antenna to listen to the communication. RF eavesdropping can also lead to Spoofing, Replay, and Tracking attacks if an adversary can figure out the encoding method. Jamming attack can be accomplished by constantly broadcasting RF signals. Doing so, any nearby RFID readers' operations will be disrupted. Therefore,

avoiding RF signals from RFID readers reach tagged items. Cloning can be attained by reverse engineering the tags or by building a device that mimic the tag's signal.

- **Data-Link Layer**: Collision is the main threat in communication layer which violates the way the RFID reader single out a particular tag for communication. When more than one tag responds to RFID reader's query, collision takes place. An attacker can send out one or more signals at the same time to respond RFID reader's query in order to create collision. When collision happens, the communication between RFID tags and readers stalls. Therefore, a collision attack is also a type of Denial of Service attack (DOS).
- **Application Layer**: Spoofing, Replay, Tracking, Desynchronization, and Virus are associated to application layer. They basically violate the properties of applications such as the identification of tag, the operation related to backend system, and personal privacy (in [9], privacy threat is considered a type of security threat). Spoofing attack can be achieved by forging a tag to act as a valid tag. Doing so, an attacker can use the forged tag to fool the RFID reader and backend system to gain products and services. Replay attack focus on consuming the computing resource of the whole system. Tracking attack is related to user's personal privacy. For example, a user with a tagged item which might be read by an attacker's reader if the reader is compatible with that tag. This will lead to several privacy issues such as location disclosure, purchase history, and so on. Desynchronization attack is a threat of desynchronizing the ID between backend system and tag's ID. This can make the tag useless. Desynchronization attack occurs when the RFID reader is failed to write ID to tags or when backend system cannot transmit ID to RFID reader. Virus attack can be accomplished by injecting virus into the tag and then use SQL injection to attack the backend system.

In [10], a different point of view looking at RFID related threats is presented. An RFID system is considered as a distributed and/or data processing system. Therefore, threats are classified using the principle of information security: Confidentiality, Availability, and Integrity. The method of attack tree is used to show lists of threats in breaching data confidentiality, availability, and integrity in a general RFID system which contains elements including tag, RFID reader, backend system, link between RFID reader and backend system, and link between RFID reader and tag (Fig. 2.2).

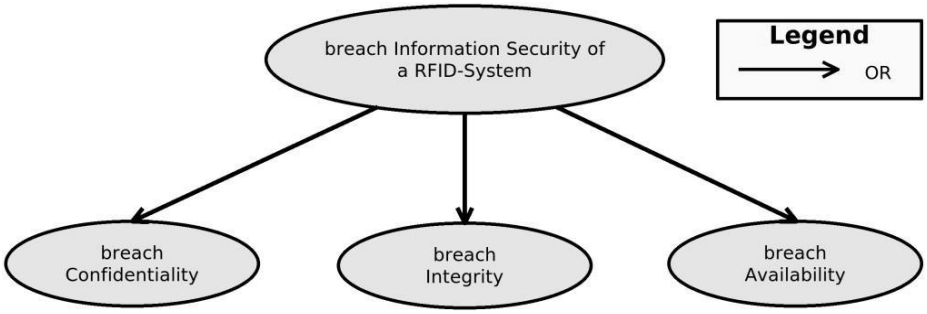

Figure 2.2 – Enumeration of RFID threats

- **Confidentiality**: In a general RFID system, confidentiality of data can be breached by an attacker through the five elements described above. Gaining data through tag, RFID reader, and backend system, an attacker needs to have physical access. In gaining data through links, close proximity is required for an attacker to listen to the communication. Example of attacks to breach confidentiality through link (RF link) between tag and RFID reader are tracking/tracing, sniffing, and spoofing. Tracking and tracing attacks can use the sniffed ID

to track a person. This also implies privacy issues. In addition, sniffed ID can be used to clone tags. Spoofing attack can be accomplished by replay and relay attacks.

- **Integrity**: Breaching integrity of data can be achieved in four ways including: Gain permanent component authority, Component replacement, Impersonate components, Data altering. Gaining permanent component authority can happen in every one of the five elements (even sub-component of each of the five elements). Backend system and RFID reader would be the most vulnerable targets because of the realization of parts and the availability of interfaces. Gaining permanent access to links is less vulnerable since for getting permanent access to link, it requires permanent close proximity which would eventually be suspicious. Moreover, the lack of interfaces in tags (the only interface is the link) also makes it less vulnerable for an attacker to get permanent access. In addition, all components in a RFID system suffer from data altering. As to component replacement and impersonate component, they probably will only happen to the tags since they are the cheapest and the most noticeable physical component in the system.
- **Availability**: Denial-of-Service (DOS), component theft, and physical destruction of component are types of threat that could lead to violation of system availability. By covering the tags with metal or jamming the RF-channel with a blocker tag, DOS can be achieved. In addition, denial of energy of either the RFID reader or backend system can also lead to DOS. Component theft and physical destruction of component are very difficult to avoid especially for tags since the tags are the most notable one in the environment, and the ICs embedded in them are very easy to be destroyed by applying high energy field.

In [11], a summary of EPCglobal C1G2 protocol related Security and Privacy Issues are presented. Even though C1G2 supports security mechanisms like Kill command, Access command (optional), and XOR, it is unfortunate that C1G2 still has some serious security and privacy issues. It is clear that the pseudo-random number used by the protocol is designed to single out a tag from a tag population. Thus the collision is taken care of in C1G2. However, the data transmitted between tag and reader is in plain text. This leads to serious problems in security and privacy such as impersonation, information leakage, and tracking/tracing threats. Besides that, the PIN being disclosed by an attacker could also happen if he can get the RN16 and the XORed PIN.

In [96], a more advanced classification of RFID attacks is presented, based on the layer that each is taking place and possible countermeasures that can be used to combat these attacks are discussed. More specifically, threats are discriminated to attacks deployed in the physical layer, the application layer, the strategic layer and multilayer attacks.

2.2 Proposals over RFID Security and Privacy

Several approaches have been proposed lately in facing the RFID security and privacy threats discussed above. Some of them are presented in this section.

2.2.1 Serial Numbering

The first approach relies on RFID product authentication using unique serial numbering [16]. By keeping a list of all valid product ID numbers in a secure online server, the absence of a product's ID from that list would serve as an indication of counterfeit. The security of this

approach relies on keeping the list secret from counterfeiters while providing needed access to legitimate users. An issue is that counterfeiters can always try to guess the valid serial numbers, especially when these numbers are issued in a systematic way. Therefore, unique serial numbering can be made more secure by assigning the serial numbers in a random way from a large name space, which is possible with RFID, due to the support of long identifiers (at least 96-bit). The clear un-addressed weakness of unique serial numbering approaches is tag cloning. However, duplicated tags can be detected and are an important indicator of counterfeit. These approaches can be implemented in RFID-enabled supply chain systems with little additional cost, with only requirement the use of re-writable RFID tags.

Generating and storing inherently dynamic profiles of individual goods as products move through the supply chain is mentioned as track and trace, which is a natural expansion of unique serial numbering approaches. The product specific records allow for heuristic plausibility checks, for example a product with a serial number registered for sale in Europe is suspicious if offered in an American store at the same time. The plausibility check is suited for being performed by customers who can reason themselves whether the product is original or not, though it can also be automated by suitable artificial intelligence [17][18][19]. Track and trace can be also used in supply chains for other purposes, such as deriving a product's history or organizing product recalls. In addition, some industries like pharmaceutical industry have legislation that demands companies to document product pedigrees [20]. Therefore track and trace based product authentication can be cost-efficient for companies, as other applications justify the expenses. However, generating and gathering track and trace profiles of products in multi-party supply chains can be hard and requires cooperation between the partners.

2.2.2 Hash Lock

Secure object authentication techniques make use of cryptographic primitives. This allows for reliable authentication while keeping the critical information secret, in order to increase the resistance against cloning. Because authentication is needed in many RFID applications, the reviewed protocols come from different fields of RFID security and privacy.

One of the first cryptographic privacy enhancing technologies for RFID is the hash-lock of Weis et al. [13]. The design principles behind the proposed scheme include the assumption that tags cannot be trusted to store long-term secrets when left in isolation. The authors proposed a way to lock the tag without storing the access key, but only a hash of the key on the tag. The key is stored in a back-end server and can be found using the tag's meta-ID. This approach can be applied in authentication, namely unlocking a tag would correspond authentication. However, the cloning resistance of the scheme is based only on the locked state of the tags and so it is more suitable for protecting privacy, since an adversary can track the tag via the metaID. Furthermore, both the random key and the tag ID are subject to eavesdropping by an attacker. Henrici et al. [22] have later extended the randomized version of the original hash-lock scheme for increased privacy and scalability. In this scheme, an attacker could impersonate a tag to a legitimate reader, or eavesdrop the transmitted "key"-values.

Avoine et al. [23] proposed another hash-based RFID protocol that provides modified identifiers for improved privacy and that can be applied for authentication. In the proposed protocol the authors solve scalability issues of the privacy-enhancing scheme from [24] by introducing a specific time-memory trade-off. In a similar hash-based protocol [25], read-access control is required. The tag requires the implementation of a hash function, but the protocol is vulnerable to reader impersonation, as no security is required for the tag to get the reader ID. In

addition, hash-based RFID protocols for mutual authentication have been proposed in [26], [27] and [28].

All these protocols rely on synchronized secrets residing on the tag and back-end server and they require a one-way hash function from the tag. These approaches show how guaranteeing the un-traceability by updating tag identifier increases the workload of back-end servers.

Texas Instruments has developed RFID based authentication techniques for pharmaceutical industry. The model presented in [19] bases on authenticating the products through digital signatures that are written on tags. By using TID and a public key, the transponder can be linked to the signer of the data in a provable way. To improve the traceability of products, tag memory is also used to store chain-of-custody events.

Juels et al. [30] presented an approach to increase tracing and forgery resistance of RFID-enabled banknotes by using digital signatures for RFID authentication. The approach uses re-encryption to avoid static identifiers and optical data on the banknote to bind the RFID tag and the paper. Authentication is performed by verifying that the data on the tag is signed using a valid public key. In order to increase cloning resistance, the authors suggest including some distinctive characteristics of the physical media into the signature (i.e. physical fingerprint of the banknote) and verifying the validity of these characteristics as a part of the authentication process. Zhang et al. [31] have later enhanced the protocol by addressing some integrity issues.

Tsudik [32] proposed an authentication protocol called YA-TRAP which provides tracking-resistant tag authentication through monotonically increasing timestamps on the tag. YA-TRAP requires a pseudo-random number generator (PRNG) from the tag and its basic version is vulnerable to DoS attack through timestamp Desynchronization between the tag and the server. The approach does not require on demand computation for the back-end as a result of a pre-computed hash-table for later tag verification, which means less load for the server than for example in [33]. Chatmon et al. [34] proposed anonymous RFID authentication protocols based on YA-TRAP that provide anonymity for authenticated transponders and address some vulnerabilities of the original design, while increasing the server workload.

Juels [35] discussed minimalist cryptography based authentication and proposed a tracking-resistant pseudonym-throttling scheme. This mutual authentication protocol bases on a list of pseudonyms and keys residing on tag and on back-end server. The protocol needs additional memory on tag and uses a way to update the tag's pseudonym list using one-time pads to resist cloning and eavesdropping. However, the communication cost is relatively high because of the tag data updates.

Juels proposed another low-cost authentication in [36], where the read-protected 32-bit kill passwords of EPC Class-1 Generation-2 tags are used to implement ad-hoc tag authentication protocol. The protocol bases on the fact that even though the EPC of a transponder can be skimmed, the kill-password remains secret. Cloned tags can be found by testing, without killing the tag, if the kill password matches the original one stored in a database. Furthermore, the protocol supports for mutual authentication.

Engberg et al. [50] proposed so called zero-knowledge device authentication as an answer to consumer privacy issues. In their proposal the tag must authenticate the reader before it returns any traceable identifier. The scheme is based on shared secrets and requires hash function from the tag.

2.2.3 Challenge-Response Protocols

Vajda et al. [37] discussed lightweight authentication protocols for low-cost tags. The proposed set of challenge-response protocols includes simply XOR encryption with secret keys (although also complex encryption like RSA was proposed, it's not considered here because it's infeasible in low-cost tags [38]). The cryptographic problem with keys being static in XOR encryption is addressed by re-keying schemes that make use of keys from multiple previous protocol runs.

Juels et al. [38] introduced an approach for low-cost authentication based on the work of Hopper and Blum (HB) [39]. The proposed HB+ protocol makes use of the hardness assumption of statistical "Learning Parity with Noise" (LPN) problem and can be implemented on low-cost tags, as it only requires bitwise AND and XOR operations and one random "noise bit". The security of HB+ against active adversaries has gained publicity in the scientific community and is discussed in details in [40]. The first version of the original protocol [38] was found to be vulnerable against a realistic active attack [42]. Proposals to address the security issues have emerged, including the modified HB++ by Piramuthu [43].

Dimitriou [44] proposed a protocol that addresses privacy issues and aims at efficient identification of multiple tags. The enhanced version of the protocol is considered here, since the basic one does not protect the tags against cloning. In this approach the tags need a PRNG and a pseudo random function (PRF) for symmetric-key encryption. The proposed protocol is efficient in terms of tag-to-reader transaction and protects the privacy by avoiding transmission of static IDs. However, since the tags share secret keys, compromise of one tag may reveal information about others. In another work [45] the author proposed a lightweight RFID protocol against traceability and cloning attacks. This approach bases on a refreshing a shared secret between tag and back-end database and requires hash calculations and PRNG from the tag.

Duc [46] proposed communication protocol for RFID devises that supports for tag-to-reader authentication based on synchronization between tag and back-end server. The proposed scheme is tailored for EPC Class-1 Generation-2 tags so that it requires only a PRNG on the tag and pre-shared keys. The approach also takes advantage of the CRC function that is supported by Generation-2 tags. The underlying idea is to use the same PRNG with the same seed on both RFID tag and on back-end side and to use it for efficient key sharing. The encryption and decryption can then be done by XORing the messages.

Ranasinghe et al. [47] presented ways to implement challenge-response authentication protocol on RFID tags without using costly cryptographic primitives. These proposals are based on a Physical Unclonable Function (PUF) residing on the tag, which allows for calculation of unique responses using only some hundreds of logical gates. A possible candidate for the PUF can be found from [48], where the manufacturing variations of each integrated circuit are used to implement a secret key on a tag. The back-end server needs to store a list of challenge-response pairs for each PUF (i.e. for each tag) because, without encryption, a PUF challenge-response pair that is once used, cannot be used again since it may have been observed by an adversary. The PUF based security is still an area of active research. Also Tuyls et al. [49] proposed the use of PUFs to increase RFID transponders resistance against both physical and communication based cloning attacks and defined an offline authentication protocol. The authors estimated that their anti-clone tag can be built with on the order of 5,000 gates.

Also Rhee et al. [51] proposed a challenge-response protocol for user's privacy. The proposed protocol doesn't update the tag ID and therefore can be applied in an environment with distributed databases. The protocol relies on hash calculations by the back-end database, so that

the tag ID is the only necessary shared secret between the devices taking part in the authentication.

Molnar et al. [52] proposed private authentication protocols for library RFID, where the tag and the reader can do mutual authentication without revealing their identities to adversaries. The protocols made use of PRNG residing on the tag. He also presented [33] another privacy enhancing scheme where an RFID pseudonym protocol takes care of emitting always a different pseudonym using PRF. In order to relate pseudonyms and real tag IDs, the authors presented an entity called Trusted Center (TC) that is able to decode the tag responses and obtain the tag's identity. In the same work the authors introduced term ownership transfer that refers to TC giving permissions to only readers of a certain entity to read an RFID tag.

Gao et al. [25] proposed protocols for improved security and privacy of supply chain RFID. In their proposals the tags store a list of licit readers to protect the tags against skimming and therefore need rewritable memory. Other tag requirements include PRNG and hash function. Though the protocol burdens the back-end server with some computational load, the approach is designed to be suitable for a large number of tags.

Yang et al. [55] proposed a mutual authentication protocol that provides protection against replay attack and Man-In-The-Middle (MITM) attack even when the reader is not trusted and the communication channel is insecure. This mutual authentication protocol provides privacy protection and cloning resistance with the expense of tag's hash calculations and storing two secrets in the tag and in the back-end server.

Dominikus et al. [56] discussed symmetric RFID authentication protocols in practice and presented five standard challenge-response protocols for reader, tag and mutual authentication. The design focuses on strong authentication for advanced, about 50¢ tags with available silicon area of 10,000 gates. The presented protocols use AES encryption (and decryption) on tags in such a way that energy constraints of Class-2 RFID systems are met. Feldhofer [57] presented an implementation of standard symmetric two-way challenge-response protocol as extinction to the standard ISO/IEC 18000 RFID protocol. The use of standard authentication protocols with standard communication protocols is important for ensuring the security and interoperability of an approach. Hardware implementation of the same protocol can be found from [58], where Feldhofer et al. presented a novel minimalist approach of a 128-bit Advanced Encryption Standard (AES) implementation. The approach provides a promising choice for strong authentication in RFID systems and the proposed low-cost AES hardware implementation is used in various other proposals as an enabler of cost-efficient RFID cryptography.

Also Bailey et al. [59] concentrate on integrating common cryptographic standards into RFID by proposing techniques to create RFID tags that are compliant with the EPC Class-1 Generation-2 tags, but offer cryptographic functionality of standards like ISO 7816-4. The proposed challenge-response protocols make use of AES on the tag and can be used for mutual authentication. In particular, the authors define a 32 or 64 bit "one-time password" that could be included in transmitted EPC data fields.

To explicitly address transponder removing and reapplying (and also cloning) attack with low-cost tags, Nochta et al. [60] proposed a cryptographic way to bind the RFID transponder and the product that it authenticates. Because of the uniqueness of the approach, we consider it as a separate category of RFID product authentication. In this approach the authentication is based on writing on the tag memory a digital signature that combines the TID number and product specific features of the item that is to be authenticated. These features can be physical or chemical properties that identify the product and that can be verified, such as very precise

weight. The chosen feature is measured as a part of the authentication and if the feature used in the tag's signature does not match the measured feature, the transponder-product pair is not original.

The proposed authentication needs a public key stored on an online database. Also an offline authentication is proposed by storing the public key on the tag, though this decreases the level of security. The disadvantage of this approach is that each unit has to be physically verified as a part of authentication.

A similar approach which prevents traceability is proposed in [86], in which, no modification of the basic functionality of RFID tags is required. The protocol relies on a cryptographic primitive but does not need the tag to have any cryptographic capabilities. This is suggested to avoid tracing. Authorized users can store encryption into a RFID chip that can be randomized by anyone. In this scheme cipher texts which is produced contains implicit proofs of being "safe" to randomize. If the proof is invalid, the randomizer has the option to obliterate the contents with "safe" but meaningless cipher-texts, destroying the adversarial hidden channel and preventing tracing. Therefore the legitimate issuers can initiate and re-set the contents of RFIDs, enabling them to use it for recognizing the tag later. Illegitimate issuers can also re-set the value of tags—these are passive entities—but any contents they write to them will be destroyed by honest readers that participate in the scheme.

2.2.4 Ultralightweight Cryptography

The previous approaches are not cost effective, so the researchers look towards ultralightweight solution which is cost effective and also resolve security issues of RFID. In this class, Peris et al. proposed a family of Ultralightweight Mutual Authentication Protocols, which is not available in commercial RFID tags yet; they are still under development. These protocols guarantee tag anonymity with the use of pseudonyms. To retrieve the information associated from a tag (tag identification phase), an index-pseudonym is used by an authorized reader. The shared secret keys are used by both readers and tags to build the messages exchanged in the mutual authentication phase. In these protocols only bitwise operations like XOR, bitwise AND, bitwise OR and addition mod 2^m are used. On the other side only reader needs to generate pseudorandom numbers. Tags only use them to build the message to the protocol. These proposed schemes consist of three phases. First identification phase in which the tag is identified by means of the index-pseudonym. Second is Authentication in which the reader and the tag are mutually authenticated and also used to transmit the static tag identifier (ID) securely. Finally the Updating phase in which the index-pseudonym and shared secret keys are updated (for details refer original papers).

Chronologically, Minimalist Mutual Authentication Protocol (M^2AP) was the first proposal [61] in the family. This protocol had some weaknesses and was attacked in next year [95]. The next protocol was Lightweight Mutual Authentication Protocol (LMAP) [63], which was also attacked [18]. Efficient Mutual Authentication Protocol (EMAP) [65] was an enhanced version of LMAP, which also had vulnerabilities [66].

Later, Hung-Yu Chien proposed Strong Authentication and Strong Integrity (SASI) [67] protocol which overcame the vulnerabilities of EMAP. This protocol incorporates the first non-triangular rotation function, which was its main strength. The rotation function provided good diffusion properties. This protocol was also attacked and its vulnerabilities were uncovered [29] and [88]. To determine secret values SASI used XOR with addition modulo and an OR functions with known public value of IDS. Still all these protocols were not strong enough and then Peris et

al. proposed a Gossamer ultra-lightweight protocol [69]. This protocol uses two non-triangular functions including RotBits and MixBits which provided good confusion and diffusion properties. It also uses addition and XOR operations to prevent a divide and conquer attack launched on earlier versions. Bilal et al. [93] present a security analysis of Gossamer protocol. It also propose a new mutual authentication protocol which can remove the possible vulnerabilities discovered in Gossamer protocol like denial of service, memory and computation exhaustive, de-synchronization, replay attack. Recently, a new pure ultralightweight protocol was proposed [71], which seems to be much lighter and faster than its predecessors. It also uses XOR, AND, Rotation and MixBits functions covering all vulnerabilities of the previous protocols, and also providing additional security against some active attacks. That protocol does not need a random number generator even on the reader's side, as with previous protocols, and is also more efficient in terms of storage, communication and computation cost. In [72], David-Prasad proposed an ultralightweight mutual authentication protocol that consumes less memory size on both server and tag side and performs only XOR and bitwise AND operations on the tag. Its vulnerabilities were soon discovered using a Tango attack and related to that use of only triangular functions, which have poor diffusion properties. Similarly, in [73], a protocol inspired by SASI and Gossamer is presented, which was proven to be vulnerable into two types of attacks, reader impersonation and traceability [74].

2.2.5 Binary Tree-Walking

The anti-collision algorithm we discussed in the previous chapter (Binary Tree-Walking) has some serious security flaw due to the nature of the algorithm as well as the asymmetry between the forward and backward channel strengths. More specifically, the threat posed by passive eavesdroppers is more their ability to hear the signals broadcast by the tag reader, which may be picked up many hundreds of meters away, than their ability to hear the signals of an RFID tag, which can only be picked up nearby. This is unfortunate, since the IDs read by the standard tree-walking singulation protocol can be inferred by hearing merely the signals broadcast by the reader. A few proposals have been made during the past few years in order to deal with this issue.

Weis et al. [13] show how to singulate tags without broadcasting their IDs on the forward communication channel, so that a passive eavesdropper cannot infer the IDs being read. Assume a population of tags that share a common prefix in their ID, such as Manufacturer and Product Code. To singulate tags, the reader can request all tags to broadcast their next bit of ID. If there is no collision, all tags share the same value in that bit (thus, the reader and the tags effectively share a secret bit value). When a collision does occur, the reader can specify which portion of the tag population will proceed. This way the reader silently singulates all of the tags. Apart from the fact that this does not defend against active attacks, the authors note that their proposal relies on the somewhat unrealistic assumption of a common, secret string shared among tags; this assumption can be removed, however, if the tags can generate their own random pseudo- ID's before singulation.

Another idea, called Randomized Tree-Walking [14], is for each tag to generate a random number, which serves as its temporary ID for the duration of the interrogation algorithm. Then, the reader performs a tree-walk, singulating these random numbers. Once a reader reaches a tree leaf, it queries the tag that generated that random number, and this tag sends its real-ID back to the reader. Since the tag's response is transmitted over the backward channel, a passive eavesdropper does not hear the response, making transmission of the real-ID secure. As an

improvement over the previous algorithm, the Randomized Pseudo-Random Function (PRF) Tree Walking Algorithm [15], efficiently identifies many tags in the presence of active eavesdroppers, and is adaptable to privacy and security requirements. The algorithm consists of three steps: Each tag generates a random number, and the reader performs a tree-walk on these random numbers. Once a tag is selected, the reader and the tag engage in a tree-walking private authentication protocol and finally the reader moves the tag to a different position in a tree.

3 Evaluation

Using a commercial UHF RFID system, we performed some benchmarking of real-life applications, both indoors and outdoors, in order to face situations that appear when designing an RFID system. The system we used consists of the following basic parts (Image 3.1):

- 1x Impinj Speedway Revolution R420 reader,
- 2x Laird Technologies S8658 antennas (Far-Field, circular polarization),
- 1x CSL CS-777 Brickyard antenna (Near-Field),
- 1x Impinj Mini Guardrail antenna (Near-Field) and
- a variety of C1G2 RFID tags (Table 3.1)

Image 3.1 – Evaluation kit

Model	Tag Chip	Dimensions	Field	EPC Mem.	User Mem.	Material
Impinj Satellite	Impinj Monza 2	18 x 32 mm	Near	96 bits	-	Copper
Impinj Satellite	-//-	18 x 32 mm	Near	96 bits	-	Aluminum
Impinj Thin Propeller	-//-	8 x 95 mm	Far	96 bits	-	Aluminum
Impinj Thin Propeller (Short)	-//-	8 x 53 mm	Far	96 bits	-	Aluminum
Avery Dennison AD-223	Impinj Monza 3	8 x 95 mm	Near	96 bits	-	Aluminum
Avery Dennison AD-230	-//-	15 x 70 mm	Near	96 bits	-	Aluminum
Avery Dennison AD-805	-//-	16 x 16 mm	Near	96 bits	-	Aluminum
Avery Dennison AD-828	-//-	15 x 40 mm	Near	96 bits	-	Aluminum
Trace-Tech TB24	Impinj Monza 4D	8 x 22 mm	Near	128 bits	32 bits	Aluminum
Trace-Tech TE24	Impinj Monza 4QT	16 x 68 mm	Far	128 bits	512 bits	Aluminum
Lab ID UH3D40	-//-	40 x 40 mm	Far	128 bits	512 bits	Aluminum
Lab ID UH600	-//-	9 x 29 mm	Near	128 bits	512 bits	Aluminum
Alien ALN-9540	Alien Higgs 2	8 x 95 mm	Far	96 bits	-	Copper
Alien ALN-9640	Alien Higgs 3	8 x 95 mm	Far	96 bits	512 bits	Copper

Table 3.1 – Tag list

In the following experiments, we only used the Far-Field antennas. The completed benchmarks are the following:

- **Antenna Mapping**
- **Read Rate versus Tag-Antenna Distance**

- **Tag performance on objects of different materials**
- **Tag interference**
- **Read range versus Antenna Output Power**
- **Tag reading sequence**
- **Antenna Power Output versus Power Consumption**

These benchmarks helped us understand what the acceptable limits are when dealing with the security of an RFID system; what is the performance of a system without using cryptography, and how reduced the performance of the system can get when improving the security of it using cryptographic primitives or other solutions.

3.1 Antenna Mapping

Using different RFID tags[1] we constructed a mapping diagram of the antennas at various angles and distances (Fig. 3.1), with the reader set at factory default configuration and the antenna's power output set at the maximum level (31.5dB in Europe). The experiment was taken both indoors and outdoors and we present here the outdoors's results, where there is no interference from walls and objects. While performing the benchmark indoors in a variety of rooms, we noticed increased range and reading sensitivity due to these reflections (the sensitivity was getting higher as the rooms area was getting lower).

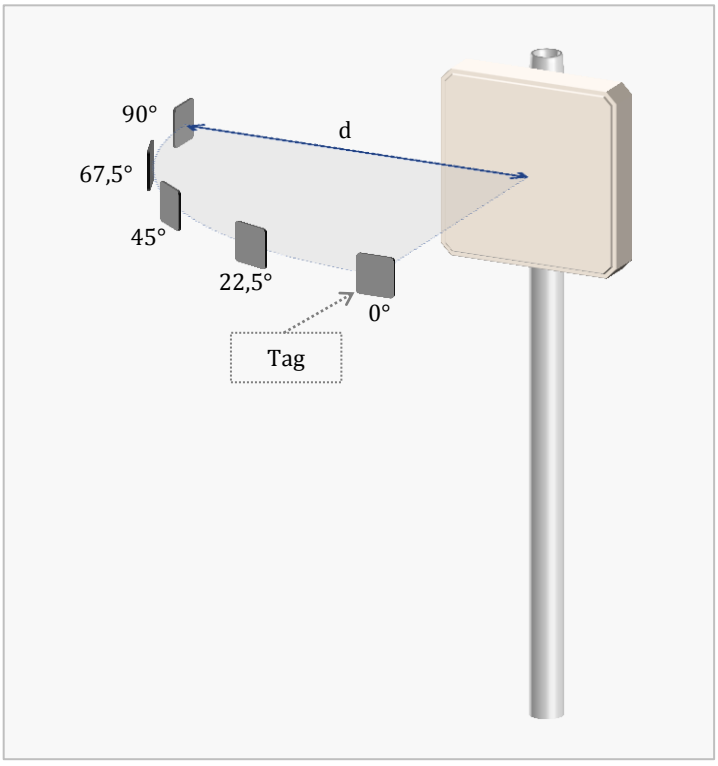

Figure 3.1 - Antenna Mapping

The resulted data are displayed in Figures 3.2-4, while the final graphical result can be seen in Figures 3.5 (distance-based) and 3.6-8 (sensitivity-based) below. Since the antennas have

[1] Tags used are the following three: Impinj Satellite, LabID UH3D40 (Impinj True3D-enabled), Alien ALN-9640

circular polarization, we noticed similar values of reading sensitivity on both the left and right side of the antenna while moving around the vertical antenna axis, as well as while moving from top to bottom around the horizontal antenna axis.

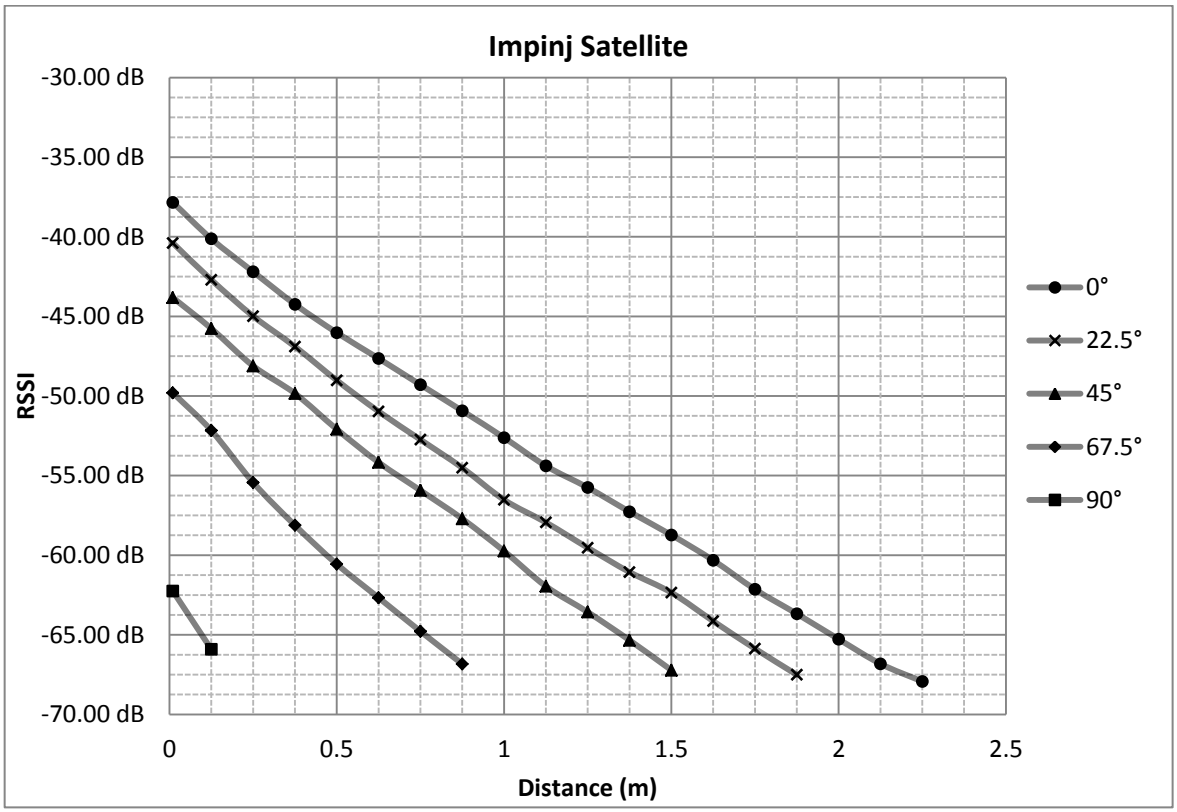

Figure 3.2 – Impinj Satellite Mapping

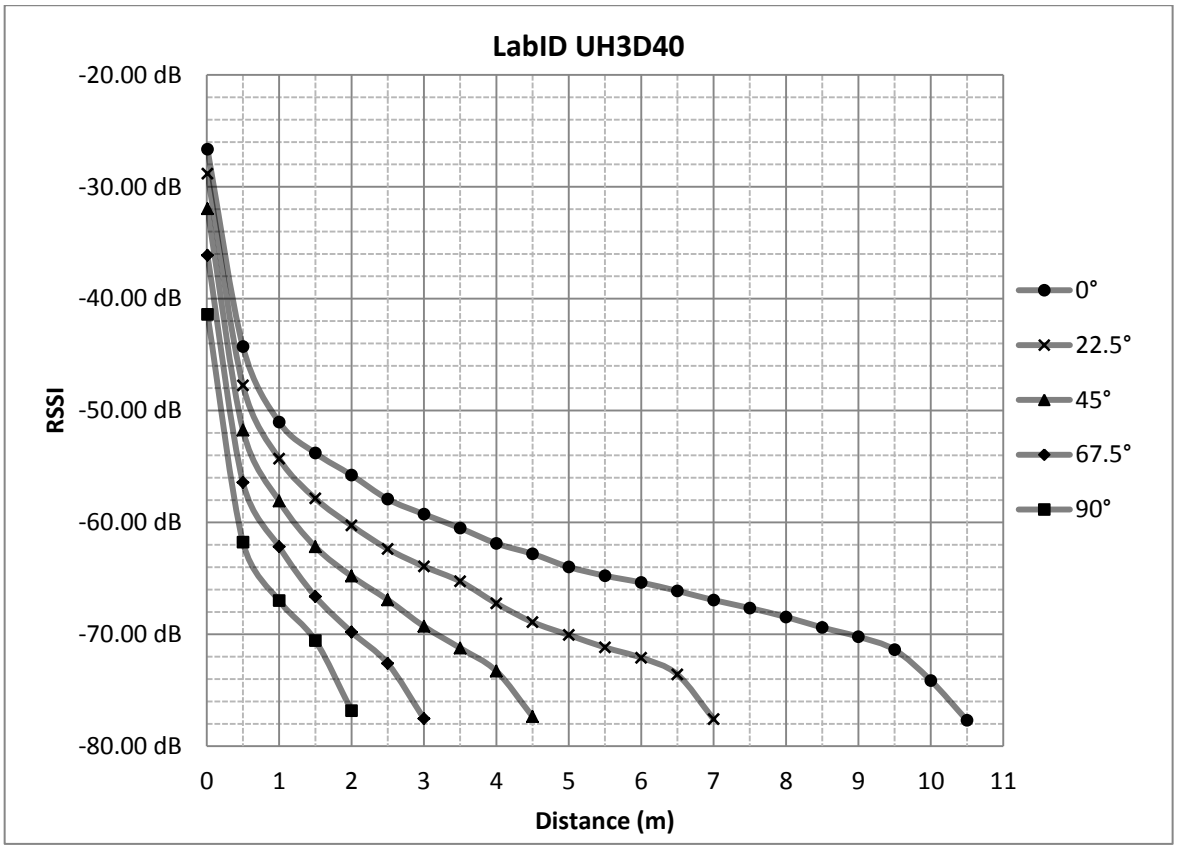

Figure 3.3 – LabID UH3D40 Mapping

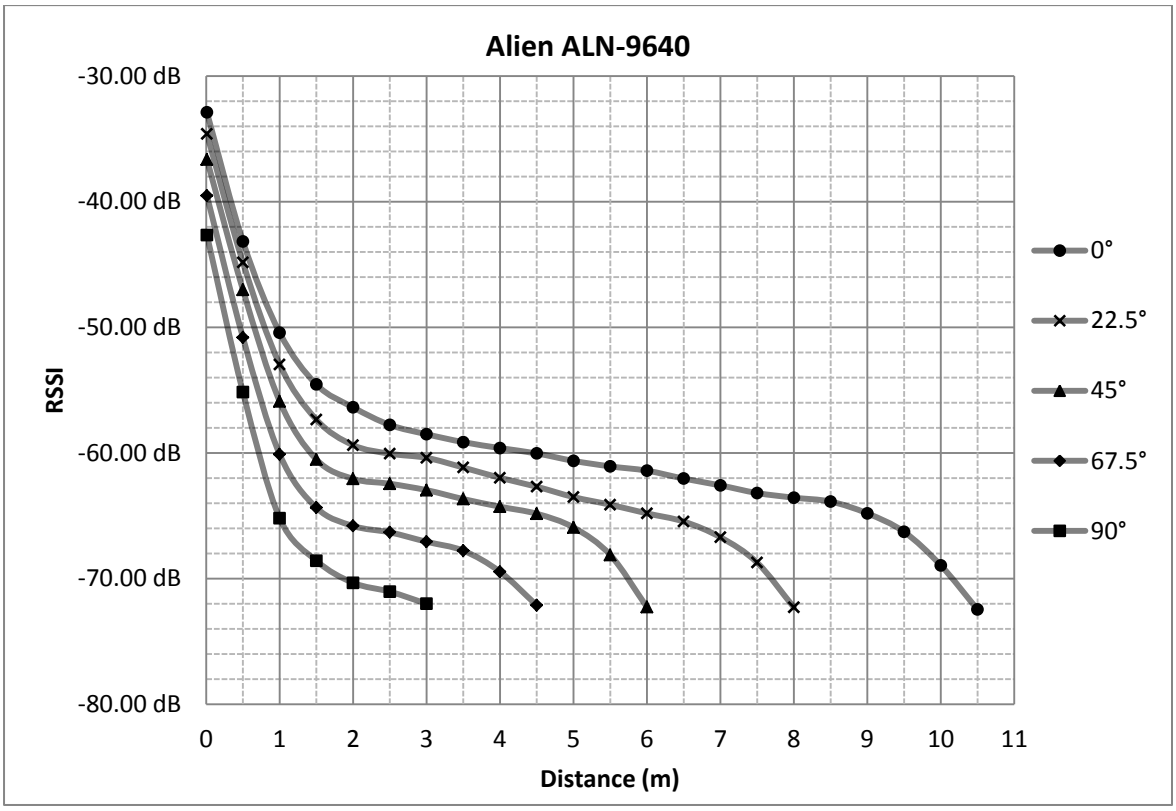

Figure 3.4 – Alien ALN-9640 Mapping

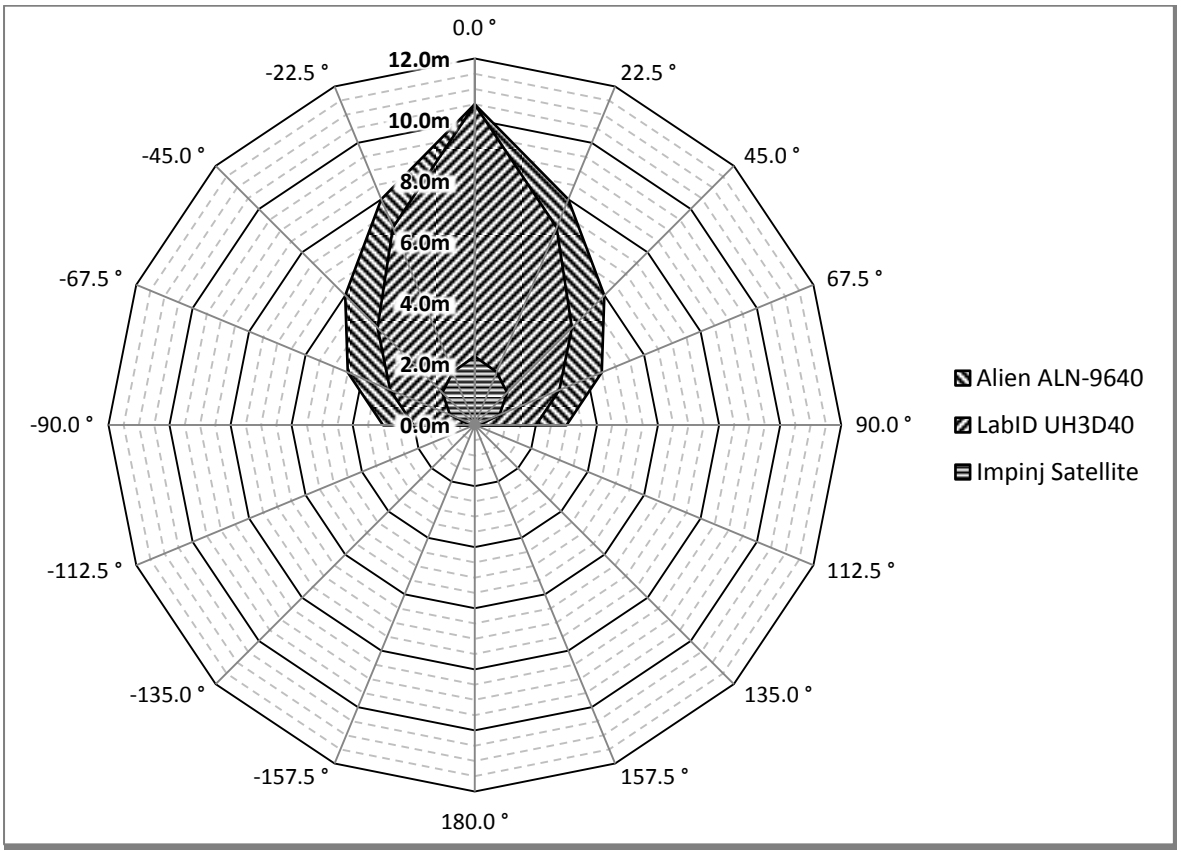

Figure 3.5 – Mapping diagram

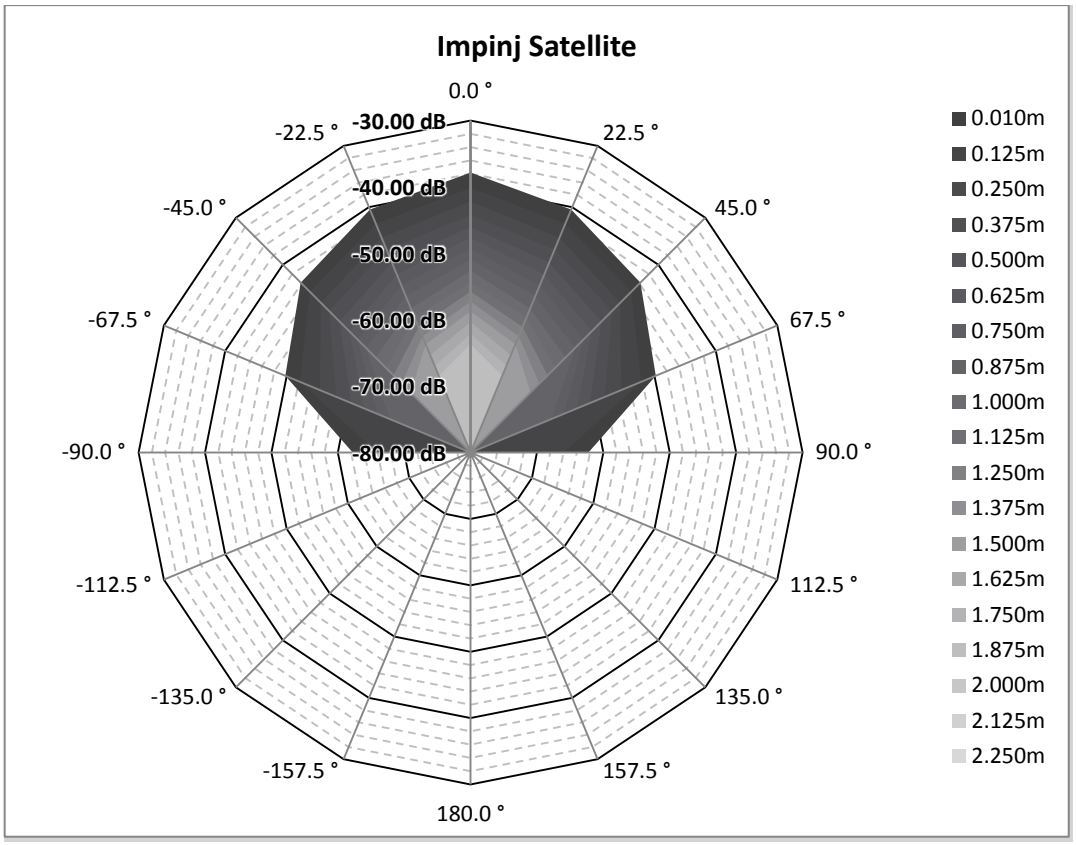

Figure 3.6 – Impinj Satellite RSSI diagram

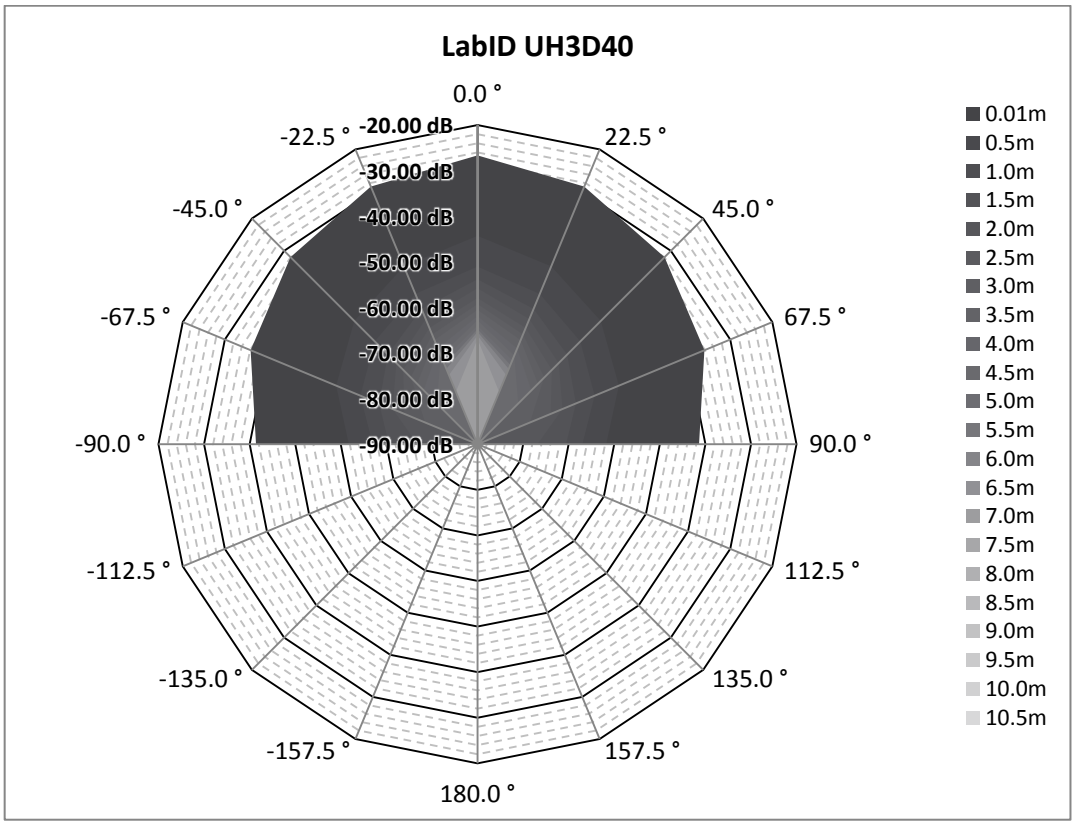

Figure 3.7 – LabID UH3D40 RSSI diagram

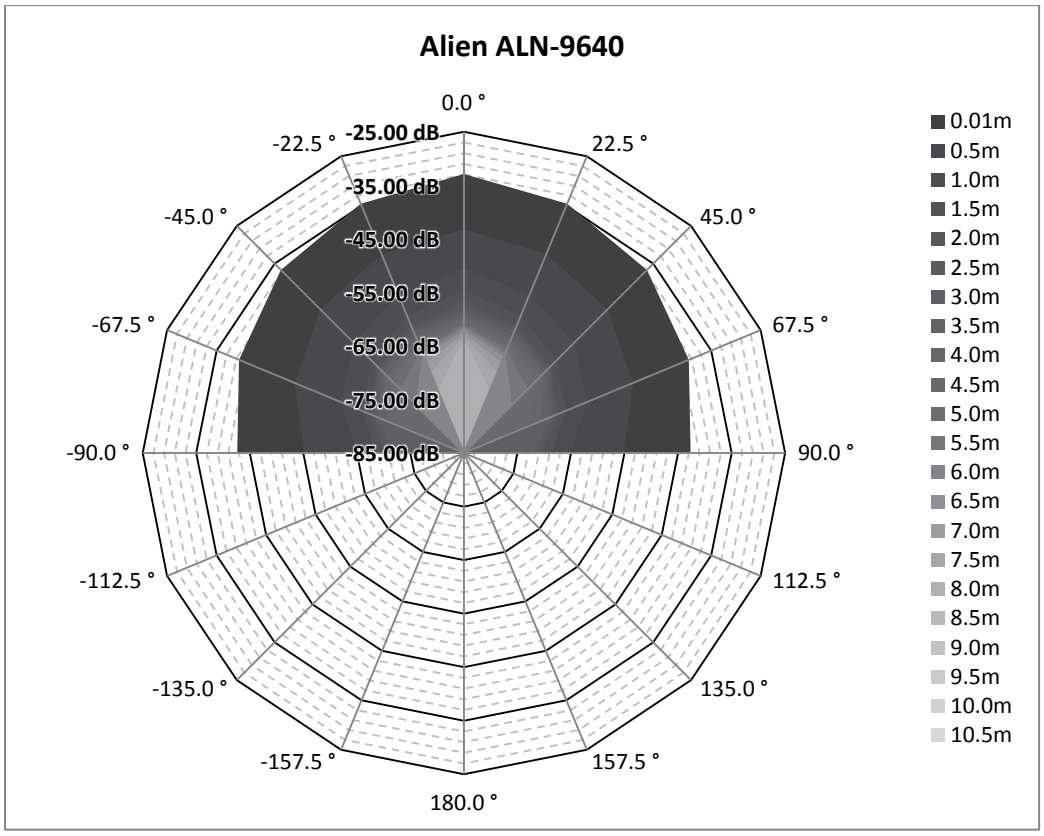

Figure 3.8 – Alien ALN-9640 RSSI diagram

In Figures 3.6-8 we can see that Impinj Satellite has the lowest performance on wide angles, where the other two perform much better, due to their newer design and the use of newer, more efficient and more sensitive tag chips. We also noticed that each tag has a different reading sensitivity boundary (Table 3.2), with the Impinj Satellite having the worst one –due to its Near-Field functionality– and the LabID UH3D40 having the best one, which is also closer to the reader's maximum reading sensitivity of -82dB. This effect is due to different tag antennas as well as different tag chips. LabID UH3D40 is an Impinj True3D-enabled tag, which introduces further improvements by providing true orientation insensitivity as well as outstanding read range performance (Fig. 3.9).

Tag	RSSI boundary
Impinj Satellite	~ -68 dB
LabID UH3D40	~ -78 dB
Alien ALN-9640	~ -73 dB

Table 3.2 – Tag RSSI boundaries

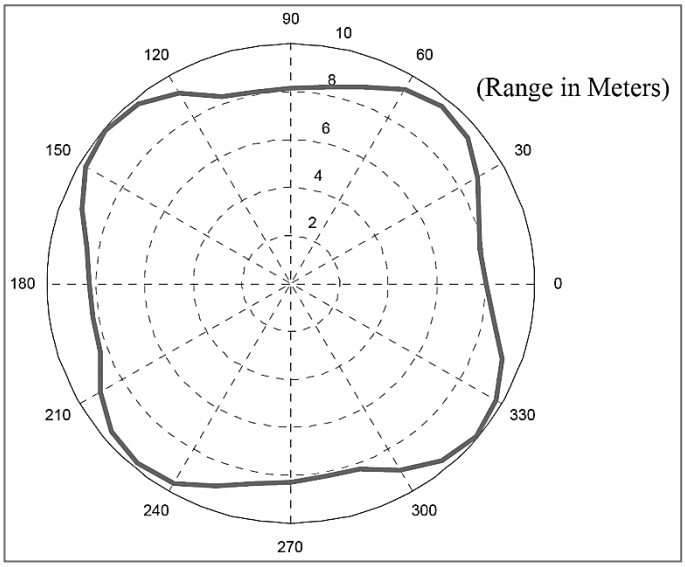

Figure 3.9 – LabID UH3D40 Range

3.2 Read Rate versus Tag-Antenna Distance

During the previous benchmarks, we managed to keep logs of our measurements, which helped us compare the various reading rates between different distance on each tag, as it can be seen in Figures 3.10-11 There was only a single tag within the scanning area each time.

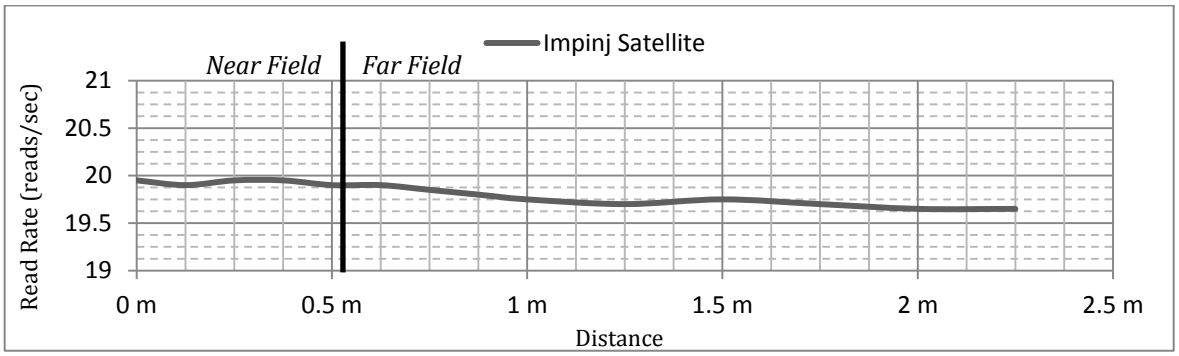

Figure 3.10 – Impinj Satellite Read rate versus Distance

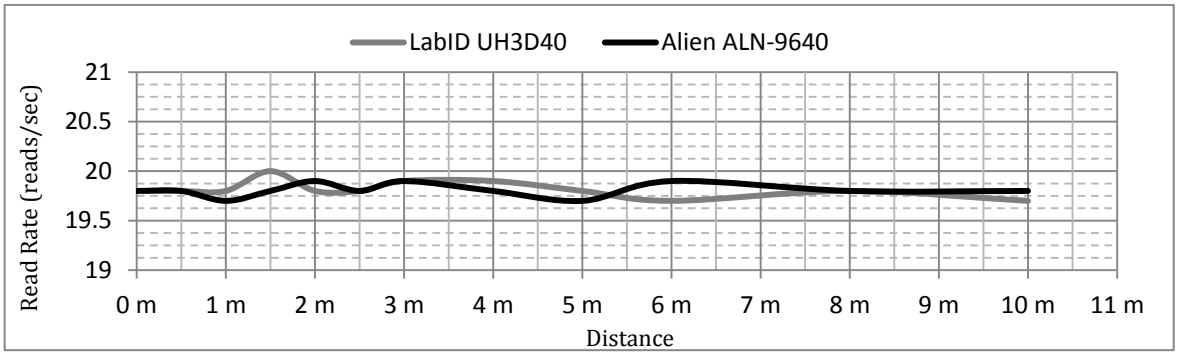

Figure 3.11 – LabID UH3D40 & Alien ALN-9640 Read rate versus Distance

As we can see, there is no noticeable difference as we are getting far from the antenna; the read rate is stable at about 20 reads per second. The only difference we noticed is with the Impinj Satellite (Near-Field) tag, where the distance was getting longer than the Near-Field boundary (0.52m in our case). Again, the reader was set at the factory default self-configuration, with one antenna connected and set at the maximum rated output power of 31.5dB.

We must keep in mind though that in large scale RFID applications there will be interference between object and other nearby tags which will result in reduced reading rates per tag, as we will see later.

3.3 Tag performance on objects of different materials

The next benchmark is to compare how tags perform when we place them either on the surface of (Fig. 3.12), or close to (Fig. 3.13) an object of different materials.

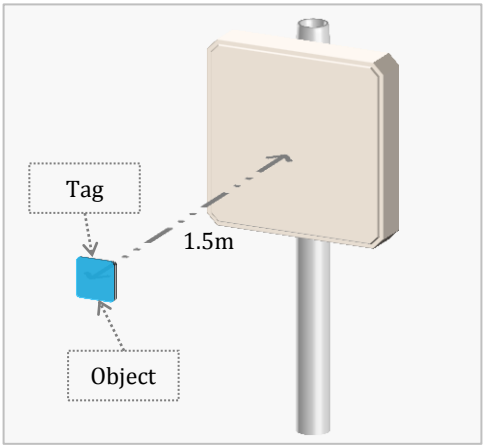

Figure 3.12 – Tagged object

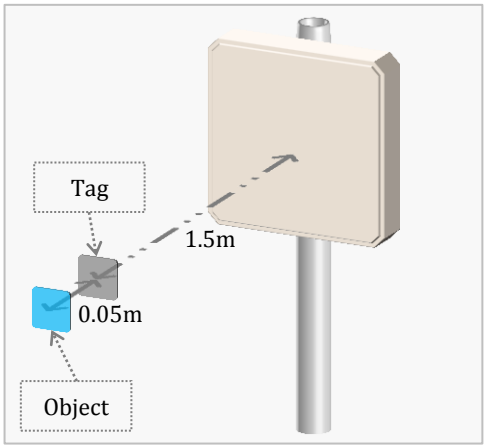

Figure 3.13 – Object behind tag

The objects we used are the following:

- Standard optical Compact Disc (CD)
- Metal Sheet, Thickness: 0.500mm / 20mils
- Aluminum Foil, Thickness: 0.016mm / 0.6mils
- Plastic Sheet, Thickness: 1.000mm / 40mils
- Wood Sheet, Thickness: 5.000mm / 200mils
- PVC Card, Thickness: 0.760mm / 30mils

The benchmark took place outdoors, with the reader set at factory default configuration, with one antenna enabled and set at the maximum rated power output of 31.5dB. The tag used in this experiment is the LabID UH3D40. The summarized results can be seen in Figure 3.14 below.

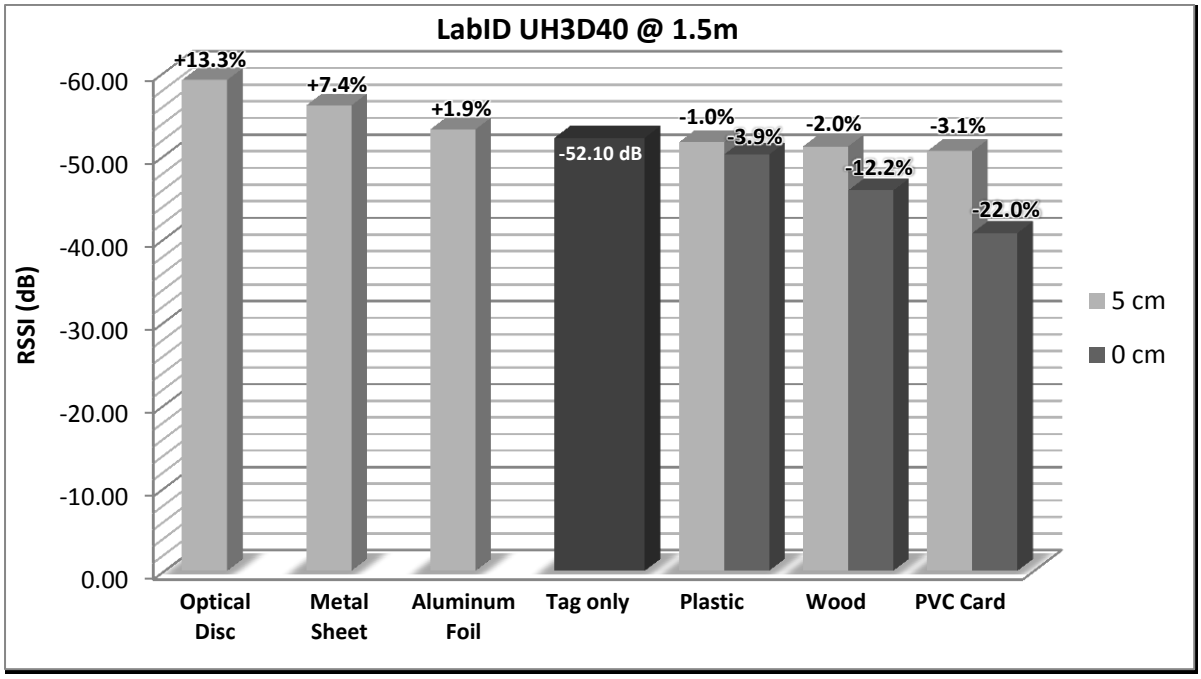

Figure 3.14 – Tag performance on different objects

The first thing we notice is that the RFID tag cannot be read while it is in contact with a metal surface (optical disc, metal sheet, aluminum foil). It can be read instead when we increase the gap between the tag and the object to about 5cm, even though the reading sensitivity is lower than with the tag alone. This leads us to the result that plain RFID tags cannot be used on objects with metallic (or even better – RF-reflective) surface; specially designed (and more expensive) tags have to be used instead. On the other hand, we see that there is an improvement on RSSI when we use objects of non-RF-reflective materials (plastic, wood, PVC), with the PVC Card giving us the best results with an improvement of 22%. This also means that there is an equal improvement in reading range. This reason, along with the increased durability of the material, makes PVC Cards a perfect combination for use with RFID tags, for example in Access Control applications (see Zebra's UHF Gen 2 RFID Card with range of up to 25 meters/75 feet [75]).

3.4 Tag interference

Large scale applications require the presence of multiple tags within an RFID reader's scanning area at the same time. This makes system designers to face with a serious issue, called RF interference. Such interference may be caused:

- when two or more tags' antennas are completely overlapping (Fig. 3.15), or
- when multiple tags are getting scanned at the same time (Fig. 3.16)

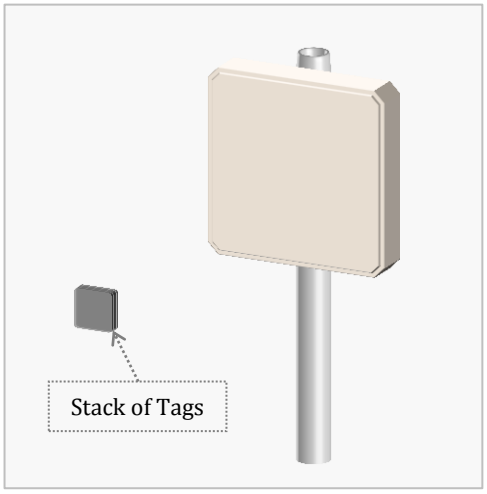

Figure 3.15 – Tag stack

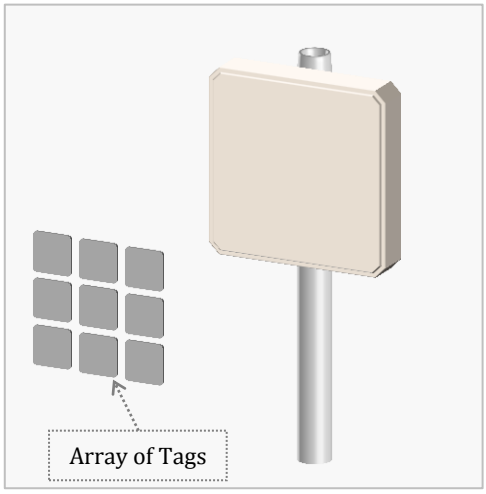

Figure 3.16 – Tag array

On both case, the reader was configured at factory default settings, with one antenna in use and set at 31.5dB.

3.4.1 Stack of Tags

On the first case, the success rate on reading tags drops down to 0% as more tags were stacked, due to the high interference of tag antennas being right on top of each other. Results, including success rates, can be seen on Table 3.3.

Tag Model	Quantity	Tags Read	Read Rate	Success Rate
Impinj Satellite	20	2	29.8	10%
	60	0	0	0%
Alien ALN-9540	5	2	39.3	40%
	10	0	0	0%

Table 3.3 – Tag stack performance

3.4.2 Array of Tags

On the second case, where multiple tags are present within the reader's read range, interference is much lower but still present. We experimented with multiple tags in order to see how read rates drop as we are trying to scan more tags. The summarized results are available on Table 3.4 and Figures 3.17-19. The success rate in all cases was 100%. The space between tags was 0.5cm and the distance between the tags and the antenna was:

- 10cm for the Impinj Satellite tags (due to its Near-Field functionality)
- 50cm for the rest of the tags

Tag Model	**Quantity**	**Read Rate**	**Reads per Tag**
Impinj Satellite	1	25.4	25.40
	2	48.8	24.40
	3	70.2	23.40
	15	194.2	12.95
	24	341	14.21
	63	478.8	7.60
	100	570.2	5.70
Alien ALN-9540	1	20.2	20.20
	2	39.5	19.75
	3	57.4	19.13
	5	90.5	18.10
	10	161	16.10
LabID UH3D40	1	23.8	23.80
	2	46.7	23.35
	3	68.2	22.73
	4	89.8	22.45

Table 3.4 – Tag array performance

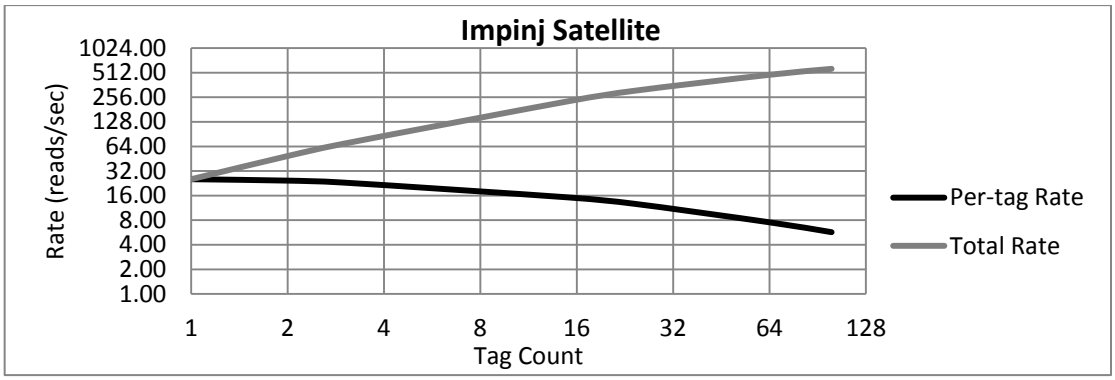

Figure 3.17 – Impinj Satellite read rate

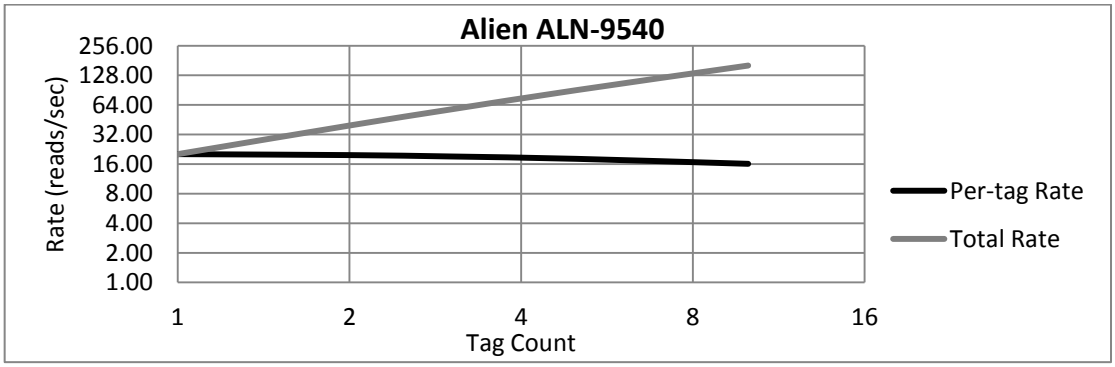

Figure 3.18 – Alien ALN-9640 read rate

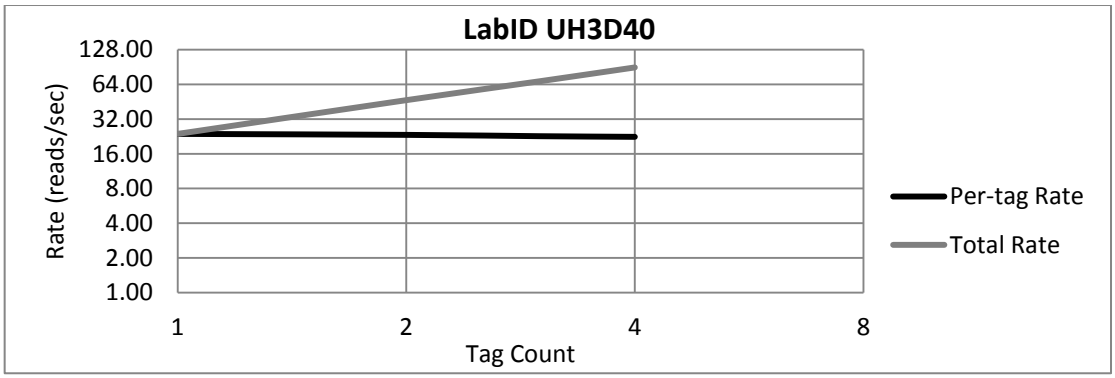

Figure 3.19 – LabID UH3D40 read rate

Then, using Far-Field tags and the same configuration, we took more in-depth measurements that can be seen on Table 3.5 and Figures 3.20-21.

Tag Model	Quantity	Min. RSSI	Max. RSSI	Avg. RSSI
LabID UH3D40	1		**-28.24 dB**	
	2	**-35.75 dB**	-30.01 dB	-32.87 dB
	3	**-38.32 dB**	-31.02 dB	-34.72 dB
	4	**-39.07 dB**	-31.57 dB	-35.41 dB
Alien ALN-9540	1		**-42.07 dB**	
	2	**-45.89 dB**	-42.97 dB	-44.53 dB
	3	**-49.38 dB**	-43.88 dB	-46.71 dB
	5	**-52.42 dB**	-44.78 dB	-48.83 dB
	10	**-55.43 dB**	-45.74 dB	-50.84 dB

Table 3.5 – Tag population interference

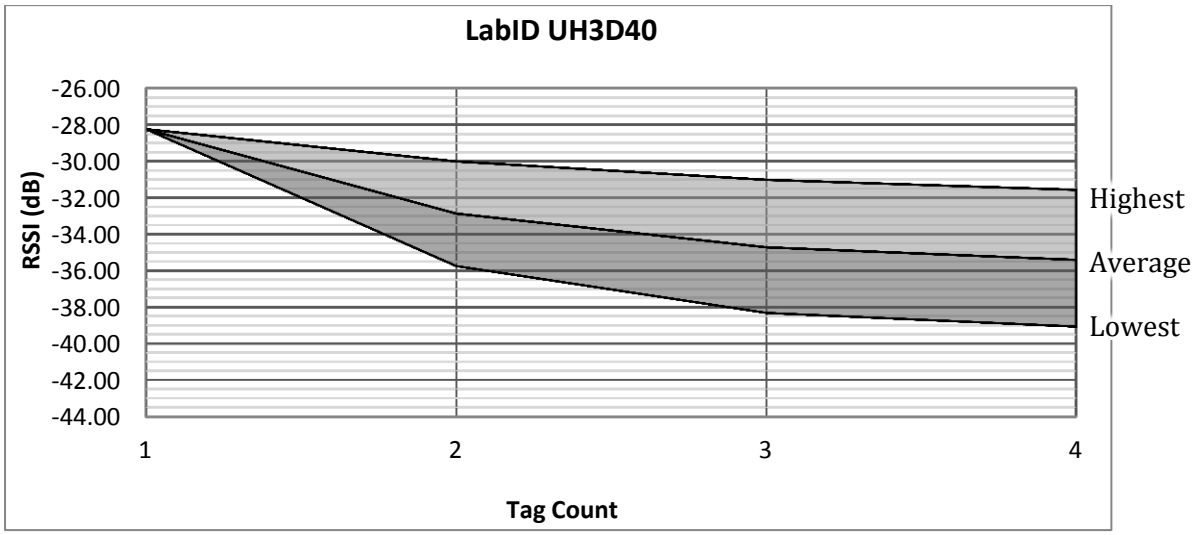

Figure 3.20 – LabID UH3D40 population interference

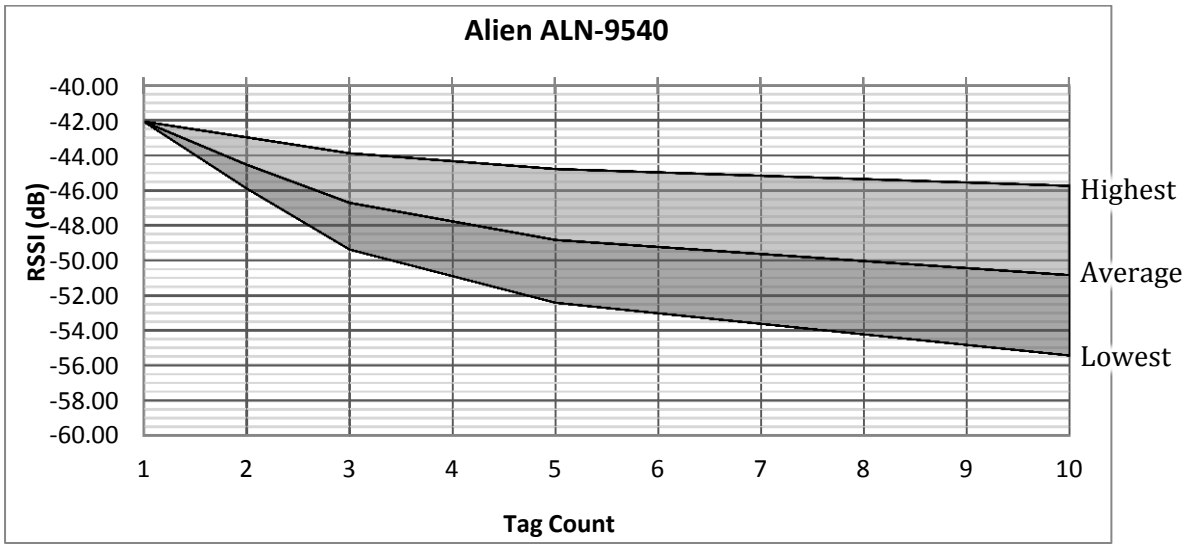

Figure 3.21 – Alien ALN-9640 population interference

As we can see, reading sensitivity is getting affected as more tags are present in the antenna's field. This leads us to the thought that except the reader's maximum read rate, we also have to consider about how many tags can be scanned at once before having any "ghost" tags due to interference. According to the end-user application, an approximate of the maximum number of tags that don't generate that problem can be estimated. Another variable to keep in mind is the type of the tag that will be used, since each tag behaves in a different way. This issue is solved by proper configuration of reader's Search Mode and Sessions.

3.5 Read range versus Antenna Output Power

Setting an antenna port of the reader at maximum power output is not always a safe way to configure an RFID system. It may give us the best range and sensitivity but it also generates some serious issues:

- **Interference**: Either with RFID systems or with other wireless systems working on the same frequency bands.

- **Eavesdropping**: When antennas transmit at high power levels, it is easier for an adversary to listen to the antenna-transmitted signals even from a hundred of meters away from the antenna.

So, configuring each antenna's power should be always taken care of when installing an RFID system.

We run the benchmark using the software supplied by Impinj (MultiReader for Speedway Gen2 RFID Reader) by changing the power output of the antenna ports of the reader in order to measure the maximum read range and sensitivity at each value. We measured distances at which we had at least 3 seconds of continuous scanning of the tag. The results are presented in Table 3.6 for both LabID UH3D40 and Impinj Satellite RFID tags, and in Figures 3.22-23. Single tags were used in each run.

Antenna Output Power	Maximum Scanning Distance	
	Impinj Satellite	LabID UH3D40
31.5dB	2.25 m	10.50 m
29.0dB	1.58 m	7.69 m
27.0dB	1.20 m	6.03 m
25.0dB	0.95 m	4.82 m
23.0dB	0.76 m	3.78 m
21.0dB	0.60 m	2.93 m
19.0dB	0.47 m	2.31 m
17.0dB	0.35 m	1.80 m
15.0dB	0.23 m	1.32 m
13.0dB	0.15 m	0.92 m
11.0dB	0.07 m	0.63 m
9.0dB	0.01 m	0.40 m

Table 3.6 – Tag scanning distance versus Antenna output power

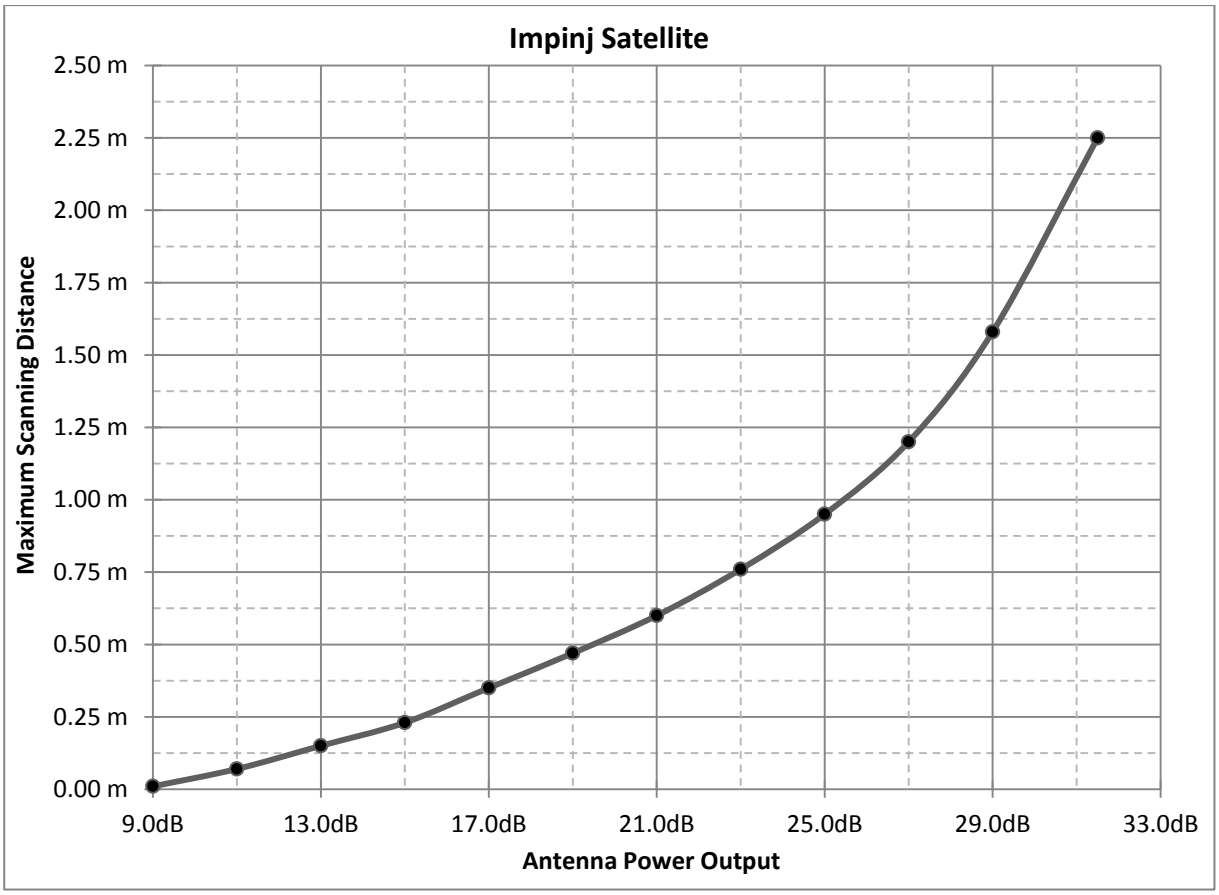

Figure 3.22 – Impinj Satellite scanning distance versus antenna power output

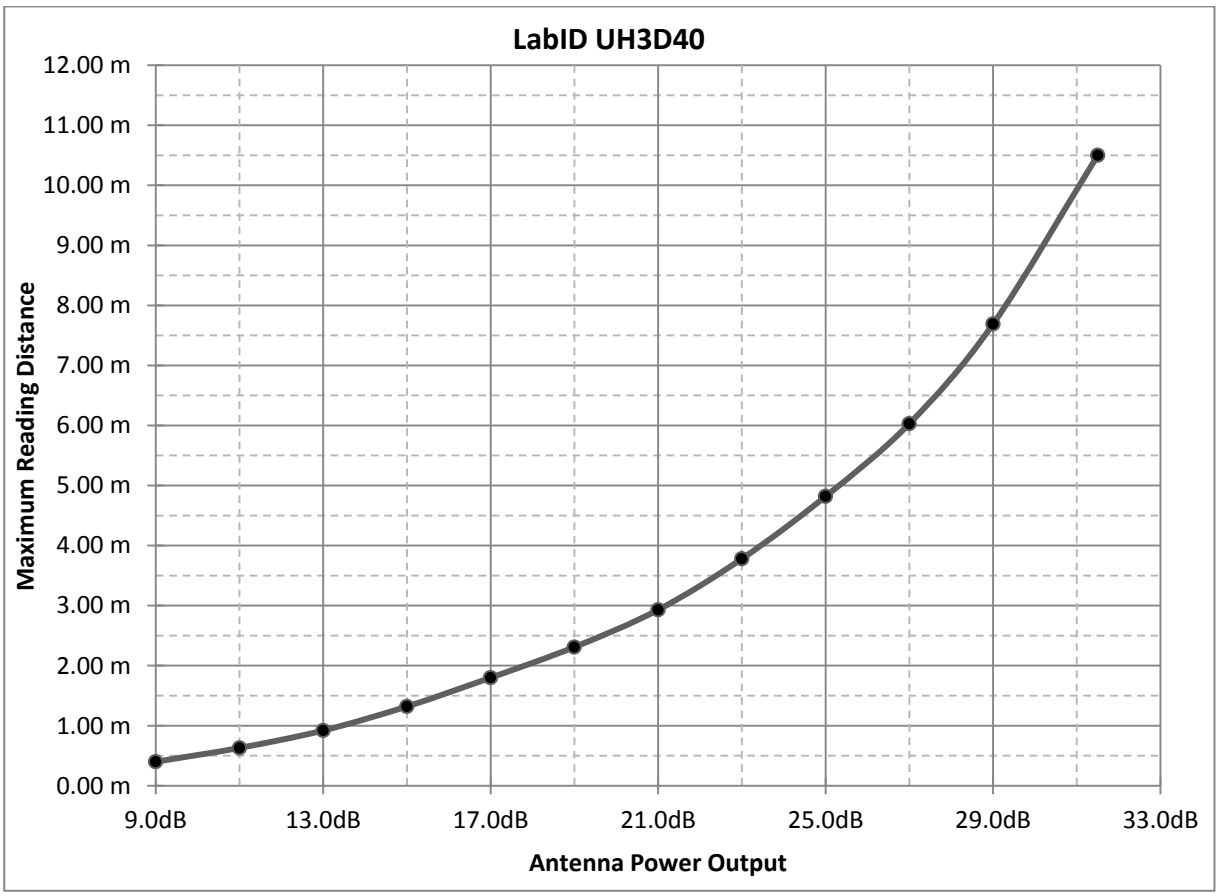

Figure 3.23 – LabID UH3D40 scanning distance versus antenna power output

3.6 Tag reading sequence

Finally, we experimented on the tag reading sequence and how that gets affected when the distance between the tags gets increased (Fig. 3.24-25).

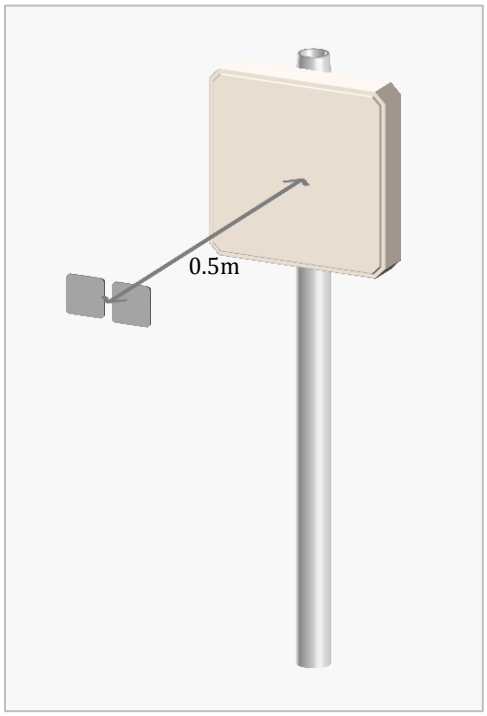

Figure 3.25 – Tags next to each other

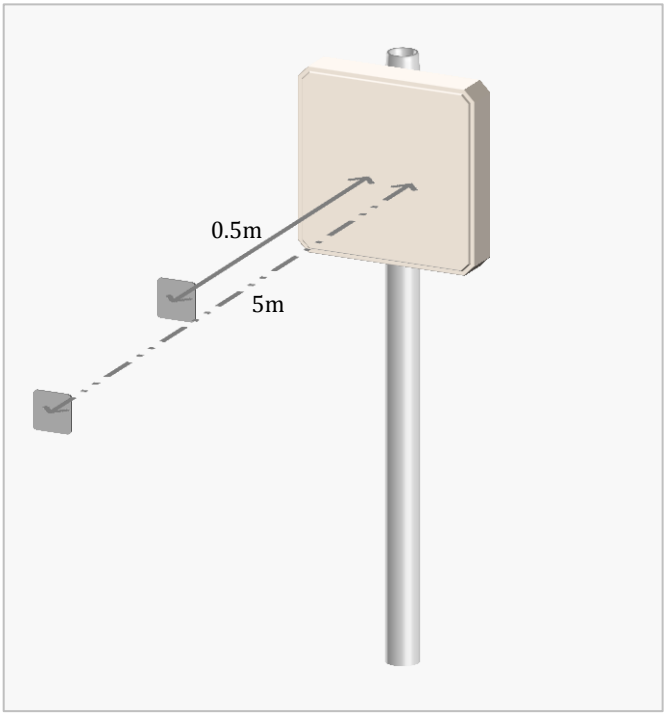

Figure 3.24 – Tags far from each other

As we saw from the results, the reading sequence does not get affected when the distance between tags gets increased. That's because of how the C1G2 protocol works. More specifically, when the reader is configured in Single Target (with/without suppression) search mode, it queries each tag once in very short time, it switches its state from A to B and then it waits until one gets back into state A. In Dual Target search mode, the reader first queries all tags in state A, then switches them to state B and re-queries them, switching them back to state A. This process repeats for as long as the reader keeps querying. So, in this case there is no difference in the reading sequence since that would mean the reader queries tags in state A as well as tags in state B at the same time.

3.7 Antenna Power Output versus Power Consumption

Proper reader configuration is necessary not only to minimize interference, but to minimize power consumption as well. We measured the power consumption of the reader on various antenna output levels, from 10dB up to 31.5dB. The measurements were taken after running an inventory for 10 seconds, with one antenna connected and 5 RFID tags within its read range. We also verified that connecting more antennas does not affect the power consumption, and that's because of the way the protocol works, using only one antenna at a time. The results can be seen in Figure 3.26 below, both for the drained current and the actual power requirements, calculated at the power outlet's voltage of 223.7V.

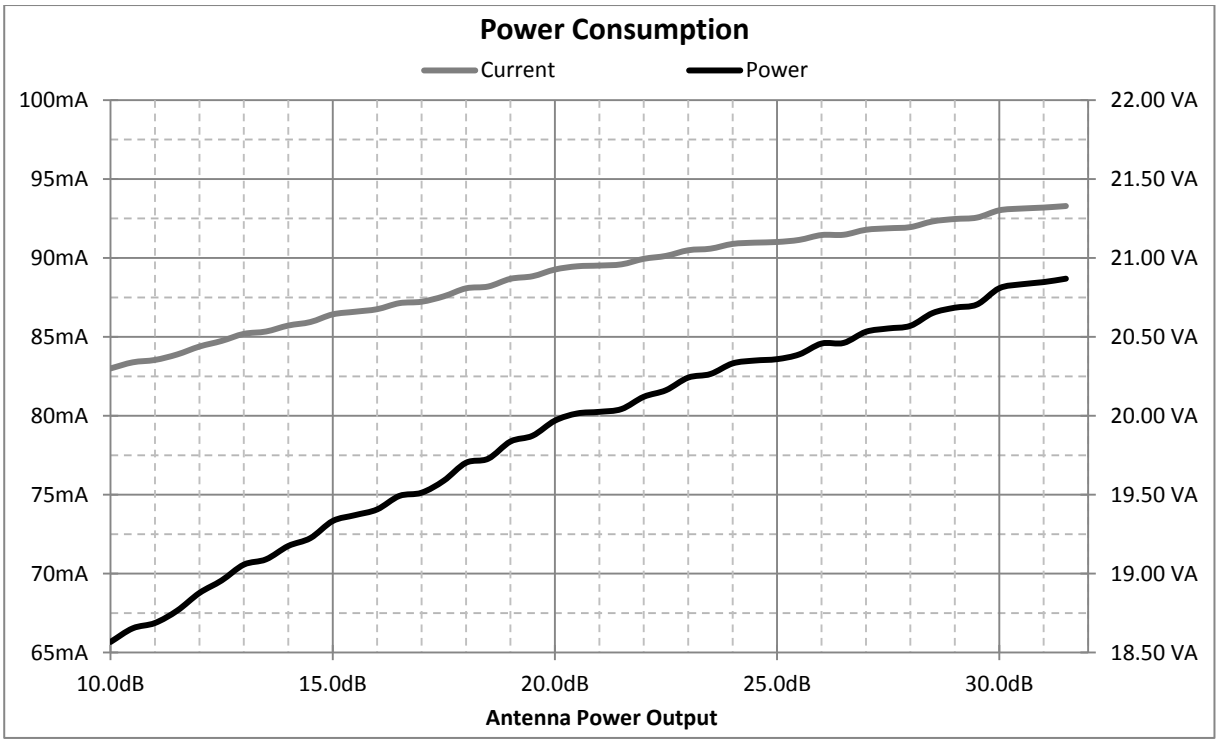

Figure 3.26 – Antenna Power Output versus Power Consumption

As we can see, there is a slight increase in power consumption as we increase the power output of the antenna, which may look negligible, but in larger applications where multiple readers are used it may be noticeable.

4 Security & Privacy

RFID technology is one of the most pervasive technologies in history. While security and privacy concerns about the possibility of abuse are existent, misinformation and hysteria should be avoided. Ways of collecting, storing and analyzing vast amounts of information about consumers and citizens existed long before the appearance of RFID technology. For example, we usually pay with credit cards, give our names and address for merchandizing, use cookies while surfing the Internet, etc.

In this chapter we first propose an overview of the risks and threats related to RFID technology, and then we will discuss possible countermeasures against one or more of these. Later we discuss the implemented software and the functionality it offers.

4.1 Components of networking security

Securing RFID systems from any unauthorized entity is a challenge, and as any other mission-critical system it is based on three major components, common to any kind of networking security as the Three Pillars: Confidentiality, Integrity and Availability (C.I.A., Figure 4.1).

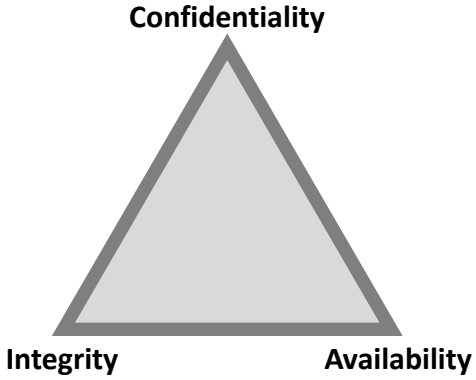

Figure 4.1 – The Three Pillars

- **Confidentiality**: Aims at limiting information access to authorized personnel only. Privacy information, such as the static identifiers transmitted by tags, fits into the confidentiality dimension. Both users and companies consider this issue of utmost importance. Furthermore, RFID technology allows the tracking of items. From a user perspective tracking should be avoided. However, companies may take advantage of it in controlling the movements of materials in the supply chains, increasing the productivity of their processes.
- **Integrity**: Ensures the accuracy and authenticity of information transmitted by the system, by preventing its accidental or malicious modification. Alteration in a RFID context may involve the capture, substitution, deletion or insertion of information and the retransmission of that altered information to a reader or a tag. Integrity of a RFID system applies to the integrity of the devices, such as the reader and the tags where it implies that a reader or a tag has not been malevolently changed. A reader receiving data from a tag needs

to be able to trust that the information received from a tag is correct, while a tag needs to be able to trust that the information it receives from a seemingly authentic reader is trustworthy. Ensuring the integrity of a system is an important consideration in addressing physical attacks, too. Spoofing (also known as Man-In-The-Middle, MITM) attack is a common threat to integrity.

- **Availability**: System availability is whether (or how often) a system is available for use by its intended users. This factor will determine the performance and the scalability level of the system. DoS attacks are usual threats against availability (i.e. active jamming of the radio channel or preventing the normal operation of vicinity tags by using some kind of blocker tag).

However, not all systems need the same security level. For example, not all systems need 99.99% availability or require that its users be authenticated via retinal scans. Because of this, it is necessary to analyze and evaluate each system (sensitivity of the data, potential loss from incidents, criticality of the mission, etc.) to determine the exact confidentiality, integrity, and availability requirements. To give another example, the security requirements of tags used in e-passports should not equal those employed in the supply chain (i.e. tag compliant to EPC Class-1 Generation-2).

4.2 Security Threats

In this section we will discuss a classification of RFID security and privacy threats divided into two main categories, based on which part of the RFID system they target (Fig. 4.2):

- **Hardware Components**: The physical devices of an RFID system (tags and interrogators), the security of which is usually not very strong. This is particularly true for low-cost passive RFID tags, since they are very resource-limited on both cost and size factors.
- **Communication**: Wireless exchange of information between tags and interrogators. Radio links usually become a prominent point of attack – everyone can listen in, and signals are easily modified or jammed.

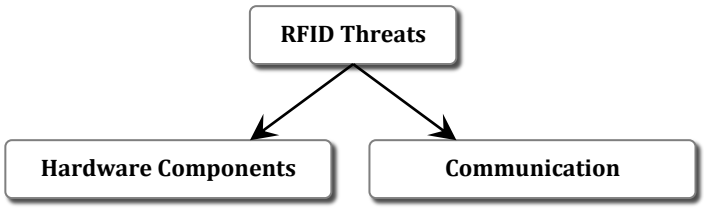

Figure 4.2 – RFID security threat division

In each of these, we will subdivide the threats according to the security property (see Chapter 4.1) that is being compromised. We won't be discussing about security of the back-end system since that part is not directly connected to the technical principles of an RFID system; it usually consists of a computer-based server connected with the RFID readers using Ethernet, which is not our central point of interest.

4.2.1 Hardware Components

This category includes attacks that may affect any of the RFID system's devices, such as interrogators and tags by exploiting their poor physical security and their inadequate resistance against physical manipulation. An overview of the threats can be seen in Figure 4.3.

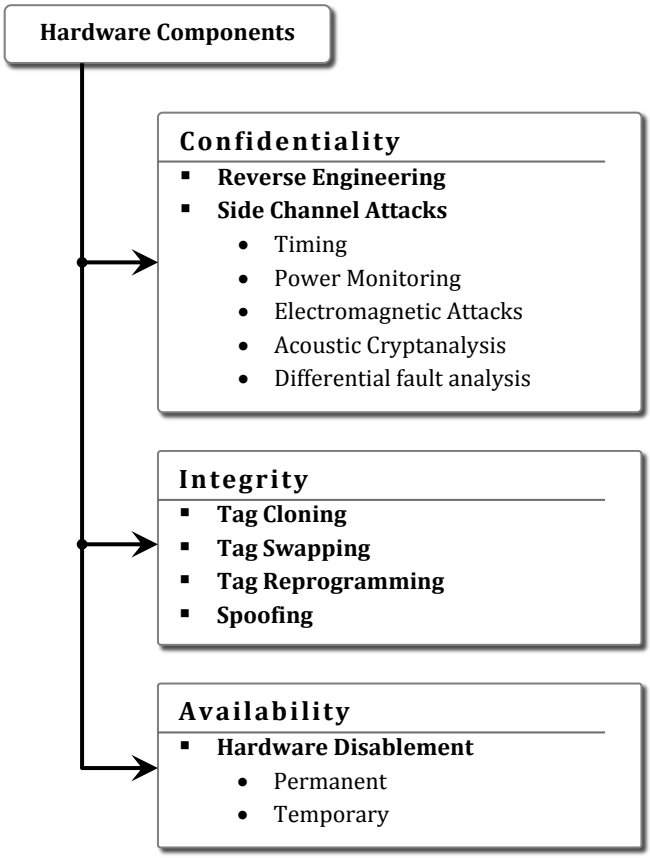

Figure 4.3 – RFID Hardware security threats

- **Confidentiality**
  - **Reverse Engineering**: Having physical access on RFID tags is always susceptible to reverse engineering attacks. Such attacks give the attacker the ability to reveal secret keys and data by proper techniques such as image analysis of the tag's IC circuits followed by protocol analysis. In a recent publication this method was used to uncover a tag chip's cryptographic vulnerabilities [12].
  - **Side Channel Attacks**: A side channel attack is any attack based on information gained from the physical implementation of a cryptosystem, such as cryptographic RFID tags. There are several types of side-channel attacks, including:
    - **Timing**: By measuring how much time various computations take to perform, one can leak information of functions used in the algorithm.
    - **Power analysis**: A side-channel attack to extract cryptographic keys and other secret information through analyzing the changes of power consumption of the tag chip.
    - **Electromagnetic Attacks**: Leaked electromagnetic radiation can directly provide plaintexts and other information if data is not properly encoded.
    - **Acoustic Cryptanalysis**: Focuses on sounds emitted by electronic components when performing computations, which may leak secret information.

- **Differential Fault Analysis**: The principle is to induce faults —unexpected environmental conditions such as high temperature, unsupported supply voltage or current, strong electric or magnetic fields, or even ionizing radiation— into cryptographic tags, to reveal their internal states.

- **Integrity**

Integrity threats related with the hardware components of an RFID system are publicly known as impersonation threats, including any kind of identity imitation action.

- **Tag Cloning**: Replication of tags is the most common aspect of impersonation and is proven to be very easy and of low cost. Tags that have no security mechanism are susceptible to identifier (ID) or even user memory cloning. Secured tags, instead, require more advanced techniques in order to imitate the legitimate one. In general, cloning means exactly what the word says, not just copying the memory banks, but making an exact copy, both visual and practical.
- **Tag Swapping**: Just like with barcodes, tag swapping refers to removing an RFID tag from an object, and attaching it to another object to imitate the first (i.e. replacing an expensive product's tag with a cheaper one's tag at a store).
- **Tag Reprogramming**: Involves either physical or wireless modification of data. Physical may be either when it is being written or by using specialized techniques and equipment directly on memory cells. Wireless modification is possible on rewritable tags by using the protocol's commands and the tag's password in order to modify its stored data.
- **Spoofing**: The main difference between tag cloning and tag spoofing is that in the second, visual representation of the original tag is not necessary. Reader spoofing is also possible, in order to imitate a legitimate reader's identity. Spoofing requires the use of more specialized equipment as well as knowledge of the authentication parameters (if any are used).

- **Availability**

- **Hardware Disablement**: Malicious hardware disablement is the most common attack on RFID system, and it can be either permanent, or temporary.
  - **Permanent**: Permanent disablement can be achieved physically either by complete removal of hardware parts such as tags, readers or antennas, or by destruction. Destruction is not always noticeable without proper inspection, and that's because of the size of the parts used. For example, an RFID tag may be destroyed by simple removing its tag chip, which is tiny enough to notice(less than $1mm^2$). Permanent disablement may also be achieved by malicious use of a tag's KILL password (if known) in order to permanently deactivate it.
  - **Temporary**: Hardware disablement may also be temporary, either by exhausting the protocols resources, or by desynchronizing the communication. As we mentioned before, C1G2 protocol allows a tag to be read only once every 50-60 seconds when the readers are configured to do so (see section 3.5 for more details). That could be maliciously used in order to temporarily make an RFID tag invisible. Desynchronization is also possible when the authentication protocol used by the system depends on some sort of synchronization between tags and readers (i.e. timestamps or rotating keys). In that case, a desynchronization may occur if values are not mutually updated on both sides as required, making the system unstable.

4.2.2 Communication

This category includes attacks that may either affect or take advantage of the communication between RFID readers and tags. An overview of the threats can be seen in Figure 4.4.

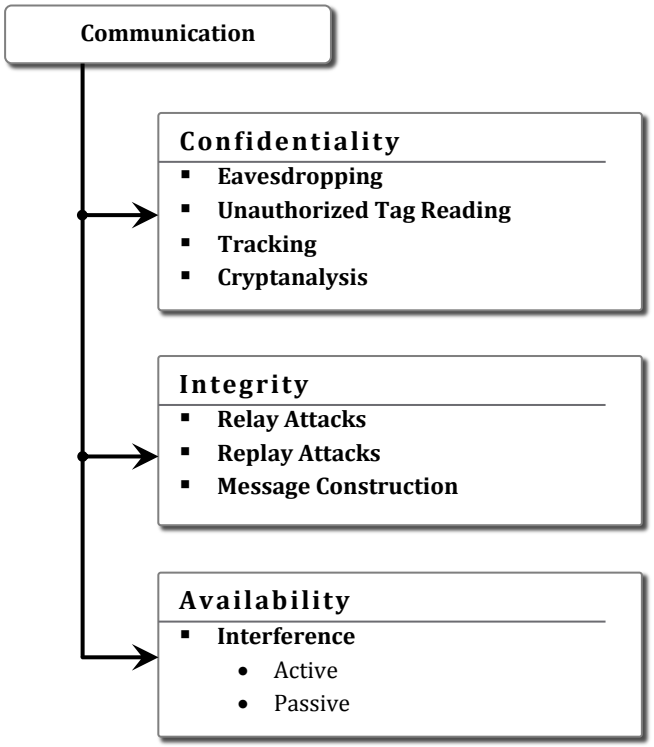

Figure 4.4 – RFID Communication security threats

- **Confidentiality**
  - **Eavesdropping**: RFID technology operates through radio, so communication can be surreptitiously overheard. An eavesdropper may intercept messages, in either the forward or the backward channel in order to extract sensitive data including secret keys. Usually, the forward channel can be listened to from a higher distance compared to the backward channel when using passive (thus of low-power) RFID tags.
  - **Unauthorized Tag Reading**: Since most low-cost RFID tags lack of any kind of authentication scheme, adversaries may easily read their contents (even from large distance) without leaving any trace.
  - **Tracking**: Most of the time, RFID tags provide the same identifier. Although an attacker cannot obtain the information about the tagged item, an association between the tag and its holder can easily be established. Even where individual tags only contain product codes rather than a unique serial number, tracking is still possible using an assembly of tags (constellations).
  - **Cryptanalysis**: This threat includes all kinds of cryptographic attacks, including brute force, chosen cipher-text attack (CCA), chosen plaintext attack (CPA) and collision attacks. Such attacks have already been used and demonstrated on cryptographic RFID tags in the past (Mifare Crypto-1, Dutch Public Transport ticketing).

- **Integrity**
  - **Relay Attacks**: Also known as "Man-In-The-Middle (MITM)", this attack is a form of active eavesdropping. In this, the attacker works between the tag and reader as an interface and gives the illusion to them that they directly communicating to each other,

when in fact the entire conversation is controlled by the attacker. The attacker easily intercepts all messages going between the tag and reader and also injects new ones, in wireless channel when attacker is in reception range of RFID system. This kind of attacks target in either imitating of a legitimate reader/tag, or modification of data in tags/backend systems by modifying transmissions. Two devices are involved in the relay attack: the ghost and the leech. The ghost is a device which fakes a tag to the reader, and the leech is a device which fakes a reader to the tag. A fast communication channel between the legitimate reader and the victim tag is created by the ghost and the leech:

1. Legitimate reader sends a message (A) to the ghost.
2. Ghost receives it and forwards this message (A) to the leech through the fast communication channel (minimum delay).
3. Leech fakes the real reader, and sends the message (A) to the legitimate tag.
4. Legitimate tag computes a new message (B) and transmits it to the leech.

- **Replay Attacks**: These are attacks in which the attacker uses a tag's response to a rogue reader's challenge to impersonate the tag. The main concern here is in the context of RFIDs being used as contactless identification cards (in substitution of magnetic swipe cards) to provide access to secured areas and/or resources. In such applications, RFIDs can be more vulnerable than other mechanisms, again due to their ability to be read at a distance by covert readers. Common techniques to avoid replay attacks are incremental sequence number (it can still be tracked though), or a nonce (random session variable).
- **Message Construction**: Protocols that make use of nonces are vulnerable to this kind of attacks when not properly designed. In message construction, forward security is breached when the attacker is able to construct new valid messages by capturing and analyzing previous authentication messages.

▪ **Availability**

- **Interference**: Interference is a very common threat to all kinds of communications, mostly wireless ones, from television signals to IEEE 802.11 (Wi-Fi). RFID is one of them.
  - **Active**: Active interference happens when any kind of RF signal interferes with the RFID systems functionality. This can be either environmental noise from nearby electronic devices (such as switching power supplies) or fraudulent. An attacker may actively interfere with an RFID system using RF jamming devices, by taking advantage of the properties of an RFID system of ceaselessly listening to all radio signals in its frequency band. A different approach on active interference is by improperly using Blocker Tags [85].
  - **Passive**: As stated in Section 1.3, the higher the frequency of an RFID system, the higher the interference with RF reflective objects such as metals, liquids, walls and (not-only-)human beings. That's what passive interference is about. Effects of passive interference vary from absorption and reflection to frequency detuning and more complex propagation effects.

4.3 Maximum security mechanisms commercially available

This section describes the security mechanisms currently provided by existing passive low-cost UHF RFID systems.

4.3.1 EPC Class-1 Generation-2 Protocol

On Class-1 Gen-2 tags, a 16-bit CRC is applied to the EPC for error detection. In addition, a 16-bit CRC is used for error detection on certain reader-to-tag commands and certain tag-to-reader responses. Class-1 Gen-2 tags also have a larger, 32-bit, kill password. The default value for a tag is all zeros and tags will not execute the kill command if the password is set to all zeros. If the tag has a nonzero password and the reader supplies it, then the tag will execute the kill command, which permanently disables the tag.

Class-1 Gen-2 tags have the ability to generate a 16-bit random or pseudo-random number (PRN), which is used to create a handle during singulation instead of using the EPC number, to encrypt reader-to-tag link communication, and to determine the number of slots to wait in the Q protocol. The 16-bit PRN is used during the inventory phase as a unique identifier that the reader is to acknowledge. Using a random number enhances security by obscuring the identity of the tag.

Although, the random number is sent from the tag to the reader unencrypted. Therefore, the random number may be intercepted by an attacker. However, the tag-to-reader link is much weaker (80-90 dB) than the reader-to-tag link, which reduces the probability that it can be intercepted. This is a trade-off between security and the cost of the tags. The write, kill, and access commands from the reader to the tag obscure the communication with a one-time pad using a 16-bit PRN from the tag. The reader requests a 16-bit PRN from the tag. The tag responds with the 16-bit PRN. The reader then encrypts the commands by performing a bit-by-bit exclusive OR (XOR) using the 16-bit PRN. The tag decrypts the commands with the same 16-bit PRN.

Furthermore, the Class-1 Generation-2 protocol offers some level of security regarding the modification of a tag's data. More specifically, a user is able to lock or unlock one or more of the tag's memory banks using the tag's 32-bit Access Password which is user-editable. Each memory bank can be in one of four lock states:

1. **Unlocked**
2. **Perma-unlocked** (can never be locked)
3. **Locked**
4. **Perma-locked** (can never be unlocked)

The memory banks are the following five:

- Reserved Memory[0:31] (**Kill Password**)
- Reserved Memory[32:63] (**Access Password**)
- **EPC Memory**
- **TID Memory**
- **User Memory** (Not all C1G2 RFID tags provide User Memory)

From these, only reserved memory bank (access and kill passwords) can be both write and read locked; all others (EPC, TID, and User) can be write-locked only. Typically, the Tag Identification (TID) memory bank is perma-locked at the factory. Lock status cannot be read, it can only be inferred. So there is no direct way to query a tag and have it reply if it is locked or not. However, in some cases when attempting to access a tag memory bank, it will return a pretty specific error

"tag memory locked". In order to lock a factory-default tag, a user should follow the following steps:

1. **Set password**: Assign a 32 bit (8 hex character) access password, this will prevent the tag lock state from being changed later
2. **Lock memory**: Lock (or perma-lock) the selected memory bank using the previously assigned password
3. **Lock Password**: Lock the Access Password - this will prevent the password from being read or over-written. Not doing this step would allow any user to simply read the access password, and then use it to unlock and over-write memory on the tag (unless it has been perma-locked).

In addition to the increased memory size, the Impinj Monza 4QT tag chips (512-bit of User memory) offer the ability to independently lock four, fixed, 128-bit sections of user memory (block perma-lock). This feature is particularly useful for situations such as in a supply chain, where various participants along the chain may want to record data, but not necessarily have it be openly available to all parties. Also, since Monza 4QT tag chips offer increased TID memory banks which is partially editable (Public EPC), that part of the memory is lock-able as well. The Impinj Monza X-2K tag chip (2176-bit of User Memory) instead offers five lock-able blocks of user memory (4x 512-bit & 1x 128-bit blocks).

4.3.2 Impinj QT Technology

The Impinj Monza QT-enabled tag chips (currently Monza 4QT and Monza X-2K) feature Impinj's patent-pending QT technology; a unique ability to maintain two data profiles (one public, one private), allowing confidentiality of business-sensitive data while assuring consumers of privacy. With QT technology, tag owners can use a private data profile to store confidential data, while a public data profile holds less sensitive information. The ability to switch between these two profiles is protected by the tag's 32-bit Access password, physical distance from a reader antenna via a short range mode, or both. One example where such a feature would be useful is in a supply chain for luxury goods. The manufacturer may want to include information in the tag that would provide a guarantee of authenticity, record the time and place of manufacturing for guarantee purposes, or include serial numbers. After that item is packaged for distribution, however, such details might provide a security risk. If anyone possessing a reader can determine details about what is in a particular box, high-value goods could get diverted. The QT Technology's unique set of features helps to solve this problem.

The Private/Public profile capability, available in Monza 4QT tag chips, provides two memory configurations (i.e. profiles) in a single chip; one Private and one Public. A Monza 4QT chip only exposes a single profile at a time. Table 4.1 shows the chip's memory configurations when in either profile.

Memory Bank	Private Data Profile	Public Data Profile
Reserved	Kill Password: 32-bit Access Password: 32-bit	Kill Password: 32-bit Access Password: 32-bit
EPC	Private EPC: 128-bit	Public EPC: 96-bit
TID	TID: 32-bit TID Header: 16-bit Serial Number: 48-bit Public EPC: 96-bit	TID: 32-bit
User	512-bit	N/A

Table 4.1 – Monza 4QT data profiles

In Private profile, the EPC typically contains an item serial number. The User memory might hold detailed information about the item. The TID memory, which includes a 32 bit base TID, a 16 bit

extended TID header, and a 48 bit serial number, uniquely identifies the tag chip itself. Also included in TID memory is a 96 bit Public EPC, which is field-writeable by a user. In typical applications, the user writes a Public EPC value into this memory location then "publicizes" the tag. Although users are free to encode as little or as much information into this 96 bit Public EPC field as they chose (including no information at all), Impinj recommends certain usage guidelines to prevent these 96 bit Public EPCs from colliding with other tags. At any point in the supply chain, for example at point-of-sale, users have the ability to switch QT tags to the Public profile. Once switched, the tag conceals its 128-bit Private EPC, 512-bit User Memory, 16-bit TID header, and 48-bit serial number. The tag exposes its Public EPC in EPC memory, remapped from its prior location in TID memory. When the tag is singulated, it sends this 96-bit Public EPC instead. The only other information available to a reader is the 32 bit base TID. All other private memory contents appear non-existent to a reader reading the tag. The Private/Public profile features of the Monza 4QT tag chip are controlled by the QT command. Tags may be switched from Private profile to Public profile and back again, using the QT command. This QT command can be protected by a Short-Range Feature, by the tag's access password, or by both.

To secure the Private profile tag data, Monza 4QT chips offer a Short-Range feature. The Short-Range feature adds a layer of physical security by preventing readers farther than roughly one meter from the tag from switching the tag from Public to Private (or vice versa) (Fig. 4.5).

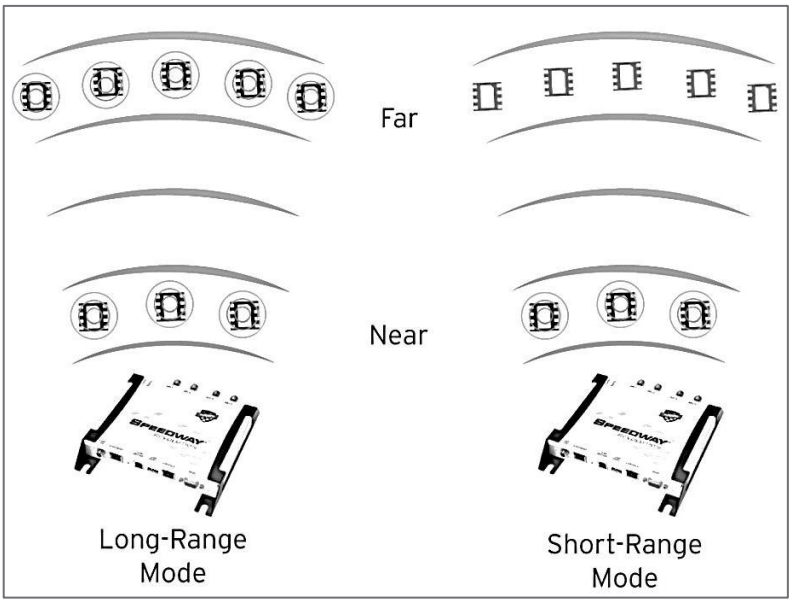

Figure 4.5 – Monza QT short range feature

When Short Range is enabled, the tag reduces its sensitivity by about 15dB. The tag has normal sensitivity during singulation. However, before executing a lock/unlock command, the tag checks the RF power level; if it is above the short-range threshold then the tag will execute state, otherwise the tag will reset back to the "listening" state. A reader is always able to read a tag's currently exposed EPC (Public EPC or Private EPC, as appropriate for the current profile) at maximum range. This feature ensures that the information the tag's rightful owner wants to protect is not readable unless the tag is close to a reader antenna. As a further layer of protection, the Access command defined in the Gen 2 specification is fully operable for QT-enabled tags. In short, a QT tag can use physical protection (Short Range), logical protection (Access password) or both to prevent unauthorized access.

Additionally, to help prevent situations where a Public tag is switched to Private by an authorized user (for example to read User memory) and inadvertently left in the Private mode, Monza QT-enabled tag chips offer a Peek feature. With Peek, a reader can temporarily switch a

Public tag to Private, access the Private information, then when the chip loses power it will automatically revert to its Public profile.

4.4 The Competing Objectives

Ideally, the most suitable lightweight cryptographic primitive would be highly secure, inexpensive, and consume negligible power. However, the reality is that providing security to resource limited platforms is a compromise between divergent parameters. A security primitive needs to balance between cost, level of security, performance and usability of the solution [77]. These trade-offs explain the challenges behind research on lightweight cryptographic primitives. Competing factors illustrated in Figure 4.6 (Cost, Performance and Security) implies that ciphers achieve a good enough compromise between each factor for a given application.

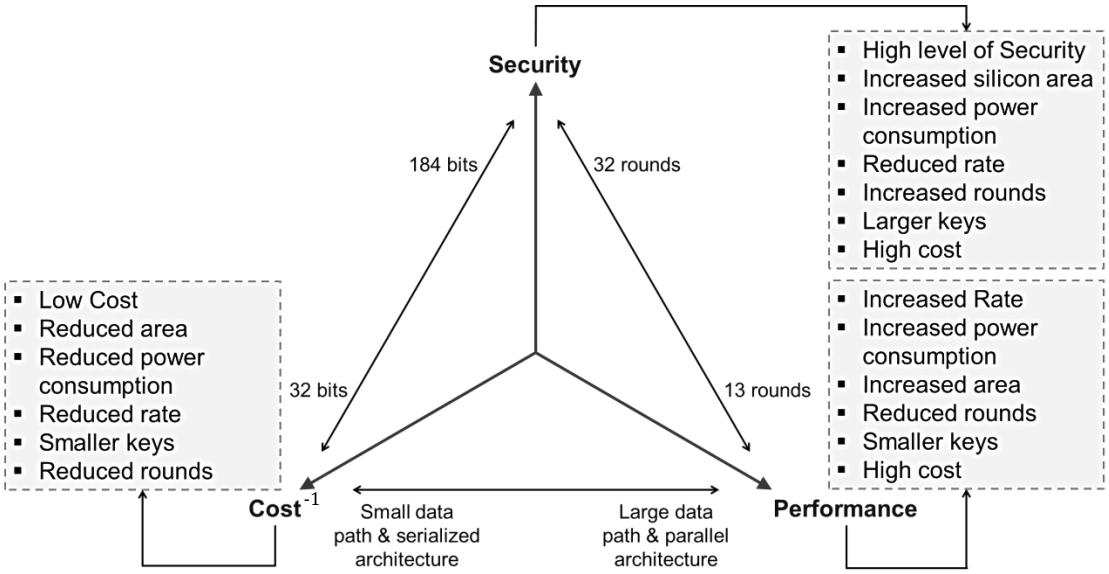

Figure 4.6 – Cost, Performance & Security trade-off

Every designer of lightweight cryptography must cope with the trade-offs between security, cost, and performance. It's generally easy to optimize any two of the three design goals—security and cost, security and performance, or cost and performance; however, it is very difficult to optimize all three design goals at once. For example, a secure and high-performance hardware implementation can be achieved by a pipelined, side-channel-resistant architecture, resulting in a high area requirement, and thus high costs. On the other hand, it's possible to design a secure, low-cost hardware implementation with the drawback of limited performance.

In our case, the most important and resource limited factor of the three mentioned above is the cost of the RFID tag, that is, limited to less than 5¢ and mostly defined by the complexity of the chip (or integrated circuit, IC). The complexity of the chip can be described by several informal metrics [78] like the number of transistors or the gate equivalent (GE), or gate count, that is about a fourth of the number of transistors. The gate count of current low-cost transponders is 5,000 – 10,000 [79], limiting their computational power to only a fraction of that of computers. In addition, the number of gates available for security features is even smaller and estimated to be below 2,000 [80] or below 5,000 [55]. The rule of thumb of gate cost says that every extra 1,000 gates increase the chip price by 1¢ [80]. Another important factor one has to

consider when dealing with security in Low-Cost RFID is the clock frequency at which the integrated circuit processes data, which is only 100 kHz. This has been proven to be the golden edge between maximum performance and minimum power consumption/silicon area [58].

4.5 Improving Security & Privacy

Summarizing from the previous chapters, we can now organize and refer the proposed solutions in hardware of two categories:

- RFID Tags **without** Cryptographic capabilities
- RFID Tags **with** Cryptographic capabilities

The first category refers to solutions on current RFID systems, where no new hardware can be purchased or installed, but an additional level of security is required, while the second category refers to new hardware designs where a new system is designed and a maximum level of security is required. A summary of the proposed solutions is available in Table 4.2.

Non- Cryptographic Tags	Cryptographic Tags
• Tag Killing	• Password Lock
• Tag Shielding	• Distance Bounding Protocols
• Triangulation	• Hash Lock
• Active Jamming	• Lightweight Cryptography
• Tag Blocking	• Ultralightweight Protocols
• Randomized (Re)Encryption	• Tree-Walking Improvements
• Antenna Configuration	• Kill Password Authentication
• Isolation	
• Read-Only Tags	
• Physical Protection	
• Data Storage	

Table 4.2 – Proposed improvements over RFID security & privacy

Other than that, we suppose that the back-end system and the communication channel between that and the RFID readers are secure.

4.5.1 RFID tags without Cryptographic capabilities

Protecting RFID tags with no encryption capabilities is one of the most challenging jobs, since multiple actions are necessary in order to achieve an acceptable level of security. Note that some of the proposed solutions may also generate other threats if used maliciously. More specifically, we discuss ways to protect the user's privacy and the system's security when there is no encryption used:

- **Tag Killing**: When a tag has served its purpose and is no longer used (i.e. when a tagged product is sold to a customer), it can be permanently deactivated using a specific 32-bit PIN key, called Kill Password in C1G2 protocol. It is necessary to only take that action when the tag is not needed any more, since killing a tag is non-reversible. This way the tag is like completely destroyed, just like if there was no tag on the product, so tracing or information leakage is not possible. Furthermore, the use of randomized and different Kill password for each tag is required in order to prevent unauthorized tag killing even if one of the

passwords gets leaked or eavesdropped. The major disadvantage of tag killing is that it also eliminates the future applications of the tag.

- **Tag Shielding**: Wrapping an RFID tag inside an enclosure or mesh formed of a conductive material (see Faraday Cage, [84]) blocks the communication between the tag and the reader if the conductor is thick enough and any holes in the mesh are significantly smaller than the radiation's wavelength. By shielding a tag we increase the privacy of the user, who can make the tag available for scanning only when necessary. The main disadvantages of tag shielding, is the high cost and the possibility of deceitful usage.
- **Triangulation**: Usually, the use of multiple antennas is needed when scanning a specific area, in order to achieve maximum area coverage without requiring specific tag orientation or routing. That can also help to improve the security of an RFID system against attacks like spoofing or relay, by using triangulation and by measuring the strength of the received signal. With triangulation we can calculate the exact location of the transmitting RFID tag and thus limit the access to only specific areas or distances, with only requirements that at least 3 antennas receive the signal of the transmitting RFID tag. By measuring the strength of the received signal we can approximate the distance between the reader and the tag and limit the access to a maximum distance. This solution may have high installation cost and requires proper configuration, but it offers an increased level of security for some applications without requiring the use of expensive cryptographic RFID tags.
- **Active Jamming**: Using a custom device that broadcasts RF signals at a specified frequency range and various time intervals, a system may disrupt unauthorized nearby RFID readers in order to prevent unauthorized reads. This action, though, requires proper configuration on the system's readers in order to prevent stability issues and not exceed the maximum transmitting power levels.
- **Tag Blocking**: A different way of protecting the user's privacy is by selective blocking of RFID tags using passive devices called blocker tags [85]. A blocker tag is a cheap passive RFID device that can simulate many ordinary RFID tags simultaneously. When carried by a consumer, a blocker tag thus "blocks" RFID readers by causing forced collision. It can do so universally by simulating all possible RFID tags, or selectively by simulating only selected subsets of ID codes, such as those by a particular manufacturer, or those in a designated "privacy zone". The way it works is by exploiting the anti-collision protocol that RFID readers use to communicate with tags. This protocol is known as singulation. One type of RFID singulation protocol is known as tree walking. A blocker tag, blocks the reader from successfully allowing a tag that is in the interrogation zone to successfully respond with its unique ID number. The blocker tag achieves this by causing a collision for each bit in the request from the reader. In effect this would "jam" tags that the consumer has in their possession, preserving their privacy but allowing the tags to remain active.
- **Randomized (Re)Encryption**: A different way to prevent tracing of tags is by using encryption, but without requiring cryptographic capabilities on them. The way it works is that the stored cipher text is randomized whenever the tag is in range of a legitimate reader. The use of efficient, secure and well-known cryptographic algorithms is necessary in such solutions in order to minimize cryptographic attacks. The tag, though, can be vulnerable to traceability if it is in range of non-legitimate readers between two legitimate reads. This also means that when a tag is not used any more (i.e. when a tagged product is sold), it has to be deactivated to prevent it from being traced. Such solutions have already been proposed in [86] (refer to section 2.2 for more information) and [87].

- **Tag Class Selection**: As we mentioned on Chapter 1.2.1, a tag's EPC memory can be either Read-Only, or Read-Write, while its range can vary from a few meters to a thousand meters. Using Read-Only tags when changing the EPC memory is not a necessity, prevents the possibility of the Data Modification threat we discussed previously, while using short range tags prevents tag scanning and eavesdropping the backward channel at long distances.
- **Physical Protection**: Protecting the physical layer of an RFID system and more specifically its components is a threat that appears on most physical systems. In our case, RFID tags can be protected by using flexible and tamper-resistant RFID tags and when possible, embedding the on products instead of applying them on the product's packaging (i.e. in clothes).
- **Product Characteristics**: Another feature that could be implemented in current RFID systems in order to reduce fraudulent actions is to store product specific characteristics such as weight and size on the backend database. That way, when for example we want to check out at an RFID-enabled store, the RFID system could also check the total weight of the order. Of course that is not applicable in products with the same weight and it doesn't offer maximum security, but it's another non-trivial improvement over security.
- **Back-end Storage**: Storing sensitive data in the tag's user memory, even when using encryption, is always susceptible to either hardware or software attacks. Thus, storing data in the tag's user memory should be limited to only when necessary, while keeping sensitive data on a back-end database.

As mentioned previously, UHF RFID systems use multiple frequency channels in order to communicate with multiple RFID tags. Both active and passive interference could lead to interruption of RFID communication or even to a complete crash of the identification systems deployed in companies, organizations and merchant stores. Some ways to protect against such threats is by proper antenna configuration and area isolation as described below.

- **Antenna Configuration**: Passive interference could be minimized by using different frequency channels on different antennas and/or readers and proper antenna location/positioning where multiple antennas are used at the same scanning area. Also, limiting each antenna's output power at the maximum necessary (and not at the maximum available), reduces the forward channel's eavesdropping range (Fig. 4.7).

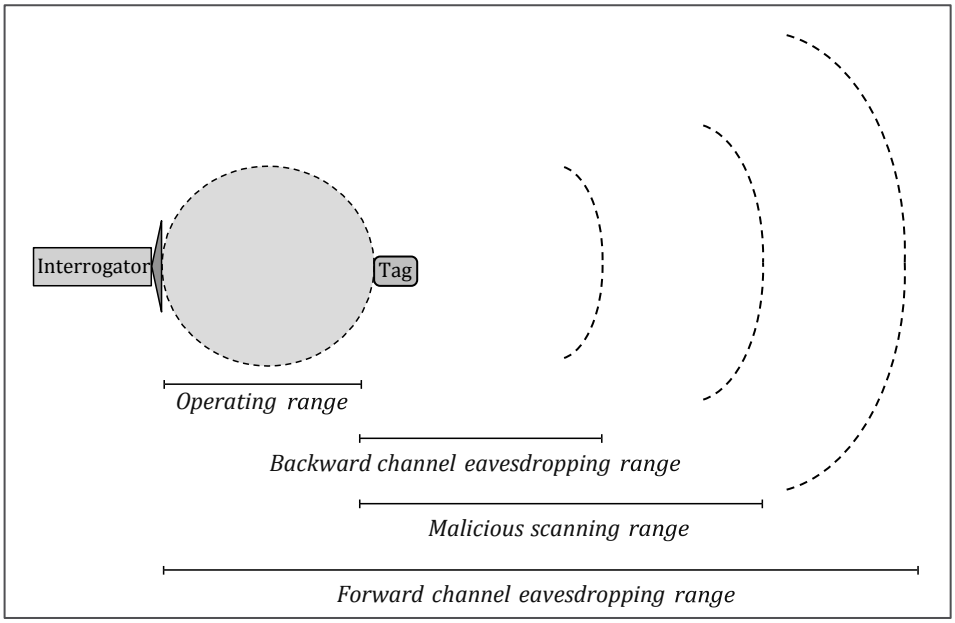

Figure 4.7 – Eavesdropping ranges

- **Isolation**: Active interference is an open issue that can only be faced by using opaque walls to minimize 3rd party interference.

4.5.2 RFID tags with Cryptographic capabilities

Since RFID is becoming very popular and is being used in a variety of items such as clothes, medicine, jewelry etc., advanced tags with either cryptographic or at least authentication capabilities have to be used. These approaches are exceptionally challenging to design, given the severe cost constraints on the basic RFID tag. Their main disadvantages are the higher cost when compared to simple RFID tags, and that the cryptographic functions are completely implemented in hardware, in order to minimize cost and size, and thus once manufactured, they can't be re-programmed in order to use a more advanced cryptographic algorithm; they have to be replaced instead. Below we discuss the proposed solutions on such RFID tags:

- **Tag design**: The first things that an advanced RFID tag should have are flexibility, tamper resistance and circuitry of high complexity. Flexibility is necessary in order to minimize faulty tags due to bending when for example it is placed on clothes. Tampering resistance is required to minimize the effects of misuse, fraudulent or not. High circuitry complexity is required to accommodate higher security and reduce the risk of secret key disclosure when physical access is acquired.
- **Password Lock**: Using a user-defined password, the tag can be locked so that only specific information can be queried. When unlocked, instead, the tag can offer full functionality and access to its complete memory bank set to the user. Such a feature has already been implemented by Impinj and is currently offered in their Monza 4QT, Monza X-2K/8K Dura tag chips as "QT Technology". Through QT technology, a tag owner/user can maintain two data profiles (one public, one private), allowing confidentiality of business-sensitive data while assuring consumers of privacy. The tag owner stores confidential data in the private data profile, which is protected by a password-controlled command. Furthermore, the QT Technology offers a Limited Range feature, as well as a Peek feature in order to protect the QT command. The first, when enabled, adds a layer of physical security by preventing readers farther than roughly one meter from the tag from switching the tag from Public to Private (or vice versa) by reducing its sensitivity. A reader, though, is always able to read a

tag's currently exposed EPC at maximum range. With the Peek feature enabled, a reader can temporarily switch a Public tag to Private, access the Private information, then when the chip loses power it will automatically revert back to its Public profile.

- **Distance Bounding Protocols**: Distance-Bounding identification protocols aim at impeding man-in-the-middle attacks by measuring response times. There are three kinds of attacks such protocols could address: (1) Mafia attacks where the adversary relays communication between honest prover and honest verifier in different sessions; (2) Terrorist attacks where the adversary gets limited active support from the prover to impersonate. (3) Distance attacks where a malicious prover claims to be closer to the verifier than it actually is. Many protocols in the literature address one or two such threats, but no rigorous cryptographic security models |nor clean security proofs| exist so far. For resource-constrained RFID tags, distance-bounding is more difficult to achieve. Some of the already proposed protocols can be found in [89]. Another similar proposal has been implemented by Impinj in their QT-enabled RFID tags, called the Peek feature (see previous paragraph for more info).
- **Hash-Lock**: This proposal is based on the public-key cryptographic primitives or symmetric primitives requiring secure key distribution. Each hash-enabled tag in this design has a portion of memory reserved for a temporary metaID. The Tag owner "locks" tags by first selecting a key at random, then computing the hash value of the key. The hash output, designated as the metaID s stored on the tag and the tag is toggled into a locked state. The key and the metaID are stored in a back-end database. To "unlock" a tag, the owner first queries the metaID from the tag and uses this value to look up the key in a back-end database. The owner transmits this key value to the tag, which hashes the received value and compares it to the stored metaID. If the values match, then the tag unlocks itself and offers its full functionality to any nearby readers.

  In this approach, a tag may be "locked" so that it refuses to reveal its ID until it is "unlocked". In the simplest scenario, when the tag is locked it is given a value (or meta-ID) y, and it is only unlocked by presentation of a key or PIN value x such that y = h(x) for a standard one-way hash function h() [85]. Such protocols are cheap to implement and the use of hash function offer nice random properties. Some have already been proposed:
  - **Hash-Lock** [13]
  - **Randomized Hash-Lock** [92]

- **Lightweight Cryptography**: Implementing cryptographic functions in low-cost RFID tags is the most challenging job, which has great dangers. Optimizing such an algorithm in order to work at reduced cycle-count at a frequency of 100 kHz can even make the most secure algorithm vulnerable to attacks. That's the main reason of why there aren't plenty of such implementations proposed yet. Such protocols are challenge response based and require the tag to implement a cryptographic function for authentication purposes. A recently proposed highly-optimized version of an AES encryption function [58], [41], [101] is finally bringing cost-efficient strong authentication closer to reality for low-cost RFID tags. Table 4.3 outlines a comparison between proposed lightweight (optimized) cryptographic primitives based on 100 kHz operation.

Cipher	Ref.	Key/Block size (bits)	Area (GE)	Power Cons. (μW)	Throughput (kbit/s)	Technology (μm)	Security[2]
AES	[41]	128/128	3400	4.50	12.40	0.35	VH
DESL	[53]	56/64	1848	1.60	44.44	0.18	L-M
DES		56/64	2309	2.14	44.44	0.18	L
DESXL		184/64	2168	-	44.44	0.18	M-H
TEA	[54]	128/64	1984	39.00[3]	22.00	0.35	L
SEA	[81]	96/96	1333	3.22	16.00	0.13	L-M
KTANTAN	[82]	80/32	464	0.15	12.50	0.13	L
mCRYPTON	[83]	64/64	2420	-	492.00	0.13	H
PRESENT	[90]	80/64	1650	3.86	200.00	0.18	H[4]
			1075	2.52	11.40	0.18	
PRINTcipher	[91]	80/48	402	2.60	6.25	0.18	M-H
SQUASH	[21]	128/32	2646	0.04	0.1	0.13	H

Table 4.3 – Comparison of lightweight security primitives

- **Ultralightweight Protocols**: A family of protocols designed especially for low-cost passive RFID tags in order to cover the gap in cost between RFID tags with and without encryption capabilities. Ultralightweight protocols require low computational recourses, due to the usage of only simple functions, as well as low in-tag memory resources. They guarantee tag anonymity with the use of pseudonyms and tags-readers communicate using shared secret keys to construct messages. These proposed schemes consist of three phases. First identification phase in which the tag is identified by means of the index-pseudonym. Second is Authentication in which the reader and the tag are mutually authenticated and also used to transmit the static tag identifier (ID) securely. Finally the Updating phase in which the index-pseudonym and shared secret keys are updated. On the latest protocols, the addition of non-triangular functions has been added in order to improve their diffusion properties and their security. Such protocols are currently under heavy development, with plenty of them being proposed nowadays, mostly because of their low resource requirements. Some of the already proposed protocols are being summarized in Table 4.4. For more information on Ultralightweight protocols refer to [94] and [97].

[2] L: Low, M: Moderate, H: High, VH: Very High
[3] 39μW @ 230kHz
[4] High Risk

	M²AP	*LMAP*	*EMAP*	*SASI*	*Gossamer*	*UMA*	*David-Prasad*	*SULMA*	*Pateriya*
Resistance to Desynchronization/Replay	No	No	No	No	No	No	No	No	Yes
Updating Confirmation	No	No	No	No	No	No	No	No	Yes
Resistance to DoS	No	No	No	No	No	No	No	No	Yes
Resistance to IDS Collision	No	No	No	No	No	No	No	No	Yes
Data Confidentiality	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Privacy & Tag Anonymity	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Mutual Authentication & Data Integrity	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Forward Security	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Total Messages for Mutual Authentication	4L[5]	4L	5L	4L	4L	3L	5L	4L	2L
Memory Size on Tag	6L	6L	6L	7L	7L	5L	4L	7L	4L
Memory Size on Server	6L	6L	6L	4L	4L	3L	3L	7L	7L
Operations on Tag •				✓			✓		
+	✓	✓	✓	✓	✓	✓		✓	✓
⊕	✓	✓	✓	✓	✓	✓	✓	✓	✓
^						✓			
Rotate				✓[6]	✓[7]	✓[6]		✓[7]	✓[7]
MixBits					✓			✓	✓

Table 4.4 – Ultralightweight protocol comparison

- **Tree-Walking improvements**: Current UHF anti-collision protocol (binary tree-walking) require that the ID of the singulated tags is transmitted over the forward channel as well, but as it can be seen in Figure 4.7, the forward channel has a quite long eavesdropping range, making it easy for a third party to listen to the transmitted IDs which may be sensitive data depending on the application. So, countermeasures should be taken in order to modify the anti-collision algorithms to silently singulate RFID tags. Already proposed solutions that offer such functionality include [13], [14] and [15]. For more info on these proposals see section 2.2.
- **Kill Password Authentication:** Current generation of EPC Class-1 Gen-2 tags (ISO 18000-6C) all specify the use of passwords to protect the KILL functionality of tags (permanent disablement of an RFID tag). Since that password is read-protected, it could be used in order to authenticate the tag without reading it. Cloned tags could be also found using that verification method. A proposal on this type of authentication has been made in [98].

[5] L denotes the bit length of variables, in our case L=96
[6] Rot(x,y)=x<<wh(y), being wh(y) the Hamming weight of vector y
[7] Rot(x,y)=x<<(y mod L) for a given value of L

4.6 Evaluation Software

During the evaluation period, we were in need of a custom software that will support all of the EPC Class-1 Generation-2 Protocol's functions, as well as it will enable us to measure the time for each command execution; features that the supplied software did not support. That said, we took advantage of the supplied Octane SDK of Impinj and implemented command-line software that enabled us to do all that. The Octane SDK is a new software API from Impinj that significantly reduces the amount of time it takes to write RFID applications. It's an extension of the Low-Level Reader Protocol (LLRP) Toolkit (LTK) that simplifies development by handling many of the details. Ratified by EPCglobal in April 2007, LLRP is the RFID-aware protocol that is intended to standardize the network interface of the RFID readers. It is designed as a standard in order for developers to have a common programmatic interface to RFID readers from different manufacturers. More specifically, the software was written in C# and it supports the following implemented functions:

- **Queries**
  - Query Reader State
  - Query Tags
  - Query Tags – In-Depth
  - Read Tag Access Password
  - Read Tag Kill Password
  - Read Tag User Memory
- **Programming**
  - Program Reader Settings
  - Program Tag EPC
  - Program Tag Public EPC (Monza QT only)
  - Program Tag Access Password
  - Program Tag Kill Password
  - Program Tag User Memory
  - Program Tag QT Profile (Monza QT only)
  - Lock/Unlock Tag Memory bank
  - Kill Tag
- **Benchmarking**
  - Bench Read Rate – Current Settings
  - Bench Read Rate – Various EPC Modes
  - Bench Read User Memory – Various Lengths
  - Bench Read User Memory – Various Locations
  - Bench Write User Memory – Various Lengths
  - Bench Write User Memory – Various Locations
  - Bench Monza QT Profile

All functions display execution time in milliseconds, as we will see later.

In comparison with Impinj's supplied software, our software offers the following additional or improved features:

- **Timing**: Detailed execution timing in milliseconds on all functions. This lets the user know how much it takes for a function to complete, in order to estimate execution times for larger tag populations.

Impinj's software: No timing available on any function.

- **Smart antenna selection**: When the user selects to execute a specific function on a tag (i.e. changing the EPC value), the software automatically selects and uses the antenna which scanned the selected tag with the highest sensitivity.
  Impinj's software: Selects and uses the last antenna that scanned the selected tag.
- **Automatic antenna enablement**: When the software connects to the reader, it automatically scans for connected antennas and enables only these, disabling the unconnected ones in order to improve reading rates.
  Impinj's software: Either enables all the antennas, or uses the last run configuration.
- **Tag IC details**: By fetching the TID of a tag, the software displays detailed information about the tag's IC, the EPC memory size as well as the User memory size.
  Impinj's software: One has to manually read the TID from the tag and translate that to tag IC model by searching through multiple Tag IC datasheets.
- **Reader information**: A function is available in order to display information about the reader's installed firmware, the board's version and the reader's region. Also, information about the connected antennas is displayed.
  Impinj's software: Only connected antennas' states are visible.
- **Tag querying**: While performing tag scanning, we get detailed information for each antenna and the tags that it scanned. Information includes antenna port, receiving sensitivity, phase angle, frequency, and rate. This information can be also used for optimal antenna alignment.
  Impinj's software: Only the highest sensitivity of all antennas that scanned each tag is available.
- **Memory Locking/Unlocking**: The user is able to either lock or unlock any of the tag's memory banks according to the C1G2 protocol's specifications. See section 4.3.1 for more details.
  Impinj's software: No such option is available.
- **Public EPC programming**: The user has the option to program the public EPC value of Monza QT-compatible RFID tags, without having to read the datasheet in order to find the public EPC location in the TID memory bank.
  Impinj's software: The user has to manually enter the pointer in the TID memory bank in order to program the public EPC value of the tag, by first reading the Monza QT datasheet.
- **Monza QT profile switching**: Through the software, a user may change the QT profile on any Monza QT-compatible RFID tag.
  Impinj's software: No option for switching QT profiles is available.
- **Tag Killing**: Using the programmed 32-bit Kill Password, a user may permanently disable an RFID tag using our software.
  Impinj's software: No tag killing option is available.
- **Best configuration selector**: Through benchmarking, our software can be used in real-time applications in order to provide details and results about all possible configuration modes and suggest the best configuration according to the results and the user's needs.
  Impinj's software: No such option is available.

- **User memory benchmarking**: Using our software, a user may automatically benchmark a tag's user memory on how fast data are written to or read from it and compare it with other RFID tags.

  Impinj's software: No such option is available

- **Monza QT benchmarking**: By switching between all possible Monza QT profiles on Monza QT-compatible RFID tags, we provide timing information so that a user knows the time needed to switch to a new profile and accordingly optimize the speed of the system such as the product line or gate-opening when scanning a truck.

  Impinj's software: No such option is available

The software communicates through Ethernet. When the user starts the software, the IP address of the reader is requested from the user in order to establish a connection. When the software connects with the reader, it pre-configures it in Auto Pilot (Auto Dense) Dual Target mode, with only the connected antennas enabled and set at maximum power output (31.5dB). Now let's see the functions in more detail.

4.6.1 Query Reader State

By querying the reader's state, we get information about the reader's model, software & firmware versions, connected antennas and more (Fig. 4.8).

```
Reader Features:
 Model              Speedway R420
 Software Version   4.6.2.240
 Firmware Version   4.6.0.240
 PCBA Version       270-004-000
 FPGA Version       4.6.2.240
 Regulator Region   ETSI_EN_302_208_91_2_1
 Antennas           1:Connected 2:Connected 3:Disconnected 4:Disconnected
```

Figure 4.8 – Software: Query reader state

4.6.2 Query Tags

Using the current reader configuration, we can run an inventory by only specifying the run time in seconds (Fig 4.9).

```
Tag Scanning:
  Enter for how many seconds should the reader run: 5
  Querying tags for 5 seconds.
  1. EPC: 300833B2DDD9BD0400BBA35A
       TID: E280110520003743AA3F0000, Tag Chip: Impinj Monza 4QT. EPC Memory: 128 bits. User memory: 512 bits
       Antenna 2: -34.00dBm, 866.90MHz, 0.78radians, 23.20reads/sec
  2. EPC: 300833B2DDD9BD0400BBA369
       TID: E280110520003744AA410000, Tag Chip: Impinj Monza 4QT. EPC Memory: 128 bits. User memory: 512 bits
       Antenna 2: -39.50dBm, 866.90MHz, 5.49radians, 23.20reads/sec
  3. EPC: 300833B2DDD9048035050000
       Antenna 1: -40.00dBm, 866.90MHz, 0.78radians, 23.60reads/sec
  4. EPC: 300833B2DDD9014000000005
       TID: E2801100200038D915310010, Tag Chip: Impinj Monza 4D. EPC Memory: 128 bits. User memory: 32 bits
       Antenna 1: -40.00dBm, 866.90MHz, 2.36radians, 23.60reads/sec
  5. EPC: 300833B2DDD9014000000002
       TID: E2801100200038DA15310010, Tag Chip: Impinj Monza 4D. EPC Memory: 128 bits. User memory: 32 bits
       Antenna 2: -65.00dBm, 866.90MHz, 2.67radians, 23.20reads/sec
  6. EPC: 111111111111111111111111
       TID: E2801100200038D615310010, Tag Chip: Impinj Monza 4D. EPC Memory: 128 bits. User memory: 32 bits
       Antenna 1: -29.00dBm, 866.90MHz, 2.36radians, 23.60reads/sec
       Antenna 2: -65.00dBm, 866.90MHz, 2.67radians, 23.20reads/sec
  7. EPC: 300833B2DDD9BD0500DB9776
       TID: E2801105200032CBABE50000, Tag Chip: Impinj Monza 4QT. EPC Memory: 128 bits. User memory: 512 bits
       Antenna 1: -27.50dBm, 866.90MHz, 0.77radians, 23.60reads/sec
       Antenna 2: -62.00dBm, 866.90MHz, 1.79radians, 23.20reads/sec
  Total: 7 tag(s) found
```

Figure 4.9 – Software: Query tags

On the results, we get the list of the tags found during the scan by any of the connected antennas. For each tag found, we get the EPC value of it and if it uses Impinj's Monza 4 tag chip we also get the TID value in the report. That value gives as information about the tag chip model, including EPC memory length and user memory length (if any). For each antenna that found each tag, we get the following information:

- Antenna Port
- Peak Read Sensitivity
- Last Read Frequency
- Last Read Phase Angle
- Read Rate

That information (getting separate reports for each antenna) is saved for use in functions such as "Tag Selection" as we will see later. It can be used for optimal antenna alignment, as well as for future triangulation applications in order to improve the security of the system, as we discussed previously in this chapter.

In-depth query mode provides the same results as the previous one, with the addition of fetching the TID value for each scanned tag (Fig. 4.10). This lets us view the tag chip's information no matter what the tag chip is. Furthermore, the tag chip model gives us specific information about the EPC memory and User Memory capacities, in order to use them in other functions of the application or just for tag model identification. Currently used TID values in the software are the following (Table 4.5):

Tag Chip	TID[0:31]
Impinj Monza 2	E2001071
Impinj Monza 3	E2001093
Impinj Monza 4D	E2801100
Impinj Monza 4E	E280110C
Impinj Monza 4QT	E2801105
Impinj Monza 5	E2801130
Impinj Monza X-2K	E2801140
Alien Higgs 2	E2003411
Alien Higgs 3	E2003412

Table 4.5 – TID values of known tag ICs

```
Tag Scanning:
  Enter for how many seconds should the reader run: 5
  Querying tags for 5 seconds.
  1. EPC: 300833B2DDD9BD0400BBA35A
       TID: E280110520003743AA3F0000, Tag Chip: Impinj Monza 4QT. EPC Memory: 128 hits. User memory: 512 bits
       Antenna 2: -34.00dBm, 866.90MHz, 0.78radians, 23.20reads/sec
  2. EPC: 300833B2DDD9BD0400BBA369
       TID: E280110520003744AA410000, Tag Chip: Impinj Monza 4QT. EPC Memory: 128 hits. User memory: 512 bits
       Antenna 2: -39.50dBm, 866.90MHz, 5.49radians, 23.20reads/sec
  3. EPC: 300833B2DDD9048035050000
       TID: E2001071, Tag Chip: Impinj Monza 2. EPC Memory: 96 hits. User memory: 0 bits
       Antenna 1: -40.00dBm, 866.90MHz, 0.78radians, 23.60reads/sec
  4. EPC: 300833B2DDD9014000000005
       TID: E2801100200038D915310010, Tag Chip: Impinj Monza 4D. EPC Memory: 128 hits. User memory: 32 bits
       Antenna 1: -40.00dBm, 866.90MHz, 2.36radians, 23.60reads/sec
  5. EPC: 300833B2DDD9014000000002
       TID: E2801100200038DA15310010, Tag Chip: Impinj Monza 4D. EPC Memory: 128 hits. User memory: 32 bits
       Antenna 2: -65.00dBm, 866.90MHz, 2.67radians, 23.20reads/sec
  6. EPC: 111111111111111111111111
       TID: E2801100200038D615310010, Tag Chip: Impinj Monza 4D. EPC Memory: 128 hits. User memory: 32 bits
       Antenna 2: -65.00dBm, 866.90MHz, 2.67radians, 23.20reads/sec
  7. EPC: 300833B2DDD9BD0500DB9776
       TID: E2801105200032CBABE50000, Tag Chip: Impinj Monza 4QT. EPC Memory: 128 hits. User memory: 512 bits
       Antenna 1: -27.50dBm, 866.90MHz, 0.77radians, 23.60reads/sec
  Total: 7 tag(s) found
```

Figure 4.10 – Software: In-depth query tags

4.6.3 Query Tag Access/Kill Password

In the EPC Class-1 Generation-2 Protocol, we have the ability to scan a tag and read its Access (or Kill) Password, if one is set and the tag is not in locked state. We use that feature in order to read Access Passwords on used tags that had a password set when we received them. Luckily those tags where unlocked, so we were able to read their Access Password with no problem (Fig. 4.11).

```
Read Access Password:
  Tag selection:
    0. Execute the function on the first tag seen by the reader (not recommended)
    1. Tag EPC: 300833B2DDD9BD0400BBA369
    2. Tag EPC: 300833B2DDD9BD0400BBA35A
    3. Tag EPC: 300833B2DDD9BD0400BBA34C
    4. Tag EPC: 300833B2DDD9014000000002
    5. Tag EPC: 000000000000000000000000
    6. Tag EPC: 300833B2DDD9014000000005
    7. Tag EPC: 111111111111111111111111
    8. Tag EPC: 300833B2DDD9048035050000
    9. Tag EPC: 300833B2DDD9BD0500DB9776
    10. Run silent tag scan for 5 seconds
    11. Cancel the execution
  Enter your selection (0-11): 0
  Select antenna to perform the operation (1-4): 2
EPC: 300833B2DDD9BD0400BBA369
Access Password: 0000 0000
Time to execute: 106.01ms
```

Figure 4.11 – Software: Query tag access password

On the previous Figure, we can also see the tag selection feature. When we select a function that applies on a single tag, the user has to select which tag to perform the action to. The list is populated when we perform a "Query Tags". The user also has the option to perform a new silent re-scan for 5 seconds (default "runtime" which can be changed) in order to renew that list (this can be useful when the user selects to perform a tag action and the tag list is empty). Otherwise, there is the option to perform the selected action on the first tag that the reader will see, by letting the user select which specific antenna to use (Fig 4.12). If the user selects to perform the operation on the "first tag seen", the software lets the user select which antenna (of the connected ones) shall be used. If he selects a specific tag instead, the software automatically selects and uses the antenna that previously scanned the tag with the higher sensitivity level.

```
  Tag selection:
    0. Execute the function on the first tag seen by the reader (not recommended)
    1. Tag EPC: 300833B2DDD9BD0400BBA369
    2. Tag EPC: 300833B2DDD9BD0400BBA35A
    3. Tag EPC: 300833B2DDD9BD0400BBA34C
    4. Tag EPC: 300833B2DDD9014000000002
    5. Tag EPC: 000000000000000000000000
    6. Tag EPC: 300833B2DDD9014000000005
    7. Tag EPC: 111111111111111111111111
    8. Tag EPC: 300833B2DDD9048035050000
    9. Tag EPC: 300833B2DDD9BD0500DB9776
    10. Run silent tag scan for 5 seconds
    11. Cancel the execution
  Enter your selection (0-11): 0
  Select antenna to perform the operation (1-4): 2
EPC: 300833B2DDD9BD0400BBA369
```

Figure 4.12 – Software: Tag selection

If the tag is in lock state, we get notified that the password could not be read (Fig. 4.13).

```
Read Access Password:
  Tag selection:
    0. Execute the function on the first tag seen by the reader (not recommended)
    1. Tag EPC: 300833B2DDD9BD0400BBA369
    2. Tag EPC: 300833B2DDD9BD0400BBA35A
    3. Tag EPC: 300833B2DDD9BD0400BBA34C
    4. Tag EPC: 300833B2DDD9014000000002
    5. Tag EPC: 000000000000000000000000
    6. Tag EPC: 300833B2DDD9014000000005
    7. Tag EPC: 111111111111111111111111
    8. Tag EPC: 300833B2DDD9048035050000
    9. Tag EPC: 300833B2DDD9BD0500DB9776
    10. Run silent tag scan for 5 seconds
    11. Cancel the execution
  Enter your selection (0-11): 5
Tag selected: 000000000000000000000000
Error. Access Password could not be read. (NonSpecificTagError)
```

Figure 4.13 – Software: Locked tag selected

4.6.4 Program Reader Settings

Using this function, a user may change the reader's settings manually in order to understand how the system works and behaves in different configurations. The available options are the following (Fig 4.14):

- Enable or Disable Antenna Ports
- Transmitting Power for each antenna port
- Minimum Receiving Sensitivity for each antenna port
- Default Tag Scanning Runtime in seconds
- Timeout in milliseconds
- Tag Population Estimate
- Reader Mode
- Search Mode (according to the Class-1 Generation-2 protocol)
- Session (according to the Class-1 Generation-2 protocol)

```
Reader Configuration:
  1. Antenna Ports
  2. Transmitting Power
  3. Receiving Sensitivity
  4. Tag Sean Runtime
  5. Timeout
  6. Tag Population Estimate
  7. Reader Node
  8. Search Node
  9. Session
  10. Return
Enter your selection (1-10):
```

Figure 4.14 – Software: Reader settings

4.6.5 Program Tag EPC

The most common programming task on an RFID reader is to program a tag's EPC value. The default value for the EPC C1G2 protocol is 96-bits. As previously, we have to select a tag to perform that operation and we have to provide the Access Password, if the tag is locked. The entered value must be supported by the tag chip, meaning that if the tag supports only 96-bit EPC, the user may only enter such a value. If the tag chip supports 128-bit EPC, the user may enter 96, 112 or 128 bits of EPC (the length must be modulo 16-bit or one hexadecimal word) (Fig. 4.15).

```
Change EPC:
  Tag selection:
    0. Execute the function on the first tag seen by the reader (not recommended)
    1. Tag EPC: 300833B2DDD9BD0400BBfl369
    2. Tag EPC: 300833B2DDD9BD0400BBfl35fl
    3. Tag EPC: 300833B2DDD9BD0400BBfl34C
    4. Tag EPC: 300833B2DDD9014000000002
    5. Tag EPC: 000000000000000000000000
    6. Tag EPC: 300833B2DDD9014000000005
    7. Tag EPC: 111111111111111111111111
    8. Tag EPC: 300833B2DDD9048035050000
    9. Tag EPC: 300833B2DDD9BD0500DB9776
    10. Run silent tag scan for 5 seconds
    11. Cancel the execution
  Enter your selection (0-11): 2
  Tag selected: 300833B2DDD9BD0400BBfl35fl
  Enter the Access Password (Enter "null" to use null password, or leave empty to use no password): null
  Enter the new EPC: 300833B2DDD9BD0400BBA35C
New EPC: 300833B2DDD9BD0400BBA35C
Time to execute: 175.01ms
```

Figure 4.15 – Software: Program tag EPC

4.6.6 Program Tag Public EPC

Monza 4QT tag chips have the ability to switch between Private and Public profiles, as we discussed earlier, which lets them switch between two different EPC values. Since EPC C1G2 protocol does not support storing two different EPC values, Impinj has integrated the second EPC value inside the TID memory bank. By changing that specific part of the TID memory bank, we actually change the EPC value of the tag, which is displayed when it's in the Public profile. Using this feature we are able to change the Public EPC of Monza 4QT tag chips (Fig 4.16).

```
Change Public EPC:
  Tag selection:
    0. Execute the function on the first tag seen by the reader (not recommended)
    1. Tag EPC: 300833B2DDD9BD0400BBA369
    2. Tag EPC: 300833B2DDD9BD0400BBA35A
    3. Tag EPC: 300833B2DDD9BD0400BBA34C
    4. Tag EPC: 300833B2DDD9014000000002
    5. Tag EPC: 000000000000000000000000
    6. Tag EPC: 300833B2DDD9014000000005
    7. Tag EPC: 111111111111111111111111
    8. Tag EPC: 300833B2DDD9048035050000
    9. Tag EPC: 300833B2DDD9BD0500DB9776
    10. Run silent tag scan for 5 seconds
    11. Cancel the execution
  Enter your selection (0-11): 1
  Tag selected: 300833B2DDD9BD0400BBA369
  Enter the Access Password (Enter "null" to use null password, or leave empty to use no password):
  Enter the new Public EPC: AAAAAAAAAAAAAAAAAAAAAAAA
New Public EPC: AAAAAAAAAAAAAAAAAAAAAAAA
Tine to execute: 166.01ms
```

Figure 4.16 – Software: Program tag Public EPC

The software also checks if the selected tag has Monza 4QT tag chip, and if not, notifies the user (Fig 4.17).

```
Change Public EPC:
  Tag selection:
    0. Execute the function on the first tag seen by the reader (not recommended)
    1. Tag EPC: 300833B2DDD9BD0400BBA369
    2. Tag EPC: 300833B2DDD9BD0400BBA35A
    3. Tag EPC: 300833B2DDD9BD0400BBA34C
    4. Tag EPC: 300833B2DDD9014000000002
    5. Tag EPC: 000000000000000000000000
    6. Tag EPC: 300833B2DDD9014000000005
    7. Tag EPC: 111111111111111111111111
    8. Tag EPC: 300833B2DDD9048035050000
    9. Tag EPC: 300833B2DDD9BD0500DB9776
    10. Run silent tag scan for 5 seconds
    11. Cancel the execution
  Enter your selection (0-11): 1
  Tag selected: 300833B2DDD9BD0400BBA369
  The tag must support the Monza QT technology.
```

Figure 4.17 – Software: Unsupported tag selected

4.6.7 Program Tag Access/Kill Password

Setting a tag's Access Password is necessary in order to make unauthorized users unable to either change any of its data or view sensitive data from its memory banks, such as passwords or user memory. Similarly, setting a tag's Kill Password is necessary so that no one will be able to kill the tag without proper permission. By default, Impinj's RFID tag chips all have null Access and Kill Passwords, which may make them vulnerable to a variety of attacks. Using the software, we managed to set both Access and Kill Passwords for all of our tags (Fig 4.18).

```
Set Access Password:
  Tag selection: (Tag list is empty)
    0. Execute the function on the first tag seen by the reader (not recommended)
    1. Run silent tag scan for 5 seconds
    2. Cancel the execution
  Enter your selection (0-2): 1
  Running silent tag scan for 5 seconds..9 tag(s) were found.
  Tag selection:
    0. Execute the function on the first tag seen by the reader (not recommended)
    1. Tag EPC: 300833B2DDD9BD0400BBA369
    2. Tag EPC: 300833B2DDD9BD0400BBA35C
    3. Tag EPC: 300833B2DDD9BD0400BBA34C
    4. Tag EPC: BBBBBBBBBBBBBBBBBBBBBBBB
    5. Tag EPC: 300833B2DDD9014000000002
    6. Tag EPC: 000000000000000000000000
    7. Tag EPC: 300833B2DDD9014000000005
    8. Tag EPC: 111111111111111111111111
    9. Tag EPC: 300833B2DDD9BD0500DB9776
    10. Run silent tag scan for 5 seconds
    11. Cancel the execution
  Enter your selection (0-11): 9
  Tag selected: 300833B2DDD9BD0500DB9776
  Enter the Access Password (Enter "null" to use null password. or leave empty to use no password): null
  Enter the new Access Password: 12345678
New password: 12345678
Time to execute: 200.01ms
```

Figure 4.18 – Software: Program tag Access/Kill password

The software first lets the user select a tag to perform the operation, and then it requests the current Access Password, if one is already set.

4.6.8 Program Tag User Memory

Some newer tag chips support for internal data storage, except the default EPC value. That memory can be used as a local database for storing product specific information such as product expiration dates, or product colors. Using the software we were able to write data within that memory. The software lets the user select tag to write to, and then it checks if the selected tag's

chip has User Memory and how much (Fig 4.19). The user also has the option to write at a specific pointer within the User Memory, without affecting the rest of the data.

```
Change User Block:
  Tag selection:
    0. Execute the function on the first tag seen by the reader (not recommended)
    1. Tag EPC: 300833B2DDD9BD0400BBA369
    2. Tag EPC: 300833B2DDD9BD0400BBA35C
    3. Tag EPC: 300833B2DDD9BD0400BBA34C
    4. Tag EPC: BBBBBBBBBBBBBBBBBBBBBBBB
    5. Tag EPC: 300833B2DDD9014000000002
    6. Tag EPC: 000000000000000000000000
    7. Tag EPC: 300833B2DDD9014000000005
    8. Tag EPC: 111111111111111111111111
    9. Tag EPC: 300833B2DDD9BD0500DB9776
    10. Run silent tag scan for 5 seconds
    11. Cancel the execution
  Enter your selection (0-11): 9
  Tag selected: 300833B2DDD9BD0500DB9776
  Enter the Access Password (Enter "null" to use null password, or leave empty to use no password):
  Enter the pointer to begin writing (0-31): 31
  Enter the data to write (up to 1 hex word): AAAA
Pointer: 31
Words written: 1
Data: 0000
Time to execute: 138.01ms
```

Figure 4.19 – Software: Program tag User Memory

4.6.9 Program Tag QT Profile

As we discussed earlier, Impinj has implemented a set of security features in Monza 4QT tag chips, called QT Technology features. Their supplied software did not support configuration of these, so we had to implement the functions within our software. That functionality let us experiment with switching between the different QT profiles and compare the behavior of the tag at each one (Fig. 4.20).

```
Set QT Profile:
  Tag selection:
    0. Execute the function on the first tag seen by the reader (not recommended)
    1. Tag EPC: 300833B2DDD9BD0400BBA369
    2. Tag EPC: 300833B2DDD9BD0400BBA35C
    3. Tag EPC: 300833B2DDD9BD0400BBA34C
    4. Tag EPC: BBBBBBBBBBBBBBBBBBBBBBBB
    5. Tag EPC: 300833B2DDD9014000000002
    6. Tag EPC: 000000000000000000000000
    7. Tag EPC: 300833B2DDD9014000000005
    8. Tag EPC: 111111111111111111111111
    9. Tag EPC: 300833B2DDD9BD0500DB9776
    10. Run silent tag scan for 5 seconds
    11. Cancel the execution
  Enter your selection (0-11): 2
  Tag selected: 300833B2DDD9BD0400BBA35C
  Enter the Access Password (Enter "null" to use null password, or leave empty to use no password):
  Select Profile (1. Private. 2. Public): 1
  Select Range (1. Normal. 2. Short): 1
  Select Persistence (1. Permanent, 2. Temporary): 1
Profile: Private, Range: Normal Range, Persistence: Permanent
Time to execute: 116.01ms
```

Figure 4.20 – Software: Program tag QT profile

The user must first select a tag, enter its Access Password (if one is set) and if the tag supports Impinj's QT Technology features, the user may select QT configuration for that tag. The QT compatibility can be checked through the tag's TID, which informs us about the tag's chip model.

4.6.10 Lock/Unlock Memory bank

Using the software, a user is able to lock/unlock (or perma-lock/perma-unlock) one or more of a tag's memory banks according to the EPCglobal Class-1 Generation-2 protocol's specifications (Fig 4.21). For more info on how the locking or unlocking works, refer to section 4.3.1. Since the tag cannon be locked if the Access Password is the factory default (null or 0x00000000), if the user enters such a password, the software returns and asks the user to change the Access Password in order to be able to lock the tag.

```
Lock/Unlock Memory Bank:
  Tag selection:
    0. Execute the function on the first tag seen by the reader (not recommended)
    1. Tag EPC: 3504F719C000000000001100
    2. Run silent tag scan for 5 seconds
    3. Cancel the execution
  Enter your selection (0-3): 1
  Tag selected: 3504F719C000000000001100
  Enter the Access Password (Enter "null" to use null password, or leave empty to use no password): 12345678
  Select Memory bank:
    1. Reserved[0:31] (Kill Password)
    2. Reserved[32:63] (Access Password)
    3. EPC
    4. TID
    5. User
    6. Return
  Enter your selection (1-6): 3
  Select new state:
    1. Locked
    2. Perma-Locked
    3. Unlocked
    4. Perma-Unlocked
    5. Return
  Enter your selection (1-5): 1
Memory bank locked successfully.
```

Figure 4.21 – Tag memory bank locking

4.6.11 Benchmarks

In order to evaluate the performance of various actions, we implemented functions and managed to measure timings as well as to export other useful information. These functions can be used in order to evaluate a system in real life applications; for example, when implementing an RFID system application, it is necessary to decide what configuration to use. The proposed software offers this functionality by giving the performance results of every configuration mode and suggesting the best configurations for that application. Furthermore, it provides performance results for applications that require reading and/or writing data to the User memory of tags. The benchmarks implemented are the following:

- **Optimal Reader Configuration**: By switching between all possible reader modes and measuring the performance (Fig. 4.22), the software is able to select and suggest to the user the best configuration in order to improve either the read rate, or the number of tags seen at a specific time frame. More specifically, it offers optimal configurations for (Fig. 4.23):
  - Most tags scanned
  - Most tags scanned, with minimal total reads (at least once each tag)
  - Most tags scanned, with highest total read rate
  - Highest total read rate

```
Benchmark Read Rate (Various Settings):
 Enter for how many seconds should the reader run (each test): 5
 Do you want to pause between each execution? [Press Enter to continue or type "cancel" to stop the benchmark] (y/n): n

 Reader Mode: AutoSetDenseReader
  Search Mode: DualTarget
   Session: 0 -> Tags found: 86, Total Reads (in 5 seconds): 1062, Read rate: 212.00 reads/second
   Session: 1 -> Tags found: 85, Total Reads (in 5 seconds): 1033, Read rate: 206.00 reads/second
   Session: 2 -> Tags found: 84, Total Reads (in 5 seconds): 1017, Read rate: 203.00 reads/second
   Session: 3 -> Tags found: 85, Total Reads (in 5 seconds): 1006, Read rate: 201.00 reads/second
  Search Mode: SingleTarget
   Session: 0 -> Tags found: 82, Total Reads (in 5 seconds): 1048, Read rate: 209.00 reads/second
   Session: 1 -> Tags found: 84, Total Reads (in 5 seconds): 393, Read rate: 78.00 reads/second
   Session: 2 -> Tags found: 75, Total Reads (in 5 seconds): 106, Read rate: 21.00 reads/second
   Session: 3 -> Tags found: 86, Total Reads (in 5 seconds): 121, Read rate: 24.00 reads/second
  Search Mode: SingleTargetWithSuppression
   Session: 0 -> Tags found: 82, Total Reads (in 5 seconds): 1025, Read rate: 205.00 reads/second
   Session: 1 -> Tags found: 86, Total Reads (in 5 seconds): 122, Read rate: 24.00 reads/second
   Session: 2 -> Tags found: 86, Total Reads (in 5 seconds): 122, Read rate: 24.00 reads/second
   Session: 3 -> Tags found: 86, Total Reads (in 5 seconds): 120, Read rate: 24.00 reads/second

 Reader Mode: DenseReaderM8
  Search Mode: DualTarget
   Session: 0 -> Tags found: 85, Total Reads (in 5 seconds): 358, Read rate: 71.00 reads/second
   Session: 1 -> Tags found: 86, Total Reads (in 5 seconds): 353, Read rate: 70.00 reads/second
   Session: 2 -> Tags found: 85, Total Reads (in 5 seconds): 357, Read rate: 71.00 reads/second
   Session: 3 -> Tags found: 85, Total Reads (in 5 seconds): 358, Read rate: 71.00 reads/second
  Search Mode: SingleTarget
   Session: 0 -> Tags found: 58, Total Reads (in 5 seconds): 308, Read rate: 61.00 reads/second
   Session: 1 -> Tags found: 86, Total Reads (in 5 seconds): 279, Read rate: 55.00 reads/second
   Session: 2 -> Tags found: 68, Total Reads (in 5 seconds): 92, Read rate: 18.00 reads/second
   Session: 3 -> Tags found: 86, Total Reads (in 5 seconds): 118, Read rate: 23.00 reads/second
  Search Mode: SingleTargetWithSuppression
   Session: 0 -> Tags found: 63, Total Reads (in 5 seconds): 314, Read rate: 62.00 reads/second
   Session: 1 -> Tags found: 86, Total Reads (in 5 seconds): 260, Read rate: 52.00 reads/second
   Session: 2 -> Tags found: 87, Total Reads (in 5 seconds): 119, Read rate: 23.00 reads/second
   Session: 3 -> Tags found: 86, Total Reads (in 5 seconds): 118, Read rate: 23.00 reads/second

...
```

Figure 4.22 – Software: Bench read rate

```
Most tags scanned (87) in the following mode(s):
   DenseReaderM8, SingleTargetWithSuppression, Session 2

Most tags scanned (87), with minimal total reads (at least once each tag) in the following mode(s):
   DenseReaderM8, SingleTargetWithSuppression, Session 2, with 119 reads

Most tags scanned (87), with highest total read rate in the following mode(s):
   Hybrid, SingleTarget, Session 1, with rate 77 reads/second

Highest total read rate (239 reads/second) in the following mode(s):
   MaxThroughput, DualTarget, Session 0, with 83 tags seen
   MaxThroughput, DualTarget, Session 1, with 82 tags seen
```

Figure 4.23 – Software: Configuration suggestions

- **User memory performance**: Measuring the performance of any tag IC's user memory by timing reading from or writing to it data of different lengths or at different locations within the memory bank. This way a user may compare to performance of multiple tags in order to select the optimal one according to its needs and the cost of it.
- **Monza QT performance**: Measuring the performance of the only available security mechanism of our RFID tags, by timing the time it takes to switch from one profile to another.

5 Results

Using the available equipment, we were able to test some of the proposed solutions in order to see how they perform in real-life applications. Since our equipment targets end-user applications and not advanced experimental usage, we were unable to evaluate solutions that require special functions implemented inside the tag's integrated circuit.

5.1 Tag Shielding

As we saw in Chapter 1, as frequency of an RFID system gets higher, surface reflection gets increased. On metallic surfaces this effect is much more noticeable, due to the RF reflective properties of metal. Using this property, we managed to block RFID tags using various materials. More specifically, at the UHF frequency band, we managed to block RFID tags using just an antistatic bag which has a very thin metallized film (0.5μm of aluminum thickness) (Image 5.2). At the HF frequency band, we managed to block the RFID tag of a biometric passport using a single sheet of aluminum foil (16μm of aluminum thickness) (Image 5.1).

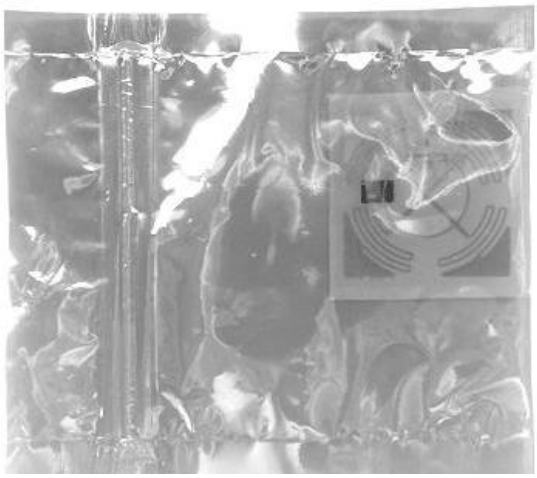

Image 5.2 – Tag shielding

Image 5.1 – ePassport Shielding

Thus, protecting our own privacy on RFID tagged items such as passports, credit cards etc. can be easy by using RFID Privacy Shields designed specifically for that scope. Companies like RFID-Shield offer such products for end-users.

5.2 Randomized (Re)Encryption

Instead of going through benchmarks of specific protocols, we went through benchmarking of how commercial RFID tags perform when writing data to their user memory. More specifically, we performed the benchmarks on two different RFID tag-chips, Impinj's Monza 4QT and Alien's Higgs 3, both with 512 bits (32x 16-bit words) of available user memory. The reader was

connected using Ethernet and in AutoPilot mode, with one antenna connected and set at maximum power output (31.5 dB). We noticed that using two antennas or lowering the power output did not affect the performance. The tests were performed using the implemented software and they are the following two:

- Performance when reading/writing data of different lengths from the beginning of the memory bank
- Performance when reading/writing 16 bits of data on different locations

The summary of the first benchmark can be seen in Figure 5.1, while the summary of the second benchmark can be seen in Figure 5.2.

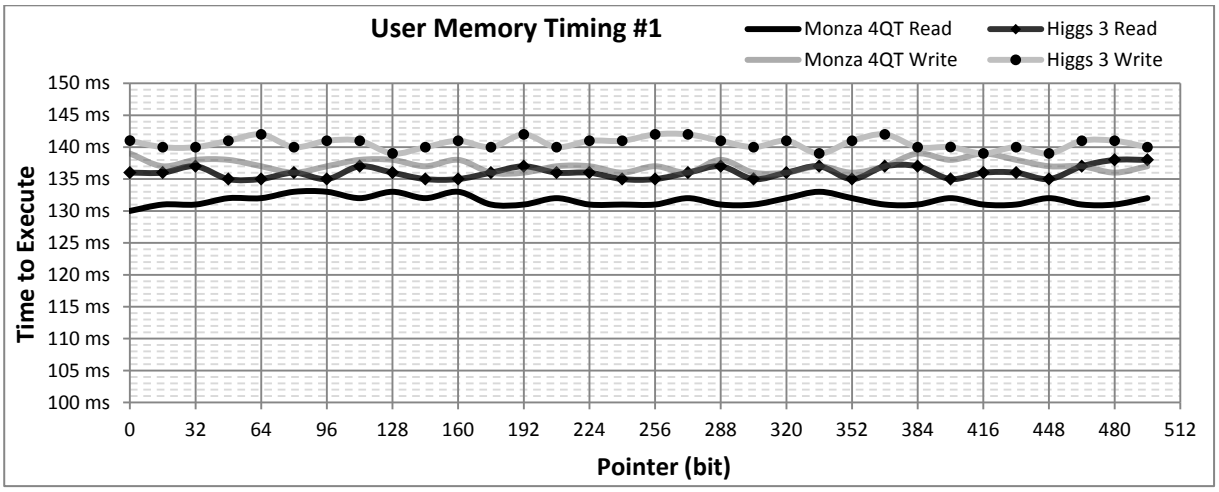

Figure 5.1 – User memory 16-bit writes performance

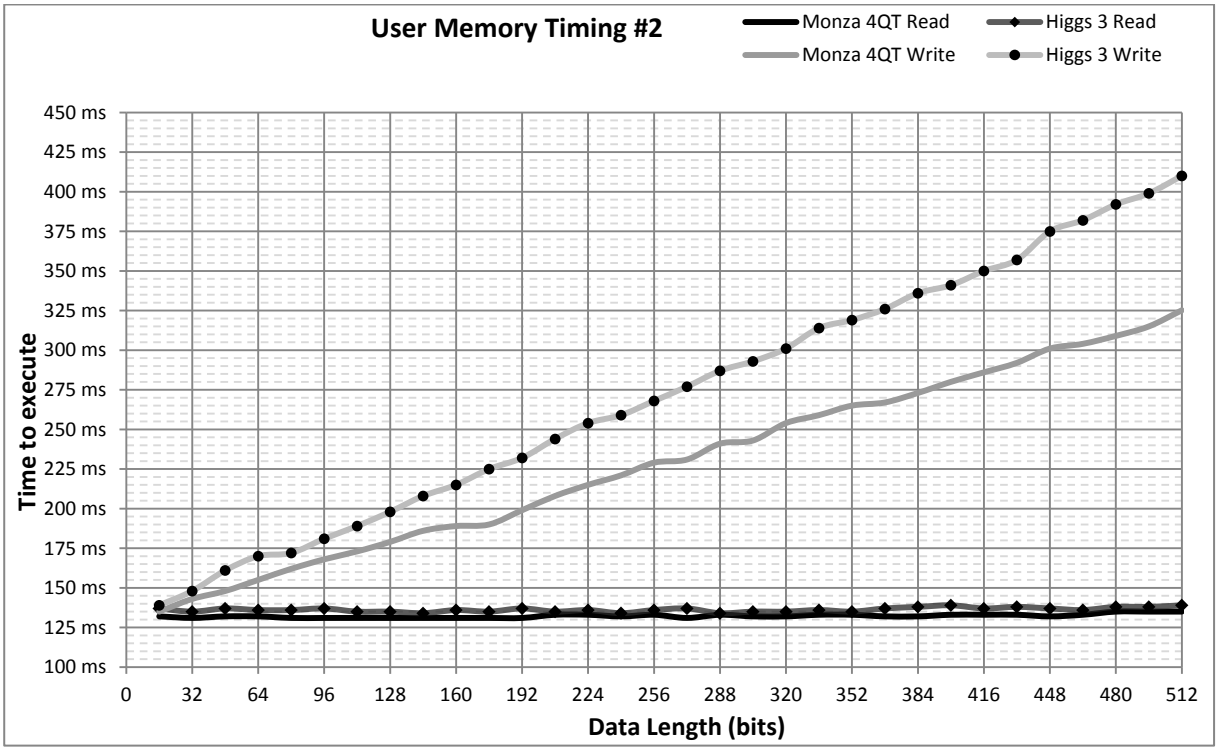

Figure 5.2 – User memory various lengths write performance

As we can see from the first benchmark, reading or writing 16-bit of data gives similar results over the entire user memory bank, with writing action being about 5ms slower than reading. Also, we can see on the second benchmark that reading data of different lengths from the user

memory gives similar results as on the first case. Instead, writing data of different lengths to the user memory takes longer as the data size increases, but it still increases linearly. From the previous figure we can clearly see that Impinj's Monza 4QT tag outperforms Alien's Higgs 3 Tag IC in terms of writing speed, so, when the speed of writing information to the tag is a key factor, Impinj's Monza 4QT is the choice.

Back to the topic of randomized (re)encryption, we conclude that such protocols may slow down the authentication process due to the need for data writing to the tag's memory. So randomized (re)encryption is only appropriate in applications like Access Control and not in application where multiple tags need to be authenticated in very short time (i.e. checking out in a supermarket or loading/unloading a truck).

5.3 Password Lock

Here we went through benchmarking of Impinj's QT Technology integrated in their Monza 4QT Tag IC. More specifically we used a LabID UH3D40 RFID tag and measured the time needed to switch between all possible QT profile configurations. The resulted data can be seen on Table 5.1 below.

Profile	Range	Persistence	Time to execute
Public	Short	Temporary	129ms
Private	Short	Temporary	116ms
Public	Normal	Temporary	117ms
Private	Normal	Temporary	115ms
Public	Short	Permanent	121ms
Private	Short	Permanent	117ms
Public	Normal	Permanent	120ms
Private	Normal	Permanent	116ms

Table 5.1 – Software: Monza QT switching times

From the above results it is clear that there is no noticeable difference when switching between two QT profile configurations, but still, the time needed to change to a new profile is not low enough in order to allow multiple tag management in a short period of time.

Next, we experimented with the functionality of the QT Range feature and how it performs on the LabID UH3D40 tag. Our benchmark was taken using the two antennas connected on the same reader and positioned as shown in Figure 5.3.

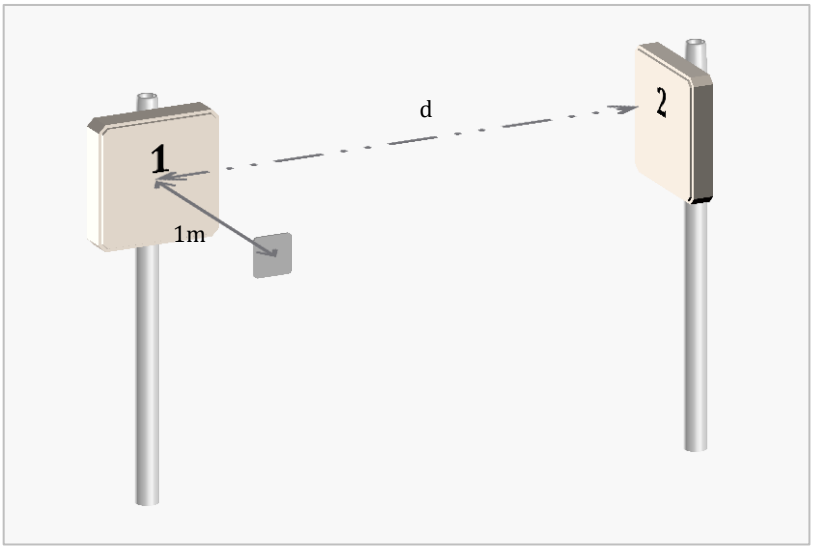

Figure 5.3 – Software: Monza QT evaluation

The distance between antenna 1 and the tag was static at 1m, while the distance between the two antennas was variable from 1,5m to 10m. When the tag was in Short-Range configuration, we were able to switch QT configuration using antenna 1, while we were unable to switch configuration using antenna 2. That leads us to the result that Short-Range reduces the configuration-range on the Monza 4QT tag chip from 10m down to 1m, confirming the state of Impinj.

So, we conclude that features like Impinj's Monza QT are applicable only where speed is not an immediate requirement, for example in Access Control or in a production line where not hundreds of products pass through the reader's range at the same time. It could be used though in applications where authentication is not required on all tagged items but only on selected ones.

5.4 Ultralightweight Mutual Authentication Protocols

Due to the lack of more advanced equipment, we were unable to evaluate the ultralightweight protocol family in hardware, but we were able to simulate them in Python by running a Reader process and multiple separate Tag processes and see how each protocol's values get updated over the time. We simulated the Gossamer protocol and run it for 50,000,000 authentication cycles without getting into any collision. The time it need to execute on a computer based system, though, is much higher than the actual time needed to authenticate in a real RFID system, which in our case was an average of 587ms per authentication when running at 100kHz. That execution time is high due to the software implementation of the protocol. In a real RFID system the protocol runs completely on hardware, and more specifically on a few hundred Gate Equivalents, clocked at about 100kHz, which makes it execute a lot faster, as show in Table 5.2 for the LMAP protocol.

Word Length	8-bit	16-bit	32-bit	64-bit	96-bit
Gates	86	173	346	691	1037
Clock Cycles	864	432	216	108	72
Auth./sec.	115	231	462	925	1388

Table 5.2 – Ultralightweight protocol (LMAP) performance

5.5 Tag read rate

Before going into the benchmark, we need to discuss a few things about Impinj's Reader Modes, as well as EPCglobal Class 1 Generation 2 Search Modes and Sessions; a way for multiple readers to independently inventory the same population of tags. There are many parameters which can be set in a C1G2[8]-compliant reader in order to optimize throughput; these can include: data rates, modulation type (both reader-to-tag and tag-to-reader), bit encoding, pulse widths and other air protocol particulars. In fact, there are over 128 combinations of settings on a typical C1G2 reader if we factor in all the variables. Impinj offers a number of preset Reader Modes (Table 5.3) to provide the best performance, as well as two separate mode settings that provide automatic control over the C1G2 Mode, called AutoPilot [76]. As a rule, there is an inverse relationship between data rate and sensitivity/interference tolerance. Higher data rates generate, and are more susceptible to, interference whereas lower data rates cause less interference and are more tolerant of it.

Reader Mode	Sensitivity	Interference Tolerance	Throughput
Max Throughput	Good	Poor	Best
Hybrid	Good	Good	Better
Dense Reader M=4	Better	Better	Better
Dense Reader M=8	Best	Excellent	Good

Table 5.3 – Impinj Reader Modes

This explains why a user may not (and most likely should not) always select "Max Throughput" mode. The name of this mode is a bit misleading, while it will support the highest data rate of any of the settings, it will not necessarily provide the best throughput or actual tag read rate due to interference and tag collisions.

- **Max Throughput**: The reader will use the mode with the highest potential throughput regardless of interference.
- **Hybrid**: Balance between throughput and interference tolerance.
- **Dense Reader M=4**: A mode that uses a Miller sub-carrier to isolate tag and reader communication in frequency allowing multiple readers to operate in close proximity.
- **Dense Reader M=8**: A mode similar to Dense Reader M=4 which uses a lower data rate and further separates the tag and reader communication frequencies

Except Reader Modes, a user may also select Search Mode and Session according to the application requirements. The C1G2 standard allows for up to four sessions which serve two purposes:

1. Determines how often a tag will respond to a query from the reader
2. Allows for multiple readers to conduct independent inventories

[8] C1G2 = EPCglobal Class 1 Generation 2 UHF RFID protocol

Each tag has four sessions S0, S1, S2, and S3. Each session has an independent inventoried flag that has two values labeled A and B. This inventoried flag can be switched from A to B or B to A by a command from the reader (Figure 5.4). The 'A' state is default when the tag powers up or after 'B' state times out (more on that later).

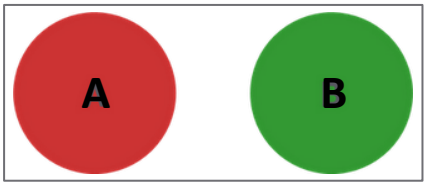

Figure 5.4 – EPC C1G2 tag states

The RFID reader will select which session is to be used, each session's inventory flag can be independently set to 'A' or 'B' as shown in Figure 5.5 below.

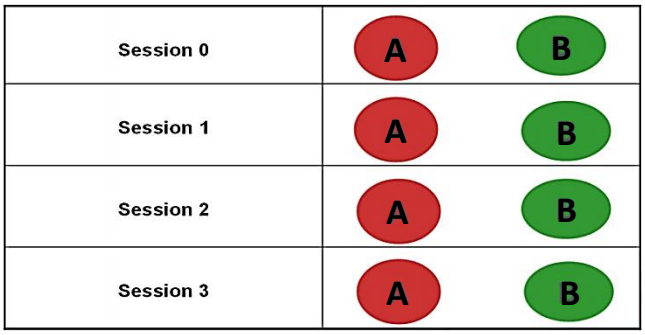

Figure 5.5 – EPC C1G2 tag sessions & states

Once the RFID reader inventories the tag, the flag state is changed from 'A' to 'B' - how long the tag stays in the 'B' state before reverting back to the 'A' state is called "persistence". It is important to realize that exact persistence times cannot be set by the user; they can only be approximated according to the Search Mode and Session.

There are three search modes available on the Impinj Revolution reader: Dual Target, Single Target and Single Target with Suppression. “Target” in this case refers to whether the reader will singulate (select) only tags that are in the 'A' state (Single Target) or if it will singulate tags in both 'A' and 'B' state (Dual Target). In Dual Target, the reader reads all ‘A’ tags then moves all ‘A’ tags into ‘B’. Reader then reads all ‘B’ tags then moves all ‘B’ tags into ‘A’ and so on. In Dual Target, session has no influence as the reader will immediately 'push' tags back into 'A' state (Figure 5.6). This search mode generates many reads and is good for small populations or static environments (i.e. smart shelf).

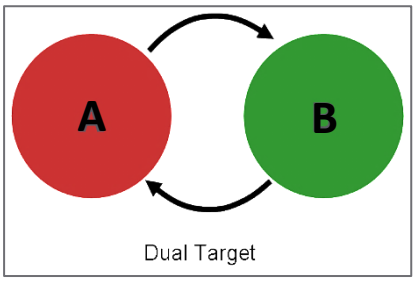

Figure 5.6 – Dual target search mode

In Single Target, the reader reads all 'A' tags then moves all 'A' tags into 'B' and allows tags to stay quiet once they are inventoried. This mode is good for high population, dynamic environments (i.e. dock door portal) (Figure 5.7).

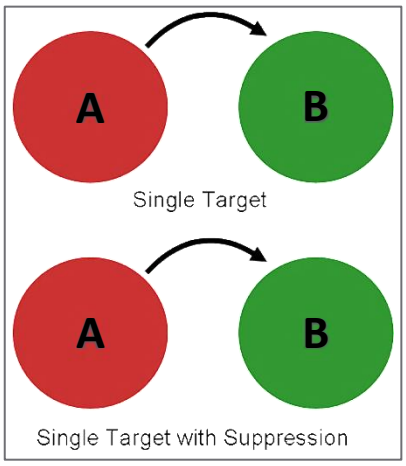

Figure 5.7 – Single target search mode

In Figure 5.8 we can see a summary of what happens when a tag enters the read field according to the Search Mode and Session.

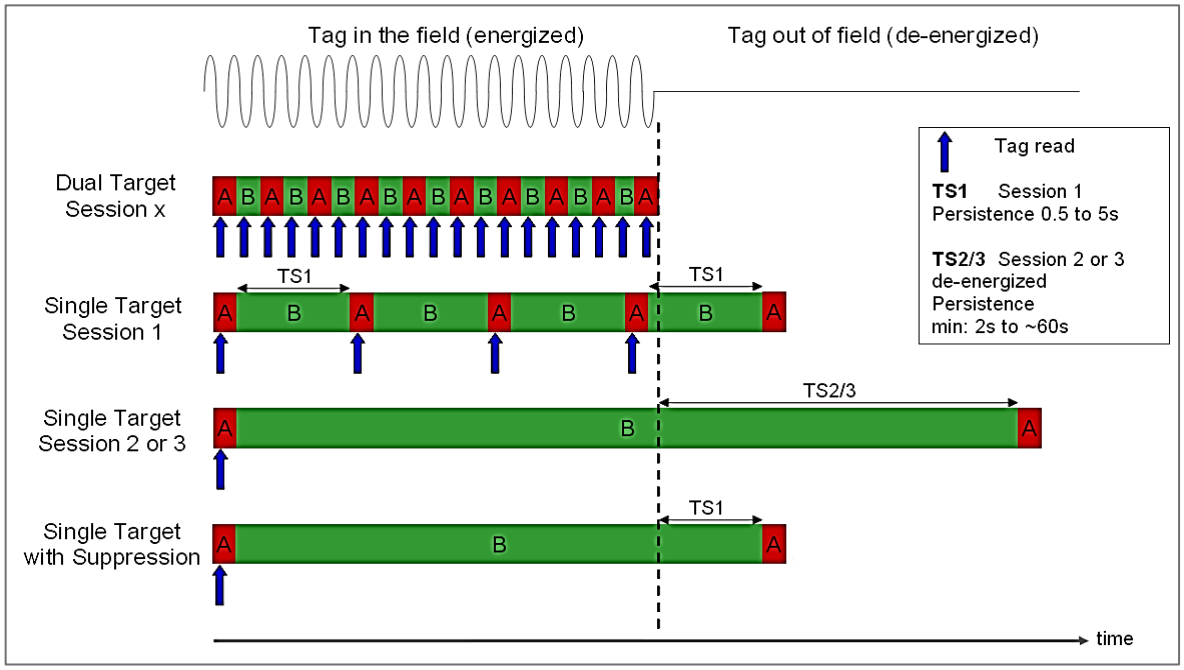

Figure 5.8 – Search modes & sessions explained

- In **Dual Target**, the tag will be read continuously regardless of tag state 'A' or 'B'; the Session setting has no influence.
- In **Single Target (Session 1)**, the tag will be read and then moved to the 'B' state. After some period of time (TS1) it will revert back to the 'A' state and be read again. This TS1 value is defined in the C1G2 standard as being between 500ms and 5 seconds; it can only be approximated. The TS1 value will vary depending on tag IC manufacturer and even specific tag IC model. (For example, the Impinj Monza 3 Session 1 persistence is approximately 1 second whereas the Monza 4 is close to 500ms. So, if we set the reader for Single Target, Session 1, we will see a Monza 4 tag being read about twice every second).

- In **Single Target (Session 2 or 3)**, the tag will be read once then switch to 'B' state and remain quiet the entire time it is in the read field (power-on state). Once the tag leaves the read field, it will have persistence (stay in the 'B' state) for a time period of TS2/3. This persistence time is only required by the C1G2 standard to be a minimum of 2 seconds with no maximum defined. Remember that during this time, the tag will not respond to a query from any reader using Single Target and the same Session.
- In **Single Target with Suppression** (also known as "Tag Focus") provides the advantage of Sessions 2 and 3 in that it will remain quiet while in the read field once inventoried thus allowing other tags which may be "quieter" (not reflecting as much power) to be read. It also provides the advantage of Session 1 in that it will revert almost immediately back to the 'A' state and be available for a reader query upon leaving the read field.

We can compare the following example scenarios (Figure 5.9):

- **Scenario 1**: There are a number of tagged items being continuously inventoried on a RFID-enabled "smart shelf". Selecting Dual Target for the search mode will allow for the fastest update of tag status and be able to provide an update alert should a tagged item be put on, or taken off, the shelf.
- **Scenario 2**: A fixed reader portal is performing an inventory on incoming items as they come off the delivery truck using Single Target, Session 2. Now, let's say we want to do a quick inventory sweep with a handheld reader (perhaps to encode the storage location). If the handheld reader uses the same session, it might miss some of the tags, or have a slow tag read rate, due to the fact that the tags were 'pushed' into the 'B' state by the fixed reader and have not yet flipped back to the 'A' state. Setting the handheld reader to a different Search Mode (i.e. Dual Target or Single Target w/ Suppression) or to Session 3, will allow the tagged items to be inventoried. Another option would be to use Single Target with Suppression (assuming the use of Impinj Monza tags) so that the large population of tags can be quickly inventoried with high probability of 100% count and still allow the tags to be re-inventoried almost immediately after leaving the portal read zone, without the need to use different Search Mode.
- **Scenario 3**: Two readers want to simultaneously inventory a population of tags and then confirm they have the same count as a way of reducing missed tags. In this case, setting one reader to Single Target, Session 2 and the other to Single Target, Session 3 will allow this to happen.

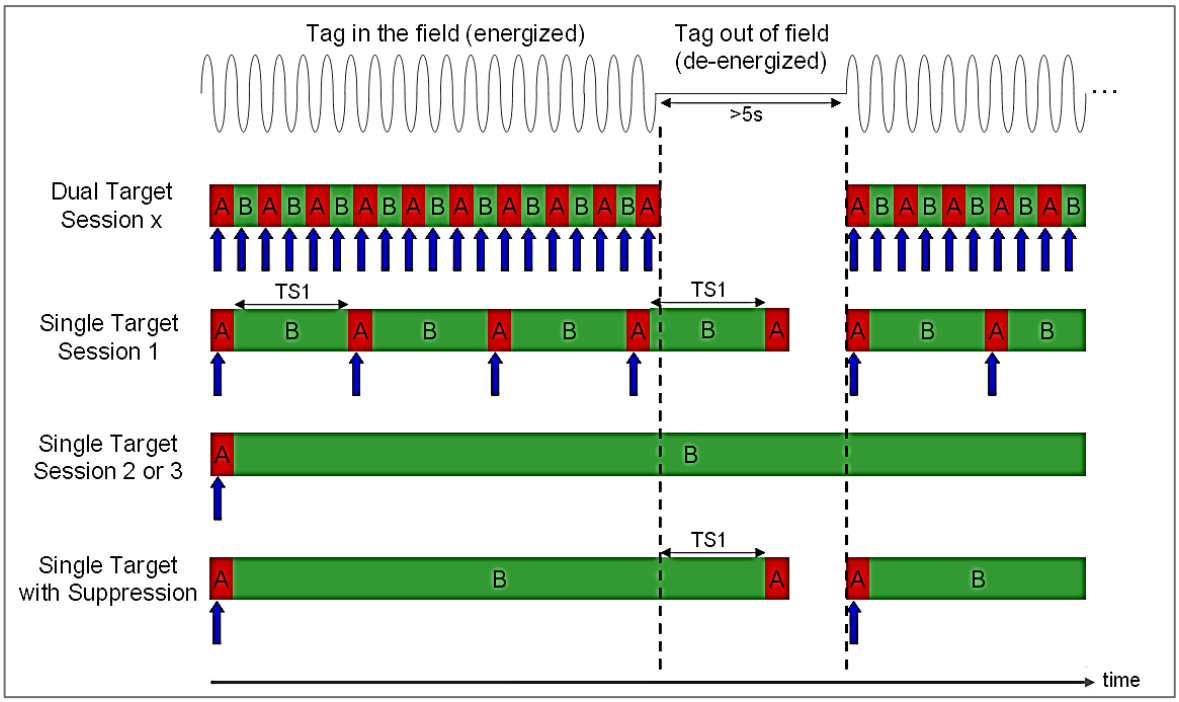

Figure 5.9 – Search modes & sessions scenarios

Now that we have discussed about the different reader configuration modes, we can get into the benchmark results. First, we experimented on how the read rate gets affected as we connect more antennas on the reader. Since we had only two Far-Field antennas available, we performed the experiments first with one, and then with two antennas. We also experimented with disabling the unused antenna ports on the reader in order to further improve the read rates (Table 5.4). The benchmark was performed using the default configuration in AutoPilot mode and with antenna ports set at 31.5dB.

Tag Model	Quantity	Read Rate	Reads per Tag	Antennas Connected	Antenna Ports Enabled
LabID UH3D40	4	89.8	22.45	1	1
		78.6	19.65		4
		91.2	22.79	2	2
		83.6	20.90		4
Impinj Thin Propeller (Short)	6	106.2	17.70	1	1
		98.2	16.37		4
		113.8	18.97	2	2
		105.1	17.52		4
Alien ALN-9540	10	188.9	18.89	1	1
		171.8	17.18		4
		190.2	19.02	2	2
		177.7	17.77		4

Table 5.4 – Antenna count versus read rate

When we inventory tags with multiple antenna ports enabled, the reader scans one antenna port at a time; so, disabling the unused antenna ports improves the read rate.

Using the implemented software we managed to benchmark the reader's performance on all possible configuration combinations of Reader Modes, Search Modes and Sessions, and find the configuration setting in order to achieve the best results according to the target application

requirements (reading rate, tag count, etc.). The evaluation was performed outdoors, with 2 antennas connected and placed close to each other and 10 RFID tags[9] placed at 50cm from the antennas (Figure 5.10). Each configuration was run for 5 seconds with enough wait time in between in order to let the tags return back to state 'A'. The results can be found in Table 5.5.

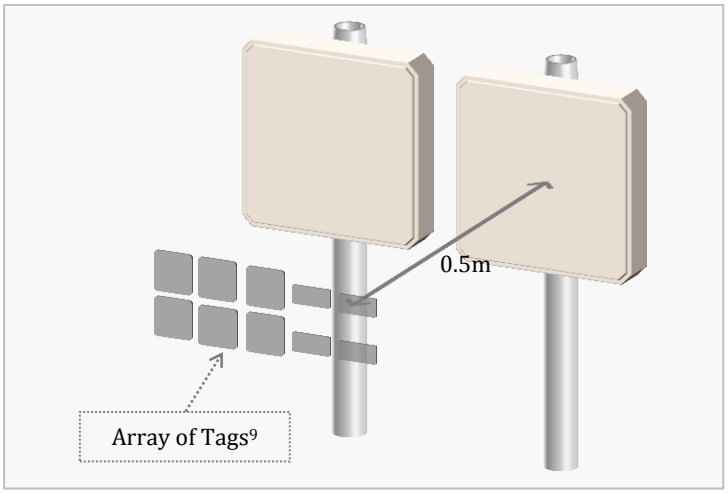

Figure 5.10 – Reader modes evaluation setup

Reader Mode	Search Mode	Session	Tags Seen	Total Reads	Average Rate
Auto Dense	Dual Target	0	10	863	172.6
		1	10	874	174.8
		2	10	857	171.4
		3	10	88	17.6
	Single Target	0	10	809	161.8
		1	10	92	18.4
		2	**10**	**10**	2.0
		3	**10**	**10**	2.0
	Single Target with Suppression	0	10	807	161.4
		1	10	11	2.2
		2	**10**	**10**	2.0
		3	**10**	**10**	2.0
Dense M=4	Dual Target	0	10	741	148.2
		1	10	732	146.4
		2	10	722	144.4
		3	10	722	144.4
	Single Target	0	10	694	138.8
		1	10	89	17.8
		2	**10**	**10**	2.0
		3	**10**	**10**	2.0
	Single Target with Suppression	0	10	688	137.6
		1	**10**	**10**	2.0
		2	**10**	**10**	2.0
		3	**10**	**10**	2.0
Dense M=8	Dual Target	0	10	466	93.2
		1	10	447	89.4
		2	10	456	91.2
		3	10	446	89.2
	Single Target	0	10	442	88.4

[9] 4x LabID UH3D40, 6x LabID UH600, all 10 with Monza 4QT tagchip

		1	10	89	17.8
		2	**10**	**10**	2.0
		3	**10**	**10**	2.0
	Single Target with Suppression	0	10	441	88.2
		1	**10**	**10**	2.0
		2	**10**	**10**	2.0
		3	**10**	**10**	2.0
Hybrid	Dual Target	0	10	795	159.0
		1	10	798	159.6
		2	10	788	157.6
		3	10	788	157.6
	Single Target	0	10	742	148.4
		1	10	89	17.8
		2	**10**	**10**	2.0
		3	**10**	**10**	2.0
	Single Target with Suppression	0	10	746	149.2
		1	**10**	**10**	2.0
		2	**10**	**10**	2.0
		3	**10**	**10**	2.0
Max Throughput	Dual Target	0	10	1552	310.4
		1	**10**	**1632**	**326.4**
		2	10	1606	321.2
		3	10	1592	318.4
	Single Target	0	10	1414	282.8
		1	10	89	17.8
		2	**10**	**10**	2.0
		3	**10**	**10**	2.0
	Single Target with Suppression	0	10	1402	280.4
		1	**10**	**10**	2.0
		2	**10**	**10**	2.0
		3	**10**	**10**	2.0

Table 5.5 – Reader modes evaluation results

In Dual Target search mode, we get the highest read rate in Max Throughput reader mode and the lowest in Dense M=8. Session doesn't seem to make any noticeable difference. In Single Target, we get the highest read rate in Max Throughput and the lowest in Dense M=8. Here, session is important as we mentioned before, and we see that with session 3 we read each tag only once, which can be useful in specific RFID applications. In Single Target with Suppression, we get the same results when comparing read rates, while we see that the session does not affect the success if the system; each tag is read only once during these 5 seconds. In our case, the most suitable configuration in order to achieve the best read rate is Max Throughput Reader Mode, with Dual Target, Session 1 Search Mode. In other cases, there may be either active or passive interference that may reduce the performance of that Reader Mode, so results will vary according to the application's environment. Similarly, Single Target Session 2/3 may give us the same results in our case no matter what the Reader Mode is, but in different applications and antenna setup it may give different results. In cases where we get the same results for different Reader Modes, the software selects the mode with the highest Interference tolerance and sensitivity, according to Table 5.3.

Auto Dense Reader Mode may be selected in cases where interference is not always present, and the mode should be switched automatically in order to achieve the best performance levels

without requiring further re-configuration. Note that between each run there is enough wait time in order to allow each tag's state to reset back to state A.

6 Conclusions

Although recent actions about RFID technology taken by Wal-Mart and U.S. Department of Defense has heat up the topic of RFID once again since World War II, the technology has not yet been proliferating as expects. This is mainly due to the reasons of the security/privacy issues, and more importantly the cost. To decrease the cost, standardization is a very important factor. In addition, security/privacy issues are barriers to people's acceptance of this technology. Therefore, more works have to be done in standardization and addressing the security/privacy issues in order to proliferate the adoption of RFID technology.

In this work we have dealt with three main subjectives. First, we classified the RFID related threats based on which part of the RFID system they target, either the hardware, or the communication. We also subdivided them based on which security objective they violate: Confidentiality, Integrity, or Availability. The existence of threats on RFID systems does not necessarily mean that they exist on every RFID system. Each system is vulnerable to only some of them, and should be handled accordingly in order to solve them. Second we presented a list of possible countermeasures in order to face one or more threats, by either using plain tags (i.e. in an already installed RFID system, or when using an already available commercial RFID system), or cryptographic ones (i.e. improving the security of current low-cost tags without affecting their cost). As a result, we conclude that security and privacy both come in many different flavors. Low-cost implies that we find mechanisms that are "good enough" and are deterrents, rather than mechanisms that are "impossible to break". It is evident that there is no universal solution but a collection of solutions suited to different applications based on compromises between level of security, power consumption, cost (area), and performance (throughput). Many defense mechanisms have already been proposed to safeguard RFID systems. Some of these attacks are easy to combat (i.e. unauthorized tag reading and tracking) by using efficiently designed protocols and cryptographic primitives as well as implementing appropriate software. Other threats are harder or more costly to defend against (i.e. hardware-related threats, like tampering attacks or signal degradation), while others are still open problems and subject to research (i.e. attacks that compromise the availability). It is obvious that there is a need for effective defense mechanisms to guarantee the reliability and security of RFID systems. This work shows that there is no silver-bullet approach for moving from radiofrequency identification to authentication and therefore accurate and well justified ways to compare the different techniques are needed. The focus of recent development in RFID authentication has been on consumer privacy, but product authentication needs also specific solutions to address the application requirements. Further research is still needed in the field of offline authentication and many network issues, before RFID product authentication will meet all its promises in practice.

Third, a software is presented that offers more and of higher level functionality than the currently available one by Impinj. More specifically it offers basic functionality for reading and writing RFID tags with in-depth information such as timing and per-antenna sensitivity, in-depth reader configuration with reader/search mode and session selection, antenna configuration, and more importantly benchmarking for real-life applications; the software can be used in an RFID

application in order to provide information about which reader/antenna configuration will provide the higher throughput or sensitivity, or a combination of both.

As future work, it would be useful first to improve the provided software by implementing it with a graphical user interface (GUI) that would make it easier to use with real-time result displaying, as well as to implement the functionality to make it able to communicate with multiple readers simultaneously, since most applications require the use of more than one RFID readers in one place. Furthermore, it could be modified in order to save the current reader configuration to a file, in order to use it during the next connection. Also, we could evaluate all of the proposed security protocols by using a more advanced RFID development tag, such as the Intel Wireless Identification and Sensing Platform (WISP, Image 6.1).

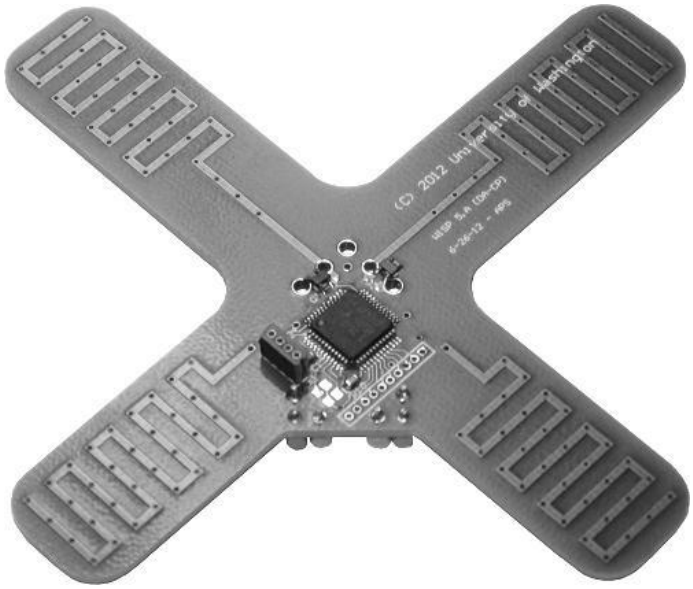

Image 6.1 – Intel WISP 5.0

References

[1] J. Banks, D. Hanny, M. Pachano, L. Thompson, *RFID Applied*, John Wiley & Sons, Inc., 2007

[2] *"The History of RFID Technology",* RFID Journal

[3] Nandita Srivastava, *"RFID Introduction, Present and Future applications and Security Implications"*, George Mason University, Virginia, 2006 , Scholarly Paper

[4] Harvey Lehpamer, *RFID Design Principles*, Artech House, Inc., 2008

[5] Korkmaz, E., *"Standards, Security & Privacy Issues about Radio Frequency Identification (RFID)"*, RFID Eurasia, 2007 1st Annual, pages 1-10

[6] N.C. Wu, M.A. Nystrom, T.R. Lin, H.C. Yu, *"Challenges to global RFID Adoption"*, Technovation, 2006, pages 1317-1323

[7] A. Razaq, W. T. Luk, K. M. Shum, L. M. Cheng, K. N. Yung, *Second-Generation RFID,* IEEE Security & Privacy, 2008, pages 21-27

[8] S. Lahiri, *RFID Sourcebook,* Prentice Hall PTR, 2005

[9] Ding Z.H., Li J.T., Feng B., *"A Taxonomy Model of RFID Security Threats"*, ICCT 2008, pages 765-768

[10] Schaberreiter, T., Wieser, C., Sanchez, I., Riekki, J., Roning, J., *"An Enumeration of RFID Related Threats"*, UBICOMM 2008, pages 381-389

[11] C. H. Huang, *"An Overview of RFID Technology, Application, and Security-Privacy Threats and Solutions"*, George Mason University, Virginia, 2009 , Scholarly Paper

[12] K. Nohl, D. Evans, S. Plötz, H. Plötz, *"Reverse-Engineering a Cryptographic RFID Tag"*, 17th USENIX Security Symposium, 2008, pages 185-193

[13] S. A. Weis , S. E. Sarma , R. L. Rivest , D. W. Engels, *"Security and privacy aspects of low-cost radio frequency identification systems"*, Security in Pervasive Computing, 2004, pages 201-212

[14] Ronald L. Rivest, *Personal correspondence*, May 2003

[15] Leonid Bolotnyy, *"Randomized Pseudo-Random Function Tree Walking Algorithm for Secure Radio-Frequency Identification"*, IEEE Workshop, 2005, pages 43-48

[16] R. Koh, E.W. Schuster, I. Chackrabarti, A. Bellman, *"Securing the Pharmaceutical Supply Chain"*, Auto-ID Labs White Paper, 2003

[17] Thorsten Staake, Frédéric Thiesse, Elgar Fleisch, *"Extending the EPC Network - The Potential of RFID in Anti-Counterfeiting"*, Auto-ID Labs White Paper, 2006

[18] M Bárász, B Boros, P Ligeti, K Lója, Nagy, *"Breaking LMAP"*, RFIDSec, 2007

[19] Joseph Pearson, *"Securing the Pharmaceutical Supply Chain with RFID and Public-key Infrastructure (PKI) Technologies"*, Texas Instruments White Paper, 2005

[20] M. Roberti, "*Congress Weighs Drug Anti-counterfeiting Bill"*, RFID Journal, 2006

[21] M. Feldhofer, J. Wolkerstorfer, V. Rijmen, *"AES implementation on a grain of sand"*, IEE Proceedings In Information Security, 2005, pages 13-20

[22] D. Henrici, P. Muller, *"Hash-based enhancement of location privacy for radiofrequency identification devices using varying identifiers"*, PERCOMW, 2004, page 149

[23] G. Avoine, P. Oechslin, *"A scalable and provably secure hash based RFID protocol"*, PERCOMW, 2005, pages 110-114

[24] M.O. Koutarou , K. Suzuki , S. Kinoshita, *"Cryptographic approach to "privacy-friendly" tags"*, RFID Privacy Workshop, 2003

[25] X. Gao, Z. Xiang, H. Wang, J. Shen, J. Huang, S. Song, *"An Approach to Security and Privacy of RFID system for Supply Chain"*, E-Commerce Technology for Dynamic E-Business, 2004. IEEE International Conference, pages 164-168

[26] S.M. Lee, Y.J. Hwang, D.H. Lee, J.I. Lim, *"Efficient authentication for low-cost RFID systems"*, ICCSA, 2005, pages 195-209

[27] E.Y. Choi, S.M. Lee, D. H. Lee, *"Efficient RFID authentication protocol for ubiquitous computing environment"*, EUC, 2005, pages 945-954

[28] S. Lee, T. Asano, K. Kim, *"RFID Mutual Authentication Scheme based on Synchronized Secret Information"*, SCIS, 2006
[29] Tianjie C., Bertino, E., Hong L., *"Security Analysis of the SASI Protocol"*, Dependable and Secure Computing, IEEE Transactions, 2009, pages 73-77
[30] A. Juels, R. Pappu, *"Squealing Euros: Privacy Protection in RFID-enabled banknotes",* Proceedings of the Financial Cryptography, 2003
[31] Zhang, X., King, B., *"Integrity Improvements to an RFID Privacy Protection Protocol for Anti-counterfeitin"*
[32] Tsudik G., *"YA-TRAP: Yet another trivial RFID authentication protocol"*, Pervasive Computing and Communications Workshops, 2006, pages 643-646
[33] D. Molnar, A. Soppera, and D. Wagner, *"A scalable, delegable, pseudonym protocol enabling ownership transfer of RFID tags"*, -, 2005, pages 276-290
[34] C. Chatmon*, "Secure anonymous RFID authentication protocols"*
[35] A. Juels, *"Minimalist cryptography for low-cost RFID tag"*, Security in communication networks, 2005, pages 149-164
[36] A. Juels, *"Strengthening EPC Tags Against Cloning"*, ACM Workshop on Wireless Security (WiSe), 2005, pages 67-76
[37] I. Vajda , L. Buttyán, *"Lightweight authentication protocols for low-cost RFID tags"*, Ubicomp , 2003
[38] Ari Juels , Stephen A. Weis, *"Authenticating pervasive devices with human protocols", -*, 2005, pages 293-308
[39] Nicholas J. Hopper , Manuel Blum, *"A Secure Human-Computer Authentication Scheme", -, 2001*
[40] J. Katz, J. S. Shin, *"Parallel and concurrent security of the HB and HB+ protocols",* EUROCRYPT, 2006, pages 73-87
[41] P. Hämäläinen, T. Alho, M. Hännikäinen, Timo D, *"Design and implementation of low area and low-power AES encryption hardware core"*, Digital System Design: Architectures, Methods and Tools, 2006. DSD 2006. 9th EUROMICRO Conference, pages 577-583
[42] Henri Gilbert , Matthew Robshaw , Hervé Sibert , Issy Les, *"An active attack against HB+ – a provably secure lightweight authentication protocol"*
[43] Selwyn Piramuthu , *"HB and related lightweight authentication protocols for secure RFID tag/reader authentication",* CollECTeR, 2006
[44] T. Dimitriou, *"A Secure and Efficient RFID Protocol that could make Big Brother (partially) Obsolete"*, Pervasive Computing and Communications, 2006. PerCom 2006. Fourth Annual IEEE International, pages 275-280
[45] T. Dimitriou, *"A Lightweight RFID Protocol to protect against Traceability and Cloning attacks"*, Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005, pages 59-66
[46] L. Hyunrok, Y. Jeongkyu, K. Kwanjo, *"Enhancing Security of EPCglobal Gen-2 RFID Tag against Traceability and Cloning"*, Networked RFID Systems and Lightweight Cryptography Raising Barriers to Product Counterfeiting, 2007
[47] L. Sun, *"Security and privacy: Modest proposals for low-cost RFID systems"*, International Journal of Security and Networks, 2010, pages 128-134
[48] Lee, J.W., *"A Technique to Build a Secret Key in Integrated Circuits for Identification and Authentication Applications"*, VLSI Circuits, 2004. Digest of Technical Papers, 2010, pages 176-179
[49] Pim Tuyls , Lejla Batina, *"RFID-tags for Anti-Counterfeiting"*, Topics in Cryptology - CT-RSA 2006, pages 115-131
[50] Stephan J. Engberg , Morten B. Harning , Christian Damsgaard Jensen, *"Zero-knowledge device authentication: Privacy & security enhanced RFID preserving business value and consumer convenience"*, Proceedings of the 2nd Annual Conference on Privacy, Security and Trust (PST'04
[51] Keunwoo Rhee, Jin Kwak, Seungjoo Kim and Dongho Won, *"Challenge-response based RFID authentication protocol for distributed database environment"*, Security in Pervasive Computing, 2005, pages 70-84

[52] D. Molnar, D. Wagner, *"Privacy and Security in Library RFID: Issues, Practices, and Architectures"*, CCS '04 Proceedings of the 11th ACM conference on Computer and communications security, pages 210-219

[53] Gregor Le, Christof Paar, Axel Poschmann, Kai Schramm, *"New lightweight DES variants"*, Proceedings of FSE 2007, LNCS

[54] P. Israsena, *"Securing ubiquitous and low-cost rfid using Tiny Encryption Algorithm"*, International Symposium on Wireless Pervasive Computing, IEEE, 2006Jeongkyu Yang, Jaemin Park, Hyunrok Lee, Kui Ren, and Kwangjo Kim*, "Mutual authentication protocol for low-cost RFID"*

[55] S. Dominikus, M. Elisabeth Oswald, M. Feldhofer, *"Symmetric Authentication for RFID Systems in Practice"*, Workshop on RFID and Leight-Weight Crypto, 2005

[56] M. Feldhofer, *"A Proposal for Authentication Protocol in a Security Layer for RFID Smart Tags"*, IEEE Mediterranean Electrotechnical Conference - MELECON, Vol. 2 (February 2004), pp. 759-762

[57] Martin Feldhofer, Sandra Dominikus, Johannes Wolkerstorfer, *"Strong authentication for RFID systems using the AES algorithm"*, Cryptographic Hardware and Embedded Systems - CHES 2004 (2004), pp. 357-370

[58] D.V. Bailey and A. Juels, *"Shoehorning security into the EPC standard"*

[59] Nochta Z., Staake T., Fleisch E., *"Product Specific Security Features Based on RFID Technology"*, SAINT-W '06 Proceedings of the International Symposium on Applications on Internet Workshops, pages 72-75

[60] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Estevez-Tapiador, A. Ribagorda, *"M²AP: A Minimalist Mutual-Authentication Protocol for Low-cost RFID Tags"*, 3rd International Conference on Ubiquitous Intelligence and Computing (UIC'06), pages 912-923

[61] B. Alomair, L. Lazos, R. Poovendran, *"Passive Attacks on a Class of Authentication Protocols for RFID"*, Information Security and Cryptology - ICISC 2007, pp. 102-115

[62] P. Peris-lopez , J. Cesar Hern , J. M. Estevez Tapiador , A. Ribagorda, *"LMAP - A real Lightweight Mutual Authentication Protocol for Low-cost RFID tags"*, 2nd Workshop on RFID Security, 2006

[63] T. Li , G. Wang, *"Security Analysis of Two Ultra-Lightweight RFID Authentication Protocols"*, IFIP SEC, 2007, pages 14-16

[64] P. Peris-lopez , J. Cesar Hern , J. M. Estevez-Tapiador , A. Ribagorda, *"EMAP: An efficient mutual authentication protocol for low-cost RFID tags"*, OTM Federated Conferences, 2006, pages 352-361

[65] Tieyan Li, *"Vulnerability Analysis of EMAP-An Efficient RFID Mutual Authentication Protocol"*, Second International Conference on Availability, Reliability and Security (AReS), 2007, pages 10-13

[66] Hung-Yu Chien, *"SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity"*, Dependable and Secure Computing, IEEE Transactions, 2007, 337-340

[67] G. Avoine, X. Carpent, B. Martin, *"Strong authentication and strong integrity (SASI) is not that strong"*, RFIDSec'10, pages 50-64

[68] P. Peris-Lopez, J. C. Hernández Castro, J. M. Estévez-Tapiador, A. Ribagorda, *"Advances in Ultralightweight Cryptography for Low-cost RFID Tags: Gossamer Protocol"*, WISA Conf., 2008

[69] K.-H. Yeh and N.W. Lo, *"Improvement of Two Lightweight RFID Authentication Protocols"*, IASL, 2010

[70] R. K. Pateriya, S. Sharma, *"An Ultralightweight Mutual Authentication Protocol for Low Cost RFID Tags"*, International Journal of Computer Applications, 2011

[71] M. David, N. R. Prasad, *"Providing Strong Security and High Privacy in Low-Cost RFID Networks"*, Security and Privacy in Mobile Information and Communication Systems, 2009, pages 172-179

[72] M. Kianersi, M. Gardeshi, M. Arjmand, *"SULMA: A Secure Ultra-Light-Weight Mutual Authentication Protocol for Low-Cost RFID Tags"*, International Journal of UbiComp, 2011, pages 17-24

[73] M. Azizi, N. Bagheri, *"Cryptanalysis of SULMA, an Ultralightweight Mutual Authentication Protocol for Low-Cost RFID Tags"*, International Journal of UbiComp, 2011, pages 15-
[74] *Zebra's UHF Gen 2 RFID Card: http://www.zebra.com/content/dam/zebra/product-information/en-us/brochures-datasheets/supplies-accessories/final-uhf-carddatasheet-en-us.pdf*
[75] C. Swedberg, *"New Impinj Reader Goes on Autopilot"*, RFID Journal, 2009
[76] T. Eisenbarth, S. Kumar, L. Uhsadel, C. Paar, A. Poschmann, *"A survey of lightweight cryptography implementations"*, Design & Test of Computers, IEEE, 2007, pages 522-533
[77] S. Sarma, *"Towards the 5¢ tag"*, International Journal of Retail and distribution Management, 2002
[78] S. E. Sarma, S. A. Weis, D. Engels, *"Mutual Authentication Protocol for Low-Cost RFID][Radio-Frequency Identification: Security Risks and Challenges"*, CryptoBytes, Vol. 6, No. 1., 2003
[79] S.A. Weis, *"Security and Privacy in Radio-Frequency Identification Devices"*, Master Thesis, MIT, 2003
[80] F. Macé , F.Xavier St, J.-J. Quisquater, *"ASIC implementations of the block cipher SEA for constrained applications"*, RFIDSec 2007
[81] C. de Cannière, Orr Dunkelman, M. Knezevic, *"KATAN and KTANTAN: a family of small and efficient hardware-oriented block ciphers"*, CHES 2009, pages 272-288
[82] Chae Hoon Lim and Tymur Korkishko, *"mCRYPTON–a lightweight block cipher for security of low-cost RFID tags and sensors"*, Information Security Applications, 2006, pages 243-258
[83] *RFID Journal Glossary: Faraday Cage*
[84] A. Juels, R. L. Rivest, and M. Szydlo, *"The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy"*, 8th ACM Conference on Computer and Communications Security, 2003, pages 103-111
[85] C. Blundo, A. de Caro, G. Persiano, *"Untraceable RFID Tags via Insubvertible Encryption"*, Data Privacy Management and Autonomous Spontaneous Security, 2010, pages 178-192
[86] P. Golle, M. Jakobsson, A. Juels, and P. Syverson, *"Universal re-encryption for mix-nets"*, RSA Conference Cryptographers' Track '04, pp. 163-178
[87] H.-M. Sun, W.-C. Ting, K.-H. Wang, *"On the Security of Chien's Ultralightweight RFID Authentication Protocol"*, IEEE Trans. Dependable Sec. Comput., 2011, pages 315-317
[88] U. Dürholz, M. Fischlin, M. Kasper, C. Onete, *"A Formal Approach to Distance-Bounding RFID Protocols"*, ISC'11 Proceedings of the 14th international conference on Information security, pages 47-62
[89] C. Rolfes, A. Poschmann, C. Paar, *"Security for 1000 Gate Equivalents"*, CiteSeerX, 2008, pages 89-103
[90] Lars Knudsen, Gregor Leander, Axel Poschmann and Matthew J. B. Robshaw, *"PRINTcipher: a block cipher for IC-printing"*, CHES 2010, pages 16-32
[91] O. Yalcin, S. Berna, *"Radio-frequency identification security and privacy"*, 6th International Workshop, RFIDSec 2010
[92] Z. Bilal, A. Masood, F. Kausar, *"Security Analysis of Ultralightweight Cryptographic Protocol for Low-cost RFID Tags: Gossamer Protocol"*, NBIS '09, pages 260-267
[93] *RFID Security & Privacy Lounge, http://www.avoine.net/rfid/*
[94] M. Bárász, B. Boros, P. Ligeti, K. Lója, D. A. Nagy, *"Passive Attack Against the M²AP Mutual Authentication Protocol for RFID Tags"*, RFIDsec 2010
[95] Aikaterini Mitrokotsa, Melanie R. Rieback, Andrew S. Tanenbaum, *"Classification of RFID Attacks"*, CiteSeerX, pages 73-86
[96] *Pedro Peris-Lopez, http://www.lightweightcryptography.com/*
[97] Ari Juels , Stephen A. Weis, *"Authenticating pervasive devices with human protocols"*, CiteSeerX, 2005, pages 293-308
[98] Serge Zhilyaev, *"Evaluating a new mac for current and next generation RFID"*, Master's Thesis, 2010

Table of Figures

Figure 1.1 – Typical RFID Application 1
Figure 1.2 – RFID System Components 3
Figure 1.3 – Frequency Influence 5
Figure 1.4 – FCC Channels & Power limits 6
Figure 1.5 – ETSI Channels & Power limits 6
Figure 1.6 – Inductive coupling 7
Figure 1.7 – Backscatter coupling 7
Figure 1.8 – The OSI model 9
Figure 1.9 – 96-bit EPC structure 10
Figure 1.10 – RFID collision 11
Figure 1.11 – Barcode scanning process 14
Figure 2.1 – Taxonomy model of RFID threats 17
Figure 2.2 – Enumeration of RFID threats 18
Figure 3.1 - Antenna Mapping 28
Figure 3.2 – Impinj Satellite Mapping 29
Figure 3.3 – LabID UH3D40 Mapping 29
Figure 3.4 – Alien ALN-9640 Mapping 30
Figure 3.5 – Mapping diagram 30
Figure 3.6 – Impinj Satellite RSSI diagram 31
Figure 3.7 – LabID UH3D40 RSSI diagram 31
Figure 3.8 – Alien ALN-9640 RSSI diagram 32
Figure 3.9 – LabID UH3D40 Range 32
Figure 3.10 – Impinj Satellite Read rate versus Distance 33
Figure 3.11 – LabID UH3D40 & Alien ALN-9640 Read rate versus Distance 33
Figure 3.12 – Tagged object 34
Figure 3.13 – Object behind tag 34
Figure 3.14 – Tag performance on different objects 34
Figure 3.15 – Tag stack 35
Figure 3.16 – Tag array 35
Figure 3.17 – Impinj Satellite read rate 37
Figure 3.18 – Alien ALN-9640 read rate 37
Figure 3.19 – LabID UH3D40 read rate 37
Figure 3.20 – LabID UH3D40 population interference 38
Figure 3.21 – Alien ALN-9640 population interference 38
Figure 3.22 – Impinj Satellite scanning distance versus antenna power output 40
Figure 3.23 – LabID UH3D40 scanning distance versus antenna power output 40
Figure 3.24 – Tags far from each other 41
Figure 3.25 – Tags next to each other 41
Figure 3.26 – Antenna Power Output versus Power Consumption 42
Figure 4.1 – The Three Pillars 43
Figure 4.2 – RFID security threat division 44
Figure 4.3 – RFID Hardware security threats 45
Figure 4.4 – RFID Communication security threats 47
Figure 4.5 – Monza QT short range feature 51
Figure 4.6 – Cost, Performance & Security trade-off 52
Figure 4.7 – Eavesdropping ranges 56
Figure 4.8 – Software: Query reader state 62
Figure 4.9 – Software: Query tags 62
Figure 4.10 – Software: In-depth query tags 63
Figure 4.11 – Software: Query tag access password 64

Figure 4.12 – Software: Tag selection 64
Figure 4.13 – Software: Locked tag selected 65
Figure 4.14 – Software: Reader settings 65
Figure 4.15 – Software: Program tag EPC 66
Figure 4.16 – Software: Program tag Public EPC 66
Figure 4.17 – Software: Unsupported tag selected 67
Figure 4.18 – Software: Program tag Access/Kill password 67
Figure 4.19 – Software: Program tag User Memory 68
Figure 4.20 – Software: Program tag QT profile 68
Figure 4.21 – Tag memory bank locking 69
Figure 4.22 – Software: Bench read rate 70
Figure 4.23 – Software: Configuration suggestions 70
Figure 5.1 – User memory 16-bit writes performance 72
Figure 5.2 – User memory various lengths write performance 72
Figure 5.3 – Software: Monza QT evaluation 74
Figure 5.4 – EPC C1G2 tag states 76
Figure 5.5 – EPC C1G2 tag sessions & states 76
Figure 5.6 – Dual target search mode 76
Figure 5.7 – Single target search mode 77
Figure 5.8 – Search modes & sessions explained 77
Figure 5.9 – Search modes & sessions scenarios 79
Figure 5.10 – Reader modes evaluation setup 80

Table 1.1 – RFID tag classification 3
Table 1.2 – RFID Frequency Bands 5
Table 3.1 – Tag list 27
Table 3.2 – Tag RSSI boundaries 32
Table 3.3 – Tag stack performance 36
Table 3.4 – Tag array performance 36
Table 3.5 – Tag population interference 37
Table 3.6 – Tag scanning distance versus Antenna output power 39
Table 4.1 – Monza 4QT data profiles 50
Table 4.2 – Proposed improvements over RFID security & privacy 53
Table 4.3 – Comparison of lightweight security primitives 58
Table 4.4 – Ultralightweight protocol comparison 59
Table 4.5 – TID values of known tag ICs 63
Table 5.1 – Software: Monza QT switching times 73
Table 5.2 – Ultralightweight protocol (LMAP) performance 75
Table 5.3 – Impinj Reader Modes 75
Table 5.4 – Antenna count versus read rate 79
Table 5.5 – Reader modes evaluation results 81

Image 3.1 – Evaluation kit 27
Image 5.1 – ePassport Shielding 71
Image 5.2 – Tag shielding 71
Image 6.1 – Intel WISP 5.0 84