CHAPTER-3

THEORETICAL BACKGROUND

3.1 Introduction:
In this section we summarize the very low cost computing platforms, more specifically Radio Frequency Identification technology, that is set to become ubiquitous over the coming years. Then we discuss the challenges of providing a layer of security to such platforms.

Radio Frequency Identification

The world today is dominated by global forces as we live in a new globalized world economy. Global competition, rapid response to customer needs at low costs and rapid technology deployments are just a few of those forces. As markets grew and became more diverse, a need emerged for a mechanized system that would simplify the process of managing complex inventories. Barcodes, which were created to solve the problem of managing large complex inventories didn’t suffice.

The successor of barcodes is said to be RFID, Radio Frequency identifier. RFID system contains, as with many other types of automatic identification systems, a set of interrelated components. Such components are tags (passive, active, semi-active or semi-passive), antennas and readers forming an RFID system. More detailed explanation will be given later in this thesis.

Network structural design identifies how sensors supposed to be report the data to the Access Points (APs). There are 3 kind of network structural design contain be regard as in the literature survey: a. flat ad-hoc, b. hierarchical ad-hoc, and c. Sensor Network with Mobile Access. Below the flat ad-hoc structural design, sensors communicate every additional data in multiple hops to the APs. Within hierarchical wireless sensor networks, sensors appearance clusters and reports their data toward the cluster heads that are accountable for transfer the comprehensive data to the application. In Sensor Network with Mobile Access, sensors communicate straightforwardly with mobile APs affecting approximately the sensor sports ground.
Problems with barcode systems today are: dirt, intense sunlight, scratches in the barcode, temperature and hazardous contamination. The main differences between barcode and RFID technology is that RFID technology offers extended data capacity (identification on item-level) and extended data capture possibilities such as collected data without line of sight. The technical differences between barcode and RFID are given in Table 3.1.

Table 3.1 – Technical Differences between Barcode and RFID

<table>
<thead>
<tr>
<th>System</th>
<th>Barcode</th>
<th>RFID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Transmission</td>
<td>Optical</td>
<td>Electromagnetic</td>
</tr>
<tr>
<td>Typical Data Volume</td>
<td>1–100 Bytes</td>
<td>128–8K Bytes</td>
</tr>
<tr>
<td>Data Modification</td>
<td>Not possible</td>
<td>Possible</td>
</tr>
<tr>
<td>Position of Data Carrier for Read/Write</td>
<td>Visual contact</td>
<td>Non line of sight possible</td>
</tr>
<tr>
<td>Reading Distance</td>
<td>Several meters (line of sight)</td>
<td>From centimeters to meters (depending on the frequency and tags)</td>
</tr>
<tr>
<td>Access Security</td>
<td>Little</td>
<td>High</td>
</tr>
<tr>
<td>Environmental Susceptibility</td>
<td>Dirt</td>
<td>Very small</td>
</tr>
<tr>
<td>Anticollision</td>
<td>Not possible</td>
<td>Possible</td>
</tr>
</tbody>
</table>

3.2 Evolution of RFID:

When the notion of Radio-Frequency Identification arose in 1940s, it was used for identification of objects, i.e., allied airplanes by the military forces. The so called active tags needed a power supply, had rather large dimensions and carried small amounts of data, e.g., a fixed unique number. As technology evolved, with modern
silicon wafer manufacturing, chip sizes with an area as small as \(0.15 \times 0.15 \text{ mm}^2\) and a thickness of only 7.5 \(\mu\text{m}\) are possible, resulting in lower energy consumption.

This enables passive tags, which draw the energy needed for operation completely from the RF1 field that is generated by a reader device. At the same time, it is now possible to put much larger memories and even microcontrollers with crypto co-processors on the chip of the tag, so that applications like contactless, cryptographically enabled smartcards and their use as credit cards or digital passports are becoming widespread and RFID can be an ubiquitous technology.

The world today is dominated by global forces as we live in a new globalized world economy. Global competition, rapid response to customer needs at low costs and rapid technology deployments are just a few of those forces. As markets grew and became more diverse, a need emerged for a mechanized system that would simplify the process of managing complex inventories.

The coverage power utilization is the extra power consumed in data compilation. It depends on the velocity of data compilation and the channel reproduction as well as the network structural design and procedures. It consists of the power inspired in transmission, response, and probably channels achievement. We notice out that power consumption might come from additional sources such as network preservation whose power spending rate is neither incessant nor connected to data compilation. Lifetime Definition Network lifetime is the moment span beginning the operation to the immediate while the network is measured nonfunctional. Once a network be supposed to be regard as nonfunctional is, conversely, application-specific. It is able to be for instance, the instantaneous when the foremost sensor dies, a proportion of sensors expire, the network separation, or the loss of exposure occurs.

Barcodes – which were created to solve the problem of managing large complex inventories – didn’t suffice. This enables passive tags, which draw the energy needed for operation completely from the RF1 field that is generated by a reader device. At the same time, it is now possible to put much larger memories and even microcontrollers with crypto co-processors on the chip of the tag, so that applications
like contactless, cryptographically enabled smartcards and their use as credit cards or digital passports are becoming widespread and RFID can be an ubiquitous technology.

The successor of barcodes is said to be RFID, Radio Frequency Identifier. RFID system contains, as with many other types of automatic identification systems, a set of interrelated components. Such components are tags (passive, active, semi-active or semi-passive), antennas and readers forming an RFID system. More detailed explanation will be given later in this thesis.

In the beginning of 2000s RFID became a “hype‖ technology. But a time of disillusion soon followed, because of the immaturity of the technology as it was not applicable for such wide-scale application. Today, RFID is a fast growing technology, but the “hype‖ seems to be over.

3.3 RFID TAGS

Tags emphasis on the use as a label and the application for item identification and transponder emphasis on the communication process, the term tag will be used in this thesis.

Tags are the devices affixed to the items or material that is to be tracked or identified within the supply chain by the RFID system and come in all sorts of shapes and sizes, where the most common construction format is the so-called disk (coin) a tag in a round injection molded housing.

In order to provide a better understanding and research work, here in this thesis the author has intended to present a brief description of technologies or protocols being implemented. In the preceding section brief of parallel techniques implemented in research work have been presented.

The tag contains three basic parts: electronic integrated circuit to store some digital ID information; a miniature antenna to transmit the ID to the rest of the RFID system which is the primary function of the tag; a substrate to hold the integrated circuit and the antenna together.
RFID can be mounted in a lot of different ways: as stickers – also called adhesive labels and is the most common mounting form for RFID tags; card transponders; glass cylinders, which is used in i.e. animal identification; plastic packaged transponders that is developed for applications involving particularly high mechanical demands; robust industrial packaging.

Tags transmit over a spectrum of frequencies, from short range low frequency to long-range ultra high frequency and microwave frequencies. According to Dong-Her Shih et.al [78] the biggest potential for passive RFID tags lies within the ultra high frequency.
The most accepted RFID protocol today is the EPC, which support read/write features.

### 3.3.1 Active tags

Active tags (Below Figure), also called radio frequency beacons, are the size of a small coin but are both significantly larger and more expensive than their passive counterparts because they contain an onboard power source with an additional circuitry. The battery powers both the tag’s internal circuitry and the onboard antenna, which results in that the range of active tags are generally far more superior to that of passive tags in which the range of a transmission for an active tag is tens to even hundreds of meters whereas passive tags have a transmission range up to just a meter.

<table>
<thead>
<tr>
<th>Frequency Band</th>
<th>Description</th>
<th>Range</th>
<th>Common Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>135 KHz</td>
<td>Low frequency</td>
<td>&lt; 0.33 m</td>
<td>- Vehicle identification</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Animal ID</td>
</tr>
<tr>
<td>13.56 MHz</td>
<td>High frequency (HF)</td>
<td>Near contact</td>
<td>1 m</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Fare collection</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Contactless payment</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Access control</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Sample tracking</td>
</tr>
<tr>
<td>860 - 960 MHz</td>
<td>Ultra high frequency (UHF)</td>
<td>1 - 3 m</td>
<td>- Compliance tagging and other case and pallet ID</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Returnable container tracking</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Work-in-process tracking</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Asset management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Baggage tacking</td>
</tr>
<tr>
<td>2.45 GHz</td>
<td>Microwave</td>
<td>1 m</td>
<td>- Long-range identification with active tags</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Airline baggage</td>
</tr>
</tbody>
</table>
The battery powers both the tag’s internal circuitry and the onboard antenna, which results in that the range of active tags are generally far more superior to that of passive tags.

Many active tag batteries resemble normal commercial batteries, but they also come in many other different shapes and sizes. Because of the higher voltage the active tag batteries may also require different battery chemistry then usual commercial battery, which utilize alkaline, nickel-cadmium or nickel metal hydride whereas the RFID battery are likely to be based on a more costly advanced battery technologies such as lithium chemistry.

Fig: 3.2 components of an active tag.
A lot of active tags have plastic housing and thus cannot simply be adhered to high-volume inventory. Because of this and the fact that the active tags are larger and more expensive than the passive counterparts they are more suitable for a different set of application, often where they will be deployed in smaller numbers; It’s very unlikely that active tags will ever be used at the individual consumer product level.

Shepard states that the choice between an active vs. a passive tag is purely dependent upon the application for which it will be used. For example, active tags are often used when the tag must be at a great distance from the reader (automated toll-paying application, E-Z Pass, as previously mentioned), tracking large items (pallets, containers, etc.), and trucking or shipping container identification application or certain supply chain implementations.

### 3.3.2 Passive Tags

Passive tags are much smaller in both size and memory than active tags and are also more popular. They do not contain any power source, and are thus only active when they come within the range of a reader’s signal. The RFID system antenna powers the tag through electromagnetic power. Since passive tags do not contain their own power source and have less memory the design can be simpler and it is cheaper to manufacture, which makes them ideal in situations where large numbers of them are required, for example: in fuel-dispensing application, bookstore/library access-control application. The passive tags have to be affixed in close proximity to the reader in order to work.

Passive tags consist of two main components: A microchip and an antenna and it are therefore, as mentioned before. Because it has no moving parts it is generally resistant to harsh environmental conditions.
While active tags are dependent on the number of times the tag is activated, passive tags are not and can therefore have an unlimited shelf life. Passive tags have therefore been the focus of most government and commercial RFID mandates and many experts believe that passive tags are the future of RFID.

The price of the passive RFID tag have steadily gone down during the last years, as a result of increased scales of production, reduced silicon prices, more economic production methods etc. When the price reaches five cent the total demand will be explosively larger, significant acceptance will be achieved. According to Dinning and Schuster, the passive tags are feasible for widespread application, especially high volume consumer goods manufacturing with high selling prices like razor blades, batteries and perfume. The price reaches five cent the total demand will be explosively larger, significant acceptance will be achieved. When the passive tag reaches one cent the demand for passive RFID tags will be equal that for barcodes.

3.3.3 Semi Active/ Semi Passive Tags:

In contrast to passive tags, semi-active tags and semi-passive tags have an onboard power source, and may also have an onboard sensor. This makes these kinds of tags
more expensive than passive tags, but they are on the other hand cheaper than active tags. They fall in the middle between passive and active tags compared to both price and capabilities.

There seems to be some confusion in the industry about the difference between semi-active and semi-passive tags (and also active and passive). The definition that has been be used in this introductory part of the thesis for semi-active and semi-passive tags are based on the definition of passive and active tags, whereas:

- An active tag uses a battery to power or boost the signal.
- A passive tag relies entirely on the energy from the signal.

Resulting in:

- A semi-active tag uses a battery to power or boost the signal, but respond only when they are within the range of a reader’s signal.

- A semi-passive tag relies entirely on the energy from the signal, but may use the onboard power for sourcing onboard sensors etc.

The difference is thus on whether the power source powers the signal or not.

The onboard power source has two purposes:

- To provide continuous power for the sensors.
- To allow the intelligence contained in the chip to function without harvesting energy.
Normally semi-active tags exist in a sleep mode to conserve battery power; this ability greatly lengthens the operational life of a semi-active tag and enables the tag to be operational for several years. This means that the RFID engineer have to design the RFID system so the semi-active tags that are stored within an interrogation zone will not be continuously activated until their batteries are exhausted.

3.4 SCANNERS AND RFID READERS

Readers have two tasks:

- To communicate with the tags through an attached antenna.
- The pass the signal the reader captures to a computer for processing.
It can therefore be seen as a bridge between the host and the emitting antenna. In a passive tag system, the reader sends out a wake-up beacon and the necessary energy for the passive tag to operate, while in an active system, the onboard power supply on the tag is used to boost the signal strength and thus the reading distance. A reader can either be affixed in a stationary position, or integrated into a mobile computer such as a barcode scanner, or embedded into electronic equipment such as a label printer.

### 3.4.1 Antennas

The largest part of the tag is the antenna, which is connected to the tag interconnect. The antenna is usually made of thin metal strips of either copper, aluminum or silver with the shape of either a spiral coil, a single dipole, dual dipoles (one perpendicular to other), or as a folded dipole. It is the geometry (both size and design) of the antenna that determines its operating frequency and thus the design of the antennas is based upon which frequency the tag is going to operate on. Large antennas operate on low frequencies, while small antennas operate on high frequencies. The actual size of the antenna can and is typically reduced with creative antenna design. The geometry (both size and design) of the antenna that determines its operating frequency and thus the design of the antennas is based upon which frequency the tag is going to operate on.

Depending on the tag, the antenna has slightly different functions when receiving a signal from the interrogator. For an active tag, it transmits the signal, while for both semi-passive and passive tag, it reflects it. Large antennas operate on low frequencies, while small antennas operate on high frequencies. The actual size of the antenna can and is typically reduced with creative antenna design. For passive tags, the antenna also supplies the tag with power collected from the radio waves.

There are three kinds of methods for manufacturing antennas: copper etching, foil stamping and screen printing. The fastest and least expensive of them all is screen printing, but the down side is that antennas created using this method are also less efficient than those created by one of the other methods.
3.4.2 Host

Host, also called software system and is composed of the following four components:

- Edge interface / system.
- Middleware.
- Enterprise back-end interface.
- Enterprise back-end.

Fig: 3.5 Logical Components of RFID

3.4.3 Edge Interface / System

The main task of the edge interface is establish communication and retrieve data from the readers, but also to control the readers’ behavior and to employ the readers to stimulate the connected external actuators and enunciators. Furthermore it can also be used for example filtering out duplicate reads from different readers or providing settings for event-based triggers for activating an enunciator or actuator.
3.4.4 Middleware

The middleware factor is the most multifaceted and imperative constituent of the host and software system. Often, a more general description is given, for example: -RFID middleware controls and manages the readers, and performs filtering, aggregation, counting of tag. The component provides for example:

- Data distribution both inside the system or enterprise and outside of an enterprise.
- Data management for the RFID system.
- Compatibility to a wide range of other systems.

The implementation of LEACH can be easily understood by the following way:

Setup phase: Steady phase: Symbolic Presentation used above CN candidate node to become the cluster head R Random variable(0 < r < 1) T(n) threshold value CH cluster head G all nodes in the network Id identification number Join_adv advertisement to join the cluster A normal node T Time slot to send the sensed data Broadcast Unicast LEACH protocol has illustrated better results in numerous scenarios, but the results obtained were not sufficient and was a huge gap for further development. The emergence of evolutionary computing has ignited a number research enhancement and protocol development. Initially Genetic algorithm based approach were used dominantly but considering the swarm behavior and its characteristics made researchers to think about its implementation for protocol development and optimization. Here in this research work the author has implemented two parallel systems for comparison, first was LEACH and it was further compared with a robust technique called as Particle Swarm optimization (PSO). Particle Swarm optimizations have also demonstrates an enhanced result as evaluate to further conservative techniques.

At diverse period, every node has the load of acquiring data commencing the nodes in the cluster, combining the data to acquire a cumulative indication, and transmitting this comprehensive indication to the bottom station. Though, the majority of the obtainable revise decomposes the resource portion difficulty at dissimilar layers, and regard as distribution of the property at every layer unconnectedly.
These all types of specific characteristics could play a vital role in network optimization and its lifetime enhancement. Evolutionary computing has ignited a new scenario for research and development in numerous engineering segments. Considering the evolutionary characteristics of elephant swarm behavior, here in this research work a robust cross layered architecture has been developed. The overall system has been developed while considering the homogenous network conditions and has been simulated with various operating parameters.

### 3.5 RFID ADOPTION PHASES

The adoption phase for RFID can be divided into three phases according to Attaran:

- **Elementary phase (or slap and ship)** – This phase includes the learning about RFID technology and the startup process. In this phase the tags are normally only applied to a small number of products. The "slap and ship" refers to RFID tags that are applied to pallets or products right before the shipment to the customer without using the information in their own system.

- **Intermediate phase** – In this phase the company applies the RFID tag during production and uses the technology for data collection. The collected information is then shared and used for improving the company’s own supply chain processes.

- **Final phase** – In this phase, RFID is enabled in all facilities and the companies uses the information to better understand customer demand and to make better supply chain decisions and thus trying to optimize the profit across the supply chain.

Another implementation model for RFID technology is given by Hellström in, where he has made a modified version of Cooper and Zmud’s model of the information technology implementation process. Often, a more general description is given, for example: "RFID middleware controls and manages the readers, and performs filtering, aggregation, counting of tag. This model is divided into six stages. A brief description is given in Table 3.3 mentioned below:"
### 3.3 RFID Adoption Phases

<table>
<thead>
<tr>
<th>Stage</th>
<th>Activity description</th>
</tr>
</thead>
</table>
| Initiation | • Problem identification – Identify the problem and define the objective.  
               • Concept development and system design – Develop different solutions. |
| Adoption | • Cost-benefit analysis – Economically assess the system design and the different solutions made from the concept development.  
              • RFID trial – Test the technology in its working environment. |
| Adaptation | • Choose system integrator – Choose system integrator based upon software, hardware and cost requirements.  
               • Installation – Software, hardware are installed along with changing the affected business process and training the employees. |
| Acceptance | • Education and training – Inform, train and discuss the use and usefulness of the system to the employees and end-users.  
                 • Communication – Inform the involved organizations about the use and implication of the system. |
| Routinization | • Improvements – Improve the level of automation and make changes to accommodate employee’s needs.  
               • Process the collected data – Analyze and interpret the accumulated data. |
| Infusion | • Expand the implementation – Use the system for other applications.  
            • Transfer the technology – Use the knowledge attained. |

### 3.6 Standards for Contactless Smartcards

Different standards are available for RFID technology, described in more detail in the RFID handbook, operating at frequencies from 135 kHz in the LF2 range to 5.8 GHz in the UHF3 range. The relevant ones for cryptographic applications, almost
exclusively operated in the HF4 range at 13.56 MHz, are mentioned briefly. Table 3.4 shows a comparison of the standards with regard to operating frequency, approximate operating range and maximum data rate. The standard for closely coupled smartcards, namely the ISO 10536, was developed between 1992 and 1995 and never succeeded in the market, due to high manufacturing costs and only small advantages compared to contact-based cards.

The ISO 14443 standard for proximity coupling, described in Section 2, is often the choice for access control and ticketing purposes. In addition, the energy consumption of an ISO 15693 compliant tag has to be lesser, due to a lower specified magnetic field strength being necessary for operation which, combined with the low data rate, very likely makes state-of-the-art cryptography impossible.

Note that the maximum operating range, given in Table 3.4, is only achievable using the long distance mode of ISO 15693 compliant tags. The NFC5 standard has been pushed mainly by Philips and Sony, is compatible to the ISO 14443 a standard, and shall be used for short-range communication between electronic devices.

<table>
<thead>
<tr>
<th>Standard</th>
<th>Card Type</th>
<th>Range</th>
<th>Frequency</th>
<th>Data Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 10536</td>
<td>Close Coupling</td>
<td>≤ 1 cm</td>
<td>4.9152 MHz</td>
<td>9600 Bit/s</td>
</tr>
<tr>
<td>ISO 14443</td>
<td>Proximity Coupling</td>
<td>8 ... 15 cm</td>
<td>13.56 MHz</td>
<td>847.5 kBit/s</td>
</tr>
<tr>
<td>ISO 15693</td>
<td>Vicinity Coupling</td>
<td>1 ... 1.5 m</td>
<td>13.56 MHz</td>
<td>26.48 kBit/s</td>
</tr>
<tr>
<td>ISO 18092</td>
<td>Near Field Comm.</td>
<td>≈ 10 cm</td>
<td>13.56 MHz</td>
<td>424 kBit/s</td>
</tr>
</tbody>
</table>

Table 3.4: Comparison of standards for contactless smartcards
3.7 RFID Technology

Radio frequency identification regroups all the objects [85], but in this thesis, we consider exclusively passive low-cost RFID tags having the characteristics presented in Table 3.4.

![Fig 3.6: Illustration of an RFID system.](image)

A simple illustration of the concept of an RFID system is provided in Figure 3.6. Here, a transmitter of interrogation signals, which is contained within an interrogator, communicates via electromagnetic waves.
The primary cost of an RFID label, which includes both an Integrated Circuit (IC) or the silicon chip and the antenna, is the cost of the silicon chip. Low cost RFID refers to an RFID system based on inexpensive RFID tags with the smallest possible implementation of the label IC. Low cost RFID labels are passive transponders since having an on-board battery would add significantly to the cost of the label.

Figure 3.7 is an illustration of a typical low cost transponder [89]. The block diagram of an HF and a UHF chip varies little. Low cost RFID chips generally have limited memory, typically around 512 bits or less and have no computing hardware except a simple finite state machine for logical functionality [90].
Firstly, we study a hierarchical network framework composing of RFID readers, storage nodes and central control center to efficiently monitor a large-scale amusement park, and propose an RFID-based children tracking (REACT) scheme, where the tag information can be forwarded from RFID readers to the storage nodes with a pocket switched network formed by park employees and visitors who carry the wireless communication devices in the amusement park. With the REACT scheme, the location of a lost child with an attached passive RFID tag can be effectively identified in a large amusement park.

To the best of our knowledge, the proposed REACT scheme is the first RFID based solution to effectively track children in a large-scale amusement park. Secondly, to prevent a privacy-curious attacker from being able to track and/or control children in a large amusement park, the child’s privacy (in particular, identity privacy and unlinkable location privacy in the proposed REACT scheme are concealed. Even though an attacker obtains the current position of a child, it still cannot infer the past locations of the child, also known as forward security. Thirdly, we develop a custom simulator to demonstrate the effectiveness of the proposed REACT scheme.

3.7.1 Single Crystal Silicon Integrated Circuit based Tags

Until recently, RFID application specific integrated circuits have been fabricated on single crystal silicon. Although advanced technologies such as 0.13 micron, 0.15 micron or 0.16 micron have been used since 2008, 0.18 micron has been the popular process in widespread usage in low cost RFID manufacture since 2006 [91, 92]. The predominant reason for using older processes has been a strategy for constraining the cost of the RFID IC critical to supporting business cases for RFID enabled applications. Instead, older fabrication processes where the capital cost of the facilities have depreciated over at least 4 to 5 years – currently the 0.18 micron process – proves to be the most cost-effective choice for low cost RFID[93].

It is expected that this situation will eventually change and manufacturer will migrate to 0.15 micron and then eventually to 0.13 micron processes in years to come [94]. In 2005, it was estimated that no more than 2,000 gates were available for security in RFID tags [95]. Moore’s Law meant that we are able to deliver more gates per unit
area of silicon since then. However, continued end-user demands for cheaper tags to support business cases of novel RFID applications that will result in mass utilization of RFID tags imply that the several thousand gates limit is still a reality. Furthermore, newer and smaller feature size fabrication processes are not used for low cost RFID devices [96].

3.8 RFID Operation Principle

![Fig 3.8: General RFID System](image)

A minimum RFID system consists of two main components, namely a reader generating a field. A chip on the tag contains data, which may be fixed and stored in a ROM, or changeable and stored in a RAM, and furthermore must have the capability to en- and decode the information interchanged with the reader. For more sophisticated applications, microcontrollers and operating systems for comfortable access to the stored data, and cryptographic co-processors, to encipher the communication, are employed. Note, that the term RFID reader is a rather misleading description for a device that does not only receive data from the tag, but of course also transmits data to it, while often being connected to another system, e.g., a PC (Personal Computer).
3.8.1 Inductive Coupling

The wavelength $\lambda$ of an electromagnetic field is calculated following equation, where $c$ denotes the speed of light and $f$ the carrier frequency, which here is equal to 13.56 MHz, as defined in the standard.

$$\lambda = \frac{c}{f} = \frac{3 \times 10^8}{13.56 MHz} \approx 22.1 m$$

Obviously, the derived wavelength is several times greater than the typical operating distance between reader and tag, which is approximately 8-15 cm. accordingly, the field emitted from the coil of the reader may be treated as purely magnetic, leading to the term inductive coupling being used to describe the communication- and energy link between reader and tag.

3.8.2 Communication Details

According to the ISO 14443, a reader transmits data to a tag by means of switching the field temporarily off, i.e., create short gaps in the field, which are detected and decoded by the tag. The tag answers employing load modulation as described below in Section, which in turn is sensed and decoded on the side of the reader, where the reader is always the master, and the tag is the slave. The reader talks first, and then listens to the answer of the tag3, while keeping the field alive to supply it with energy.

1. Reader sends data to the tag (termed downlink)

2. Waiting time until to the answer of the tag

3. Tag answers (termed uplink)

4. Waiting time until to the next request from the reader

...proceed with 1 until finished.

3.8.2.1 Reader $\rightarrow$ Transponder

For the downlink, modified (pulsed) Miller coding is used, where the data is represented as follows.
Modified Miller Coding

The correlation between NRZ4, Miller code and the modified variant (at the bottom) is depicted in Figure 3.9.

![Fig. 3.9: (Pulsed) Miller Coding](image)

Logic 1: pause in the middle of the bit period i.e after 4.72 micron second.

Logic 0: Previously 0- Pause at the beginning of the bit period

Previsouly-1: No modulation for the full bit duration

SOC: Pause at the beginning of a bit period (equals 0 after 0)

EOC: Logic 0 followed by no modulation for full bit period

Pauses have to be created with a duration of approximately 2.5 micron second with 100% ASK.
3.8.2.2 Transponder → Reader

Load Modulation

As explained in the above Section, the energy consumed by a tag is supplied by the reader via the two transformer-like coupled coils of the RFID system. The tag transmits its data to the reader, sometimes referred to as OOK in the literature. The subcarrier of the reader’s carrier frequency is generated by the tag and used to switch the resistor, leading to the transmitted information being placed in sidebands of the carrier and making the detection of the achieved 10 mV change of useful signal at a carrier amplitude of 100 V10 possible [100].

(Modulated) Manchester Coding

For the uplink, the described load modulation is utilized to transmit Manchester encoded data, modulated with a subcarrier of $f_c = 847.5$ kHz, which shall be synchronous to the field of the reader? Figure 3.10 illustrates the generation of the modulated code. One bit duration equals eight subcarrier-periods at the data rate of $f_c = 128 = 106$ kBit/s.

- **Logic 1**: Falling edge at the centre, i.e., modulation with the subcarrier for the first half of the bit period
- **Logic 0**: Rising edge at the centre, i.e., modulation with the subcarrier for the second half of the bit period
- **SOC**: Equals logic 1
- **EOC**: No modulation for a full bit period
Manchester coding is sometimes referred to as bi-phase coding.

Note that, when Manchester coding is employed, a reader can easily detect two cards sending distinct bits simultaneously, as this leads to a modulation for a full bit period. This is of use during the anti-collision phase of the ISO 14443 protocol.

### 3.8.2.3 Initialization Phase

Collisions between two tags being in the same field, answering simultaneously to a request of a reader, and thus preventing it from acquiring valid data from any of the tags, usually don’t play a role due to the short operating range. Hence, the anti-collision part of the protocol is not explained here, and, in the following brief description of a typical communication sequence, it is assumed that only one card is present in the field of a reader. The following section shall give only an idea of the protocol – further details can be found in part 3 of the standard [101].
3.9 ECC Implementation of Authentication Protocols

In this section, we describe our hardware implementation for both authentication. We also compare results for both cases.

3.9.1 Elliptic Curve Cryptography

The main operation in any ECC-based primitive is the scalar multiplication. Point Multiplication. The point scalar multiplication is achieved by repeated point addition and doubling. We can use the basic double-and-add algorithm in both cases. In the case of Schnorr’s identification protocol, we can also use the Montgomery ladder method and benefit from the Lopez-Dahab projective coordinates. Point Addition and doubling the point addition/doubling depend on the type of projective coordinate used. Table 3.5 summarizes the number of operations required for known projective coordinates in terms of multiplications, squaring, and additions. The number of operations are assuming general operands, i.e., no particular values for Z or the curve coefficients a; b are considered.

Table: 3.5 Operation Counts for point addition and doubling

<table>
<thead>
<tr>
<th>Coordinate System</th>
<th>Addition</th>
<th>Doubling</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mult.</td>
<td>Sqr.</td>
</tr>
<tr>
<td>Jacobian projective (X/Z², Y/Z³)</td>
<td>32</td>
<td>6</td>
</tr>
<tr>
<td>Lopez-Dahab (X/Z, Y/Z) [23]</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>Modified Lopez-Dahab (X/Z, Y/Z) [36]</td>
<td>6</td>
<td>1</td>
</tr>
</tbody>
</table>
Addition of two elements
\[ c = a + b \in F_{2^n} \] is performed via an n-bit wise logical XOR operation. The standard way to compute the product \( c = a \cdot b \in F_{2^n} \cong F_2[x]/f(x) \) is:

\[ a = \sum_{j=0}^{n-1} a_j x^j, \quad b = \sum_{j=0}^{n-1} b_j x^j, \quad f = x^n + \sum_{i=0}^{s} f_i x^i, \quad s \leq n \]

is the one that uses convolution.

Here \( b = \sum_{j=0}^{n-1} b_j x^j \) rather than being considered as n coefficient of F2 is considered as being composed of \( d=\lceil n/D \rceil \) words, where each word containing D elements of F2.

### 3.9.2 ECC processor

Our Elliptic Curve Processor (ECP) for RFID is shown in Fig. 3.11. The operational blocks are as follows: a Control Unit (CU), an Arithmetic Unit (ALU), and Memory (RAM and ROM). The ECC parameters and the constants are stored in ROM.

![Fig. 3.11. ECP Architecture.](image-url)
Fig. 3.12 ALU Architecture.
3.10 Physical Unclonable Function

PUF is a function that conceived a set of battles to a set of reaction sustained on a determinedly multifaceted personal scheme; a dispute is an input to the function and an answer is the yield. The function may merely be estimated along with the physical structure, as well as is exceptional for every physical example. Whereas Physical Unclonable Function may be performed among different physical methods, this paper focuses on semiconductor PUFs that square measure stand on the hid moment and holdup info of enclosed circuits.

Even through identical explained masks, the variations within the mechanized procedure reason important impediment dissimilarity among various ICs. As a result of chemical element PUFs faucet into the random variation that happens throughout and the integrated circuits production development, the secret(s) are inherent to the semiconducting material itself, area unit tremendously sophisticated to predict or -program‖ ahead of manufacture, and area unit basically non-replicable from chip to chip. First, PUFs significantly enhance physical security through making unbalanced secrets that just survive in a very digital kind whenever a fraction is steam-powered on with running.

That represents associate degree opponent, slightly than solely examining associate degree integrated circuits memory to interpret its accumulate secret, instead would needed to mount associate degree attack whereas the chip area unit running and applying the key -- a significantly sophisticated proposal than deciding non-volatile keys. As a result of chemical element PUFs faucet into the random variation that happens throughout and the integrated circuits production development, the secret(s) are inherent to the semiconducting material itself. Associate degree close physical attack would need to precisely measuring Physical Unclonable Function holdup with no altering the delays or else find out unstable keys in recorded devoid of wounding power or tripping tamper-sensitive electronic equipment that clears out the registers. Second, even the IC manufacturer cannot clone a PUF-enabled IC.
That’s reason area unit the random a part of developed difference may not be forbidden or programmed in some conservative sense through the producer- it’s accepted to the procedure itself. Finally, PUFs conjointly change key provisioning (which is important with crypto-chips) as a result of makers doesn’t got to program the IC with secrets.

Figure 3.13 illustrates a Si PUF delay circuit supported MUXes associated with an arbiter. The circuits have a multiple-bit contribution X and calculate a one-bit outcome Y supported the relative dissimilarity among 2 paths as well as the similar explained length. The entered bits established the holdup methods by scheming the MUXes. Here, a combination of MUXes controlled by a similar input bit X[i] work as a shift box (dotted boxes within the figure). The MUXes submit to the 2 delay signals from the left aspect if the input management bit X[i] is zero.

Otherwise, the highest and bottom signals square measure switched. during this method, the circuit will produce a combine of delay methods for every input X toward calculable the output used for a exacting input increasing sign are agreed to mutually ways at identical time, the indication race throughout the two holdup ways, moreover because the arbiter (latch) at the tip decides that indication is faster. The generated output can behave as a condition indicator so as to latch data input (D) in much efficient way, and zero otherwise.

Fig: 3.13 an arbiter PUF delays circuit.
There are two ways in which to construct a k-bit response from the 1-bit output of this PUF delay circuit. First, one circuit may be used k times with completely different inputs. Then, the PUF delay circuit is evaluated k times; mistreatment k completely different bit vectors from the pseudo-random range generator serving because the input X to assemble the delay ways.

It is conjointly attainable to duplicate the single-output PUF circuit multiple times to get k bits with one analysis. PUF responses will either be directly accustomed attest a tool or will function a secret key for crypto-logic operations like secret writing and digital signatures to reinforce security on the far side authentication.

This paper solely focuses on the authentication with minimally-sized circuits in RFIDs, rather than authentication that depends on pricy crypto-logic operations. For straightforward authentication, a booster saves indiscriminately elite challenge-response-pairs (CRPs) from a tool once the device is thought to be authentic, and later checks a response within the field to attest the device.

To interrupt the PUF-based authentication theme while not having the ability to make 2 identical PUFs, attackers could try and construct an exact temporal arrangement model and learn the parameters for a selected PUF from several challenge response pairs equivalent to that PUF. To handle this, we have a tendency to use a PUF circuit specifically designed to scramble its output that thwarts such model building attacks.

### 3.11 UF-Enabled Unclonable RFID

While traditional Radio Frequency Identifier technologies are restrictions in this employ as a accurate anti-counterfeiting determine, this is still has been an approximately perfect technology to converse to "things." in contrast to different solutions, like special printing, holograms, tamper-evident seals etc, RFID doesn't need manual intervention; it needn't block the provision chain outturn, and might leverage cost-reduction curves and scale economies related to ICs and electronic elements in common.
A significant constituent that are absent could be a ascendible, efficient methodology to stop biological research. A Radio Frequency Identifier tag that is an undisclosed that may not be unoriginal would enable single to instantly distinguish a imitation tag from the important one. Such a RFID tag would match the wants for hymenopterans counterfeiting. Currently if this PUF-equipped IC is AN RFID chip, the PUF would mean that such AN RFID chip would have its own exclusive secrets (corresponding to AN exponential range of challenge-response-pairs), derived beginning the semiconducting material itself. In addition to those secrets could be:

Essentially not possible to predict or – control‖ earlier of manufacture.

Essentially unacceptable to repeat instead clone from one chip toward the afterward.

Therefore, the PUF will add a secure authentication feature to associate degree RFID if it may be incorporated into associate degree RFID effectively (with lowest further semiconducting material space and power utilization).

Fig.3.14 PUF-based RFID authentication mechanism
The above figure 3.14 illustrates the PUF-based authentication method for anti-counterfeiting. In our approach, each RFID comprises a selected, possibly exclusive, fixed-length identifier such as an EPC code in non-volatile memory for identification. While PUF answers can furthermore be utilized as an identifier given that they are unique for each IC (provided they are long enough), we select to have a distinct accepted identifier so that the PUF-enabled RFID can furthermore be utilized for customary track-and-trace applications and to endow accepted database lookups.

For protected authentication, the RFID contains a PUF circuit and exploits the reality that the Physical Unclonable Function may contain an exponential digit of challenge-reaction couple where the reply will exclusive for every IC and all challenge. Regard as the verification procedure exposed in Figure 3.14.

A confidence party such as a invention seller, when in control of an genuine Radio Frequency Identifier with an genuine product, concern arbitrarily selected challenges to get random reply. The faithfully party provisions these challenge-response couple during a info supposed for future verification method. This info can index through the (unique) symbol typically connected with every Radio Frequency Identifier or creation, for instance, an EPC code which will store up in non-volatile recollection memory on the frequency symbol. the popularity of the frequency symbol and manufacture is predicated on the conservative symbol.

To verify the credibility of RFID and therefore the associated product later within the field, the trust party selects a confront that can be earlier evidenced but have never been utilized for a verification ensure operation, and finds the PUF reply from the Radio Frequency Identifier. If the reply is matching, the sooner recorded one, the frequency symbol are real as a result of just the real IC and therefore the dependably party can acknowledge that challenge-response pair. To defend against man-in-the-center assault, confronts are never use again. For that reason, the challenges and reply may be sending in the obvious above the network through verification operations.
Note down so as to the challenge-response record are going to be rested with latest challenge-response-pairs to boost the digit of verification measures. We intended and made-up Radio Frequency Identifier ICs along with the element PUF route supported MUXes ANd an authority. Our PUF allow Radio Frequency Identifier IC function at 13.56 MHz with is predicated on the ISO-14443 kind a demand. This reflexive Radio Frequency Identifier IC controllers presently similar to a usual Radio Frequency Identifier IC for store up a exclusive identifier; the PUF track can be stimulate for verification. The same PUF circuit is employed again and again for a given 64-bit challenge to provide a 64-bit or longer response. to permit AN RFID reader to access the PUF, our RFID tags support a brand new command: challenge. As well, the getable browse and WRITE directions in Radio Frequency Identifier will be utilize as the PUF commands.

On a challenge command, the tag accepts a 64-bit challenge from the reader and sends a response for the given challenge back to the reader. A WRITE into a particular address is known just like the confront command, with a browse from a particular address retrieves the PUF response. Figure 3.15 shows the ground arranges of the PUF-enabled PUF, that implements the ISO-14443A commonplace with a full anti-collision protocol. As shown within the figure, the bulk of the chemical element space is consumed by commonplace RFID parts like the RF front-end, OTP memory, digital logic to implement varied commands.

The PUF element has been enforced in but zero.02mm2 in our initial chip that is designed in zero.18μ fabrication technology. The PUF consumes dynamic power solely throughout analysis – once it generates the response. Outside of analysis, that is most of the time, solely ancient CMOS run currents square measure gift. The facility needed throughout analysis is little compared to the facility keep in a very typical RFID device such the VDD drop is insignificant.

Although PUF technology and its RFID commands area unit able to be incorporated into frequencies symbol that management at extra frequencies. For instance, an equivalent PUF module is employed in passive radio frequency tags. We tend to solely use a HF tag as a vehicle to demonstrate that PUF technology allows robust
authentication even in low-priced, low-power passive RFID tags there's no distinction between HF and radio frequency tags from the PUF authentication perspective.

Fig 3.15 Basic architecture of a PUF-enabled RFID.
3.12 PUF-Enabled Unclonable RFID Applications

The advantages over basic passive RFIDs with easy identifiers or secure RFIDs supported typical cryptanalytic operations:

- **Highly Secure:** The Radio Frequency Identifier fragment itself will not be duplicated. The replied to confront has been made energetically, and be unstable. Unstable information can be more difficult to extort other than non-volatile information. Through almost infinite statistics of challenge-response pair off obtainable, every pair be able to be used merely one time. This fundamentally serve up as a once protection. A play again assault can be not passing as the challenger will not forecast the confront and reply that is to be used for the next verification.

- **Low Cost, Low Power Consumption:** PUF circuits have a moderately insubstantial adding to the Radio Frequency Identifier chip. The first completion of an essential 64 step PUF circuit with a linear feedback register (LRSR) superimposed but zero.02mm2 within the zero.18μ technology and consumes few extra powers. Chip dimension, charge and power utilization has key marketplace reception parameter for frequency symbol. PUF primarily based RFID improve the flexibility of essential Radio Frequency Identifier in the mainly rate efficient mode, even intended for thing phase utilization.

- **Simple, Robust Authentication:** PUFs give sturdy authentication of AN RFID tag in contrast to ancient tags that may be simply cloned. So, it has been tag produce will be genuine at every end-point of a offer chain (or anyplace in between) in merely compare to the reply produced through a verification occasion through the reaction recorded at the protected locality. As well, PUF confront reaction pairs will be produced and stock up by multiple freelance parties that don't share data.

PUF based mostly Unclonable RFIDs offer easy and strong anti-counterfeiting mechanism compared to item level pedigree, as planned in pharmaceutical business. Ever since the PUF frequency symbol chips won't be duplicated, an easy verification by multiple freelance parties that don't share data. PUF based mostly Unclonable RFIDs offer straightforward and sturdy anti-counterfeiting mechanism compared to item level pedigree, as planned in pharmaceutical business. Ever since the PUF
oftenest symbol chips won't be at the location make sure simply a true turn out is commercialism to the emptor.

This could even be achieved while not publication (providing distinctive serial # to every marketable unit), by exploitation the PUF RFID tag symbol and PUF authentication. Whereas this straightforward PUF authentication doesn't determine the weak link within the offer chain, wherever a compromise might need been created, it sure guarantee simply a true invention is sell to the patron. PUF RFIDs don't forestall building a fancy e-pedigree; however will definitely be the primary step in making certain client safety. in addition, PUF authentication could be a lot of quicker operation compared to e-pedigree, which may be of significance once responding to pandemics and alternative imperative things.

The short value and energy expenditure of PUF based mostly Radio Frequency Identifier creates them appropriate for item level use, a big advantage over scientific discipline techniques. For scientific discipline approaches, important investment must be created to firmly store secrets within the chips, and in advanced infrastructure (hardware and software) to try to authenticate. PUF primarily don't store any secrets, and don't want advanced infrastructure for authentication.