The University of Adelaide

AUTO–ID LABS

Security in Low Cost RFID

Damith C. Ranasinghe and Peter H. Cole

Auto-ID Labs White Paper WP-HARDWARE-027

Mr. Damith C. Ranasinghe
PhD Student, Auto-ID Lab, ADELAIDE
School of Electrical and Electronics Engineering,
The University of Adelaide

Prof. Peter H. Cole
Research Director, Auto-ID Lab, ADELAIDE
School of Electrical and Electronics Engineering,
The University of Adelaide

Contact:

E-Mail: damith@eleceng.adelaide.edu.au or cole@eleceng.adelaide.edu.au.

Internet: www.autoidlabs.org

Hardware

Abstract

RFID systems, and indeed other forms of wireless technology, are now a pervasive form of computing. In the context of security and privacy, the most threatening (to privacy) and vulnerable (to insecurity) are the 'low cost RFID systems'. The problems are further aggravated by the fact that it is this form of RFID that is set to proliferate through various consumer goods supply chains throughout the world. This is occurring through the actions of multinational companies like Wal-Mart, Tesco, Metro UPS and of powerful government organizations such as the United States DOD (department of defence) and FDA (food and drug administration). This paper examines the security and privacy issues brought about by vulnerabilities of present low cost RFID systems and explore the security and privacy threats posed as a result of those vulnerabilities.

The paper will also outlines a set of objectives for mitigating such vulnerabilities and consider the challenges faced in discovering solutions to such problems. Then the paper is concluded with a survey of available solutions for addressing various security and privacy issues of low cost RFID.

1. Introduction

One of the inhibitors to wide-scale adoption of RFID technology is the cost of a label. Thus low cost RFID refers to a RFID system based on inexpensive RFID tags. It is imperative to reduce the cost of RFID labels if RFID technology is to gain any significant market penetration. For example, the current cost of a gate of silicon logic is about one thousandth of a cent [1 and 2]. Thus, a company producing 100 billion units of a product per year would loose $1 million in profits due to the addition of a single logic gate to a label. For reasons such as this, there is a great deal of focus placed on low cost RFID.

The proposed Class I and Class II labels by EPCglobal [3] represent the low cost end of RFID labels. These RFID labels are passive transponders. Labels in the category of passive systems the most common operating principle is that of RF backscatter or load modulation [4 and 5] in which a powering signal or communication carrier supplies power or command signals via an HF or UHF link. However the circuits within the label operate at the carrier frequency or at a lower frequency, and reply via sidebands generated by modulation, within the label, or by modulation of a portion of the powering carrier. This approach combines the benefits of relatively good propagation of signals at HF and UHF and the low power operation of microcircuits at RF or lower. Powering at UHF is employed when a longer interrogation range (several meters) is required, and HF powering is employed when electromagnetic fields, which exhibit good material penetration and sharp spatial field confinement is required, or sometimes when a very low cost RFID system implementation is desired.

2. Characteristics of a Low Cost RFID System

The most dominant form of low cost RFID technology set to spread through out the consumer goods supply chain is that advocated by EPCgloabal as Class I and Class II. The proposed Class I and Class II labels represent the low cost end of RFID labels. The low cost RFID labels involving Class I and Class II labels are based on passive RFID technology as will be discussed in Section 2.2. Due to their potential for prolific use in the future most discussions regarding low cost RFID inevitably consider various aspects of such labels. The following sections provide an overview of low cost label manufacturing costs and IC components in an RFID label and focus on describing low cost RFID systems based around Class I and Class II labels.

2.1. A Low Cost Tag

Current fabrications of Class I labels consist of around 1000 to 4000 logic gates [1 and 2] while Class II labels may have several thousand more gates. An RFID microcircuit can be subdivided into three primary sections: RF front-end, Memory circuitry, and Finite State machine (label logic circuitry). Fig. 1 is an illustration of a typical low cost RFID transponder (that is a passive label). The block diagram of a HF chip and a UHF varies little in that the primary difference being the way in which the local oscillator clock is derived. In a UHF chip there is a dedicated low power oscillator, while in a HF chip the clock signal is derived from the received carrier by dividing down the carrier (at 13.56 MHz) in steps.

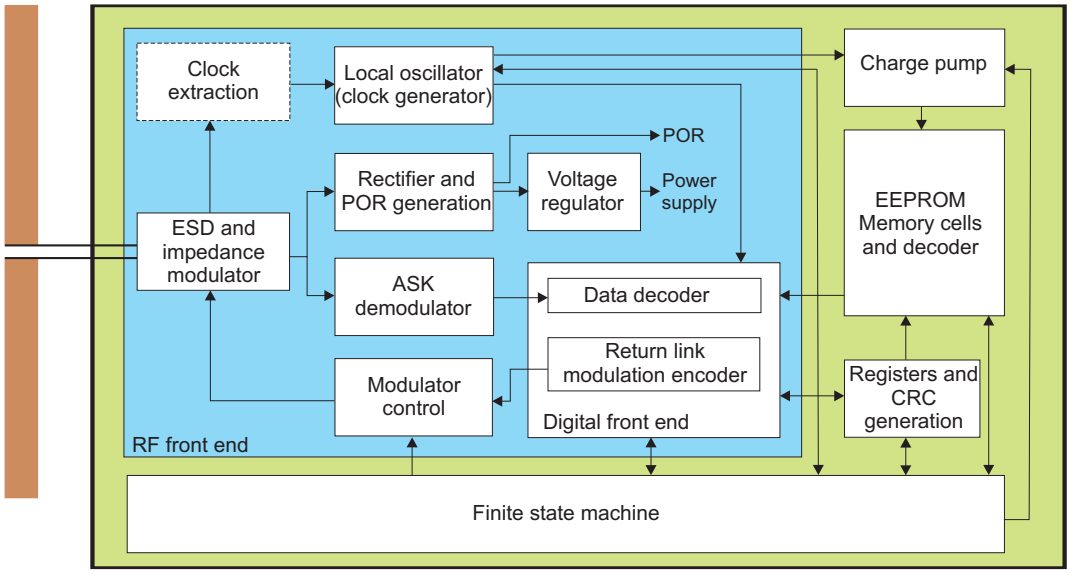

Fig. 1: Block diagram of a passive UHF/HF RFID label.

2.1.1. RF Front-end

RF front-end consists of antenna pads for attaching the terminal of the antenna to the label IC. The antenna input passes through circuits for ESD (electrostatic discharge) protection. The ASK (Amplitude Shift Keying) demodulation circuits extract the modulation dips from the received signal while the Rectifier, rectifies the received signal to generate power which must be regulated using a voltage regulator to avoid voltage surges due to variations in RF field intensities.

Passive RFID chips consist of a relatively large capacitor following a rectifier for storing charge to power the circuit in the absence of a battery. It is important to note here that the capacitor occupies a relatively large portion of the silicon area and RFID chips consuming larger amounts of power will need higher capacity capacitors and thus will cost more.

2.1.2. Memory Circuitry

Low cost tags have limited memory that is either write once or a read write memory. Class 1 labels have only read only memory while class II labels may have some read-write memory. Read write memory, at the time of writing is implemented using EEPROM and thus requires a large voltage before information can be written to memory. Thus a charge pump, consisting of a series of capacitors, is required to achieve a voltage of about 17V for writing to the tag's memory.

The CRC circuits are used in validating the CRC in the received data and commands from an interrogator. The CRC generation unit is also used in the computation of the CRC for data sent from the tag to an interrogator before being encoded for modulation by the Return link modulation encoder.

In the implementation of an EPC tag the EEPROM will store the EPC number of the tag, and the rest of the memory (generally of the order of a few kilobytes) is available to the users. A tags memory resources account for a significant portion of the tag cost.

2.1.3. Finite State Machine (Logic Circuitry)

The logic on board the chip will define the label functionality. Primarily, chip logic will execute reader commands and implement an anti-collision scheme that allows the reading of multiple labels by a reader. These logic circuits are highly specialised and optimised for their tasks.

Furthermore, the logic circuits also control read and write access to the EEPROM memory circuits.

The block diagram of a low cost RFID tag is given in Fig. 1 along with a description of the various functionalities of the tag components. The following Sections provides quantitative characteristics of low cost RFID systems and reasonable assumptions that needs to be taken into consideration when solutions for security and privacy issues are developed.

Computation capability of a low cost tag is limited to a state machine with hard wired logic functionality. The only arithmetic operation performed by current low cost RFID tags is the calculation of a CRC for checking errors in received data and the computation of a CRC prior to transmitting data. Thus for a low cost tag any additional hardware required to implement security needs to be designed and fabricated incurring additional cost.

2.2. Tag Cost

Generally tag cost is based on evaluating the area of silicon needed for a physical implementation, while this includes the analogue front end of the tag, reduction in costs have been achieved through the miniaturization of digital functional blocks and not through devices such as capacitors, inductors or resistors. Hence keeping tag costs low requires focusing on limiting the number of gates on a tag even though the bulk of the tag cost is associated with the analogue components whose costs are difficult to reduce due the nature of passive components.

2.2.1. Manufacturing Costs

There are a number of key stages involved in the manufacture of RFID labels after the design of the IC. An outline of the stages is given in Fig. 2 below. Today, the cheapest RFID labels are passive and cost around 5 US cents in large quantities [7]. Presently RFID read only chips have design sizes ranging from 0.16mm^2 [8] to 0.25mm^2 [9] IC foot prints.

Further improvements to IC manufacturing processes will bring the cost of microcircuits even lower. This invariably involves producing more microcircuits per silicon wafer. However, reducing die sizes to very small levels can incur added costs due to the increase in cost of handling smaller die.

A more practical avenue for reducing costs is the use of obsolete IC manufacturing processes and filling up such fabrication pipelines with RFID IC chips. This is a worth while consideration as people migrate to smaller and smaller micron processes and larger, highly tuned micron processes such as 0.5 micron become available at fraction of the cost as a result of depreciated fabrication equipment and the availability of smaller processes. This will reduce the cost of the IC component of the chip considerably. The older processes have the added advantage of having few or no reliability concerns while being able to provide stable yields.

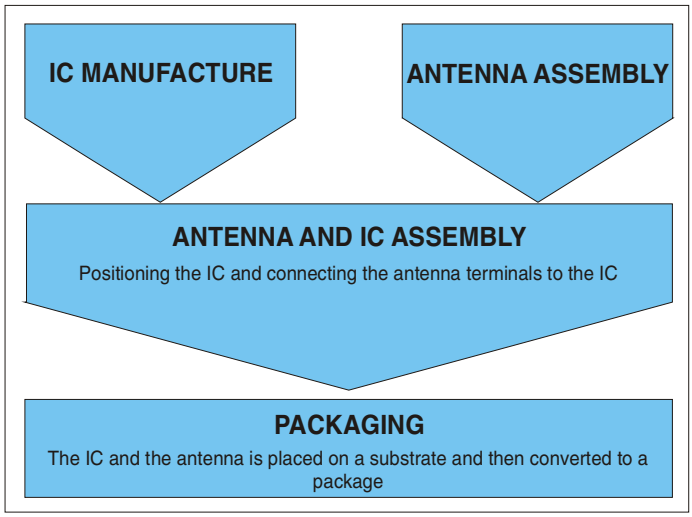

Fig. 2: RFID Label Manufacture.

2.2.2. Tag Power Consumption

A tag's power consumption will vary depending on whether the tag is just being interrogated or whether the tag is required to perform a write operation. Tag power consumption is also influenced by other factors such as the data transmission rate, the feature size of the fabrication process used, as well as the effort spent in designing low power CMOS circuitry. A tag performing a read operation will require about 5 µW – 10 µW, while a tag attempting to perform a write operation to its E^2PROM will require about 50 µW or more.

2.2.3. Physical Protection (Tamper Proof)

Low cost tags do not utilize anti-tampering technology due to cost constraints and hence the contents of a labels memory or the layout of logic circuits are not protected from physical access. Hence the long-term security of label contents cannot be guaranteed.

2.2.4. Standards

There are a variety of standards encompassing all aspects of RFID systems. The ISO 18000 is a multi-part standard that defines the air interface standard of a number of different frequencies from LF, HF to UHF. However for UHF tags the most prevalent standard is that ratified by EPCglobal, called the Class I Generation II air interface protocol [6].

Accordingly, the labels within reading range have a means of revealing their presence, but not their data, when interrogated by a reader. The labels then reply with a non-identifying signal to an interrogation by using a randomly generated number as described in C1G2 air interface protocol [6].

However for HF tags there is no such prevalent standard though EPCglobal is currently developing a HF specification to complement its UHF air interface protocol. The existing standards most commonly in use for HF tags, other than the ISO 18000 are listed below.

- ISO 14443 (types A and B). Devices operating under this standard are proximity RFID devices with reading range of few centimetres,
- ISO 15693 is a recent addition for “vicinity card” RFID devices, where the operating range of the devices can be close to 1 meter (The operating mode I of ISO part 3 specification is based on ISO 15693).

2.2.5. System Operational Requirements

RFID systems are required to meet various minimum performance criteria to justify its benefits to the end used community. Two such important and related performance parameters are the number of label reads per second and data transmission speeds. Performance criteria of an RFID system demand a minimum label reading speed of 100-200 labels per second. In accordance with C1G2 protocol, a maximum tag to reader data transmission rate bound of 640 kbps and a reader to tag data transmission rate bound of 126 kbps based on equiprobable binary ones and zeros in the transmission can calculated.

2.2.6. Communication Range

Considering the current electromagnetic compatibility (EMC) regulations, the operating range of low cost labels is limited to a few meters for those operating in the UHF spectrum and few centimetre for those operating under the FCC regulations for the HF spectrum [69] (HF systems operating under current European regulations for the HF spectrum can have a operating range well in excess of 1 meter as discussed in Section 2.2.7).

2.2.7. Frequency of Operation and Regulations

An important consideration affecting all EM related issues, especially the powering of RFID labels, are the regulations that govern the operating frequency, power, and bandwidth in different regions of the world. There are a number of regulatory organisations and different EMC regulations around the world. Australian regulators are likely to follow the footsteps of

their US counterparts; hence, treatment given here for EMC regulations will not focus on Australian regulations. It is important to note here that the EMC regulations are enforced in the far field.

Most RFID systems operate in the Industrial, Scientific and Medical (ISM) bands designated by the ITU [70]. The ISM radio bands were originally reserved internationally for non-commercial use of RF electromagnetic fields for industrial, scientific and medical purposes. The most commonly used HF ISM band in Europe and America is centred at 13.56 MHz and the UHF band in the US is 902-928 MHz [71].

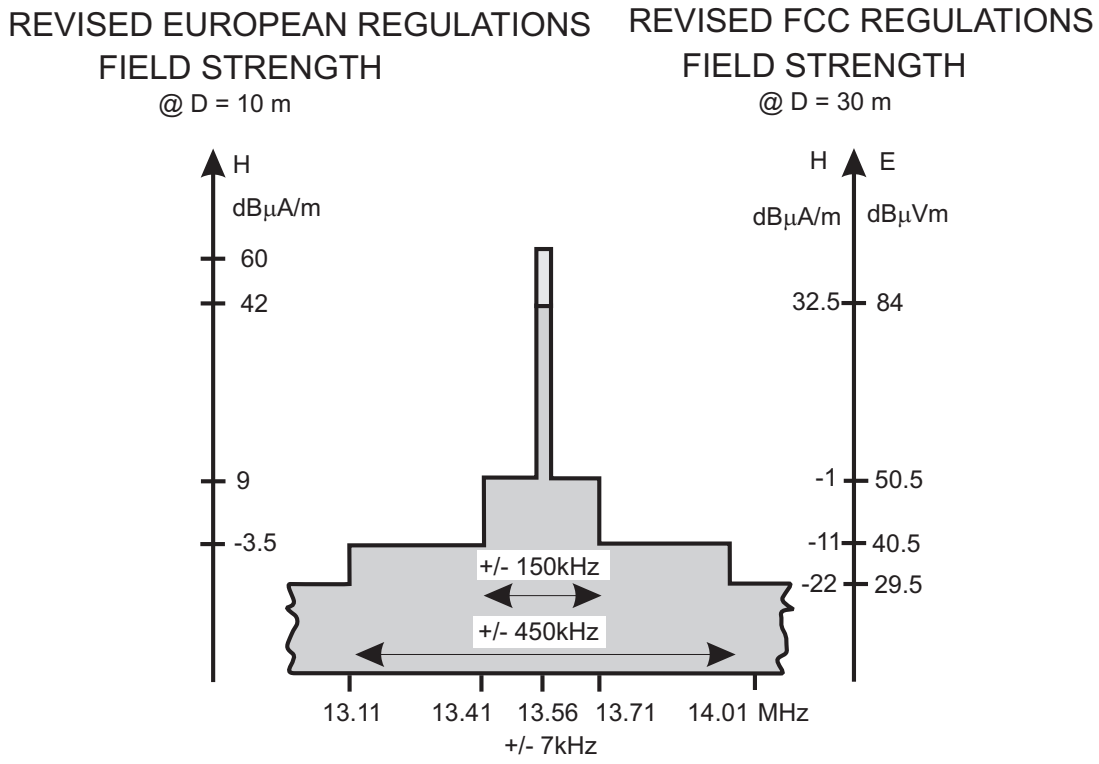

Fig. 3: HF electromagnetic compatibility regulations.

Fig. 3 shows the revised European regulations at 13.56MHz and the revised FCC regulations [71, 72]. FCC regulations for the HF spectrum allow only minimal 5 mW radiation when using an antenna of gain 1.76dBi. Hence devices operating under these regulations only have very small reading rage in the order of a few centimetres. However European regulations depicted in Fig. 3 allow radiating 320 mW of power with an antenna gain of 1.76 dBi. Using larger interrogator antennas and large label antennas have shown that reading ranges under European regulations [72] can be increased to approach the mid field distance (that is around the 3 meter range).

Near and far fields scale differently with distance, and in particular, the near field energy density per unit volume decreases as the inverse sixth power of distance from the antenna [73 and 74]. The result is that close to the antenna, substantial energy densities may be obtained, but these diminish very quickly as distance increases. The limits on the radiated power generally ensures that the previously mentioned inverse sixth power of the reactive

power density sufficiently reduce the label energising signal to a level below an acceptable level for practical operation before the boundary of the far field. Thus under current regulations operation of HF systems is almost entirely confined to the near field and short distances. On the contrary, at UHF frequencies, the boundary between the near field and the far field is in the vicinity of the antenna; thus, the operation of UHF systems is almost entirely in the far field region.

Each frequency band provides its own set of advantages and disadvantages. The 13.56 MHz band has a 14 KHz bandwidth. This places a limitation on the bandwidth of the reader to label communication since the central portion of the spectrum shown in Figure 3.2 regulates the operation of RFID equipment in the HF region.

The 902-928 MHz band, under US regulations, allows multiple reader to label communication choices with much higher communication bandwidths and hence data rates. The regulations allowing the longest communication range require the reader to change its communication frequency every 400 milliseconds. . The reader may hop between any numbers of channels however the maximum bandwidth of a channel cannot exceed 500 kHz [43]. The technique is referred to as frequency hopping. Table 1 below highlights the range of frequencies in use in the UHF region around the world.

Table 1: UHF RFID frequency allocations.

Region	Frequency range (MHz)	Bandwidth (MHz)
Europe	865 - 868	3
USA	902 - 928	26
Japan	952 - 954	2

2.2.8. Security Provided by Class I and Class II labels

The most dominant form of low cost RFID technology set to spread through out the consumer goods supply chain is that advocated by EPCgloabal as Class I and Class II. The low cost RFID labels involving Class I and Class II labels are based on passive RFID technology. Due to their potential for prolific use in the future most discussions regarding low cost RFID inevitably consider various aspects of such labels.

Lead by EPCglobal, the RFID community in its efforts towards standardization, has produced a list of end user requirements for Class I and II labels that has flawed into the current C1G2 protocol standards and outlined in the following sections. One aim of that list has been to address the privacy and security risks posed by RFID Class I and Class II labels containing an EPC. The security requirements are an appropriate guideline for considering the level of security and privacy that can be expected and required from Class I and Class II RFID

labels. The following is an outline of the security features that can be expected from previously mentioned classes of labels.

2.2.8.1. Security Features of Class I Generation 2 UHF Labels

The characteristics Class I labels have been identified in Section 2, have only a read only or a write-once memory and are incapable of participating in a complex security mechanism. Hence Class I labels are required to provide “Kill” capability and a password to control access to the kill command, so that consumers have the choice of completely disabling an RFID label at the time an RFID labelled item is purchased.

“Killing” a label involves the destruction of the label thus rendering it inoperable [6] by perhaps setting off a fuse or disconnecting the antenna. Unfortunately the destruction of the label denies the user of the profuse benefits that could have been obtained from a “smart object”. As a solution an alternative idea to killing entertained previously involved the removal of the unique serial number of the EPC code in articles that allows the label owners to be tracked albeit in practice with difficulty. This does not remove all the privacy concerns, as tracking is still possible by associating a “constellation” of a label group with an individual. This implies that a particular taste in clothes and shoes may allow an individual’s location privacy or anonymity to be violated. However “killing” a label will eliminate privacy concerns and prevent access by unauthorised readers when combined with a password to control access to the kill command.

While throttling is not specified as part of the C1G2 standard, it is reasonable to assume the employment of a delay based throttling mechanisms on tags to prevent the guessing of kill or access passwords [75]. The concept behind delay based throttling is that on the occasions a tag is given an invalid password, the tag enters a sleep state where it will not accept another kill attempt for a specified amount of time. This method can significantly increase the time required by an attacker attempting to kill a tag, and in a situation such as a retail environment the time factor can be an adequate deterrent to such brute force attacks.

Class I labels should also have the ability to lock EPC data so as to provide one-time, permanent lock of EPC data on the label, so that EPC data cannot be changed by an unauthorised interrogator once it has been written. Interrogators are also prevented from transmitting complete EPC data except when data needs to be written to an RFID label so that the EPC information may not be eavesdropped upon from a distance without being discovered.

2.2.8.2. Security Features Expected from Class II labels

Other requirements were identified as necessary for higher class labels since these labels will have greater functionality and thus more hardware. Higher class labels are required to provide a secure forward link for communication with an RFID label while providing access control to label functionalities.

2.3. Backend System Services: Track and Trace Capability

RFID labels are given a unique identification number, for Class I and Class II labels, the unique identifier is an EPC. Using information technology services offered by backend systems such as the EPC Network services it is possible to dynamically generate a profile of the RFID label to create an electronic history of the label as it passes though various stages of the supply chain. The electronic history called an electronic pedigree can serve to thwart cloning attacks.

3. Vulnerabilities of Low Cost RFID Systems

While lows cost RFID technology described in Section 2 can bring many security benefits, current low cost RFID systems generate significant security risks, mainly due to their cost constrained implementations and the insecure channel over which readers and tags communicate. The security risks that arise as a result are due to a number of reasons outlined below.

- Communication between a tag and a reader takes place over an insecure channel
- Tags are readable by any reader implementing the air interface protocol
- Tags IC designs are constrained by costs
- Tags are not tamper proof
- Air Interface protocol to reduce tag complexity
- Design flaws in reader implementations due to cost constraints

The Sections below discuss various vulnerabilities that arise as a result of the reasons listed above.

3.1. Eavesdropping and Scanning

Transmissions from a reader and a tag takes place over a clear communication channel which may be observed by a third party. Low cost labels with minimum functionality are only able to identify themselves by transmitting a unique identifier, and these labels can be read by any reader adhering to the air interface protocol used by a RFID tag. Hence a third party may monitor a conversation between a label and a reader to obtain sensitive information. Illicitly obtained information in this manner may be used to create fraudulent labels, unauthorised readers, or used to discover secret information stored on labels (such as a tag password).

Similarly, competitors of an organization (such as a rival supermarket) may over time scan another organizations inventory labelled with RFID labels or eavesdrop on the organization's own valid operations to obtain valuable information, such as sales data, to ascertain the performance of its competitors (an act commonly referred to as corporate espionage) [12]. Publications such as [13] have attempted to define various eavesdropping ranges based on the reading ranges of tags. Similar descriptions of the eavesdropping distances possible are stated below so that vulnerabilities of eavesdropping can be better understood. However, it should be stated here that while it is useful to define terms to explain ideas the fact that a third party can eavesdrop on a conversation between a tag and reader from whatever the distance still remains a fundamental vulnerability.

Considering the possible distances at which a third party can listen to a conversation allows the following general ideas of a tag and an adversary's behaviour to be categorised. Fig. 1 gives an illustration of the latter distinctions discussed and explained below.

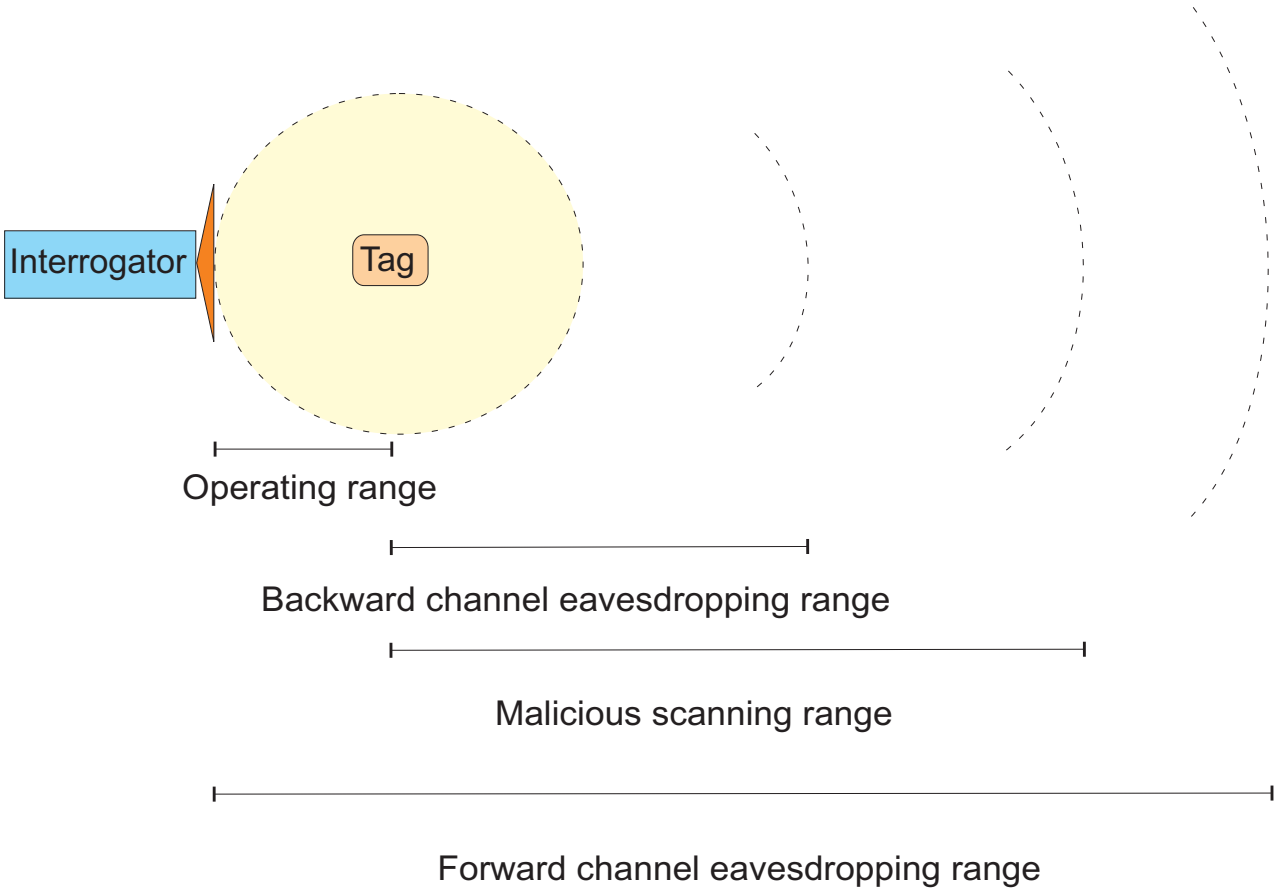

Fig. 1: Tag reading range classification.

3.1.1.1. Operating range

Tag operating range is either defined by product specification based on user requirements or it may be based on a certain standard. The operation range of a tag will also be application dependent as tag reading distances are affected by various environmental factors. The operating range of tags is then the maximum distance at which any given tag will read to a given reliability when illuminated by a reader operating under the electromagnetic compatibility regulations of that region for a particular frequency band of operation.

3.1.1.2. Backward channel eavesdropping range

The backward channel refers to the communications sent from a tag to a reader. In a low cost system, where the tags are passive this reply is weaker in signal strength than a reader

transmission as it is achieved by reflecting some of the incident RF energy at the label antenna.

The backward channel range is generally much greater than the operating range of the tag since a third party is capable of using a narrow beam antenna, with an RF receiver of higher sensitivity and because the third party does not have to use the same antenna for powering and receiving (unlike most low cost systems which use a monostotic antenna configuration, that is a single antenna for powering, transmitting and receiving).

3.1.1.3. Forward channel eavesdropping range

The forward channel refers to the transmissions from a reader to a tag, and the forward channel eavesdropping range is the distance at which a third party with a high gain antenna and a highly sensitive RF receiver can correctly record a tag transmission.

3.1.1.4. Malicious scanning range

This read range is derived by considering an adversary with no regard for electromagnetic compliance or standards and whose only intention is to either power and read the tag at any cost or to eavesdrop on a conversation between a tag and a reader at any cost. Combined with the prospect of a highly sensitive RF receiver, a narrow beam antenna and the willingness to break electromagnetic regulations, malicious scanning rage will have reading distances in excess of that possible for backward channel eavesdropping.

There are generally two forms of eavesdropping possible with low cost RFID systems; passive eavesdropping and scanning (active eavesdropping). The following Section will discuss the previously mentioned forms in an RFID context.

3.1.2. Passive eavesdropping

As the names suggest, passive eavesdropping relates to the observation and or recording of communication between a reader and a tag by an unintended recipient. Passive eavesdropping may be performed by a third party in either the operating range, backward channel eavesdropping range or the forward channel eaves dropping range.

3.1.3. Scanning (Active eavesdropping)

In this situation a third party or an adversary is actively attempting to read the contents of a tag without the authority of the tag owner. In a scanning scenario with respect to a low cost RFID system an adversary is using a rogue reader to power the tag and communicate with the tag without raising the suspicions of a tag owner. An active eavesdropper will have a working range within the malicious scanning range outlined in Fig. 1.

3.2. Cloning

Devices designed to impersonate tags or readers (imitating the behaviour of a genuine label or a reader) present a serious threat to an RFID system. Impersonation will add a new dimension to thieving as attackers are able to write EPC data onto devices that function like RFID tags. A direct consequence of cloning is the possibility for counterfeiting, where a genuine article tagged with an RFID label, may be reproduced as a cheap counterfeit and tagged with a clone of the authentic RFID label. The 'track and trace' concept outlined in [14] is one possible solution to cloning in a supply chain application.

At the time of writing there is no mechanism for a reader to verify that it is communicating with a genuine RFID label and not a fraudulent label. Thus a thief may replace a tag of a valid item with a fake tag or replace the tag of an expensive item with that of a fake tag with data obtained from a cheaper item. Hence the lack of a means for authentication allows an adversary to fool a security system into perceiving that the item is still present or this may fool automated checkout counters into charging for a cheaper item. Such fake labels may also be used to create imitation items. There is presently no mechanism for a reader to authenticate itself to a label or a label to authenticate itself to a reader. Thus labels and readers are constantly in an un-trusted environment where the integrity of messages is doubtful and there are no means for establishing the legitimacy of a reader by a label or the legitimacy of a reader by a label.

Clearly more expensive RFID system implementations are also not immune from cloning as shown by a more recent cloning attack published in [15] where a cloned tag was used in the purchase of fuel at a service station and to start an automobile locked with a RFID based car immobiliser. A similar example of cloning of proximity cards is given in [16] while the possibility of cloning the VeriChip [17] in a discussion of its possible use to tag employees was outlined in [18].

The EPC Class I tags have no mechanism for preventing cloning as the tags are simple bit storage devices that transmit a string on bits on request from any valid reader. All an adversary has to do is to scan a tag and copy its EPC number to another tag or another device that is capable of impersonating a tag.

3.3. Man-in-the-Middle

An RFID system is constantly under threat from man-in-the-middle attacks resulting from eavesdropping on reader and tag transmissions. A third party may monitor a conversation between a label and a reader, record that conversation and use parts of the conversation or alter parts of a conversation and retransmit messages to illicitly obtain information from RFID devices or to command RFID devices to the detriment of the system.

Retransmission of such recorded information may be used to query RFID labels or fool RFID readers. Such an attack has the ability to fool RFID systems based personal access control systems and contactless payment systems [19].

For instance the EPC C1G2 protocol uses a “kill” command [6], protected by a password, to damage the label so that it can not be read. It is possible for a third party to record the conversation between a reader and tag that performs a kill operation and use that information to kill other tags provided that they are protected with the same identical kill password.

3.4. Denial of Service

An adversary may initiate a denial of service (DoS) attack to bypass or avoid security systems. A DOS attack is easily carried out by placing a large number of fake labels for identification by a reader. Persons also have the ability to disrupt an RFID system implementation by destroying or corrupting a large batch of labels. Labels are also vulnerable to protocol attacks. Labels may be repeatedly asked to perform an operation, thus making them unavailable to an authorised reader.

In addition tags may be prevented from being read by using the simple concept of a Faraday cage or by jamming the RFID interrogator signals, for instance by intentionally creating noise in the frequency band in use. For critical applications, a DoS attack may pose devastating effects.

3.4.1. Code Injection

In addition RFID interrogation signals can be disrupted or blocked or RFID readers can be attacked using RFID tags designed to manipulate weaknesses in the air interface protocol or the implementation of the reader to create a denial of service attack during an RFID interrogation process by creating situations of system unavailability. The possibility of RFID viruses have been highlighted in [20] where a more sophisticated tag may exploit interrogator or protocol vulnerabilities to effect a number of systems by using a reader to cause a system failure by way of a code insertion attack caused by causing a buffer overflow in a reader’s memory stack using carefully constructed SQL instructions disguised on the tag as data that gets transmitted to an RFID reader. This vulnerability is only present if the middleware is intentionally made vulnerable by accepting any data transmitted by the tag without checking

for validity of the format of the data sent. Also modern SQL servers are guarded against malformed SQL instructions.

3.5. Communication Layer weaknesses

Recently ratified EPCglobal C1G2 air interface protocol [6] has a number of security features based on the use of tag specific passwords. Probably the most important feature that is protected is the *KILL* command by using a kill password. There is also a means for access control on the tag using an access password.

A recent publication in [21] has shown how the kill password of a tag can be deduced by the careful analysis of the tag power consumption to a series of well constructed test passwords. This highlights a particular vulnerability of low cost tags to power analysis attacks and the vulnerabilities of storing long term secret information of a tag. However it is possible to prevent such an attack, as power analysis attacks have been well studied in the context of smart card devices. The RFID ICs in the future will need to be designed to avoid such an attack but this will take place at added cost to a RFID tag.

While power analysis attacks may be prevented in the future, the fact that each RFID tag has at least two unique passwords will create both potential security and logistical nightmares if the problem of careful key management is not considered. This problem will be aggravated in the future as item-level tagging begins to proliferate through the global supply chains and POS (point of sale) devices may need real time access to passwords as consumers purchasing goods may want their tags deactivated at the point of sale. Hence the problem of careful key management needs to be considered in the context of low cost RFID systems where the potential for key discovery is highlighted by the global aspects of supply chains. It is not difficult to imagine a scenario in the future where a list of kill passwords anonymously appearing on a public web site.

The recently ratified C1G2 protocol also relies on the tag generating a random number to be used as an input to an exclusive or operation. The risks associated with inefficient or inadequate random number generation in RFID tags (that is a high correlation between the random numbers, in a pseudo-random number sequence) is emphasized in [22]. The consequences are two fold for tags using the C1G2 protocol. Primarily the lack of randomness may cause particular tags to respond with an identical time slot during the execution of the slot selection process. Thus an attacker may be able to track a tag depending on the time slot in which it randomly picks. Since the security of the information sent to a reader relies on the randomness of the number that the tag generates, a lack of randomness may allow an adversary to easily decrypt information transmitted once the attacker successfully decrypts an encrypted message or discover the seed used in pseudorandom generator.

Though with great technical difficulty [22] also point out the possibility of identifying a tag using a “radio fingerprint”. For instance by using manufacturing variations that may cause

physical glitches in the signals, where best cryptography protocols would be ineffective, to the situation where each RFID tag can be distinctly identified.

3.6. Physical Attacks

In addition, the labels themselves are exposed to physical attacks due to the absence of tamper proofing as dictated by cost limitations of low cost tags. Physical attacks are possible irrespective of whether measures are in place to protect labels. However, the ability to gain useful information from a protected label is a much more difficult problem. A physical attack on an RFID label or a reader may yield an adversary secret information, such as passwords in case of Class I labels, providing security to an RFID system. The importance of physical attacks is more prominent in cases where RFID tags are used as a means for authentication. The problem is compounded when a physical attack leads to the construction of a clone.

An insight into to possibilities of physical attacks can be gleaned from an increasing body of work in the area of smart cards. A complete overview of possible physical attacks and countermeasures are outlined in [23] while specific lower cost physical attacks are presented in [24].

The majority of physical attacks possible on devices in general can be bundled into two broad categories based on the means used for accessing the device. These attacks are relevant to RFID devices, especially since they have no tamper protection to safeguard label contents.

3.6.1. Non-invasive attacks

These attacks are as a result of timing analysis, power analysis, analysis of certain glitches [radio finger printing], and exploitation of data remanence. Non-invasive attacks are low cost and require little expertise to execute. While non-invasive attacks are generally thwarted by increasing chip complexity in most devices, it is not the case with RFID chips with minimalist implementations that may have design flaws as a result of human errors or insufficient error checking. Non invasive attacks are particularly dangerous as there is no physical evidence or the owner of the tag may not be aware that such an attack has taken place.

3.6.2. Invasive attacks

In addition, an adversary may simply reverse engineer labels to create fraudulent labels for cloning or DoS attacks or use probing techniques to obtain information stored in memory (microprobing and Focus Ion Beam editing) or alter information stored in memory (using a

laser cutter microscope [24]). A recent exploitation by reverse engineering of a more costly implementation of an RFID device with added security to carry out a fraudulent payment was published in [15]. Using microprobe needles to read out the memory contents of a smart card is published in [25].

Attacks, such as optical probing and fault injection attacks where the chip is removed from its packaging with the passivation layer still unbroken are also invasive attacks but these attacks are may be further qualified as semi-invasive attacks.

3.7. Privacy violations

The mass utilization of RFID labelled items create an imminent and potentially widespread threat to consumer privacy. The privacy issues raised by RFID labels have been receiving a wider audience as a result of the popular press. The mass movement by civil libertarians have seen RFID trials cancelled [27] (despite misunderstandings of the company's intentions [28]) and negative press coverage for other manufactures causing delays in RFID test trials [29]. Press coverage on privacy issues have also managed to tarnish the image of RFID with a satanic persona and nicknames such as "spy-chips" [76 and 77].

It is possible to imagine various scenarios of privacy violations and most of those are already existing concerns from technologies such as credit cards, browser cookies, mobile phones and Bluetooth devices. However RFID, due to is artefacts resulting from its cost constraints, presence of a unique identifier readable by anyone, and the encoding of product information on the unique numbering scheme such as the EPC creates two possible scenarios; profiling and, tracking and surveillance, where privacy of people as well as corporations may be infringed. These scenarios are discussed in the following sections.

3.7.1. Profiling

There are clear possibilities for unauthorised interrogators to read label contents from unprotected RFID labels due the lack of a mechanism for authentication and the fact that low cost RFID labels as well as interrogators broadcast unique item identifiers such as the EPC. Even if labels are protected, a traffic analysis attack (or predictable label responses) may be used. Hence an individual with a number of labelled items may be scanned by a third party to identify individual possessions or "taste", and specific EPC numbers on products may then be associated with an individual.

The data obtained can be misused to violate an individual's wishes to remain anonymous. For instance persons carrying religious material, material related to a certain political affiliation may no longer be able to pursue their beliefs or interests in their own privacy and apart from their reading material becoming public knowledge, their beliefs and opinions may be used in acts of persecution, jealousy, or hatred. While at the same time, data collected

and associated to individuals will be valuable to market researchers or thieves in search of wealthy victims. This information will form a powerful tool for marketing products as more target marketing to individual tastes and affordability become possible by scanning RFID tagged possessions of an individual.

It is possible to imagine a variety of plausible ways of using such information. For instance if Bob purchases a brand named blazer using a credit card, the shop can immediately associate “Bob” with the tag id of the apparel. When Bob enters the store again, the shop has the ability to automatically establish his identity along with a history of his spending habits and tastes. While this information may be positive for Bob, Alice who might enter the same store may be wearing cheap shoes and the shop assistants then have the ability to provide preferential treatment to Bob while perhaps neglecting Alice. At the same time, if Bob decides to walk down the street at night, a thief hiding in the corner who read the tag id of Bobs blazer might conclude from the tag id (by way of careful observation and without having access to any backend databases) that the tag id is indicative of an expensive apparel, and Bob might be the unfortunate victim of a theft.

3.7.2. Tracking and Surveillance

A further privacy concern resulting from the association of unique identifier to individuals and the unobtrusive scanning RFID labelled items carried by an individual is posed by the possibility of tracking, albeit with technical difficulty. Correlating data from readers obtained from multiple locations can reveal the movement, social interactions or financial transactions of an individual once an association is made between a unique tag identifier and a person. In response to such concerns there have been suggestions to remove the unique identifier in an EPC to prevent a specific EPC from being associated with individuals. Even if such a scheme is implemented, individuals may be tracked through a “constellation” of predictable label responses. Hence, a person’s unique taste in items may betray their location, movements, or identity.

4. Addressing Vulnerabilities

Issues resulting from vulnerabilities discussed in Section 3 can be divided into the two broad categories of security related issues (exemplified by eavesdropping, cloning, man-in-the-middle, DoS, communication layer weaknesses and physical attacks) and privacy related issues (profiling and, tracking and surveillance). Overcoming these seemingly divergent issues can be achieved by the provision of services to enforce measures to address both the privacy and security related issues. These services can be implemented on low cost RFID systems by identifying existing mechanisms or inventing new mechanisms or by re-engineering existing mechanism for meeting the required security and privacy objectives.

Table 2: Sources of unreliability.

	Description
1	Effects of metal and liquids on the propagation of electromagnetic waves
2	Effects of permeability of materials on tag antennas
3	Interference and noise from other uses of the RF band
4	Tag orientation with respect to the reader propagation field
5	Distance of the tag from a reader
6	Electromagnetic compatibility regulations
7	Cost and power constrained implementation of RFID chips

However, there is a notion among the advocates of RFID technology that the general nature that is partly hindering the mass scale deployment of RFID technology, that is the unreliability of low cost systems, mainly due to the reasons given in Table 2 makes the exploitation of vulnerabilities such as profiling and tracking discussed in the previous section impractical.

Clearly, low cost RFID tags are unreliable. For instance an RFID tag placed on your Rolex watch may work while it is on the shop shelf, but it may stop working once the watch is worn around your arm as your body will affect the properties of the RFID tag antenna.

It is due to the reasons given in Table 2 that some of the vulnerabilities discussed in Section 3, in practice, are far from being feasible. Ironically though, the unreliability of RFID tags has prevented much of the security and privacy violations from being realised, with the exception of perhaps in laboratory experiments or in the realm of possibility. While this is the present reality of low cost RFID technology, it is expected that cost benefits of RFID technology will eventually propel the research community to solve the technical issues outlined above. Hence the idea of using unreliability to brush aside the possible threats posed is not a long term solution.

Generally, it is clear that the technology of tomorrow is what is being developed currently. Even though deployment of current RFID technology do not adequately satisfy expectation, despite various mandates for RFID compliance, it is beginning to proliferate gradually [31, 31 and 32]. Hence, it is important to address vulnerabilities discussed in the Section 3, albeit some being implausible, so that the systems deployed today do not become problems of tomorrow.

The following sections consider measures required for addressing security related issues and privacy related issues.

5. Addressing Security Issues

Eliminating security related concerns regarding RFID systems illuminated by way of examples in Section 3 require the enforcement of suitable security measures. Prior to deciding on a set of security measures, the security objectives that need to be satisfied need to be resolved.

Table 3: List of security objectives.

	Security Objective
1	Confidentiality
2	Message content security
3	Authentication
4	Access control
5	Availability [33]
6	Integrity [33]

Table 3 lists a necessary set of security objectives that will be required to address the posed security threats. RFID systems must employ mechanisms to achieve one or more of the above security objectives to alleviate various concerns sighted in Section 3. While security cannot be solely accomplished by security mechanisms, it should be mentioned that proper legislation, procedural techniques and enforcement of laws is also required. The following sections describe the security objectives outlined in Table 3 and show that meeting these security objectives eliminates the security threats posed by inherent weaknesses in low cost RFID systems.

5.1. Confidentiality

The term ‘confidentiality’ can be used to describe a mechanism to keep information from all but those that are authorized to see it [10].

In an RFID system the communicated information between a reader and a tag needs to be confidential when sensitive data such as secret keys or other such information, which must not be collected by an eavesdropper, is communicated between a reader and a tag. The

confidentiality of any secret information stored on a tag is also at risk and needs to be secured.

Confidentiality may be achieved by having the communication link between tags and readers encrypted, and thus by establishing a secure communication link. Confidentiality of tag contents may be achieved by tamper proofing the tag to prevent physical access to tag contents. Currently there is no secure means of establishing a secure communication link between a tag and tamper proofing a tag has cost implications that will hinder the economics of low cost RFID technology.

5.2. Message Content Security

Providing message content security or data integrity involves a method by which it is ensured that information has not been altered by unauthorised or unknown means. Alteration in an RFID context may involve the capture, substitution, or deletion or insertion of information and the retransmission of that altered information to a reader or to a tag. Ensuring message content security will prevent man-in-the middle attacks where an attempt is made retransmit altered messages. Present low cost RFID systems have no means of providing message content security.

5.3. Authentication

The simple objective of meeting authentication can be expressed as authenticating the devices involved (the tags and the reader) or in a supply chain application where the tags are used to label products, as product authentication. In some applications where perhaps the tag is an integral part of the tagged object, authentication of the tag may be adequate to guarantee the authenticity of the object to which it is associated, in other application where tags are placed as an external label to a high value item, authentication of the tag may not be adequate. The objectives of tag and interrogator authentication and product authentication are discussed below.

5.3.1. Tag and Interrogator Authentication

In an RFID context authentication simplifies to the corroboration of the identity of a tag or a reader. Authentication is an important RFID security measure for preventing counterfeit manufacture or substitution. It is also important for controlling access to label contents. Use of authentication may also be required in other applications of RFID technology such as

baggage reconciliation or secure entry systems. Authentication of a tag is useful in addressing vulnerabilities posed as a result of cloning.

5.3.2. Product Authentication

While authentication described above has the objective of establishing that a tag is legitimate and a reader is authorised, in certain application use case scenarios authentication of the tag is not sufficient to guarantee the authenticity of the product to which the tag is attached as brand or goods substitution may have taken place. Hence in the case of using a low cost RFID tags to label a product, product authentication refers to the establishment of the authenticity of a product by the corroboration of the identity of a tag and or the legitimacy of the product by creating an irrefutable link between the product and the tag that can be verified by a third party.

5.4. Access Control

In the context of interaction between RFID interrogators and tags, access control implies a mechanism by which a tag or an interrogator grant access or revoke the right to access some data or perform some operation. Generally tags will require access control mechanisms to prevent unauthorised access to tag contents.

5.5. Availability

Ensuring availability in RFID systems is an important issue since readers need to be ready to detect tags that may enter their reading range at ad-hoc intervals of time (depending on the application). In an RFID context availability applies to ensuring that the services offered by a reader to an RFID tag or the services offered by a tag to an RFID reader are available when expected [33]. RFID systems meeting the availability criteria will ensure that there are services in place to thwart or prevent a DoS attack.

5.6. Integrity

Integrity of an 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 [33]. Ensuring the integrity of a system is an important consideration in addressing physical attacks.

6. Addressing Violations of Privacy

While it is difficult to define privacy, and a number of different interpretations can be found, it can be most simply stated as the *interests* that a person or persons have in "sustaining a 'personal space' free from interference by other people and organisations" [26]. The ideas captured by *interests* that a person has in an RFID context can be further elaborated as given below in Table 4 [26].

Table 4: An elaboration of privacy.

Privacy interests	Description
Privacy of personal behaviour	As the name suggests privacy of behaviour encompasses all aspects of a person's manners. In reality this narrows down to areas that are sensitive to individual people such as political activities, sexual orientation or religious conduct.
Privacy of personal data	Personal data privacy refers to the more commonly used term, data privacy. In essence, data associated with a person should not be accessible by a third party without the consent of the individual. This applied to cases where the data is collected, or processed by a third party.

It is not possible to describe the number of privacy violations RFID technology can potentially cause, since they are numerous as described in [80]. However, it is sufficient to realise that the root cause of such violations stems from the potential to automatically associate human identification information with object identification information and thus addressing privacy requires certain goals to ensure that the latter association is not possible. Privacy goals outlined in Table 5 are an adequate set of goals for addressing the issue of associating object identification data with human identification data and the related concerns outlined in Section 3.

It is important to note that privacy is a multi dimensional issue involving many areas. The successful implementation of privacy objectives outlined in Table 5 will not only require security mechanisms but will also require the formulation of public policies, legislation and the enforcement of the law by the relevant law enforcement agencies. The latter statement is especially important in the events of ensuring privacy of personal data (In Australia such laws

are legislated in the Commonwealth Privacy Act 1988 and the Commonwealth Freedom of information Act 1982, Australia].

Table 5: List of privacy objectives.

	Privacy objective
1	Anonymity
2	Untraceability (Location privacy)

Public policy is a vital aspect because the security mechanisms used to ensure privacy are most effective when implemented in conjunction with a well-formed policy. However, there are already existing privacy polices that can be applied directly in the context of RFID [35]. They may however need to be clarified, refined or amended to cover aspects specific to RFID Systems. Major issues that must be dealt within policy formulation or amendment in relations to RFID are those generated by the following items.

- Unique Identification of all label items
- Collection of information (who collects data generated from RFID systems, how do you exploit that data, ownership of information obtained form the data)
- Dissemination of that information
- Mass utilization of RFID technology

It is important to note that existing barcode systems have many of the same risks; they can be read by a simple bar code reader, can be destroyed easily, and can be cloned, however they do not have the potential for these operations to be performed wirelessly and apparently unobtrusively on an immense scale.

While public policy and legislations is an ongoing topic of discussion, it is beyond the scope of this thesis to address policy tools and legal tools for addressing security and privacy issues however technical solutions for addressing previously mentioned issues are considered in Section 9. The following sections discuss in detail the privacy objectives introduced in Table 5.

6.1. Anonymity

While anonymity can be described in a number of ways, the most appropriate is probably the concealment of the identity of a particular person involved in some process, such as the purchasing of an item, visit to a doctor or a cash transaction [26].

Mitigating the problem of anonymity in an RFID context will involve the prevention of associating an EPC of an item with a particular individual. As the EPC can be used to obtain information regarding a particular process and that information may be associated with a particular person. For instance a person will not be able to walk into a book store and purchase a book of their choosing and walk on the street without the possibility of being able to conceal their identity with regards to the purchase. The same person may carry an expensive medication which might be scanned by thieves, and targeted for theft or scanned by potential employers to your detriment.

6.2. Untraceability (Location Privacy)

Untraceability in and RFID context is aimed to addressing location privacy issues. Location privacy is an issue that has surfaced more recently with the availability of reliable and timely information about the location of people as a result of pervasive computing. It is also an issue associated with mobile users and other users of such wireless devices. While this is not an issue specific to RFID [34], it does apply to modern RFID systems that are being developed because of their pervasive nature and their ability to leverage the internet to form a global network that can receive and transfer data in real time.

There are number of ways of defining untreaceability and in the an RFID systems environment it can be stated as a means by which the ability of other parties to learn or track the location of people, or transactions from current or present location, based on information obtained from one or many RFID tags in possession of that person or persons or party to that transaction, is prevented.

Hence providing untraceability in an RFID system would need to involve the prevention of other parties from obtaining RFID tag data without the tag owners consent and or the prevention of associating an EPC of an item with a particular individual and or preventing tags from emitting any kind of a unique identification signal on performing a tag query by an authorized reader. Hence a mechanism is required by which a person can hide his or her true identity from devices that scan our personal RFID tags while still being able to take advantage of the benefits of RFID for the consumer.

7. Cryptography

Achieving the security and privacy objectives outlined in Table 3 and Table 5 respectively, require an enormous anthology of technical and legal tools. While legal tools are not considered in this dissertation, the required technical tools may be provided through cryptography. The following sections of the chapter considers cryptography, the science from which a plethora of technical tools for providing services to achieve the privacy and security objectives identified previously can be obtained.

Cryptography is defined as the study of mathematical techniques related to aspects of information security in [11]. However, cryptography is not the only mechanism by which information security may be provided.

Security and privacy issues concerning RFID may be solvable using a set of security mechanisms derivable from various cryptographic primitives. A security mechanism is a collective term used to refer to a combination of cryptographic primitives and protocols used to provide security. Hence, it is appropriate to briefly consider the subject of cryptography in the following sections to examine the range of cryptographic tools available for various applications, the level of security provided by such primitives and a simple classification of vulnerabilities of various security mechanisms.

7.1. Cryptographic primitives

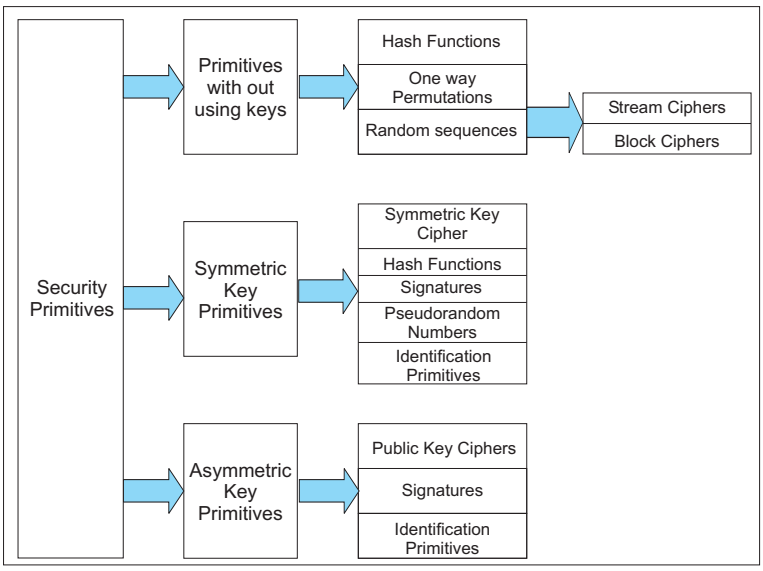

Fig. 4: Classification of cryptographic tools [17].

Cryptography is an ancient art that has been used throughout human evolution to provide security and to protect the privacy of individuals or organisations. Providing security and privacy for RFID systems will inevitably involve using some cryptographic primitive already in existence or newly defined along with suitable protocols that take into account the unique nature of RFID systems. Fig. 4 gives a classification of a broad range of cryptographic primitives. A more complete description of these primitives can be found in [10].

Most modern cryptosystems, such as the RSA cryptosystem (with the exception of few, such as one-time pads) are based on some mathematically hard problem and the level of security provided by the system will depend on the difficulty of the mathematical problem.

It is important to define the difficulty of a problem before the level of security provided by a cryptographic system can be discussed. A mathematical problem is said to be difficult if the time it takes to solve the problem is immense compared to the size of the inputs to the problem. Modern cryptographic systems are based on mathematical problems where the fastest known algorithm takes exponential time to find a solution. This implies that the time taken to solve the problem increases exponentially as the size of the inputs to the problem increases linearly. Thus the level of security provided by a cryptosystem is often expressed in the number of operation required to break the cryptosystem or the time taken and the level of security provided by a cipher compliment the commercial value of the information protected by the cryptographic system. A discussion on quantifying the security provided by a security mechanism is considered in Section 7.3.

While there are numerous cryptographic systems in use based on various primitives outlined in Fig. 4, all such systems are not without their own set of weaknesses. There are specific attacks on any cryptosystem, or protocol employed by a security mechanism used to provide security. These weaknesses are a result of certain infirmities in the cryptographic scheme or due to certain flaws that may have entered into the protocol employed in the security mechanism. A classification of attacks on cryptographic systems in general is discussed in Section 7.2.

7.2. Classification of Attacks

Cryptanalysis is the art of recovering the plaintext of a message without the key by using an algorithm to infer the plaintext from a given ciphertext or by deducing the key so that ciphertext can de decrypted to obtain the plaintext. An attempt made by an adversary at cryptanalysis is termed an attack [78]. The following sections consider the possible attacks on cryptographic primitives and protocols to defeat a security mechanism.

7.2.1. Attacks on Cryptographic Primitives

There are various forms of attacks possible on cryptographic primitives, with various names, however the most common forms are outlined in Table 6 (refer to [10, 11, and 78], for more details).

Table 6: Attacks on cryptosystems.

Cryptanalysis Method	Description
Ciphertext-only	This type of attack is carried out by an adversary who is in ownership of a string of ciphertext [11]. Here the adversary tries to deduce the decryption key or the corresponding plaintext from the string of ciphertext [10]. An encryption process that can be broken by a ciphertext-only attack is considered to be completely insecure [10].
Known plaintext	In this type of attack, a cryptosystem is attacked by an adversary in ownership of both a string of plaintext and the analogous cipertext [11].
Chosen plaintext	In this case the adversary is in possession of a ciphertext string corresponding to a plaintext of his choosing (may be as a result of gaining temporary access to the encryption engine) [11]. Then the adversary uses any information deduced from analysing the plaintext and ciphertext pair to obtain the plaintext of another ciphertext message.
Chosen ciphertext	In this scenario the adversary is in possession of a plaintext string corresponding to a cipertext of his choosing (may be as a result of gaining temporary access to the decryption engine) [11]. Then the adversary uses any information deduced from analysing the ciphertext to decipher plaintext from other ciphertext messages.
Adaptive chosen-plain text	It is a chosen-plaintext attack where the choice of the plaintext used by the adversary may depend of the ciphertext observed from previous requests [10].
Adaptive chosen ciphertext	It is a chosen-ciphertext attack where the choice of the ciphertext used by the adversary may depend of the plaintext observed from previous requests [10].

7.2.2. Attacks on Protocols

Similarly to attacks on cryptographic primitives, there is a vast array of attacks on the protocols used, and the collection of attacks has grown with the emergence of new protocols. Table 7 is summary of a prevalent list of possible attacks.

Table 7: Attacks on cryptographic protocols.

Protocol Attack Method	Description
Replay	As discussed in Section 3.3 in a replay attack the adversary records a conversation between trusted parties and then replays a section, or all of the recorded information at a different time to break the security.
Known key	An adversary attempts to determine the secret keys to be used in the future based on certain secret keys obtained in the past [10].
Impersonation	The term is taken to refer to an attack in which the attacker creates a misleading context, to trick a legitimate party into making an inappropriate security-relevant decision, or fooling the legitimate party into believing that the attacker is legitimate.
Dictionary	The adversary uses a dictionary consisting of a large number of probable keys or passwords and applies it to defeat the security imposed by guessing the accepted key or password. This type of attack is usually applied to defeat the security of password protected systems [10].

7.3. Level of Security

Many cryptographic systems have been broken because of increased computational resources, development of faster and better algorithms or problems being proved to be easier than when they were first conceived. This is the reality of any cryptographic system. However, the concerning issue is not that the system will eventually be broken, but the range of possible attacks on a security mechanism to breach security and the time taken to break the security system.

Table 8: Level of Security.

Level of Security	Description
Unconditional Security	A cryptographic system is described as being unconditionally secure if the security of the system can not be broken if an adversary is given unconditional resources. Encryption systems with perfect secrecy (where the observation of the ciphertext do not provide any information regarding the plain text) are unconditionally secure [10]. An example of an unconditionally secure encryption system is one-time pads.
Ad-hoc Security	System are classified as having a had-hoc security when postulations are made using any number of apparently convincing arguments that all possible attacks on the system requires a level of resources (computational and time) that is beyond the level of resources available to some hypothetical adversary. Security systems of this type are generally designed to counter some well known attacks and where they survive such attacks they are said to have “heuristic security” [10].
Computational Security	Computational security is given as a measure of the amount of computational work required using the best available method to defeat the security of a system. A system is considered computationally secure if the amount of computer resources or time required to break the system is far more that that available to an adversary considered in the security analysis of the system. Computation security is also termed as Practical security [10]. As described in [10] computational security can be evaluated in terms of the number of computational operations (as measured by clock cycles times or number of fundamental operations) required to defeat an intended security objective. As such the level of security can be defined as the minimum amount of work required break the security of system. The amount of work thus required is termed as the “work factor” [10]. Clearly as technology and algorithms improve, the work factor will vary. Thus a more practical definition is the “historical work factor” [10] which estimates the amount of work (in terms of time) taken to defeat a security objective using the best available methods at a given point in time.
Provable Security	A system is has a level of security described as having provable security if it can be shown that breaching the security of the system involves evaluating the solution to a problem classifies the problem as belonging to a class of problems that can not be calculated in polynomial time, such as the integer factorisation problem or the discrete logarithm problem

It should be noted here that in general, the security of a systems is difficult to quantify. The usage of the term, 'level of security' is generally used to refer to the number of operations required or the amount of time taken to break the security of a given system using state of the art technology and the best available algorithms.

However, it is possible to evaluate the security provided by a certain mechanism and describe them using a number of classifications, some of which was published in [36]. Terms use to describe the level of security of a system are outlined in Table 8.

8. Low Cost RFID and Cryptography

The plethora of available security primitives are too extravagant to be implemented on a cost constrained RFID chip with around 4000 gates for logical functions (refer to Section 2.1). Low cost labels are also not self-powered and only consist of limited logic functionality unlike smart card processors. However, they may be more suitable for higher class labels with a greater opening price point. For instance, private key cryptosystems such as AES are not suitable, since a commercial implementation of AES typically requires 20,00 -30,000 gates [37, 10]. This is far more than the number of gates on an entire low cost label. However the SHA-1 specified by the US Department of Commerce is a possible candidate for an encryption rule but hardware implementations of SHA-1 are also currently too costly to meet the cost budget of low cost RFID labels [38]. Cryptographic systems and protocols need to fit into a label footprint without dramatically increasing the cost of a label.

Considering cryptographic solutions for RFID require a careful understanding of low Cost RFID, underlying assumptions of the system, limitations, and expectations from the end user community. There are particular challenges that need to be considered as a result of the nature of low cost RFID systems. These challenges are discussed in the following section.

8.1. Challenges

Challenging aspects to providing security and privacy for low cost RFID systems using traditional cryptographic mechanisms and existing hardware are outlined in Table 9. Each of the listed constraints needs to be considered before designing a practicable security of privacy measure.

It is evident from the description of low cost RFID systems provided in Section 2 and their associated implementation in supply chain applications as Class I and Class II tags that the main constraint hindering the adoption of more traditional cryptographic solutions is the scarcity of hardware resources as a result of cost limitations. Nevertheless, cost is not the only limitation, there are many other such restrictions and difficulties that result as a

consequence of the nature of electromagnetic waves and the constraints placed by end users and electromagnetic compatibility regulations.

Table 9: An outline of challenges faced by low cost RFID

Challenge	Description
Cost	Minimizing cost implies limited memory and silicon area constraints. Tag costs are expected to be less than 5 US cents. The cost of tags has reduced over the years and the trend is expected to continue thanks to Moore's Law. This has two implications; more hardware intensive cryptographic function will slowly enter low cost RFID chips and the cost of an RFID will continue to go down. Unfortunately, analogue devices fabricated on IC's do not scale in the same manner at the digital devices so RF front end on chips will still remain a cost factor.
Regulations	Transmit power restrictions and spectral masks, frequency of operations, available bandwidth, time available for computations.
Power consumption	Important to minimize the power consumption of the label IC circuit to gain maximum performance. A cryptographic device being the highest consumer of a passive chips power will severely affect its performance as it will reduce a label's read range.
Performance	Label performance and system performance goals (data transmission rates, number of label reads per second, percentage of correct reads). Performance goals also place a limit of the time available for any computations by cryptographic hardware. Cryptographic systems requiring access to backend systems will need to take into consideration network delays associated with a security mechanism as such delays will affect system performance.
Power disruptions	Sudden loss of power is a practical reality and any security mechanism should not leave the chip in a vulnerable state during such an event.

As outlined in Table 9, EM regulations pose restrictions on the isotropic radiated power at stated distances. This implies that there is a maximum limit on the power available at a given label distance from a transmitter. Thus, passive labels with size limited by a particular label class or an application are receiving power from a stated power flow per unit area. The power available to the label is one factor contributing to the determination of the type of security scheme and the cryptographic hardware used in a label. Cryptographic hardware consuming considerable power (in the range of tens of microwatts) will severely diminish the label

reading distances and degrade the performance of the whole RFID system implementation. Furthermore, a security mechanism employing a memory write will have to account for the additional power required to operate a labels E^2PROM.

The power utilization of any security related hardware should not exceed the typical tag power consumption of 10-15 microwatts required for writing to a passive RFID label, as explained in Section 2.2.2. Ideally the power consumed should be a fraction of this value for any security related hardware to be viable as considerable power requirements will constrain the label performance by limiting the operating range of the label. However reducing power consumption of any encryption hardware is a challenging prospect.

Power dissipation in integrated circuits is a function of many factors; the fabrication technology, the layout of the design and the scale of the fabrication process. Static CMOS technology is very attractive in low power devices due the almost negligible power consumption in steady-state operation. Power dissipation in CMOS circuits is mostly due to the charging and discharging of capacitances during dynamic operation. Power consumption can be reduced by the proper choice of circuit, logical or architectural structure. This might come at the expense of silicon area, which is critical to controlling tag costs.

The power consumption in static CMOS circuits is due to the static (or steady state) power consumption and the dynamic power consumption (power consumption during the switching of logic levels). The dominant power dissipation in CMOS circuits is caused by the switching while the static power consumption due to leakage current flow through the reversed-biased diode junctions in the transistors are almost negligible.

$$P_i = P_{i\_static} + P_{i\_switching} \quad \text{W} \tag{1}$$

$$P_{i\_static} = I_{static} V_{dd} \quad \text{W} \tag{2}$$

$$P_{i\_switching} = C_L V_{dd}^2 f_{0\to1} \quad \text{W} \tag{3}$$

Equation (1) illustrates the total power consumption of a device i while (2) expresses the static power dissipation as the leakage current I_{stat} and the supply voltage to the device Vdd. Equation (3) formulates the power consumption during $f_{0\to1}$ switching operations (logic 0→1 an 1→0 transition) per second, where C_L represents the sum of the intrinsic capacitance (junction capacitance and other parasitic capacitances) and the extrinsic load capacitance (due to the wires and connecting gate) of the device.

It is clear from (3) that higher throughput from a device leads to more frequent signal transitions and results in increased power dissipation. There is always a trade off between the power dissipation and area of silicon used (and hence costs) as use of parallel architectures can reduce the power consumption by reducing the rate of switching components and the supply voltage required. Reducing the supply voltage alone is not sufficient as that reduces the latency of the circuit and any security related hardware may not be able to meet timing constraints or performance constraints. Use of parallelism allows to

trade off, silicon area for power. Design methodologies for reducing power consumption in CMOS logic is an active area of research and much details can be found in [79].

However, read range might not be a concern in certain applications and thus it is difficult to set a bound on the required power level, except to sate that, it should not exceed the power required by the tag during writing data to the memory as this is the most power consuming task a low cost tag is likely to perform. In addition, requiring more power would imply that a tag in its current position of being just able to operate (as it can be read by an interrogator) may not be able to complete a security related function causing that operation to fail. This failure may expose or lead to vulnerabilities in the security mechanism. Hence power consumption is an issue that needs to be carefully considered.

Security mechanisms and communication protocols also need to be carefully designed to avoid leaving the label in a vulnerable state during sudden loss of power or interruptions to communications. It is also important for security mechanisms to take into account the more powerful signal strength of the forward channel (reader to label transmissions) which can be detected hundreds of meters away compared to the tag to reader communication channel which can be received from no greater than 20m using highly sensitive receivers.

Once the vulnerabilities have been understood and the nature of low cost RFID, its unique set of challenges to providing cryptographic solutions have been considered, it is then possible to formulate solutions provide various security services identified by Table 3 and Table 5. The following section details a various methods proposed for eliminating security and privacy concerns discussed with regards to low cost RFID deployments.

9. A Survey of Solutions

Section 7 considered the subject of cryptography in a general perspective and introduced concepts that will be useful in the discussion of security mechanisms for RFID. The following sections consider cryptographic primitives, protocols and security schemes suitable for low cost RFID systems.

An important consideration that is often overlooked is the ability for a cryptographic system to use a piece of hardware repeatedly to result in a more secure encryption engine. Most modern UHF RFID chips use on board oscillators with frequencies over 1 MHz. Thus within the operation trimming constraints imposed as a result of US regulations, will allow a tag to expend around 400,000 clock cycles during a 400 millisecond period. Thus, it may be possible to redesign hardware for existing cryptographic primitives to exploit this unique scenario. However, this will be at the compromise of tag reading speeds. In addition a security mechanism that is capable of leveraging existing hardware on the tag will also reduce the cost of implementation; such a possibility may be found by using the hardware used to calculate the CRC (cyclic redundancy checks) on the tags.

In addition to the possible vulnerabilities discussed in Section 3, there will be specific attacks on any cryptosystem, or protocol employed by a security mechanism used to provide

security. These attacks are a result of certain weaknesses in the cryptographic scheme or due to certain flaws that may have entered into the protocol employed in the security mechanism. A description of such attacks was provided in Section 7.2 and examples of such attacks can be found in [10 and 11].

The following sections will detail more recent developments addressing the issue of security and privacy for resource intensive environments. While an attempt it made to detail as many developments as possible advances in authentication protocols suitable for low cost RFID have not been considered.

9.1. Hash Based Schemes

There have been a number of security schemes outlined in [38 and 39]. A proposed scheme for controlling access to a label uses the difficulty of inverting a one-way hash function [38]. This mechanism can prevent unauthorised readers from reading labels.

The primary flaw in this approach lies in the fact that a successful discovery of a MetaID and a label ID pair will allow an adversary to engage in a cloning attack. The hash locking method requires the implementation of a suitable hash function and the appropriate logic to implement the details of a communication protocol. The greatest challenge lies in the successful implementation of a hardware efficient hash algorithm on the label IC. Since any reader can obtain the MetaIDs from labels, this scheme does not solve the problem of location privacy violations. The scheme is also susceptible to man in the middle attacks since an adversary can query a label, obtain its MetaID, retransmit the value to a reader, and later unlock the label with the reader response.

The hash locking method requires the implementation of a suitable hash function and the appropriate logic to implement the details of a communication protocol. The greatest challenge lies in the successful implementation of a hardware efficient hash algorithm.

However, the hash based access control can be extended to provide access control to multiple users or control access to label functionalities, such as write access. It is also possible to allow a third party to process labelled items using the MetaIDs and a database lookup scheme without having to unlock the labels. However, it should be noted here that any system that will function using the MetaIDs alone will suffer from the same security flaws as an unprotected label since the MetaID will act as a unique identifier (similar to an EPC on an unprotected label).

Randomised access control is another variation of the above scheme described in [38 and 39] but with similar flaws and difficulties. The emphasis is placed on removing the predictable nature of the label responses to reader interrogations. A detailed description of this scheme can be found in [38].

Readers are still susceptible to replay attacks. An adversary only needs to obtain a label response and the corresponding reader response to create a fake label. An important consideration in this scheme is the number of labels that can be successfully supported,

since a large number of labels will cause increasing processing delays at the back end database systems. It is also not known whether keyed pseudorandom number functions required to implement the scheme are a more efficient hardware implementation than a symmetric key encryption such as a hash function. The hardware complexity of keyed pseudorandom number functions is still an active area of research [40].

9.2. Cellular Automata Based Schemes

The theory of Cellular Automata (CA) [41] developed by Wolfram has been used do develop a number of different cryptographic systems. Cellular Hash (CH) [42] is one such outcome and there is a rich variety of inexpensive encryption mechanisms developed based on the chaotic nature of CA system [43 and 44]. CA may be built out of a feedback shift register and a single pair of gates providing a compact solution for low cost RFID. In addition, CA based hashes scale well as the size of the hash digest increases but CA hashes require many parallel calculations and thus they may impose considerable demands on a tag's available power. However it is possible to perform CA operation in series but that will be at the expense of RFID system performance.

The CA cryptosystem encountered in CAC [43] while being promising has been shown to be vulnerable to differential cryptanalysis or have been shown to form an affine group [45]. However, the estimated size of the un-optimized pre-layout area is about 4.25 sq. mm, which is far bigger than a typical RFID silicon design, which is about 0.25 sq mm. Even if optimisation halves the design, it is still too extravagant for a low cost RFID chip. Nevertheless improvements and a scaling down of the design may be possible since the analysed design was for a 128 bit key.

9.3. Use of Non Linear Feedback Shift Registers

Use of non linear feed back shift (NLFSR) registers to design a hash by using a complicated feed back function is a possibility since a shift register implementation does not require complex hardware. However an important consideration should be whether the additional cost of a NLFSR provides an adequate security [10].

9.4. Message Authentication Codes

The use of Message Authentication Codes (MACs) has been discussed in previous literature. Takaragi [11] and his team of researchers have been the first to make available commercially an RFID chip (µ-chip) equipped with a MAC. The chip manufactured using a 0.18 micron

CMOS technology occupies less than 0.25 mm^2 of silicon wafer, placing the IC into the low cost end of the RFID labels.

The MAC implementation takes a very simple approach. The security of the µ-chip relies on a 128bit ID stored permanently on the chip at manufacturing time. This ID is a concatenation of a previously encrypted MAC and chip data, the MAC being derived by encrypting a portion of the data using a hash function and a secret key, where the secret key is known to the manufacture and the clients. This mechanism does raise the difficulty level for forgers as the process of eavesdropping and creation of fake labels is made more difficult, however it does not provide privacy as the ID code embedded in the chip will breach anonymity and location privacy. There is also the risk of the key, which is common to many labels, becoming known.

9.5. NTRU

The NTRU cipher appeared in 1995 [49]. NTRU is based on the Closest Vector Problem, which involves finding the closest vector given a lattice *L*, and a target vector *y* [11]. It is similar to the knapsack problem. A lattice is defined as “the set of intersection points of a regular (but not necessarily orthogonal) n-dimensional grid”. This is an NP-Hard problem where there is no known algorithm for solving it in polynomial time [50].

There are several cryptosystems based on this problem [51 and 52], but they have not gained in popularity due the excessive size of the keys needed to provide security comparable with other public key cryptosystems. The main advantages of NTRU are that it requires moderate resources and it is a faster operating algorithm. However, it is difficult to make accurate comparisons with other algorithms, as NTRU depends on many parameters that govern its behavior. Early research indicates that NTRU is generally faster, relatively easier to implement both in hardware and software than other public key cryptosystems such as RSA and NTRU needs only a modest size memory [3]. Its simple implementation and limited demand on memory have already proven its relevance in RFID applications.

Nonetheless, NTRU is susceptible to brute force attacks and multiple message transmissions [49]. A more detailed treatment of attacks on NTRU can be found in [53]. In addition, NTRU has a relatively large message expansion. Encrypted messages are almost twice the length of the plain text messages. This may not be a pressing concern as RFID messages are not of very long lengths.

9.6. Tiny Encryption Algorithm

TEA is an encryption algorithm designed for simplicity and ease of implementation. The encryption algorithm is based on the Feistel cipher [11] and a large number of iterations to gain security with out compromising simplicity. A description of the algorithm is provided in [54].

TEA can be effortlessly translated into any language as long as 'exclusive or' is an available operation. A hardware implementation of the algorithm is stated to have the same complexity as DES [54]. Despite the simplicity and the ease of implementation of the cipher, TEA is a more recent invention and the level of security or its' vulnerability to attacks is still not very clear.

9.7. Small Encryption Algorithm (SEA)

The authors in [55] have noted that resource constrained encryption using symmetric cryptography does not have a long history. They cite TEA above and indicate the vulnerabilities of TEA to linear and differential cryptanalysis attacks.

SEA (Scalable Encryption Algorithm) is a scalable encryption algorithm for small embedded applications [55]. Typical performances of the SEA algorithm on encryption and decryption using a 128 bit key and 1 MHz 8-bit RISC processors can be done in a few milliseconds, using a few hundred bytes of ROM [55].

9.8. Lightweight Cryptography

Lightweight cryptography is a branch of cryptography that aims to develop fast and efficient cryptographic mechanisms for resource constrained environments. Hence this branch of cryptography has been the most promising avenue to generate secure cryptographic solutions to low cost RFID systems. Several lightweight cryptographic models relevant to RFID are summarized below.

Building cost effective cryptographic hardware for RFID is still not a reality though certain advances have been made towards the development of hardware optimized encryptions engines in [56, 57, and 58], they still present a performance hindrance and an extravagant solution to current RFID systems.

Building on prior work, Hopper and Blum have suggests two shared-key authentication protocols, HB and HB+ protocols [59]. HB protocol is proven secure against a passive (eavesdropping) adversary. The HB+ protocol is proven secure against the active attacks. Security of these protocols are based on the conjectured hardness of the "learning parity with noise" (LPN) problem. Their extremely low computational overhead makes them very suitable for low power, bandwidth and low cost devices such as RFID. In [60] it has been proven that the security of these protocols only hold for sequential executions and the question of whether the security also holds in the case of parallel or concurrent executions is explicitly left open.

Katz and Shin [81] suggest in addition to guaranteeing security against a stronger class of adversaries, a confirmation of the security in parallel and concurrent operations would allow

the HB+ protocol to be parallelized. This would also reduce substantially its round complexity. Katz and Shin prove the security above. They also suggest simpler security proofs for these protocols, which are more complete. In effect they also explicitly address the dependence of the soundness error and the number of iterations.

An improved version of the HB++ (and an improved version of the HB+ protocol) developed by [61] is analysed in [62] where a number of improvements have been made against various vulnerabilities outlined in [61].

9.9. Radio Fingerprinting

If tags have distinct “radio fingerprints” that are difficult to reproduce, then these fingerprints, on their own, could help strengthen device authentication [63]. The technique while sound in theory is not a practicable avenue as obtaining such a radio fingerprint is expensive and difficult.

9.10. Minimalist Cryptography

The formulation of mechanisms to achieve security and or privacy objectives under the constraints presented by low cost RFID systems to real-world tags form the basis for minimalist cryptography.

9.10.1. Pseudonyms

An early version of minimalist cryptography was proposed in [64] where a list of randomly generated tag identifiers was used on a tag. On querying a tag, a reader is able to hash the response and access tag related data on a secure hash table. The idea of using completely random EPCs and an outline of such a scheme was also given in [64]. A similar version was also published in [65] with a minimalist security model and accompanying protocols for low-cost tags. The proposed method has every tag containing a collection of pseudonyms; it releases these pseudonyms on each interrogator query. Both schemes have left open the possibility for a valid reader to renew the list of pseudonyms on a tag.

The use of pseudonyms in [65] are based on the assumption that the intruder only comes into the scanning range of a tag on a periodic basis as a complete analysis of the limited number of pseudonyms will allow the identification of the tag. The model is also based on the underlying assumption, that the tags release their data at a limited rate [65]. The minimalist model sets an upper limit on the number of times an intruder or an adversary can scan a given a tag or try to spoof a valid reader.

9.10.2. One time pads and random numbers

In addition to the schemes presented above, there are many security schemes in the patent literature. Information security is a secretive realm, with many holding firmly onto their intellectual property with a whole array of patents. It is the nature of the beast.

Most methods outlined in patent literature are too complicated for low cost RFID. However, [47] demonstrates a very simplistic approach. The patented scheme relies on a simple one-time pad concept, where the intended application is that of bank notes. The scheme involves the recording of a random number, a time, and a date stamp on a RFID label of a bank note on release of the note for circulation. The bank note keeps a track of the number of times it has been scanned and this number is used as part of its authentication process. When a bank note is read by a bank teller, the random number, date, time stamp and the number of scans are sent to the central bank computer for comparison to verifying the notes authenticity.

This scheme is subject to imitation, simply because the label can not be trusted as a secure place of storage for valuable information as bank notes provide adequate incentives for a physical attack on the RFID label.

A different application of one-time pads can be found in another patent [48]. In the novel scheme, labels are equipped with a small rewritable memory. Prior to the release of a label, a set of random numbers (authentication keys) generated by a completely random physical process is stored into the label along with a label ID. A back end database stores a copy of the random codes and the associated label IDs.

The label ID may be read from the label during an interrogation. The ID provides knowledge of the label being authenticated by the reader by consulting the relevant records in a secure back end database. In consultation with the database, the interrogator may transmit one or more of the random numbers stored in the database. One of the numbers should match a series of random numbers stored on the label. If a match occurs the label responds with a return authentication code known exclusively to the database and increments a counter to select a set of new random number for the next authentication procedure. An identical counter that determines which of several authentication numbers is next in force, is incremented at the database.

Hence, the above mechanism prevents an eavesdropper from obtaining any information regarding the next correct authentication key, or the next label authentication response. The only available information to an eavesdropper is an apparent burst of random numbers.

In the event of an unauthorised reader, the label will not respond unless the reader knows the next random number expected by the label. In case a counterfeit label is interrogated, the label may respond with a random number, but the interrogator will fail to find a match, and thus detect the counterfeit.

Nevertheless, this scheme still leaves the possibility of a physical attack, where the contents of the label may be discovered. However, in the worst case, this information cannot be used

to counterfeit labels in massive quantities as the set of authentication keys and authentication responses are all different and completely random on each individual label.

9.10.3. Noisy Tags

RFID systems are based on limited computing power and are not suitable for public key cryptography. Hence a protocol with low computations is outlined in [66].The protocol in [66] takes advantage signal noise on a communication channel to secretly exchange a key in the presence of an eavesdropper.

An alternative proposal was presented in [67]. Similar to the blocker tags [68], the special tag in this proposal is named as the noisy tag. Noisy tags are owned by a reader's manager and set out within a reader's field. They are regular RFID tags that generate noise on the communication channel between the reader and the queried tag. This is done in such a manner, that the intruder or eavesdropper cannot differentiate the messages sent between by the queried tag and those sent by the noisy tags. Hence the intruder is unable to identify the secret bits that are sent to the reader. Afterwards, the secret shared by the reader and the tag can be used to launch a secure channel in order to protect communications against eavesdroppers. Also the tag's identifier can be refreshed by xoring the new identifier with the exchanged secret [67].

9.11. Re-encryption

The use of re-encryption to achieve untraceability, and banknote authentication was published in [37] to provide privacy and security protection to banknotes embedded with RFID labels. In a traditional setting, the entity conducting the re-encryption will not be aware of the plaintext, however in the re-encryption scheme discussed in [37], the plaintext is known to the entity performing the re-encryption. The scheme is elaborate, the details are complicated, and thus, an overview of the scheme is given in Fig. 5.

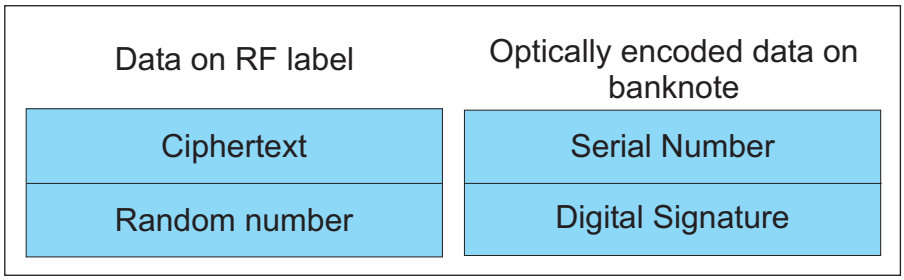

Fig. 5: Data on a banknote.

The security of the mechanism is based on the ciphertext created by encrypting the digital signature stored on the RFID chip by a central bank authority, the serial number of the bank

note and a random number. The authenticity of the banknote can be verified by comparing the ciphertext stored on the banknote to the ciphertext obtained by encrypting the digital signature, the serial number, and the random number using a public key stored on an RFID reader. A match indicates an authentic banknote. Fig. 5 provides an overview of the data placed on each banknote. In addition, an access control mechanism prevents the data on an RFID label from being read without making optical contact first. This prevents remote alteration and interrogation of an RFID label's memory contents.

The significant privacy and security achievements outlined include consumer privacy (tracing of individuals or banknotes are only possible with the use of a key), forgery resistance, fraud detection and tamper resistance. In contrast with the previously mentioned mechanisms using secret keys, the primary significance of the re-encryption mechanism is that a banknote is not in possession of any secret keys and the RFID label is not required to perform any resource intensive operations. The encryption engines and secret keys have been shifted away from the RFID label to more secure locations, such as the readers and the central bank authority.

Despite the appeal of the re-encryption scheme, the significant drawback is the adequacy of the information obtainable from a banknote to create fraudulent banknotes. The digital signature is not verified during a transaction; hence, the fake banknotes can be created with ciphertext obtained from a collection of believable serial numbers. Nevertheless creating fake banknotes is a difficult proposition, as it requires a criminal to steal RFID labels or manufacture RFID labels with identical functionality to those embedded in banknotes. Other shortcomings that might be exploited by a resourceful adversary are provided in [37].

10. Conclusion

The paper has identified numerous vulnerabilities of low cost RFID systems deployed in supply chain applications under the UHF EPCglobal air interface protocol. It is apparent that engineering solutions to such vulnerabilities is impeded by the low cost nature of the underlying technology which must be maintained to achieve its viability in real life applications. While perfect secrecy is a fine mathematical concept; in reality, there will always be a human element that is difficult to quantify into any mathematical formulation. Thus, it is practically impossible to have a perfectly secure system. Once this is understood then it is possible to move onto addressing security and privacy issues overshadowing RFID.

Most issues concerning privacy are public policy issues however; those that arise from anonymity and location privacy are solvable using a combination of security mechanism and public policy.

Traditional solutions available from proven cryptographic primitives appear to be area or power hungry to fit well within the limitations of low cost RFID systems, and much of the encryption hardware available is for smart card technology. Even though the solutions can be applied directly to RFID, the main obstacle is that smart card processors are much more

powerful than a typical RFID label consisting of only 200-4000 gates. Thus, the solutions are not portable to an RFID platform if we expect the cost of the secure labels to remain below the 5 cents mark.

It is clear (especially looking at Moore's Law) those cryptographic solutions that seem too expensive for low cost RFID may become the solutions in the future. However, it is not possible to wait for a future time frame while the deployment of RFID systems is taking place around the world at present and inaction will result in future problems that may be more expensive to mend. Since advances in cryptography are slow to arise, due to time taken for scrutinising new mechanism and finding faults, the best option might be to fall back on simple and proven techniques, such as those presented in minimalist encryption and lightweight cryptography.

There are a number of specific areas of research which will greatly benefit efforts in the areas of lightweight cryptography and minimalist cryptography while the outcome of such research will be the wide spread adoption of this technology. Cost effective and efficient hardware implementations of symmetric or asymmetric cryptosystems such a useful area of research. This may involve finding ways to optimise and improve on the existing cryptographic systems for cost effective and efficient hardware implementation, taking into consideration the specialised nature of low cost RFID labels. While the development of new hardware efficient cryptosystems suitable for low cost RFID systems involving the development of hardware efficient hash functions, symmetric and asymmetric encryption, MACs and random and pseudorandom number generators will also aid in the effort to develop lightweight cryptosystems. Alongside encryption hardware it is also important to have protocols with the flexibility to incorporate different cryptographic primitives, security measures and safeguards to prevent rendering labels vulnerable during sudden communication interruptions.

It is important to recognize that the resource limitation of low cost labels suggests that simplicity of small one time pads, which involve one or more small shared secrets between a label and an interrogator, and relatively simple chip implementations should also be considered and must not be discounted. Some of the concerns arising from privacy and security may also be removed by occasional use of shielded electromagnetic communications between the label and the reader system.

It is important to note that the level of security and privacy will depend on the application. It is evident that there is no universal solution but a collection of solutions suited to different applications. This is addressed within the class hierarchy. There are unique opportunities within the Auto-ID Centre class hierarchy to develop various schemes for meeting the security and privacy levels expected by labels belonging to their respective classes. This opens the gate to a vast number of research avenues that could be pursued in regards to providing both security and privacy to low cost RFID systems.

It must be realised that security will come in many flavours and strength, but low cost will imply that we find mechanisms that are 'good enough' and are deterrents than mechanism that are hard to crack. Proposals for implementations of these concepts are outlined in a paper yet to be published.

References

[1] Sarma, S. (2001):, Towards The 5c Tag in: Technical Report MIT-AUTOID-WH-006, 2001. http://www.autoidcenter.org/research/MIT-AUTOID-WH-006.pdf.

[2] Hall, D.(2004), Senior Design Engineer, TAGSYS, Australia. Personal Conversation, July 2004.

[3] EPCglobal Inc. home page, http://www.epcglobalinc.org.

[4] K. Eshraghian, P. H. Cole, and A. K. Roy (1982): Electromagnetic coupling in subharmonic transponders in: Journal of Electrical and Electronic Engineering: vol. 2, pp. 28-35,1982.

[5] T. A., Scharfeld (2001): An analysis of the fundamental constraints on low cost passive radiofrequency identification system design in: Masters thesis, Massachusetts Institute of Technology, August 2001.

[6] EPCglobal Inc., Specification for RFID air interface v1.1.0 (2006), accessed June 2006, http://www.epcglobalinc.org/standards_technology.

[7] SmartCode Debuts Smallest Chip (2006): accessed February 2006 in RFID Journal, http://www.rfidjournal.com/article/articleprint/764/-1/1/, 23rd January, 2004

[8] EM Micro Readies New RFID Chip (2003): accessed March 2003 in RFID Journal article, http://www.rfidjournal.com/article/articleview/350/1/1.

[9] Takaragi, T., Usami, M., Imura, R., Itsuki, R., and Satoh, T. (2001): An Ultra Small Individual Recognition Security Chip in: IEEE Micro, November-December 2001.

[10] A. Menezes, P. van Oorschot and S. Vanstone (1996): Handbook of Applied Cryptography, CRC Press, 1996.

[11] D. R. Stinson (1995): Cryptography Theory and Practice, CRC Press, 1995.

[12] Sarma, S., and Engels, D. W., RFID Systems (2003): Security & Privacy Implications in: Auto-ID center white paper, Feb 2003. http://www.autoidlabs.org/researcharchive/.

[13] A. Juels (2005): RFID Security and Privacy: A research Survey in: RSA Laboratories, September 2005.

[14] D. C. Ranasinghe, K. S. Leong, M. L. Ng, D. W. Engels, P. H. Cole (2005): A distributed architecture for a ubiquitous item identification network in Seventh International Conference on Ubiquitous computing, Tokyo, Japan, Sept 2005.

[15] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin and M. Szydlo (2004): Security analysis of a cryptographically-enabled RFID Device in: Proceedings of 14th USENIX Security Symposium, pp 1-16.

[16] J. Westhues (2005). Hacking the prox card in: RFID: Applications, Security and Privacy, Addisonn-Wesley, pp. 291-300, 2005.

[17] Verichip corporation home page (2004): http://www.4verichip.com/.

[18] K. Albrecht (2006): Chipping workers poses huge security risks in: Freemarket news, February 2006, http://www.freemarketnews.com/Analysis/139/3812/2006-02-15.asp?wid=139&nid=3812,

[19] Z. K_r and A. Wool (2005): Picking virtual pockets using relay attacks on contactless smartcard systems in: Proceedings IEEE/CreateNet SecureComm, pp. 47-58, 2005.

[20] M. R. Rieback, R. Crispo, A. S. Tanenbaum (2006): Is your cat infected with a computer virus? In: Fourth IEEE International Conference on Pervasive Computing and Communications (percom), pp. 169-179, 2006.

[21] Y. Oren, and A. Shamir (2006): Power analysis of RFID Tags, accessed on March 2006, http://www.wisdom.weizmann.ac.il/~yossio/rfid/.

[22] G. Avoine and P.Oeschlin (2005): RFID Traceability: A Multilayer Problem in: Financial Cryptography, 2005.

[23] S.H. Weigart: Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defences in: Workshop on Cryptographic Hardware and Embedded Systems, LNCS, vol. 1965, pages 302-317.

[24] R. Andreson, and M. Kuhn (1997): Low cost attacks on tamper resistant devices in: International Workshop on Security Protocols, LNCS, 1997.

[25] E Bovenlander (1997): invited talk on smartcard security, Eurocrypt 97.

[26] Roger Clarke (1997): Introduction to Data surveillance and Information Privacy and Definition of Terms, accessed April 2006, http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html#Id, 15 Aug 1997,

[27] Boycott Benetton web site, accessed December 2005, http:/www.boycottbenetton.com.

[28] M. Benetton (2004): Benetton explains RFID privacy flap in: RFID Journal, 23 June 2004, http://www.rfidjournal.com/article/articleview/471/1/1/.

[29] M. Roberti (2003): Analysis: RFID and Wal-Mart, accessed September 2003, http://www.cioinsight.com/article2/0,1540,1455103,00.asp.

[30] J Collins (2004): Marks & Spencer expands RFID retail trial in RFID Journal, 10 February 2004.

[31] D. Molnar and D. Wagner (2004): Privacy and security in library RFID: Issues, practice, and architectures in: B. Pfitzmann and P. McDaniel, editors, ACM Conference on Communications Security, pages 210-219. ACM Press, 2004, M Roberti.

[32] RFID Upgrades Gets Goods to Iraq (2004) in RFID Journal, 23 July 2004.

[33] F. Stajano, and R. Anderson (1999): The resurrecting duckling: security issues for ad-hoc wireless networks in International Workshop on Security Protocols, LNCS, vol. 1796, pp 172-194, 1999.

[34] A. Beresford, and F. Stajano (2003): Location Privacy in Pervasive Computing in Pervasive computing, January-March 2003.

[35] Electronic Privacy Information Centre (2004): EPIC web site, accessed March 2004, http://www.epic.org.

[36] C. Shannon (1949): Communication Theory of Secrecy Systems in Bell Systems Technical Journal 1949.

[37] A. Juels and R. Pappu (2003): Squealing Euros: Privacy Protection in RFID-Enabled Banknotes in: Financial Cryptography; Springer Lecture Notes in Computer Science; Volume 2742; Pages 103-121; 2003.

[38] S. A. Weis, S. Sarma, R. L. Rivest, and D. W. Engels, D. W (2003): Security and privacy aspects of low-cost radio frequency identification systems in: Security in Pervasive Computing, 2003.

[39] A. Juels, and S. A. Weis (2006): Defining Strong Privacy for RFID", RSA Laboratories, 2006.

[40] S. H. Weigart: Physical security devices for computer subsystems: a survey of attacks and defences in: WCHES, LNCS, vol. 1965, pages 302-317.

[41] S. Wolfram (2002): A New Kind of Science, 2nd edition, Wolfram Media, 2002.

[42] J. Daemen, R. Govaerts, and J. Vandewalle (1991): Hash functions based on block ciphers: a synthetic approach in Advances in Cryptology, LNCS. Springer-Verlag, 1991.

[43] S. Sen, C. Shaw, D. R. Chowdhuri, N. Ganguly and P. P. Chaudhuri (2002): Cellular automata based cryptosystem (CAC) in: LNCS, vol. 2513, pp 303-314, 2002.

[44] S. Wolfram (1986): Cryptography with cellular automata in Advances in Cryptology: Crypto '85 Proceedings, LNCS, vol. 218, pp 429-432, 1986.

[45] S. R. Blackburn, S. Murphy and K. G. Paterson (1997): Comments on "theory and applications of cellular automata in cryptography" in: IEEE Transactions on Computers, vol. 46, no. 5, pp 637-638, May 1997.

[46] NTRU web site, accessed August 2003, http:www.ntru.com/products/genuid.html

[47] Szewczykowski (1998): United States Patent, Patent number 5818021,Date of patent Oct. 6 1998.

[48] P. H. Cole (2003): Secure Data Tagging Systems, In International Patent Application, Applicant TagSys Australia Pty. Ltd, Patent number PCT/AU02/01671,Date Feb. 10 2003.

[49] J. Hoffstein, J. Pipher, and J.H. Silverman (1998): NTRU: A Ring-Based Public Key Cryptosystem in Proceedings of ANTS III, Portland, June 1998.

[50] D. Micciancio (2001): The hardness of the closest vector problem with pre processing in: IEEE Transactions on Information Theory, vol. 47, no 3, pages 1212-1215, March 2001.

[51] R. J. McEliece (1978): A public key cryptosystem based on algebraic coding theory in: JPL Pasadena, 1978.

[52] O. Goldreich, S. Goldwasser, and S. Halvei (1996) Public-key cryptosystems from lattice reductions problems, MIT LCS, 1996.

[53] Coppersmith, D., and Shamir, A (1997): Lattice attacks on NTRU, In Lecture Notes in Computer Science, Springer-Verlag, 1997.

[54] Wheeler, D., and Needham, R (1994): TEA, a Tiny Encryption Algorithm, Computer Laboratory, Cambridge University, England, 1994. http://www.ftp.cl.cam.uk/ftp/papers/djw-rmn/djw-rmn-tea.html

[55] Francois-Xavier Stnadaert, Gilles Piret, Neil Gershenfeld, Jean-Jacques Quisquater: SEA: A Scalable Encryption Algorithm for Small Embedded Applications

[56] M. Aigner, and M. Feldhofer (2005): Secure Symmetric Authentication for RFID Tags in Telecommunications and Mobile Computing TCMC2005, March 8th-9th, 2005.

[57] M. Feldhofer M, S. Dominikus and J. Wolkerstorfer (2004): Strong Authentication for RFID Systems using the AES Algorithm, Lecture Notes in Computer Science (LNCS), vol. 3156, pp. 357-370, 2004.

[58] J.Wolkerstorfer (2005): Is Elliptic-Curve Cryptography. Suitable to Secure RFID Tags in: Workshop on RFID and Light-Weight Cryptography, Graz (Austria), 2005.

[59] N. J. hopper and M. Blum (2001): Secure human Identification, Protocols in: LNCS, vol. 2248 pp. 52, 2001.

[60] A. Juels and S. Weis (2005): Authenticating pervasive devices with human protocols in: Advances in Cryptology, Crypto 2005. LNCS vol. 3621, pp. 293-308.

[61] T. Dimitriou (2005): A Lightweight RFID Protocol to Protect Against Traceability and Cloning Attacks in Proceedings of IEEE Conference on Security and Privacy for Emerging Areas in Communication Networks - SECURECOMM, 2005.

[62] S.Pramuthu: HB and Related Lightweight Authentication Protocols for Secure RFID Tag/Reader Authentication in: CollECTeR Europe Conference, Basel, Switzerland

[63] R. Jules: T Daniels, M. Mina, S. Russell (2005): A small fingerprinting paradigm for physical layer security in conventional and sensor networks in: IEEE/CreateNet Secure Comm., 2005 to appear.

[64] D. Ranasinghe, D. W. Engels, P. H. Cole (2004): Security and Privacy Solutions for Low Cost RFID Systems in Proc. of the 2004 Intelligent Sensors, Sensor Networks & Information Processing Conference, Melbourne, Australia. pp. 337-342, 14-17 December, 2004.

[65] A. Juels (2001): Minimalist cryptography for low cost RFID tags, LNCS vol. 3352, pp.149-164, Springer-Verlag, 2001

[66] H. Chabanne, and G. Avoine (2005): Noisy Cryptographic Protocols for low RFID tags in Workshop on RFID lightweight Crypto, 2005

[67] Claude Castelluccia and Gildas Avoine (2006): Noisy Tags: A Pretty Good Key Exchange Protocol for RFID Tags in: International Conference on Smart Card Research and Advanced Applications (CARDIS'06), Spain, April 2006.

[68] A. Juels, R.L. Rivest and Mszydlo (2003): The blocker tag: selective blocking of RFID tags for consumer privacy in: V. Atluri editor, 8th ACM conference on Computer and Communications Security, pp. 103-111., ACM Press, 2003.

[69] FCC Regulations, http://www.fcc.gov.

[70] ETSI, European Telecommunications Standards Institute, http://www.etsi.org/.

[71] FCC Regulations, Title 47, telecommunications, chapter1, Part 15, radio frequency devices, http://www.fcc.gov.

[72] ETSI EN 302 208-1 V1.1.1 (2004-09), http://www.etsi.rog

[73] P. H. Cole, D. C. Ranasinghe, B. Jamali (2003): Coupling Relations in RFID Systems II: Practical performance measurements in: Auto-ID Center workshop, June 2003.

[74] P. H. Cole (2003): A Study of Factors Affecting the Design of EPC Antennas and Readers for Supermarket Shelves Auto-ID Center workshop, October 2003.

[75] RFID Privacy and coporate data: RFID Journal, 2 June 2003, www.rfidjournal.com, accessed on August 2005.

[76] Spychips web site, http://www.spychips.com, accessed on August 2005.

[77] A. Jha (2003): Tesco tests spy chip technology in The guardian, July 19, 2003, http://www.guardian.co.uk/uk_news/story/0,3604,1001211,00.html.

[78] B. Schinner (2002): Cryptography book.

[79] J. Rabaey, and M. Pedram (1996): Low-Power Design Methodologies, Kulwer Academic Publishers, 1996.

[80] B. Subirana, and M. Bain (2004): Towards Legal Programming of Software Agents. Research Monograph, Kluwer. 2004.

[81] J. Katz, and J. S. Shin: Parallel and Concurrent Security of the HB and HB+ Protocols.