NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DESIGN CONSIDERATIONS FOR A COMPUTATIONALLY-LIGHTWEIGHT AUTHENTICATION MECHANISM FOR PASSIVE RFID TAGS

by

John H. Frushour

September 2009

Thesis Co-Advisors: J.D. Fulp
Ted Huffmire

Approved for public release; distribution is unlimited

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2009	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Design Considerations for a Computationally-Lightweight Authentication Mechanism for Passive RFID Tags			**5. FUNDING NUMBERS**
6. AUTHOR(S) John H. Frushour			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release, distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Passive RFID tags are attractive for their low cost, small footprint, and ability to function without batteries. The lack of onboard power, however, limits the complexity of operations that can be performed by the tags' integrated circuits, and this limitation prevents the tags from being able to perform typical functions required to support e-authentication. This thesis quantifies the delta between the power that would be required to perform MAC-based authentication, and the power made available to a tag via the reader. A modified MAC protocol is then proposed that would theoretically close this delta while still providing sufficient authentication assurance.

14. SUBJECT TERMS Passive RFID Systems, Tags, Clock, Electro-magnetic induction, authentication, hash, SHA–1			**15. NUMBER OF PAGES** 81
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release, distribution is unlimited

DESIGN CONSIDERATIONS FOR A COMPUTATIONALLY-LIGHTWEIGHT AUTHENTICATION MECHANISM FOR PASSIVE RFID TAGS

John H. Frushour
Captain, United States Marine Corps
B.S., University of Kentucky, 1998

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
September 2009

Author: John H. Frushour

Approved by: J.D. Fulp
Co-Advisor

Ted Huffmire
Co-Advisor

Peter Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Passive RFID tags are attractive for their low cost, small footprint, and ability to function without batteries. The lack of onboard power, however, limits the complexity of operations that can be performed by the tags' integrated circuits, and this limitation prevents the tags from being able to perform typical functions required to support e-authentication. This thesis quantifies the delta between the power that would be required to perform MAC-based authentication, and the power made available to a tag via the interrogator. A modified MAC protocol is then proposed that would theoretically close this delta while still providing sufficient authentication assurance.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

RFID:	Radio Frequency Identification
ASIC:	Application Specific Integrated Circuit
SAW:	Surface Acoustic Wave
ALU:	Arithmetic Logic Unit
RF:	Radio-Frequency
CRC:	Cyclic Redundancy Check
IC:	Integrated-Circuit
FPGA:	Field Programmable Gate Array
CMOS:	Complementary Metal-Oxide Semiconductor
PIE:	Pulse-interval encoding
IDT:	Inter-digital transducer
AES:	Advanced Encryption Standard
EEPROM:	Electrically Erasable Programmable Read-Only Memory
VHDL:	Very High Speed Integrated Circuit Hardware Description Language
MAC:	Message Authentication Code

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Radio frequency identification (RFID) devices are becoming more and more popular as their usage scope moves from an environment purely of logistical tracking to one of information retrieval, cataloging, and personal information management. Passive tags, in particular, offer several advantages when used in this environment. Their absence of power makes them more eco-friendly, their size makes them adaptable to any environment, and their cost makes them producible en-masse with minimal concern for bloated production control issues. However, these advantages are not without their drawbacks. Because of their lack of an onboard power source, passive tags must make several compromises. For instance, they cannot perform complex cryptographic security calculations and, thus, are less capable of supporting electronic authentication protocols than their cousins, active tags. Passive tags also typically do not involve a microcontroller or any other high gate-count application-specific integrated circuit (ASIC). Their lack of onboard power means that the tag interrogation procedure must be performed at relatively close distances. Even given these restrictions, passive tags still represent the natural progression towards smaller, more versatile, and more ubiquitous identification mechanisms.

Passive RFID tags can potentially be used for tracking vehicles through checkpoints in combat environments, displaying a soldier's shot record, and other uses as trivial as warranty tracking of high-end consumer goods. Unfortunately, passive RFID tags currently offer only minimalistic versions of authentication mechanisms that do not elicit the necessary level of trust to be used in the above listed applications. These authentication mechanisms include simple XOR and shift ciphers that, when paralleled, create rather rudimentary authentication schemes. Such rudimentary schemes are subject to being impersonated; typically via an attack called "cloning." Additionally, the use of a singular pre-shared key among all production tags dramatically increases the viability of such malicious attacks.

Current advances in low-power mechanisms—which normally are involved in more complex cryptographic algorithms—are now feasible for implementation in low-power environments, such as for passive RFID tags. Until they can be used effectively, however, several considerations must be made for their employment including power efficiency, clock synchronization, key management, and resistance to attack. A secure, passive RFID environment must be robust enough to provide real-time tag authentication, powerful enough to energize tags from a prescribed distance, and secure enough so that would-be attackers do not easily gain mission-critical information. Thus, there are several design considerations involved in the fielding and production of a secure passive RFID system. The main research question pursued in this thesis is: Given the current state of passive RFID technology, is it possible to support a sufficiently secure, keyed-hash (MAC) authentication mechanism on an RFID tag void of a native power source?

Through the use of component analysis, this thesis analyzes the major factors in designing a lightweight authentication scheme for passive RFID tags. Each component of the RFID system is critical to its success. For instance, inducing an electromagnetic field onto a passive tag must generate a native clock signal via its carrier wave that successfully drives the tag's circuitry. This induced electromagnetic field must be fast enough so that the tag receives a sufficient amount of power, both to generate a security response and broadcast that response back to the tag reader. So, in this thesis, we ask: Is it feasible that a sufficiently complex security algorithm such as SHA–1, can be employed on a passive tag? If the answer is "no," then what reductions might be made to any existing MAC authentication mechanism so that it can be employed on a passive tag without losing too much entropy?

This thesis presents a model that answers the aforementioned question, and is scrutinized against the foundational metrics of passive tags. Questions surrounding key management, proximity, and malicious attacks are all satisfied in fulfillment of the model specifications.

ACKNOWLEDGMENTS

This work is dedicated to my wife, who has tirelessly endured the endless frustrations of a master's student trying to garner hardened facts in the myriad of theorems, hypotheses, and conjectures that is Computer Science.

I would specifically like to thank Peter Ateshian, Doug Fouts, and Dan Zulaica for their exhaustive aid in circuit design and hardware coding. Their selfless donation of time towards aiding me in understanding the technical aspects of FPGA construction was invaluable in the completion of this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. IMPACT OF RFID TECHNOLOGY

RFID technology is one of the fastest growing areas of identification and tracking management today. The potential ubiquity of such a technology has become evident from its adoption by major global corporations such as Wal-Mart. At a 2003 Retail Systems conference at the McCormick Center in Chicago, Wal-Mart announced it was mandating RFID tracking technology from its suppliers "in the near future" [1]. Shortly thereafter, the EPCGlobal standard was released in 2005 [2]. This standard, designed to augment and eventually replace traditional bar code scanning, has become wildly popular in Europe but has been slow to saturate the U.S. market. Regardless, the integration of EPC information into RFID systems has been the single-largest reason for the recent prevalence of RFID tags.

Owing to their extremely small size, RFID tags offer an impressive range of capabilities in both powered and unpowered forms. Powered tags, or those with a native on-board power source such as a battery, are also known as "active tags." These tags can be programmed to continuously broadcast their information, aiding in the use of real-time tracking. For instance, active tags are widely used in vehicle tracking systems by the U.S. Department of Defense (DoD) [3]. Active tags are affixed to vehicles so that a tag reader can accurately read their information, wirelessly, even while on the move. Unpowered tags—those without a native power source, also called "passive" tags—do not continuously broadcast any information. Passive tags obtain all their operating energy wirelessly from a tag reader. This reader can be mounted in a relatively fixed location, or can be a handheld device. One such method of implementing this wireless power generation is called electromagnetic induction, and this is the most common method of energizing a passive tag.

While passive tags suffer from several limitations, such as energy, distance, and efficiency, they represent the forefront of RFID design. Passive tags can be fabricated to be wafer-thin, some less than a micrometer in thickness. Their size also enables a low

manufacturing cost and simplistic distribution scheme. For instance, many DVD cases now include RFID security mechanisms with an adhesive backing that can simply be affixed to the inside of the case (Figure 1).

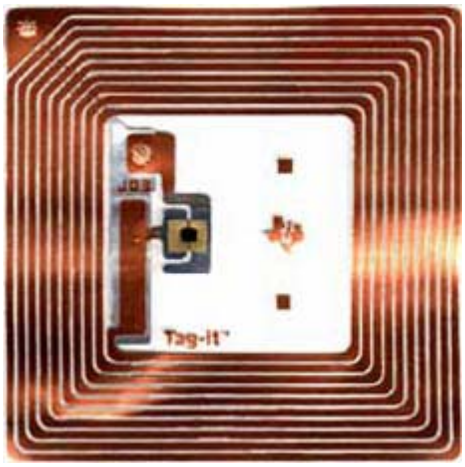

Figure 1. A Passive RFID tag developed by Texas Instruments for use in anti-theft DVD cases

Because of their low cost (often under $0.15 per tag [3]), passive tags often take on a disposable role. That is, the cost to manufacture the tags is so minute that companies consider them to be expendable. This is not to say that passive tags are not without their importance, however. Passive tags are preferred in generating the aforementioned EPC code in logistical tracking applications, and thus must have the appropriate measures of security. If the EPC code placed on a passive tag is "exploitable" for whatever reason, necessary security precautions must be made to guarantee the tag's authenticity. Otherwise, opportunities are abundant for attacks such as tag cloning, replaying, falsifying codes, etc. By "exploitable," we mean that there exists some motivation for a bad actor to impersonate the EPC code. As a simple example, we might imagine containers queued-up for a security inspection of their contents prior to being loaded onto a commercial container ship. Each container receives an RFID tag after it passes inspection, and the tag's EPC is entered into a database that is made available to security screeners at the port of debarkation. If a bad actor can impersonate the EPC of a tag that has already been affixed to a cleared container, and

affix this “cloned” tag to an un-screened container, he may be successful in getting contraband through the security screening at the port of debarkation.

Therefore, our intent is to determine whether, given the limitations of passive tags, it is possible to support a sufficiently secure authentication mechanism on an RFID tag void of a native power source. This sufficiency might be satisfied with a keyed hash solution, as hash algorithms are traditionally less computationally expensive than reversible cryptographic mechanisms (i.e., symmetric and asymmetric encryption algorithms) [4]. Later, this thesis will explore a model that attempts to answer this question, and then scrutinize the model against the foundational principles of passive tags. Such questions of proximity, efficiency, and policy satisfaction will be answered in fulfillment of the model’s design goals.

B. PASSIVE TAG STRUCTURE

Passive RFID tags operate via one of three power generation methodologies. Overwhelmingly, power generation dominates the capabilities and limitations of a passive tag. To answer any question involving the choice of a security mechanism on a passive tag, a thorough understanding of how power is obtained by the tag must be considered. Two of the power generation methodologies (near and far-field coupling) are quite popular and a third (Surface Acoustic Wave, SAW) is just becoming popular. Each has strengths and weaknesses, mostly related to the operating range at which the reader interacts with the tag, and the frequency at which the tag can be energized. A summary is given below in Table 1.

Near/Far Field	Near → Far			
Frequency Range	< 135 KHz	13.56 MHz [HF]	860-960 MHz [UHF]	2.45 GHz [Microwave]
Relevant Standards	ISO 11784 & 11785 ISO/IEC 18000-2 ISO 14223-1	ISO/IEC 18000-3 EPC Class-1 ISO 15693 ISO 14443 (A/B)	ISO/IEC 18000-6 EPC class-0, class-1	ISO/IEC 18000-4
Typical Read Range	<0.5m	~1 m	~4-5 m	~1 m
Tag Type	Passive-inductive coupling	Passive-inductive coupling	Passive or active	Passive or active
Typical Applications	Access control, animal tagging, vehicle immobilizer	Smart cards, access control, payment ID, item-level tagging, baggage control, biometrics, libraries, transports, apparel	Supply chain pallet and box tagging, baggage handling, electronic toll collection	Electronic toll collection, cold chain management, environment monitoring
Multiple Tag Read Rate	Slower → Faster			
Ability to read near metal or wet surfaces	Better → Worse			
Passive Tag Size	Larger → Smaller			

Table 1. Frequency characteristics of RFID systems. After [1]

Near-field coupling is typically produced at close-range distances and at lower frequencies, due to the magnetic properties of an induced current. Suppose there are two pieces of conductive material, or conductors, placed relatively close together. When a current is applied to the first (primary) conductor, the alternating movement of electrons forms a magnetic field around that conductor. Because this magnetic field was produced via the use of electricity, we call it an electromagnetic field. The electromagnetic field is polarized either north or south. When the second (secondary) conductor is brought within a prescribed distance of the first, the electromagnetic field induces electron flow (current) in the second conductor. Note that this second conductor had no electrical current to begin with. This is the foundational principle of Faraday's electromagnetic induction, which is key to the operation of passive tags. The new, induced, current in the second conductor has similar properties to the first. It has a measurable current, voltage, and frequency. The induced current is somewhat smaller than that of the primary due to less than 100% coupling efficiency, but enough energy is transmitted to perform electrical work on the secondary side.

Passive tags that operate via near-field coupling (Figure 2) use the energy gained from the above described transaction to perform some type of computation. They then transmit the result of this computation back via their own antenna (the secondary conductor in the above description), again generating an electromagnetic field. This time, however, the electromagnetic field induces a current on the reader's antenna (the primary conductor). If this current is the same as the one originally used to generate the electromagnetic field traveling from reader to tag, the reader will never be able to distinguish this new current, from the original one. So, the reader continually varies the current that generates its electromagnetic field via varying the load on its antenna coil. This technique is called load modulation. This variation in current can be seen as a variation in current on the reader's antenna coil, due to the mutual inductance between the two. One might assume that it would be more efficient for the reader to transmit energy, and then proceed towards a "listen mode" where it is not transmitting energy, so that any current received is known to be from a tag. However, passive tags do not contain any onboard power source. For tags to generate a current, and thus an electromagnetic field, strong enough to propagate back to the reader, continual energy must arrive from the reader. Additionally, a passive tag reader could potentially read tens, or hundreds, of tags concurrently. The wait periods accrued for "listen mode" can accumulate quickly and give rise to massive inefficiency.

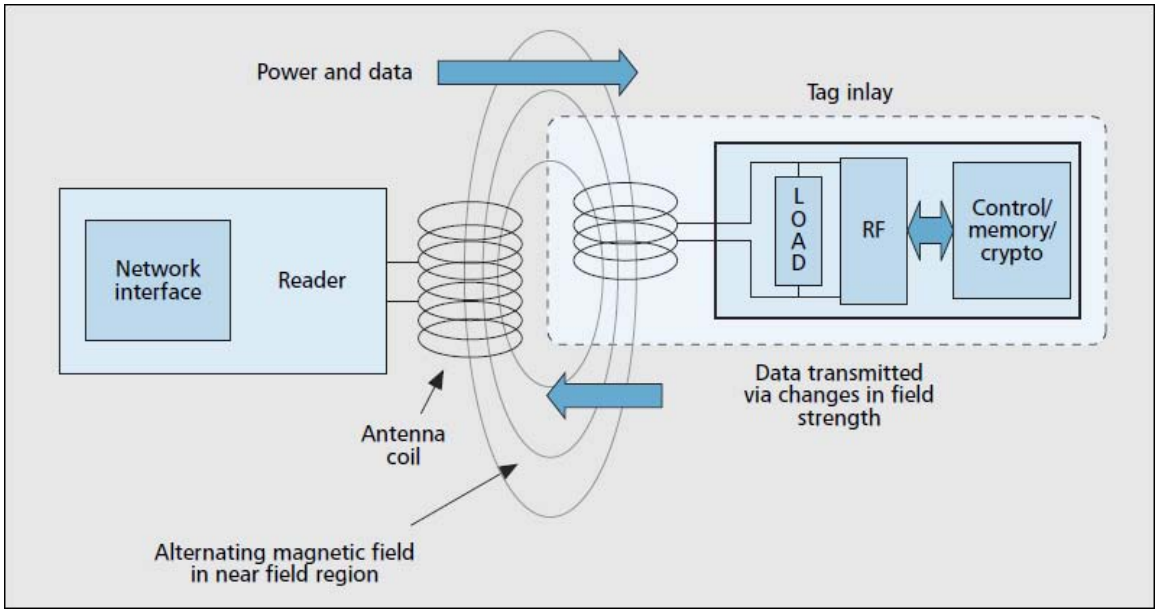

Figure 2. Electro-magnetic induction in relation to passive RFID systems. From [1]

Far-field coupling differs from near-field coupling in that there is no restriction on the field boundary [1]. The field boundary is the distance at which near-field coupling becomes inefficient, and far-field coupling becomes more attractive. In other words, this is the boundary distance at which the tag's modulated current cannot be seen in the antenna coil of the reader. In the equation below, $d_{boundary}$ is the boundary distance, c is the speed of light, and f is the frequency of the electromagnetic wave:

$$d_{boundary} = c / 2\pi f \tag{1.1}$$

Equation (1.1) shows the inversely proportional relationship of frequency to the boundary distance. Because of this, only higher frequencies are used in far-field coupling [5]. In other words, as the frequency of the electromagnetic wave increases, the boundary distance decreases, meaning that near-field coupling is only applicable at smaller distances between tag and reader. Thus, low frequencies lend themselves better to near-field power transfers at greater distances, while higher frequencies are more attractive for far-field power transfers, where greater distances between tag and reader are possible.

In far-field coupling, a current is applied to the primary conductor at (typically) a much higher frequency, due to (1.1). Again, this current creates an electromagnetic field that radiates outward. A portion of this electromagnetic field (a form of energy) is captured upon the second conductor as a potential difference [1]. Because higher frequencies produce greater amounts of energy, as will be explained shortly, far-field coupling does not require a dependence on the continual application of energy from one conductor to the next as in near-field coupling. The electromagnetic energy is high enough that it can be reflected back from the secondary (receiving) conductor. Intelligence can be reflected back to the primary conductor due to an impedance mismatch between the secondary conductor and whatever circuit it is connected to. By changing the mismatch with a varying load (load modulation), as in near-field coupling, the second conductor can encode a message on the reflected transmission. This technique is known as backscatter. The portion of energy not reflected back can be used for electric work, including varying the load on the antenna.

Far-field coupling (Figure 3) supports greater distances between an RFID tag and reader than does near-field coupling. This is due to the fact that signal attenuation, as a function of distance, is less dramatic with far-field techniques than with near-field techniques. The attenuation of the EM field in the far-field region is proportional to $1/d^2$, where d is the distance between tag and reader [5]. In the near-field this attenuation is $1/d^6$, a considerably larger value [1]. However, while the greater distances can be achieved due to reduced attenuation over distance, more energy must be dedicated to changing the impedance mismatch of the reflected wave. This starves the processing subsystem of crucial energy needed for complex computation. In this thesis, we will explore just how much energy is needed for computation.

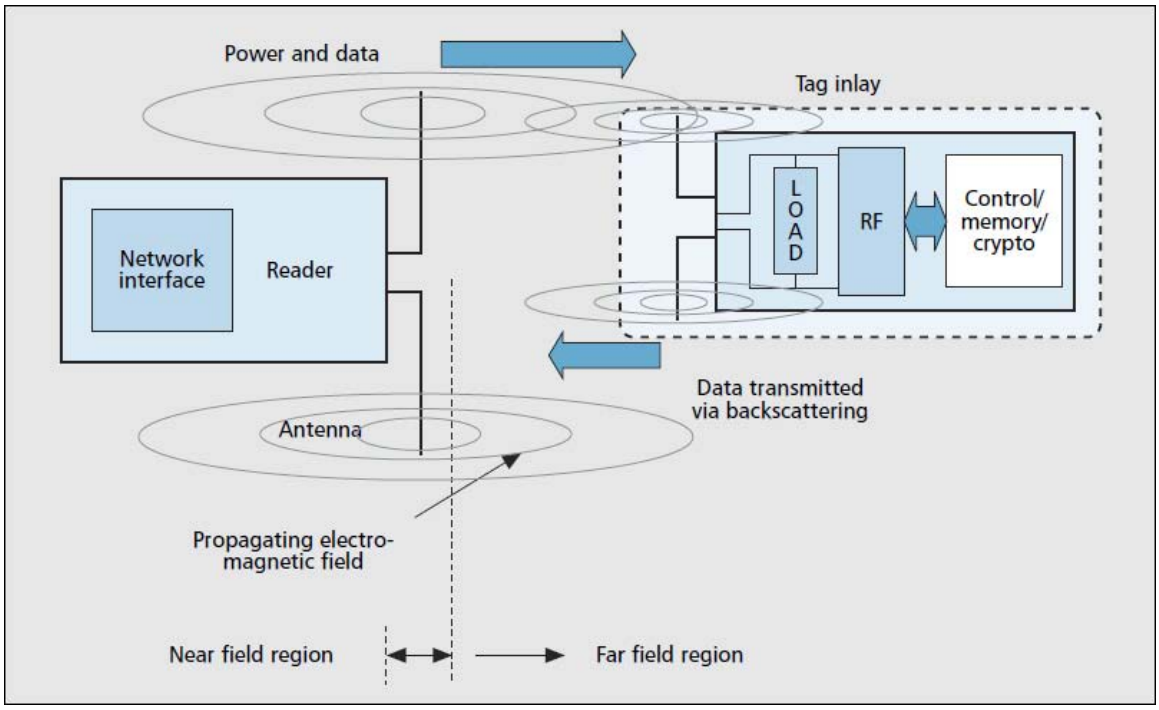

Figure 3. Far-field RFID interaction, otherwise known as backscatter. From [1]

A third methodology for the wireless transfer of operating power to passive tags is surface acoustic wave technology (SAW). SAW technology relies on an inter-digital transducer (IDT), which converts radio wave pulses into an airborne pressure differential, or acoustic wave, and vice versa. The inter-digital transducer relies on the piezoelectric effect and, thus, does not require a DC power source. First, an electromagnetic wave is transferred from reader to tag in the normal way. Next, the IDT converts the electromagnetic wave to an acoustic wave and propagates it across a tag's circuitry into a set of programmed reflectors. These acoustic reflectors are tuned only to react/respond to the appropriate frequencies and pulse widths of the original (sender's) signal. Their reflected signal is sent back through the transducer and transmitted again as a radio wave to the tag reader. This reflected signal usually will contain the EPC code of the tag. While SAW technology is already quite advanced, recent innovations in device miniaturization have allowed SAW RFID devices to be built even smaller and faster than their traditional silicon counterparts. Unfortunately, acoustic waves cannot be used for

complex computation because they deteriorate rapidly [1] and would not be a good choice for tag circuits, such as authentication mechanisms.

Closely tied to how a tag receives its wireless power, is how that tag uses the power to perform its computation. Passive RFID tags typically operate on the micro-watt scale, with 20 micro-watts being the notional mean among tags. Although as much as 1 watt of power can be transmitted in the near-field design, hardly any of that power is induced onto the tag's processing subsystem. Therefore, the circuitry on the passive tags must be efficient enough to not only use this power for generating a response, but also to broadcast that response back to the tag reader. Additionally, certain useful circuit components, such as a clock, are very costly in terms of their power consumption. Complex symmetric and asymmetric cryptography mechanisms also have hefty processing and power requirements.

Passive RFID technology operates in an area where a plethora of factors all work together to generate a result. The near- and far-field boundaries correlate a distance and frequency with how much power can be induced onto the tag itself. The storage mechanism for the induced energy must be small enough to keep the tag size, and thus the production cost, down while still being large enough to deliver voltage at the prescribed levels for the duration of the communication session. Finally, any security mechanism on the tag will add to the total amount of energy necessary. Conversely, for a fixed amount of power, the complexity of any security mechanism will be limited accordingly. The security mechanism is typically a single-purpose gate array instead of more power-hungry arithmetic-logic-unit (ALU) style circuits.

Currently, there are few passive RFID security mechanisms that are both in production, and have shown resistance to exploitation. In 2005 [6], a team from Johns Hopkins University successfully cracked a passive RFID tag with relatively simple brute force strategies. The tag they cracked, built by Texas Instruments, was used in thousands of Mobil gas station Speedpass pay-at-the-pump systems, as well as the keyed anti-theft security device used by Ford Motor Vehicles. In a relatively short amount of time, the Johns Hopkins team of graduate students not only brute-forced the encryption mechanism, but were also able to completely reverse engineer the passive tags' circuitry

so as to clone them. Their attack enabled them to demonstrate stealing a car and purchasing gas, all with a cloned RFID tag instead of the real one. The paper they published raised awareness of an issue not seriously considered before. That is, passive tags are so inexpensive and have such a disposable nature that their security was never given much priority. However, we now see passive tags used in a broader spectrum of environments and applications, many of which involve the access to information of a sensitive nature. Medical prescriptions, credit cards, and even luggage have been "tagged." These areas offer a wealth of information to any would-be attacker, far more than a free tank of gas. A security mechanism must be used that offers adequate protection while maximizing power economy and cost.

C. SCOPE OF THESIS

This thesis explores the technical considerations and limitations of passive RFID systems. Power generation alone generates a plethora of factors that must be analyzed and decided on before a passive RFID tag structure can begin to evolve. Additionally, physical proximity boundaries must be weighed, as well as the complexity of any security algorithm employed. Such analysis produces a measure of affordable complexity in a passive RFID system. This "affordable" complexity is a synergy of all the mitigating factors of passive RFID tag technology to produce a system that can provide a sufficient measure of authenticity. Ultimately, the question is *whether* a sufficiently secure authentication mechanism can be employed on a tag void of a native power source.

This thesis is organized into the following chapters. Chapter II covers the basic physical characteristics of an RFID system, as well as current physical characteristics of production-grade passive tags. A brief description is given of historical attacks against passive tags that have garnered massive success.

Chapter III addresses security concerns for a passive RFID system, in relation to secret key distribution, a roll-over keyset, and transmission requirements. Chapter IV proposes a lightweight tag authentication mechanism utilizing the SHA–1 hashing algorithm on a passive tag. In this chapter, several of the fundamentals of passive tag design are used as metrics for judging the effectiveness of the proposed mechanism. The

mechanism is scrutinized in order to satisfy the primary research question by showing that the proposed mechanism is sufficiently "lightweight," sufficiently secure, and operational via one of the aforementioned passive power delivery coupling schemes.

Chapter V is a discussion of the best practice uses of such a mechanism as proposed in Chapter IV. Also included, is a description of how the proposed mechanism satisfies the design criteria for a passive tag of this nature.

THIS PAGE INTENTIONALLY LEFT BLANK

II. PASSIVE TAG FOUNDATIONS AND CHALLENGES

A. AUTHENTICATION CAPABILITIES

Passive RFID systems can exhibit several aspects of authentication mechanisms. From a minimalistic point of view, passive tags can exhibit no authentication mechanism at all. In this way, a passive tag simply reports a serial number or other piece of information hardwired to the tag [7]. Neither the reader nor the tag authenticates the other device, so no real security mechanism exists. In order to properly authenticate either side (reader or tag) of the message exchange, one of the known factors for authentication must be used: something you know, something you have, or something you are. Some active RFID systems use the "something you have" factor for authentication, relying on a complex cryptographic function involving a public key infrastructure [8]. Calculations surrounding the public key systems are usually processor intensive and require a significant amount of power, neither of which is available to a passive tag.

Now consider a passive RFID system that authenticates both the tag and reader with a simple pre-shared key and cryptographic function. Every tag would need a copy not only of its own key, but a copy of the key for every reader in the system. In a passive RFID tag, the additional circuitry required for storing all this excess information, not to mention the cryptographic mechanism's additional power requirement, is far too extreme. Most passive tags avoid this by performing no authentication at all, as mentioned above.

In Figure 4, a simple tag authentication mechanism is shown. First, a challenge is generated from the reader. This challenge is a bit string of sufficient length and randomness so as to mitigate the possibility of a replay attack. Second, the challenge is sent to the tag, which uses one of the power capture methods mentioned in Chapter I to generate a response. The response can be generated with a simple XOR operation, shift cipher, or hash mechanism. It is critical to the response, however, for the response to involve some secret known only to the tag and reader (or back-end system, which is

available to the reader). Without the secret, the response could easily be analyzed and reconstructed by someone intent on subverting the authenticity of the tag's data. Therefore, the shared secret provides authenticity to the exchange. The third and fourth steps involve concatenating some identification string to the response to authenticate the tag. This identity string gives the reader a critical piece of information. The reader can now look up the associated shared secret applicable to that tag, and then process the sent challenge itself and compare the result with that received from the tag. If the response the reader generates is the same as the one received from the tag, then the tag is proven to be authentic.

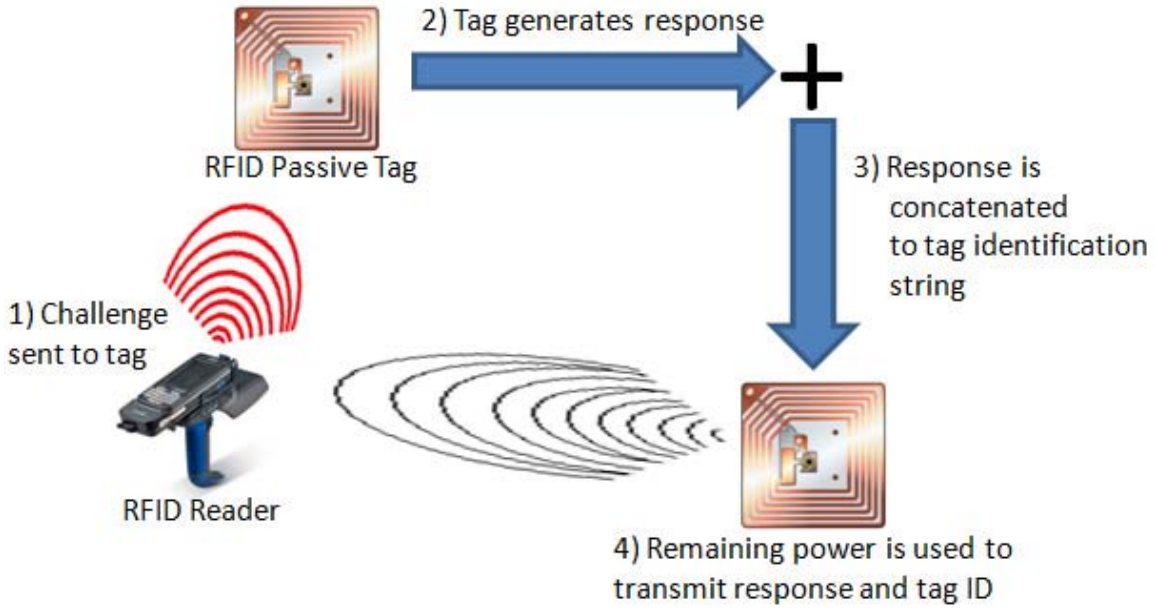

Figure 4. A simple authentication scheme for passive tags

Figure 5 defines the protocol flow illustrated in Figure 4. This model is the foundation for most passive tag authentication mechanisms. A challenge is sent from reader to tag, the tag computes a response, based in some way on the challenge and a shared secret, and the response is returned to the reader along with some identification string. The "tag_mech" is the security algorithm run on the tag and is the same as "reader_mech." Some passive tags such as those seen in [9] use a hash function for the

security mechanism. The mutual protocol in [9] is based on write-many passive tags that also include additional inputs to the hash function. Such a technique is known as salting the hash function. This salt is some additional input that makes the result of the hash function unique. A downside to the advantage of salting is that the passive tag must include some storage mechanism, such as flash memory cells, that can consistently be written and overwritten with a new salt value every time a tag and reader communicate. As will be discussed in Chapter IV, a sufficiently random challenge structure (C_{reader} in Figure 5) omits the necessity of using salt.

C = challenge
K = shared secret
P = result of security mechanism function (tag_mech or reader_mech)
Id = tag identification string
R = response string
1. C_{reader}
2. $\{C_{reader}, K_{shared}\}_{tag\_mech} \equiv P_{tag}$
3. $P_{tag} + Id_{tag} = R_{tag}$
4. Resolve Id_{tag} to K_{shared}
5. If $\{C_{reader}, K_{shared}\}_{reader\_mech} = P_{tag}$ then authentic

Figure 5. The logical flow of a passive tag authentication mechanism

B. CURRENT PHYSICAL CHARACTERISTICS OF PASSIVE TAGS

1. Near- and Far-field Power Generation

Several factors contribute to the power available to a passive tag. First, the choice between near-field and far-field power generation must be made before tag production. Most often, the goal of a passive RFID system is to maximize the amount of power able to be garnered at the tag from the reader to tag interaction. The choice, then, involves a number of factors to be considered such as frequency, wavelength, distance, gain, efficiency, and path loss. At first glance, it would seem that Planck's constant defines enough information to make this choice simple:

$$E = h\nu \tag{2.1}$$

Put simply, Plank's constant (h) in Equation (2.1) defines a relationship such that, as frequency increases (v), the amount of energy produced (E) also increases. Thus, the backscatter methodology, with the use of higher frequencies producing more energy, is more mathematically justified. However, higher frequencies are also considerably more directional, something difficult to control in an RFID environment. We can imagine a scenario where several boxes are stacked on a shipping palette, all with RFID tags. Some of the tags on these boxes are not directly within the line-of-sight of the RFID reader. This line-of-sight means that both the tag and reader suffer from no occlusion or obstruction inside the path between them. Higher frequencies, being more directional, require a degree of clear line-of-sight because absorption affects them more drastically. In this example, if the higher frequency electromagnetic wave from the reader must travel through several boxes to reach the one of interest, the signal could be drastically reduced when it reaches the RFID tag. The boxes and their contents, as well as any reflections of the wave, all absorb energy from the higher frequency, thereby reducing its ability to induce as much energy as when it left the reader. A lower frequency, on the other hand, does not suffer as much from absorption. Thus, a lower frequency arrives at the box of interest not nearly as degraded from absorption as the higher frequency. The advantages of using higher frequencies are not without the requirements of line-of-sight, or in other words, a minimization of the factors that contribute to absorption.

As we explore the advantages/disadvantages of using higher frequencies, we must also address the inverse relationship of frequency to wavelength. As frequency goes up, wavelength decreases, having effects of the size of the antenna used. Since antenna size is one of the more tangible elements controlled in the construction of a passive RFID tag, it is useful to see Planck's equation incorporating wavelength:

$$\nu = c / \lambda \tag{2.2}$$

$$E = hc / \lambda \tag{2.3}$$

Equation (2.2) is the mathematical relationship showing that, as frequency increases, wavelength decreases and vice versa (c is the speed of light). Thus, we can

create a new equation, Equation (2.3), that shows a relationship involving Planck's constant, wavelength, and energy. It follows from Equation (2.3) that, as wavelength decreases, the energy produced increases.

Up until this point, our discussion of the factors involved in power generation and the choice of near-field and far-field methodologies has been largely based around the RFID reader and the energy it is emitting. A more dominant factor, however, is the RFID tag's ability to receive the energy transmitted from the reader. From Equation (2.3), it appears we desire a smaller wavelength (i.e., higher frequency) for reader to tag communication in order to produce more energy. As noted above, smaller wavelengths are directly proportional to the size of the antenna used to receive them. Notably, smaller antennas are less capable of garnering as much current via electromagnetic induction as are larger antennas. So again, it seems that higher frequencies (smaller wavelengths and antennas) are unattractive for maximizing the energy received in the tag.

There must be some other factor that allows us to choose between near- or far-field power generation so as to maximize the positive aspects of higher frequencies (producing more power for complex computation), and mitigate the negative effects of smaller antennas. This factor is known as antenna gain. Antenna gain, or the measure of an antenna's directional intensity, allows antennas to achieve the best of both worlds. Succinctly put, increasing an antenna's gain allows it to more efficiently receive electromagnetic energy. The following equation (Frii's equation) provides the basic mathematical structure for measuring how much power is available to a passive tag, while incorporating the factor of antenna gain [3], [10]:

$$P_{received} = (P_{transmitted} \times G_{receiver} \times G_{transmitter} \times \lambda^2) / (4\pi d)^2 \qquad (2.4)$$

In Equation (2.4), $P_{received}$ is the power received by the tag, $P_{transmitted}$ is the power transmitted from the reader, G is the antenna gain, and d is the distance between tag and reader. At first glance, it would seem that maximizing wavelength, not gain, would have the greater effect on $P_{received}$, but this is incorrect due to the calculation for antenna gain ($G = 4\pi A_e / \lambda^2$). This new factor introduced, (A_e), is the effective aperture of the antenna, or the measure of the antenna's efficiency inside a specific medium (air, space, etc.).

$$P_{received} = (P_{transmitted} \text{ x } A_r \text{ x } A_t) / (\lambda^2 \text{ x } d^2) \quad (2.5)$$

Via substitution, Frii's equation can be modeled as in Equation (2.5) using the equation for antenna gain. We now see again that smaller wavelengths (higher frequencies) produce more power; this time with the inclusion of the measure of distance between tag and antenna, and the affective aperture (efficiency) of the respective antennas.

Antenna gain (and consequently effective aperture) can be achieved a number of different ways, but most popular is the looping of antenna elements (seen in Figure 6) so as to create an increased surface area for the captured wavelength. This increased surface area produces a semi-directional tag that maximizes the potential of higher frequencies. In turn, this maximizes the power received ($P_{received}$) at the tag.

Figure 6. The EPC "Butterfly" tag. From [7], [2]

Figure 6 portrays one example of maximizing the directional gain of the antenna in a passive tag. The "butterfly" tag attempts to maximize $G_{receiver,}$ and thus obtain more power at higher frequencies. This particular tag is tuned to 865–868 MHz and falls under the EPC Class 1, Generation 1 standard [2]. It is listed as having a maximum read range of 6 m, although it is probably somewhat less. Observing a typical operating scenario from Equation (2.4) with $P_{transmitted}$ ~ 1W (FCC maximum), $G_{transmitter}$ ~ 6 dBi, $G_{receiver}$ ~ 1–2 dBi (omni-directional), d ~ 6 meters, and a frequency of 915 MHz: the power

delivered to the tag ($P_{receiver}$) is ~ 100 μW. Considering that the operating environment often includes performance inhibitors, such as electromagnetic interference, fading, path loss, and noise, this is rarely the amount of power that can be expected to be received by the tag. Additionally, at the higher 865–868 MHz band, far-field coupling consumes a large portion of power in order to communicate via backscatter, as described earlier.

2. Power Consumption

The above section describes typical operating ranges for passive RFID tags with two interesting factors, $P_{transmitted}$ and $P_{received}$. While 1W is the maximum power ($P_{transmitted}$) approved by the FCC in regards to typical frequencies used for RFID transmissions, additional local or vendor specific regulations may apply. Some systems [11] cap the power transmission from the reader to just 10 dbM, or roughly 10 mW. Observing normal values as described earlier, this puts $P_{received}$ at roughly 10 μW, a drastic reduction from the previous estimation.

Unfortunately, merely calculating $P_{received}$ does not provide enough clarity to determine how much power is available to the tag-processing subsystem. Earlier, it was calculated that 100 μW of power is effectively applied to the tag from a 1W $P_{transmitted}$, however, it cannot be assumed that this amount of power is available to the tag's circuitry. A portion of this power is used to perform load modulation, clock signaling, and rectification. As will be discussed later, the rectification and conversion of the analog waveform is a costly process, which reduces the overall power available to the tag-processing subsystem. For this reason, a passive tag's processing subsystem must operate within a threshold, typically 20μW. The model described in [12] describes a circuit consuming only 16.7 μW, yet lacking any authentication mechanism. The 20 μW threshold can be raised, given the proximity factor (d) and other adaptations made to the variables in Frii's equation (2.4), such as $P_{transmitted}$, but serves as the floor value given normal operating scenarios (~6 meters max, single frequency, etc.).

Additionally, a notion of voltage must be considered. However, voltage requirements are highly entangled with IC design and layout. Many passive tags are structured around a 0.5 μm CMOS process, functioning off of an average 1.5 V [13].

Reducing this CMOS process, or in effect reducing the transistor size, could lead to a significant drop in voltage requirements. Unfortunately, a smaller CMOS process drastically increases the cost per tag.

3. Time and Charging Requirements

Effecting power upon a passive tag is only half of the equation necessary to establish communication from tag back to reader. An interesting question to broach is what temporal requirement must be satisfied between tag and reader. In effect, how long must the reader energize the tag for a successful transmission session? Thus, a transmission requirement must involve the time it takes for the reader to apply power to the tag, and consequently the time allotted for a passive tag to perform its computation whilst being powered. To this end, most passive tags employ some type of voltage sensor (as in Figure 7) for determining the amount of time necessary to gain a sufficient charge for powering the passive tag's processing subsystem [14].

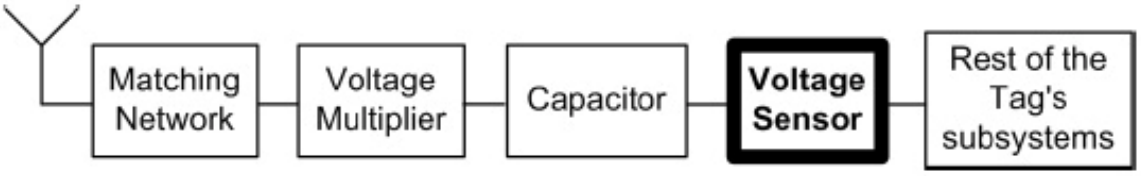

Figure 7. Logical depiction of RFID voltage sensor, which determines whether the system's capacitor is fully charged. From [14]

In Figure 7, a depiction is shown of the traversal of energy through an RFID circuit. First, RF energy is obtained via the antenna and drawn through a matching network on its way to a rectifier, in this case represented by a voltage multiplier. The matching network's job is to maximize the power extracted from the incoming RF energy and subsequently delivered to the rectifier. A rectifier's job is to convert AC voltage (in this case obtained via electromagnetic induction) into a DC voltage that can then be stored by a capacitor. Because the RF energy is constantly fluctuating when applied to the tag due to atmospheric conditions, electro-magnetic interference, etc., the matching network must be able to adapt and deliver a "cleaner" RF signal to the rectifier, thus maximizing the power delivered. Technically, the matching network is designed to

match the impedance between the RF energy and rectifier load, but this is outside the scope of this thesis. Regardless, as the rectifier produces a DC voltage, it is used to charge a capacitor. The capacitor stores this charge and discharges only when a voltage sensor has deemed the capacitor to contain sufficient charge to power the RFID tag's subsystem. The time it takes for a capacitor to fully charge, or the time until the voltage sensor is "satisfied," is a restrictive feature of passive RFID systems.

This time requirement creates a temporal restriction unique to passive RFIDs. The RFID reader must then remain in proximity with the tag for enough time so as to satisfy the voltage sensor. Currently, the United States restricts communication interactions occurring inside the 915 MHz band to a mere 400 ms, per session [15]. A session is the interaction between exactly two devices, or a one-to-one relationship. This restriction is typical of frequency-hopping techniques used by many radios and cordless phones. Passive tags typically respond to only one predetermined frequency, yet that same 400 ms restriction applies.

Thus, any security mechanism employed on a passive tag must gain the necessary amount of energy inside this 400 ms window. The traditional mechanism for storing energy in a passive tag is a capacitor, which has an associated time constant. We can use the time constant to judge how much time it would take to charge the capacitor. and whether that time is over the 400 ms window.

$$\text{time constant} = R \times C \tag{2.5}$$

Ex: $R=50k\Omega$, $C=20\mu F$, $RC= 1.0$ sec

Equation (2.5) shows the calculation of a capacitor's time constant for a relatively large resistance. Since the resistance inside a passive tag will typically be several orders of magnitude smaller, the time constant will also be drastically reduced. The smaller the time constant is, the less time it takes to charge the capacitor. Thus as the resistance is reduced, the time constant (and thus the charging time) can be brought inside the 400 ms window. The matching network and rectifier both work to clean and deliver DC voltage to the capacitor at this desired minimal resistance. This charging time can also be reduced by decreasing the C value (measure of capacitance), but such reduction is limited

due to the direct relationship between C and the amount of power the capacitor can store. Less stored power translates into less potential work by the tag's circuitry.

4. Hardware Clocking and Physical Layout

The hardware structure of an RFID tag's processing subsystem is critical to how power is efficiently moved throughout the structure of the tag in order to accomplish the desired function. A processing subsystem that includes too many one-time-use gate structures suffers both from large power consumption and an increase in time to completion. In other words, as the physical area of the RFID tag's processing circuitry increases, so does power consumption. Thus, the hardware structure must maximize the re-use of certain circuits to achieve efficiency. The primary components of a passive RFID tag are the antenna, some type of voltage conversion and storage mechanism, and the processing subsystem that is responsible for the security function. It is at this processing subsystem where circuit re-use has its advantages. The processing subsystem could output something as simple as the EPC standard of responding with a 96-bit identification code. Or, it might contain something as complex as the MD5 hashing algorithm and output a 128-bit hash string, as shown in Figure 8.

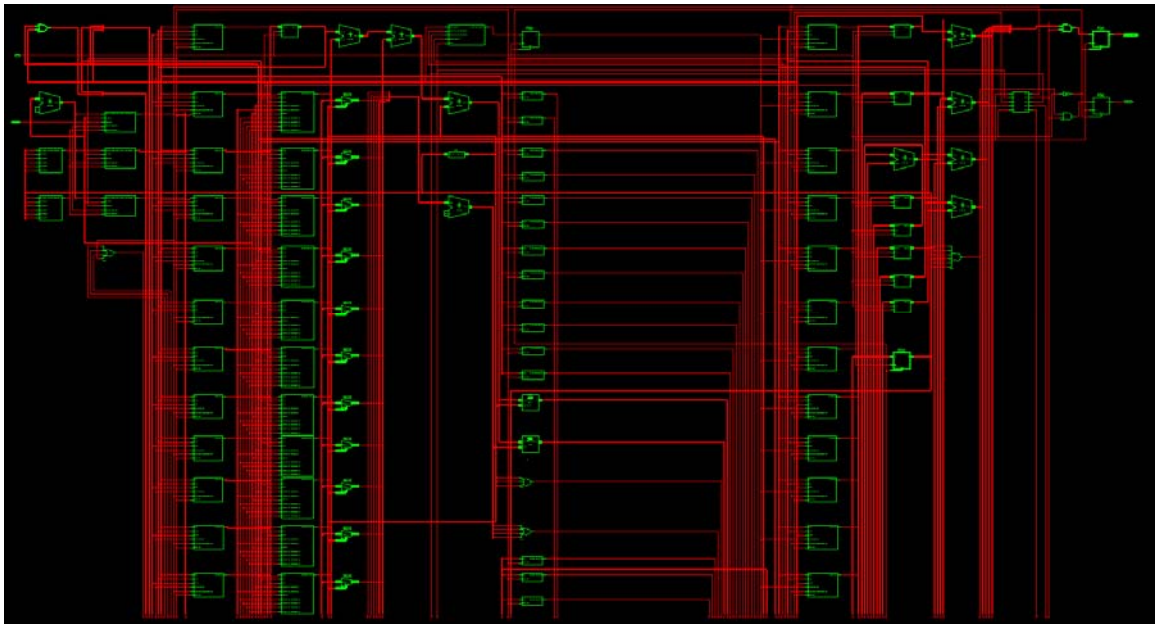

Figure 8. The MD5 hashing algorithm as simulated on a Virtex V XFT70, using Xilinx ISE tools

The above figure shows the massive complexity involved in building a security mechanism (MD5) into the hardware of a passive tag. Additionally, all that is depicted is the MD5 algorithm itself, not the control mechanisms that regulate clock speed, modulation, or CRC checks. Note that in Figure 8, there are several structures that look similar. These are the concatenation registers for each stage in the MD5 algorithm's execution. Depending on the implementation, a hardware implementation could have several one-time-use registers that waste power. Using one register continually is often a way to achieve circuit re-use and save power. It is outside the scope of this thesis to investigate the physical fabrication of one-time-use structures such as concatenation registers; however, they do elicit dependencies on the processing subsystem that must be explored. One such structure that must be explored is the clocking mechanism.

The clocking mechanism on a passive RFID is responsible for propagating synchronously-timed voltage through the processing subsystem at the appropriate intervals. If the clock is too fast, certain gates may not complete their function before the subsequent clock cycle arrives, thus disrupting the overall circuit's proper execution. If the clock is too slow, energy is wasted while the processing subsystem "stalls" (energy is expended from the capacitor, yet no circuit work is being done).

The clock mechanism on a passive tag can be designed in one of two ways. First, the clocking structure can be pulled directly from the carrier wave of the RF energy received by the tag. When a clocking scheme is encoded onto the carrier wave, this is known as a derived clocking technique. The clock signal then is essentially relayed directly to the processing subsystem. Manchester and PIE encoding [13] are popular methods for encoding a clock signal within the carrier wave from reader to tag. This method offers a drastic reduction in chip circuitry and power consumption. Unfortunately, a derived clock signal is also inherently dirty. Due to propagation loss and noise in the transmission of energy from reader to tag, the clock signal can be skewed, especially over long distances. Thus, while a derived clock signal is more electronically affordable, it may not always be the most reliable.

The second way to generate a clock signal on the tag is via the use of an inductive oscillator. This method avoids the dirty signal obtained from a derived clock signal, but

also has a drawback. An inductive oscillator must be powered from the energy stored in the capacitor on the tag. This reduces the power available to the processing subsystem, thus reducing the complexity of the operations able to be performed by the subsystems' circuitry. This could equate to a minimalistic hash function of low bit strength, no ability to use a secret key, or other factors crippling to properly authenticated communications. An inductive oscillator (as seen in Figure 9) also requires a higher circuit footprint on the tag itself than the circuitry needed for a derived clock signal. As stated before, a higher physical area consumes more power; a basic property of power consumption in relation to ICs.

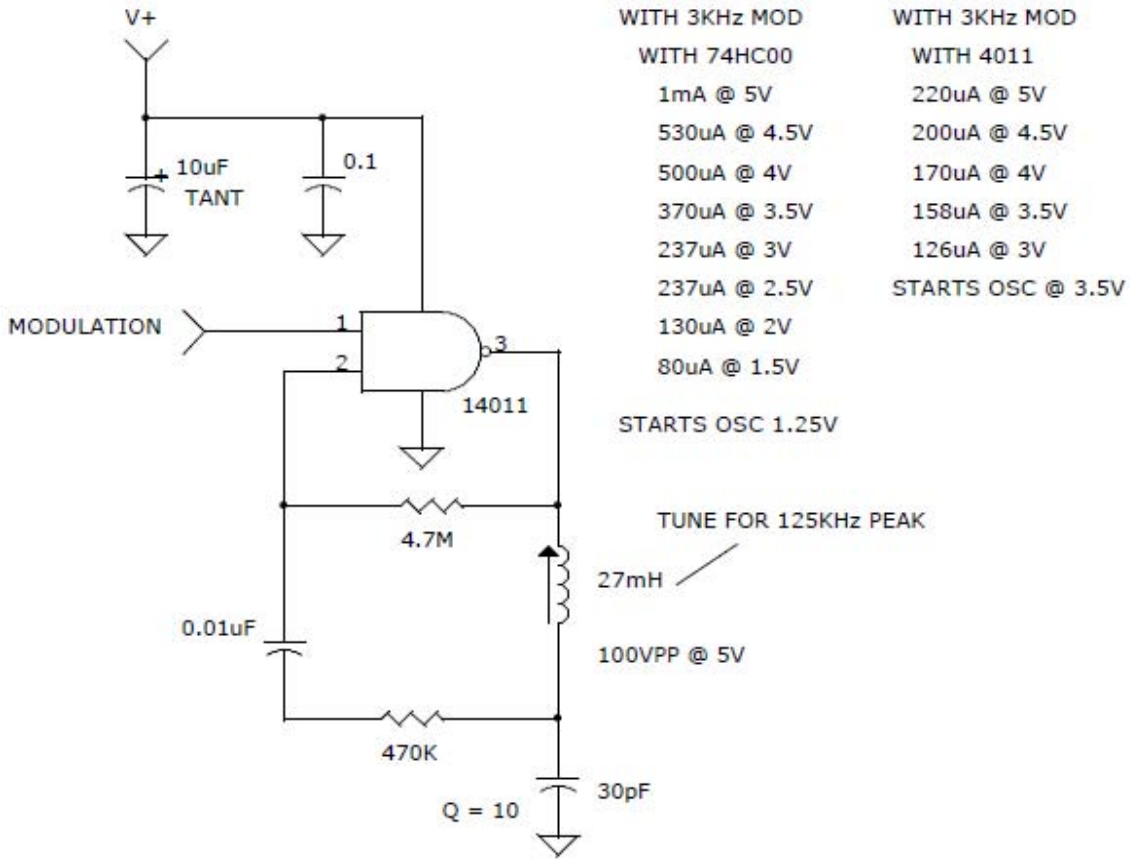

Figure 9. An inductive oscillator for passive RFID tags (125 KHz band). After [16]

The above figure shows the circuitry involved in building an inductive oscillator. Overall, the components are quite simple and can be replicated quite compactly in a passive RFID tag, often under .18 μm. However, the additional logic required to control the oscillator's cycling and modulation represents an extreme cost of both power consumption and time in passive RFID communication. This particular model is a gated oscillator. Gated oscillators can be "turned on" via some external mechanism (such as a throttling voltage sensor), thus consuming no power when the tag does not require any clocking mechanism. Examples are the periods of time when the tag is charging and transmitting.

Currently, a hybrid scheme is most often found in passive RFID tags. In this way, the carrier wave of the RFID reader is encoded with a clock signal as described earlier. This derived clock signal is then passed to some separation oscillator. This special oscillator generates two signals, one sufficiently lower than the other. The lower signal is used to clock the digital circuitry, or the tag-processing subsystem. The higher signal is used to clock the sampling frequency of the returning transmission from the tag. Because a lower clock signal (typically 100 KHz) is used to drive the tag's digital subsystem, less power is consumed. Overall, this is currently the most efficient way to drive digital circuits aboard passive RFID systems. Most often, passive RFID devices (and passive electronics in general) operate at clock frequencies between 32 KHz and 135 KHz [6], [10].

C. SECURITY MECHANISMS

1. Symmetric and Asymmetric Design Criteria

For properly authenticated communication sessions, the use of some keying mechanism is critical. Two methods exist in this realm: asymmetric and symmetric key systems. Asymmetric key systems are typically referred to as public key systems; where each public key has a related private key that is never shared, whereas the public keys can be freely distributed once they have been certified. Asymmetric keys are widely used in public key infrastructures (PKI) where additional criteria such as signatures and certificate authorities are required. Only via the use of power-hungry, complex

cryptographic techniques such as Diffie-Hellman or RSA [17], can PKI be implemented and asymmetric keying techniques be employed. Public key cryptography is thus too involved for an application in passive RFID communications. The verification process alone involved in authenticating a public certificate requires a hashing operation that exceeds 20 mW on a typical x86 architecture. The x86 architecture is the standard instruction set for 32-bit desktop and laptop processors made by companies such as VIA, Intel, and AMD. Obviously, this processing capability far exceeds that which can be implemented on low-cost, extremely low power RFID tag.

Symmetric key systems are far more attractive for their applicability to passive tags. Symmetric keys do not require complex cryptography to be verified and thus are much more applicable to low-power applications. Symmetric keys do require the same protection as do private keys in asymmetric keying systems, but possession alone usually guarantees authenticity (via the use of some security verification procedure). Symmetric keys, for instance, can be used as input to a hash function thereby adding authenticity to the hash function's output. As long as the symmetric keys are shared by all participants communicating together, then each participant can use the same hash function to generate an output. The comparison and eventual equality of keyed-hash outputs provides a level of authenticity largely commensurate with the protection afforded the underlying keys. In an RFID network, the symmetric key must be stored on each tag in the network, and also on the reader, or at least a back-end network database that the reader interacts with. The use of a single pre-shared key throughout an RFID network represents an extreme security risk, however.

For instance, if all RFID tags shared the same symmetric key in a network, and that key was used in a basic authentication mechanism such as depicted in Figure 5, an attacker would merely have to sit and watch a single authentication session between tag and reader to ultimately brute-force attack the exchange and determine the key for the entire network! Since a passive tag system could typically read thousands of tags in a short amount of time (eg. logistical tracking), the attacker could garner thousands of message exchanges between tag and reader, thereby statistically reducing the complexity

of such an attack. This was the case for attacks against the Wired Equivalency Protocol (WEP), used in wireless computer networks.

So, most symmetric key systems do not replicate the key amongst participants. Each participant, or RFID tag in this case, has a different key. It is up to the reader to manage all the keys in the system. Via the use of a tag authentication scheme such as a hash algorithm, the reader can validate the tag's shared key. Such a system is depicted below in Figure 10:

C = challenge
K = symmetric key, unique to tag
P = result of hash function
Id = tag identification string
R = response string

1. C_{reader}
2. $\{C_{reader}, K_{tag}\}_{hash} \equiv P_{tag}$
3. $P_{tag} + Id_{tag} = R_{tag}$
4. Resolve Id_{tag} to K_{tag}
5. If $\{C_{reader}, K_{tag}\}_{hash} = P_{tag}$ then authentic

Figure 10. A symmetric key authentication mechanism for passive RFID tags utilizing a hash function.

Figure 10 is similar to Figure 5, although a unique symmetric key is used on a per tag basis. Additionally, the tag_mech security function is enforced via some hash function. This hash function could be as simple as a 4-bit output or as complex 160-bit output as in the case of SHA–1. When authentication keys are added to the input of a hash function, the resultant output is referred to as a message authentication code or MAC. This is also sometimes referred to as a message integrity code or MIC. It is the goal of this thesis to investigate whether a sufficiently complex hash function is supportable on passive RFID tags given their limited operational power.

2. Hash Authentication Algorithms

Hash algorithms are within the scope of passive RFID systems. They can be integrated into a MAC scheme for authentication, but do not suffer the power and complexity requirements of a public key system.

In [18], a simulation of the SHA–1 algorithm is performed on a Xilinx FPGA circuit and the power consumption is displayed in Table 2.

Technology	Area (gates)	Power consumption		
		@ 10 MHz	@ 1 MHz	@ 100 kHz
Samsung 0.25 µ	10,641	1.68 mW	93 µW	19.5 µW
Hyundai 0.25 µ	10,382	1.069 mW	97.7 µW	14.1 µW

Table 2. Power consumption of SHA–1 simulation. From [18]

This simulation is then further replicated onto two different CMOS platforms, from Samsung and Hyundai, both at 0.25 µm. Currently, it is feasible to employ an even smaller manufacturing process (such as 130 nm, or .13 µm) on a passive tag, but the. 25 µm process comes at a reduced cost, something critical to passive RFID tag construction.

The techniques used in [18] are notable in that the authors emphasized the re-use of critical components in the SHA–1 algorithm. A single 32-bit adder and pipelining of SHA–1's "round" functions contributed to a significant drop in power.

In [19], a simulation is presented of the Advanced Encryption Standard (AES) cryptographic protocol for a passive RFID environment. This simulation of AES has been altered to take advantage of re-use in the ten iterations of the round function, the heart of most symmetric ciphers. However, the algorithm proposed can only accept an input of 128 bits, along with a 128-bit round key, similar to a symmetric key used in MAC protocols.

The low-power SHA–1 core presented in [18] uses a 512-bit input, considerably larger than both the input and round key of the AES simulation proposed in [19]. This higher bit count significantly increases the complexity of any brute force attack against it. So, any cryptographic function used in an authentication mechanism implemented on a passive RFID tag must be complex enough (a high bit count and even distribution of

outputs) to be sufficiently resistant to a brute force attack. While known complexity attacks do exist on algorithms such as SHA–1, the frequency of a hash collision in these attacks is 1 in 2^{69} [20]. This frequency is sufficiently small to make SHA–1 an attractive algorithm for implementation in a passive RFID system.

Any authentication mechanism employed in a passive RFID system, whether using a hash function or encryption algorithm, must also have a notion of timeliness. As described earlier, the clocking mechanism is highly crucial to the successful propagation of energy through the tag's processing subsystem. The encryption algorithm in [19] operates from a derived clock signal (reduced) of 100 kHz and consumes 1,016 clock cycles. This equates to a time consumption of ~ 10 ms. Given the FCC standard of 400 ms for the 900 MHz band; a 10 ms time consumption for computation is well within reasonable limits. Unfortunately, the AES standard achieves its high level of efficiency by using expensive Electrically Erasable Programmable Read-Only Memory (EEPROM) technology. EEPROM can potentially raise the price of the tag to an unaffordable level. Now consider the implementation of the hash function in [18]; this implementation consumes a mere 330 clock cycles and requires no EEPROM memory. While the specific implementation does not include any notion of a pre-shared key for use in an authentication scheme, it is evident that the hash algorithm is more attractive for use in passive RFID tags owing to the much lower cycle count.

D. KNOWN VULNERABILITIES

1. Exxon Mobil SpeedPass

Passive tags represent an area of increased attack in recent years. Since they are unpowered, they are often void of power-controlled tampering mechanisms designed to thwart intruders. They cannot perform complex cryptography that increases the chance of an attacker being able to brute force their authentication protocol. The low cost of passive tags makes them affordable not only to the user, but to the attacker who means to exploit them. The attack described in [6] is notable because it has taken advantage of all these aspects of passive tags.

In 2005, a group of graduate students from Johns Hopkins University successfully exploited a Texas Instruments passive RFID tag, known collectively as the Digital Signature Transponder 40 (DST40) [6]. The DST40 is used in Mobil SpeedPass™ payment keys and the ignition keys of 2005 Ford motor vehicles. In both keys, the user brings their DST40 within a few centimeters of the tag reader either located in a gas pump kiosk (SpeedPass) or the ignition system of their vehicle (Ford). During the initial communication establishment, the DST40 emits a 24-bit identification string to the reader, whereby the reader generates a 40-bit challenge, sent back to the tag. The DST40 encrypts this challenge using its symmetric key and returns a response back to the reader. The response is formatted differently depending on which system (Mobil SpeedPass or Ford vehicles) is used. In the Mobil SpeedPass system, the response is truncated to a mere 24 bits, significantly reducing the uniqueness of the encrypted response.

Using a rough schematic of the DST40's logical construction, the Johns Hopkins team was able to recover the secret key on an arbitrary DST40 tag using just two observed challenge-response pairs. The students successfully observed those challenge-response pairs using a rudimentary Texas Instruments 2000 Low Frequency RFID Kit. Going further, they then created lookup tables for an arbitrary challenge-response pair that could forge an appropriate response based on an arbitrary key. These lookup tables were based on 16 paralleled FPGA devices and could compute the lookup tables in under an hour.

The DST40 attack was notable in that most of the work was done without physical access to the tag's processing subsystem. The team discovered all their results by simply sniffing the message exchanges out of the air. Using the logical diagram of the DST40, they were then able to replicate the circuitry of the DST40 tag identically. They discovered that the DST40 used a type of encryption known as a feedback shift register. The Texas Instruments DST40's particular implementation of the feedback shift register was proprietary, meaning not publicly available and operating under the theory of "security through obscurity." Feedback shift registers, while not reversible, are a very basic form of cryptography used for encryption. Inputs are combined together using operations that are typically not reversible in multiples, such as "and" and "nor." The

generated output in then used as input to the same operation but with an additional input not yet seen. Feedback shifting, then, is the process of using input from the resulting output of a previous state. The DST40 generates a 40-bit output, but is truncated in the Mobil SpeedPass system. This truncation is the equivalent of having to only guess the first four characters of a user's 16 character password in order to gain entry to a secure system.

The DST40 was thus proven to be a weak implementation of a secure passive RFID authentication protocol, via its use of "security through obscurity" and truncated responses. The Johns Hopkins team was able to successfully clone a passive tag and purchase gas, as well as "hot-wire" their Ford automobile.

There are several lessons learned from the DST40 exploit, some of which are identified in [6]. Most notably is that any authentication mechanism employed on a passive tag must not suffer from the "security through obscurity" approach to devising secure protocols. The authentication mechanism should be a standardized, publicly scrutinized algorithm of sufficient key strength (bit length). Additionally, the truncation of response messages from challenge-response generation should be avoided. Enough power must be conserved in the production of the authentication response so as to not reduce the entropy of the encrypted response.

THIS PAGE INTENTIONALLY LEFT BLANK

III. RFID SECURE AUTHENTICATION CONCERNS

A. AFFORDABLE COMPLEXITY

1. Definition-in-Terms

An interesting question to broach before designing any authentication scheme for a passive RFID tag is whether that authentication mechanism can achieve affordable complexity. This notion of affordable refers to whether the proposed authentication mechanism is low enough in power consumption to be employed on a passive tag. We already know that a rough estimate for the power consumption of a tag's processing subsystem is 20 μW. This power consumption is directly tied to the operational clock frequency of the passive tag. Most passive tags in production today, if they include any processing capability at all, clock themselves in the kilohertz range [6], [10], [19] . One hundred KHz is a rough estimate for the clock frequency that is applicable to passive tags. Thus, affordability can be defined numerically. If the proposed authentication mechanism, operating at a clock frequency ~ 100 KHz, consumes no more than 20 μW, then it is affordable and is justified for use in a passive tag.

The above qualification, however, is void of any notion of cost. Cost must—of course—also be considered in the assessment of affordability of the authentication mechanism. If passive RFID tags are meant to be produced en masse, for instance, on the order of 15,000 tags, then the cost must be sufficiently minimal. Typical passive tags marketed for inter-operation with the EPC standard (which has a minimal processing capability requirement) are on the order of $0.05 to $0.10 per tag [3], [21]. However, while the EPC standard includes clearing, locking, and cyclic redundancy check processing capability, it is void of any complex authentication mechanism that requires a larger processing capability. Obviously, the incorporation of an authentication mechanism would drive the cost of a tag up considerably. Thus along with the power and

clocking requirements described above, a passive tag with an onboard authentication mechanism should involve some notion of cost and not exceed outside this boundary of $0.05 to $0.10.

Closely tied to cost is the choice of a manufacturing process for a passive tag. The larger the manufacturing process (for instance, .5 μm compared to 130 nm), the less expensive the tag is to manufacture. However, a larger manufacturing process also consumes more power per unit area, so this may not always be the most effective choice. Additionally, certain manufacturing processes are optimized for high radio-frequency (RF) environments such as the IBM Conductive Carbon Nanotube Composite (C-CNTC) 32 nm process. This chip is designed to suffer minimally from RF interference such as in RFID environments, but comes at a high cost. The choice of a manufacturing process represents a step in the natural progression from algorithm design to the creation of an ASIC, and thus cannot be abstracted away when trying to determine whether any RFID mechanism attains affordable complexity.

2. Design Progression

Assuming the above-listed specifications must be met, the design and integration of an authentication mechanism into a passive RFID tag proceeds in this way: 1) A high level language (HLL) design of the authentication algorithm is written in a hardware programming language such as Verilog or Very High Speed Integrated Circuit Hardware Description Language (VHDL). 2) This "hardware code" is simulated to see if the authentication proceeds as described in Figure 10. The output of such an authentication must be mathematically correct. 3) If so, the hardware code can then be synthesized to either an FPGA or ASIC circuit design. The synthesis process optimizes the circuit for whatever manufacturing process was chosen. This step has the greatest effect on the overall power consumption of the device and its corresponding monetary cost. Certain manufacturing processes run more efficiently at lower clock speeds; can be better optimized with logical gate constructions; suffer less from RF interference, etc. 4) Software emulation of the composed circuit can now be performed on the synthesis, producing values such as power consumption at particular clock speeds, gate level design

criteria, and circuit parallelism. 5) Finally, if the synthesis produces results within the limits of a passive RFID tag, the circuit design can be "burned" into the same FPGA or ASIC chosen in Step 3. Production en masse can then ensue.

While verbally lengthy, the above-listed steps are actually quite simple to complete. At Step 4, software tools can allow us to estimate power consumption of the proposed authentication mechanism quite easily. No two syntheses between different manufacturing processes will result in the same circuit design; thus, it behooves the creator to pick a manufacturing process and continually adjust elements of the design to obtain the desired measures of power consumption, clock frequency, and timely output (referring to the 400 ms window imposed by the FCC).

It might be interesting to explore a particular industry standard for passive RFID tags in use today, and then mathematically deduce the per-gate power consumption of that (standard) tag's processing subsystem. Ultimately, the goal would be to determine the power consumption of a new RFID tag design (including an authentication mechanism) by multiplying its (assumed larger) gate count by the per-gate power consumption of the standard design. Unfortunately, this calculation suffers from an incorrect assumption. Namely, an industry standard reference design is not applicable to the plethora of different passive RFID circuits in use today. An RFID processing subsystem chip uses a manufacturing process that is particularly well suited to the circuit that it is to employ. Once an algorithm is written in Verilog or VHDL and then synthesized to a circuit design, a particular manufacturing process is chosen that best meets the needs of that design. Some manufacturing processes have a deeper execution pipeline, more input/output registers, or a more minimalistic clocking mechanism. This matchup between manufacturing process and circuit design attempts to maximize efficiency or, using a previously-defined term, attain affordable complexity. Thus, the creation of a new authentication mechanism, and its corresponding synthesis, may not gain the best measure of efficiency by calculating its power consumption according to some standard design.

Overall, the design of an RFID authentication mechanism must follow the normal step-wise progression. Using mathematical abstractions to estimate power consumption,

while an interesting approach, ultimately does not provide the precision needed for the judgment of "affordability" for such a design in a passive environment. Using synthesis tools for a specific manufacturing process well suited to the proposed circuit design, gives a more accurate picture of real world power consumption.

B. KEY DISTRIBUTION

1. Roll-over Key Set Expiration and Management

We have previously shown that hash algorithms are a justified means of accomplishing authentication, via the use of a MAC scheme. Furthermore, they lend themselves better to a passive RFID environment than complex encryption schemes due to their smaller size and lack of dependency on random number generators, logarithmic computation, etc. So, a MAC scheme utilizing a hash algorithm is the logical choice for the passive RFID environment. Yet, what are the security concerns for the symmetric key used in the MAC scheme? If tag level production meets or exceeds 15,000 tags, how do the symmetric keys emblazoned on each tag need to be distributed so as to be sufficiently resistant against attack?

We can answer these questions by considering what an attack against the MAC scheme aboard an RFID device might entail. The attacker would first need to intercept/record a MAC-authenticated communication session between reader and tag. Then, the attacker would separate the challenge message, hashed response, and identity number of the tag. Since the MAC protocol relies on a publicly-available hash algorithm, the attacker could make key guesses that are hashed together with the intercepted challenge until a match (i.e., same as the tag's MAC reply) is found. A match indicates that the attacker has discovered a key that will likely permit the attacker to authenticate a cloned tag that has the same EPC code (or similar data string unique to that tag). We are careful to say "a key" here rather than "the key" as hash collisions are possible that may have resulted in a false-positive regarding the attacker's discovery of a key that results in the same MAC as that which was intercepted. Stated more formally: $\text{hash}(\text{key}_{\text{Real}}, \text{challenge}_{\mathbf{1}})$ may be the same as $\text{hash}(\text{key}_{\text{Guessed}}, \text{challenge}_{\mathbf{1}})$; however $\text{hash}(\text{key}_{\text{Real}},$

challenge$_2$) may *not* be the same as hash(key$_{Guessed}$, challenge$_2$). To be certain of discovering "the key," the attacker would need to exhaustively try all keys in the key space to ascertain if there are any other apparent correct keys. Certitude that the attacker has discovered "the key" would come after intercepting additional challenge-response communications and testing which of the candidate keys worked with the additional intercept(s). This scenario seems trivial until a time computation is calculated. Consider that the challenge from reader to tag is 256 bits, and the pre-shared key is also 256 bits. Thus, the construction of a hash table would need 2^{512} independent comparisons. It is known that hash collisions of the SHA–1 algorithm can occur every 2^{69} iterations but, fortunately, this does not help the attacker. Instead, this would only garner multiple instances where the observed communication session matched up against results from the hash lookup table. The time to find such instances in a massive hash table would surely exceed the lifespan of any would-be attacker.

Key length then is incredibly important to increasing the resistance against a cloning attack, and is the biggest factor in establishing the "complexity" aspect of the affordable complexity desired of a passive RFID authentication scheme. Randomness of the challenge should also be considered. If the challenge sent from reader to tag is not sufficiently random, this drastically reduces the complexity of any brute force attack. So, randomness and key length affect the complexity of any attack against an RFID authentication mechanism using a hash-based MAC scheme. Unfortunately, increased key (bit) length of the challenge increases the amount of transmission time from reader to tag. Calculating the time to transmit a single bit, per usable frequency, while incorporating the factors that could degrade the transmission, is outside the scope of this thesis. It suffices, however, to set as an upper limit a bit string that can be transmitted inside a 400 ms window, since that is an operational constraint. We will then "plug" this into our HLL/VHDL model and see what challenge bit length results, then assess the overall security from that point.

It is within the scope of this thesis, however, to address how the length of the symmetric key is affected by a "roll-over" key management scheme. In a roll-over scheme, the symmetric key space is determined by key length. So, in the case of a 10-bit

symmetric key used for passive RFID tags, all the keys would have been used up after 1,024 tags have been produced. Thus, it makes much more sense to use a key of sufficient length (increased key space size) so as to mitigate the effect of a roll-over key management scheme that produces multiple tags with the same symmetric key. For instance, the use of a key with length 128-bits would roll-over after ~3.4 x 10^{38} tags have been produced. Considered independently, these ~3.4 x 10^{38} tags (a single 128-bit key per tag) equate to ~4 x 10^{25} terabytes of storage in the traditional rainbow-table generation process. The enormous size of this rainbow table would be something incredibly challenging using today's technology.

C. SECURE CHANNEL TRANSMISSION REQUIREMENTS

1. Real-time Tracking

An observation attack against a passive RFID environment is most successful when the response sent from tag back to reader is a plain-text serial number used for tracking as in the case of the EPC product codes. In this scenario, an attacker can observe that serial number easily and use it to track the movement of the RFID tag from place to place. Unfortunately, the use of an authentication mechanism on a passive RFID tag does not inhibit this attack, and is outside the scope of this thesis.

When an RFID reader receives the hash response from an RFID tag, it must also receive the identity of the tag in plain text so as to enable the lookup process of that particular tag's symmetric key. Not receiving the tag's identity would make the lookup process by the reader incredibly complex. Thus, the tag's identity must be transmitted in plain text along with the hash response for proper authentication of the tag. By simply observing this tag identity, an attacker can perform real-time tracking of the tag. Luckily, the authentication scheme does prevent cloning and/or replay of the tag to reader.

2. Provision against Spoofing

Another attack method is a spoofing attack, whereby the attacker impersonates a valid RFID reader so as to gather up many different communication sessions. Since, as

noted previously, an authentication mechanism aboard a tag that authenticates the reader is too computationally expensive for a passive RFID environment, this spoofing attack can be accomplished quite easily. This is of little concern here, as we are not focused on providing confidentiality of the EPC (or whatever data) code held by the RFID tag. Any reader can learn the EPC code of any tag. So long as these spurious readers do not have access to the legitimate readers' back end database and, thus, cannot discover tag keys, we can accept the reader impersonation problem as inconsequential.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. A MODEL FOR SECURE PASSIVE TAG AUTHENTICATION

A. DESIGN GOALS

The proposed design of a passive RFID authentication mechanism must meet the design criteria outlined above. First, the mechanism must attain affordable complexity as described earlier. This design goal encompasses a number of factors including power consumption, choice of manufacturing process, logical gate quantity, etc. Second, the mechanism must appropriately accomplish a MAC authentication scheme, via the use of a pre-shared key and publicly scrutinized hash algorithm. Third, the authentication mechanism must do all this within the physical boundaries of passive RFID tag interaction. Namely, the challenge/response scenario must take place within the 400 ms window, not consume more than 20 μW of power, and use the appropriate frequency that enables the accomplishment of these requirements.

At the heart of this authentication mechanism is the hash algorithm itself. Other devices onboard the passive RFID tag all have an effect on affordable complexity, but none is more crucial than the hash algorithm and its corresponding circuit. From [11], [12], [18], and [20] we can estimate that the power consumption of the processing subsystem should not exceed 20 μW. We can model all other devices quite conservatively by using a previously contrived example. Using our 900 MHz band (far-field only), we can theoretically generate 100 μW of power onto the passive tag, some of which is consumed by the rectifiers, load modulator, clocking mechanism, etc. Subtracting out the processing subsystem's consumption, this leaves 80 μW of power for those additional devices. It is outside the scope of this thesis to determine their actual power consumption, even in a synthesized FPGA circuit, so our assumption must suffice. The 20 μW left for the processing subsystem must power the hash function and its corresponding inputs. We can abstract away the power consumption of the two inputs because the pre-shared key, is permanently stored in the chip, and the challenge message is not generated by the chip at all. Thus, our ultimate design goal for the processing subsystem is a power consumption of no greater than 20 μW.

B. HARDWARE ARCHITECTURE

For this implementation of a low-power hash algorithm for a passive RFID device, the choice between FPGA and ASIC design is difficult. ASICs can be mass produced at a significantly lower cost than FPGAs. However, successful synthesis of the ASIC circuit design requires several fabrication templates (or masks) to be produced. These fabrication templates are physical, "burned" syntheses of the proposed circuit, according to a specific manufacturing process. Templates can become quite costly before production begins as circuit designers constantly tweak and alter circuit-specific settings such as clocking, gate pre-charge delay, input control, etc. Each change produces a different template, which must be fabricated, and thus a cost accrued. FPGAs can be reconfigured and changed without successive template generation. Designers simply change a setting, re-synthesize, and re-program the FPGA, all without wasting costly silicon on an inappropriate ASIC design. When ASIC fabrication can cost upwards of $10,000 per template (excluding the per-unit recurring costs), FPGAs become much more attractive as their cost is a one-time fee (per-unit) as low as $0.99 [22].

In this model, we will consider an FPGA design because of the numerous changes that can be made in pursuit of low power consumption. The Actel Igloo family of FPGAs can consume as little as 5 μW of power for associated designs, while being clocked as low as 1.5 MHz. In the scope of passive RFID design, we desire a clock speed significantly lower, but this can only be achieved via an ASIC design, something already described as too expensive for rigorous testing. Thus, we will need to estimate the appropriate clock speed on an Actel FPGA so as to arrive at an appropriate estimate of power consumption. It is feasible, however, to assume that whatever circuit is constructed using FPGA technology, can be constructed using ASIC technology. Since ASICs are single-purpose circuits, they can achieve far better power levels and optimization than an FPGA. Additionally, the life-cycle production cost of ASIC chips is far more economical than FPGAs.

The Actel Igloo AGL600V2 FPGA device contains a minimal set of input/output registers, which is appropriate for a hash circuit employed in a MAC scheme. While

larger FPGAs do exist, they typically have more input/output registers than are needed by a hash circuit such as MD5 or SHA–1. Larger quantities of input/output registers result in larger overall chip area and, as described before, equate to greater aggregate power consumption.

C. MESSAGE EXCHANGE PROTOCOL

The hash algorithm to be synthesized is adapted from [23], an efficient implementation of the SHA–1 algorithm for small-core FPGA design. Small-core FPGA design is the process by which a circuit is adapted to use the minimal amount of logic modules and gate sequences necessary to arrive at the correct output. The resulting FPGA usually has a smaller physical footprint (hence the term small-core) than associated designs and ultimately consumes less power. However, small-core FPGAs suffer from a longer circuit execution time and potential loss in efficiency (comparably, to ASICs). The particular syntheses in [23] were performed on Xilinx FPGA devices and optimized for low slice count (gate depth per instruction cell). Unfortunately, the Xilinx FPGA devices are not as comparable to an ASIC design (as are the Actel chips) based on clocking structure and additional chip computation mechanisms. However, the VHDL code used for the design in [23] can be easily ported to achieve power efficiency aboard an Actel Igloo FPGA. Using the VHDL code from [23], we were able to successfully simulate the SHA–1 circuit in accordance with the MAC scheme, as described earlier in Figure 10.

SHA–1, being a publicly-scrutinized algorithm, cannot produce results as fast as other hashing algorithms such as MD5. This is due to a longer hash chain sequence (80-rounds as in the case of SHA–1) that consumes more clock cycles given similar clock speeds between SHA–1 and MD5. However, the SHA–1 algorithm is more resistant to brute force attack and has a larger hash space. Therefore, SHA-1 represents a suitable hash algorithm to be used in a MAC scheme for passive RFID authentication.

SHA–1 accepts as input a message of length up to 2^{64} bits, separated into 512-bit blocks. The 512-bit blocks are then divided up according to 32-bit words and sent

through a serialized set of combinatorial hash operations (shown in Figure 11) that ultimately result in a 160-bit message digest, or hash code.

$$f_t(x, y, z) = \begin{cases} Ch(x, y, z)=(x \wedge y) \oplus (\neg x \wedge z) & 0 \le t \le 19 \\ Parity(x, y, z)=x \oplus y \oplus z & 20 \le t \le 39 \\ Maj(x, y, z)=(x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z) & 40 \le t \le 59 \\ Parity(x, y, z)=x \oplus y \oplus z & 60 \le t \le 79. \end{cases}$$

Figure 11. The serialized hash functions at the core of SHA–1. *x*, *y*, and *z* are 32-bit words from the 512-bit block size. Each function (*Ch*, *Parity*, and *Maj*) is called depending on the position in the 80-round iterative round count. From [24]

When incorporated into a MAC mechanism, SHA-1 operates according to the following logic:

1) An input message is received by the algorithm, up to 2^{64} bits. The input message consists of a challenge message from the RFID reader, and the pre-shared key on the tag.

2) Initial hash values are set up. These are determined by the algorithm definition and are globally static throughout the algorithm.

3) The input message is padded so that the total message length can be evenly divided into 512-bit sections. This padding is first done with the number of zero bits (*k)* that corresponds to the smallest non-negative solution to $l + k + 1 \equiv 448 \bmod 512$, where l is the message length. Then a 64 bit section is added, which represents l in binary.

4) The first 512-bit block section is sent through an 80-round session of combinatorial operations seen in Figure 11. At each operation, only three 32-bit words are operated upon. This operation uses the static values set up in step 2.

5) The output of step 3, a 160-bit message digest, is passed as input to the next 512-bit block. This is similar to feedback shifting.

6) Successive 512-bit blocks are hashed in the same manner, and the 160-bit result is generated.

7) The response is transmitted back to the reader along with the tag identification string. After the comparison, the reader properly authenticates the tag.

The focus of synthesis for the Actel Igloo chip is steps two through six. Again, if the VHDL code (properly adapted) results in a synthesis that achieves affordable complexity aboard this chip, then we can safely assume that SHA–1 can be employed in a MAC scheme aboard a passive RFID tag.

D. HASH MECHANISM

1. Optimization

The stepwise description of the procession of SHA–1 in a MAC protocol is important in that it shows two places where optimization can occur. During the message padding procedure in step three, we can avoid the power consumption and precious computing cycles consumed, completely. We do this by organizing the challenge message and pre-shared key to occupy completely the 512-bit block space. Our model does not go so far as to decide exactly how many bits comprise the key and response; we simply assume that both together consume the entire 512 bits. This completely avoids the computational overhead of padding an input message smaller than 512 bits and drastically reduces the complexity of the circuit.

We also achieve optimization as a result of the omission of recursively hashing successive 512-bit blocks, as outlined in step six of the SHA–1 progression. Because we are only interested in hashing the first 512-bit block containing the challenge message and pre-shared key, we can strip out the piping mechanism and shift registers needed to pass successive 160-bit message digests from one 512-bit block of input to the next. So

instead of trying to take advantage of circuit re-use over successive 512-bit inputs, we avoid it altogether by omitting that functionality from the circuit.

The next section shows the comparison between the un-optimized SHA–1 synthesis to the optimized version, a drastic reduction in power consumption.

2. Power Usage

The un-optimized SHA–1 algorithm taken from [23] was synthesized to the Actel Igloo AGL600V2 FPGA using the Libero Project Manager 8.4, and corresponding synthesis tool, Synplify Pro 9.4A1. A simulation was performed using ModelSim 6.3g to verify the correctness of the hash algorithms output, given some arbitrary input. Once synthesis was completed, power consumption of the circuit was calculated using SmartPower, a plug-in for the Libero Project Manager. The following table (Table 3) displays results of the synthesis and corresponding power analysis. Figure 12 shows the power consumption and proportionality of the 1.5 MHz clocked circuit.

Clock Freq (KHz)	Power Consumption (μW)
1500	654
1800	776
2000	858
5000	2082
10000	4122
25000	11813
50000	24237
100000	48432

Table 3. Clock frequency/power consumption of pre-optimized SHA–1 core on an Actel Igloo AGL600V2. From [23]

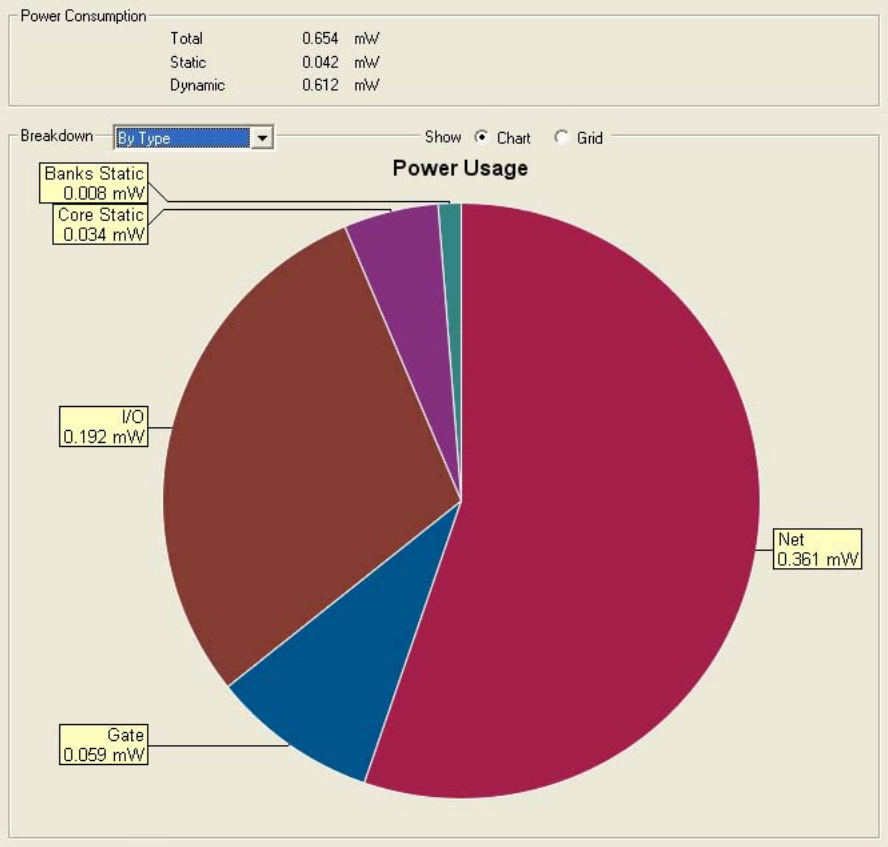

Figure 12. Power consumption of the un-optimized SHA–1 core on an Actel Igloo AGL600V2.

Next, a chart (Figure 13) was generated depicting the line of best fit in accordance with the data in Table 3. Neither the Actel Igloo AGL600V2, nor any other Igloo chip, clocks as low as that which is applicable to a passive RFID tag. So, using the method of least squares regression, the data points representing clock frequencies at 1.5 MHz and above were used to calculate the line of best fit. Then a clock frequency appropriate to passive RFID tags was used to generate estimated power consumption. The equation for the slope of the regression line is shown in Figure 14.

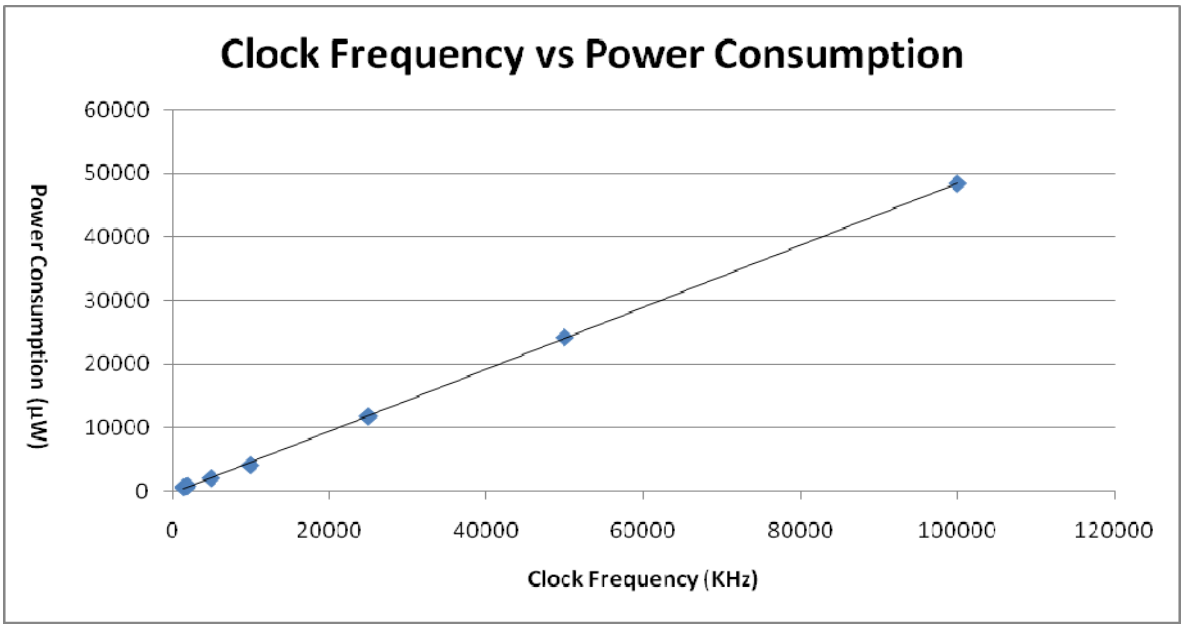

Figure 13. The regression line used for an estimate of power consumption at lower clock frequencies.

$$\hat{\beta} = \frac{\sum_{i=1}^{N} (X_i - \bar{X})(Y_i - \bar{Y})}{\sum_{i=1}^{N} (X_i - \bar{X})^2}$$

Figure 14. Slope equation for line of best fit in least squares regression. X_i represents an individual clock frequency measurement, $\bar{X}$ is the associated mean. Y_i is the power consumption and $\bar{Y}$ is the mean.

Using the equation from Figure 13, we calculated a slope for the best fit line as 0.4871. The y-intercept (*b*) is calculated as $b = \bar{Y} - \beta \bar{X}$. Thus our equation for the line of best fit becomes y = .4871x + 269.

Using a clock frequency of 100 KHz results in a power consumption of 317.71 μW, something still too high for applicability in a passive RFID system. This value warranted the use of the optimized SHA–1 core, omitting the padding mechanism and recursive piping registers for successive 512-bit blocks. Additionally, the input was serialized (pipelined) as in [18], versus being passed in all at the same time (parallel

loading). Parallel input loading means that every 512-bit input to the algorithm is loaded at the same time. This wastes energy because the algorithm only operates on three 32-bit word sections at a time during the 80-round hash process. By loading the input serially, bit by bit, the circuit does not waste energy (and ultimately power) by storing values not needed until later. Optimization was performed simply by omitting both the padding logic and recursive chaining mechanisms in the SHA–1 circuit. Serialized input loading is an "on-the-fly" synthesis option in the Synplify Pro suite.

The now-optimized SHA–1 circuit produced the graph seen in Figure 15, and had a regression line equation of y = .2019 – 2.731. The corresponding power consumption levels according to clock frequency can be seen in Table 4. Using a clock frequency of 100 KHz, we arrive at a power consumption measurement of 17.46 μW. This value is safely inside the 20 μW threshold.

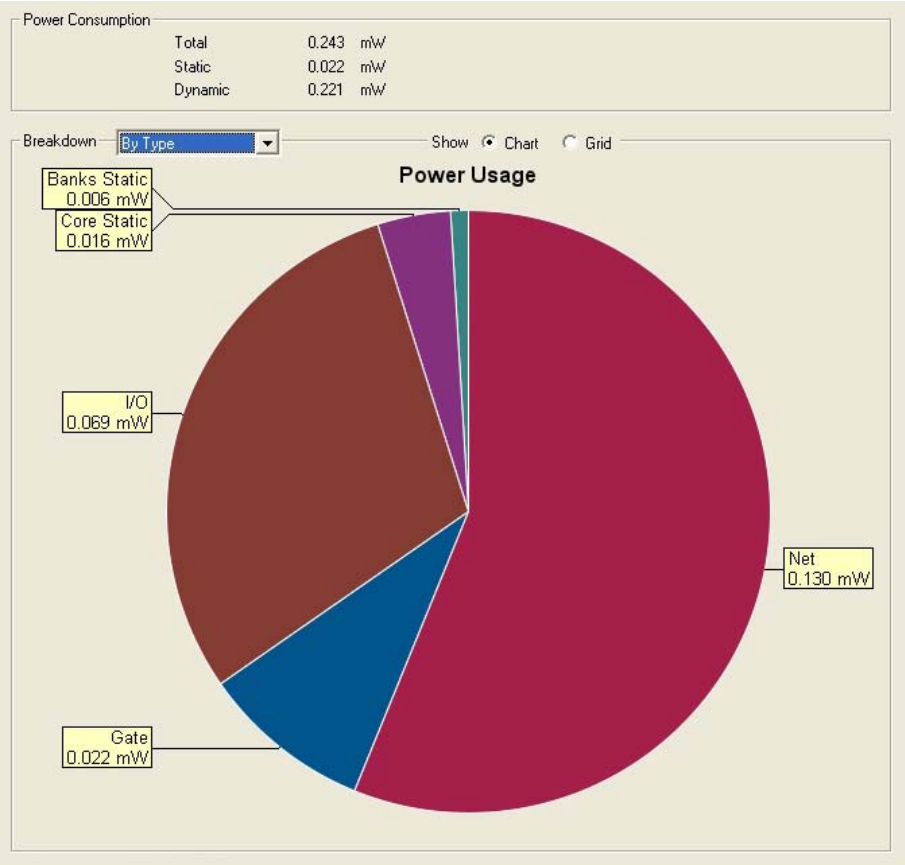

Figure 15. Power consumption of the optimized SHA–1 core on an Actel Igloo AGL600V2 at 1500 KHz clock speed.

Clock Freq (KHz)	Power Consumption (μW)
1500	243
1800	302
2000	373
5000	987
10000	2017
25000	5115
50000	10383
100000	20050

Table 4. Clock frequency/power consumption of the optimized SHA–1 algorithm.

3. Clock Structure

During synthesis of both optimized and pre-optimized SHA–1 algorithms, the clocking structure was important to reducing power consumption. First, the Phase Lock Loop (PLL) clocking mechanism, resident on most FPGAs, was omitted. The PLL is responsible for keeping the generated clock frequency synchronized. Since the PLL can draw as much as 100 μW to perform synchronization, and had no observable effect on the output, it was deemed unnecessary.

Second, the synthesized circuit had an external clock signal. It can be assumed that the passive RFID tag itself is using an inductive oscillator or similar mechanism to generate the clock signal. The power consumption of this external clock mechanism was initially assumed to operate within the 80 μW of power devoted to any device on the tag other than the processing subsystem. It is interesting to note that the use of a derived clock signal, with no onboard oscillator (a frequency divider in this case), would consume even less power.

Our assumption of a 100 KHz clocking frequency is somewhat conservative given the ultimate incorporation of the circuit into an ASIC. While an FPGA typically will not run at such low speeds, ASICs can be clocked considerably lower, some (as noted earlier) down to 32 KHz. It suffices to say that, given the relationship observed between clock frequency and power consumption, the optimized SHA–1 algorithm may enjoy power consumption even lower than 17.46 μW on an ASIC design.

A final factor to note in relation to the clocking structure is whether the proposed mechanism can safely generate the hash digest inside the 400 ms FCC-mandated window. Our optimized SHA–1 core consumed 16,134 cycles along its "worst-path" circuit trace. This worst-path is actually indicative of all paths that input would take through the circuit, since the input is not of variable length (does not need to be padded) and is only sent through the 80-round functions a single time (a single 512-bit input). At our 100 KHz assumption, it would take approximately 161 ms to complete the hash digest (authentication response). Additional time would be required for the resultant transmission, but we can safely assume there is ample time left to handle this.

E. PRE-SHARED KEY STORAGE

1. Benefits of Roll-over System

As described in Chapter III, a roll-over keying system with high enough bit count renders the chance of an attacker gaining the key nearly impossible. If we split the 512-bit input message evenly, we can donate 256 bits to the pre-shared key alone. Along with a sufficiently random challenge, this combination would be quite difficult to generate a look-up table or perform a brute-force attack. Since the 256-bit key would only roll-over after 2^{256} RFID tags had been produced, we can safely assume the odds of two tags with the same key being observed in two separate communication sessions—by the same attacker—are quite small.

F. HARDWARE CONSTRAINTS

A drawback to synthesis aboard an FPGA is that gate *count* is somewhat inapplicable, contrary to ASIC design. When performing synthesis, the FPGA design software uses a design library for the particular chip. The Actel AGL600V2 chip has a set of logic modules pre-built into the chip that somewhat substitute for a gate-level architecture. The synthesis process uses these logic modules to generate the circuit. In an ASIC design, the gates are literally "burned" into the silicon of whatever

manufacturing process is chosen. On the other hand, FPGAs re-use their logic modules by reprogramming which are used (and in what way) from one design to the next.

Our optimized SHA–1 synthesis consumed 1875 logic modules, of the available 13,824 on the AGL600V2 chip. Unfortunately, there is no mathematical conversion from logic modules on an FPGA design to gate count on an ASIC process. The drastic difference in syntheses from one type of chip to the next, as outlined in Chapter III, makes this comparison inapplicable.

It is left for future work to design an ASIC based SHA–1 core for use in a passive RFID authentication mechanism and concurrently compare its power consumption and gate count to the logical module design of the FPGA version.

G. ANALYSIS OF MODEL

1. Resistance to Known Attacks

a. Cloning

Our design offers little resistance to a physical cloning attack. If the attacker can gain physical access to the tag itself, and its underlying circuitry as described in Chapter I, there is no complex anti-theft mechanism or self-destruct circuit to prevent replication. We have not analyzed the power consumption of such devices because this is outside the scope of this thesis. On the other hand, our model does provide sufficient resistance to an over-the-air cloning attack. In this way, our policy of a sufficiently random challenge and lengthy symmetric key (which is never sent in the clear over-the-air) renders the ability of an attacker to gain these pieces of information and use them in a cloning attack, nearly impossible. While the SHA–1 algorithm is freely available and thus "cloneable," our model's incorporation of it inside a MAC scheme precludes any impersonation vulnerability based solely upon knowledge of the algorithm.

b. Replay

In a replay attack, the attacker successfully replays a previous communication session between reader and tag in order to thwart the reader's ability to properly authenticate the tag. In our model, we have made certain requirements on the reader's challenge message. Omitting the need for salt, the reader's message must be sufficiently random on a per-session basis. Thus, the reader's message should not be used continually from one communication session to the next. A sufficiently random message then, with a mathematically small frequency of re-use, is enough to preclude the threat of a replay attack.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

A. BEST PRACTICE SUGGESTIONS

In our model, we choose far-field coupling because of the greater energy that can generated from reader to tag at higher frequencies. This greater energy gives us a larger measure of assurance that we can indeed garner enough energy towards the tag's processing subsystem needs so as to effectively power a MAC mechanism. Far-field coupling, though, is not without its downside. The tag's antenna structure must be designed so that it maximizes directional efficiency/gain in relation to the Frii's equation. Additionally, we must require a degree of line-of-sight between tag and reader so as to minimize the adverse effects of absorption and path loss. In practice, this means that passive RFID tags should be placed on exterior surfaces where interaction between tag and reader is nearly un-obstructed. Highway toll collection devices, such as Illinois' iPass, suffer from this requirement: The iPass RFID tag must be placed inside the occupant's windshield in a position such that, as their car moves through the interrogation device (an RFID reader), the only obstruction between it and the RFID tag is the windshield glass itself.

Additional best practice guidelines surround the use of a roll-over keyset and challenge for the MAC scheme. Our model uses a lengthy roll-over keyset that results in a statistically-miniscule chance of seeing the same key on two separate RFID tags. Any symmetric key system for use in a passive RFID system must be focused on this length, as well as the length and randomness of the challenge string. A weak challenge string, as in the case of the Mobil SpeedPass, invites attacker exploitation. This can be mitigated by salting techniques, but this is less effective than simply employing lengthier and more random challenges.

Overall, power consumption is the dominating factor in passive RFID systems. Our model has successfully shown how a publicly-scrutinized algorithm, such as SHA–1, can be effectively optimized without loss of complexity, to be employed under a specific power threshold. Any algorithm employed on a passive RFID system, regardless of the

complexity or resistance to known attacks, must ultimately be judged by its power consumption for a specific manufacturing process. That manufacturing process (in the scope of ASIC design) must further achieve a measure of affordable complexity. This affordable complexity is defined as a sufficiently complex security mechanism that is both cost effective and operates within the limited power available to a passive tag.

B. SATISFACTION OF PASSIVE DESIGN CRITERION

Our model's resistance to key and protocol attacks is more sufficient than RFID tags with minimal or no authentication mechanisms. Our requirements of randomness, key length, and physical constraints define the structure of a passive RFID tag that could be used in several environments.

The model consumed no more than 20 μW of power, given a typical operating scenario in far-field coupling, while supporting a sufficiently secure MAC authentication scheme that does not suffer from "security through obscurity." While the power consumption could change drastically from one manufacturing process to the next, the design is portable enough to be adapted easily. There is no complex dependency on a derived- or oscillator-generated clocking structure that produces friction when moving the circuit design from one process (or even chip type, FPGA or ASIC) to the next.

C. FUTURE WORK

Our model was restricted to FPGA design because of the ease of modification from the obtained VHDL code. Looking ahead, the processing subsystem would benefit (presumably) from an even lower power consumption on an ASIC design. Thus, future work would entail re-synthesizing the optimized SHA–1 authentication mechanism from our model on a similar ASIC process. Software tools can aid in the estimate of power consumption for this type of synthesis but, ultimately, template generation would need to be performed. While this can be a costly process, especially if further modification is made to the circuit design, this does represent the best way to take our model forward.

Additionally, an analysis should be performed of several of the factors abstracted away in our design. For instance, antenna construction (gain, efficiency, composition) is

crucial to induced power generation. Additionally, consideration should be given to the rectifier, clocking mechanism, and matching network, all of which consume power and could potentially degrade that which is available to the processing subsystem. While our 80 μW estimate of power consumption for these devices is sufficient for academic analysis, a production grade RFID tag would need rigorous quantitative analysis.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] V. Chawla and D. S. Ha, "An overview of passive RFID," *IEEE Communications Magazine*, vol. 45, pp. 11–17, 2007.

[2] EPC Global Incorporated, "EPC Generation 1 Tag Data Standards Version 1.1 Revision 1.27," 2005.

[3] S. Garfinkel and B. Rosenberg, *RFID: Applications, Security, and Privacy*. Addison-Wesley Professional, 2005.

[4] B. Schneier, *Applied Cryptography*. Wiley New York, 1996.

[5] R. Want, "RFID explained: A primer on radio frequency identification technologies," *Synthesis Lectures on Mobile and Pervasive Computing*, vol. 1, pp. 1–94, 2006.

[6] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, and M. Szydlo, "Security analysis of a cryptographically-enabled RFID device," in *14th USENIX Security Symposium*, 2005, pp. 1–16.

[7] EPC Global Incorporated, "EPC Global Class-1 Generation-2 UHF RFID Standard," vol. 2009, May 7th. 2008.

[8] T. Instruments and I. VeriSign, "Securing the pharmaceutical supply chain with RFID and public-key infrastructure technologies," *Whitepaper.Referenced*, 2005.

[9] Z. Luo, T. Chan, and J. Li, "A lightweight mutual authentication protocol for RFID networks," in *IEEE International Conference on e-Business Engineering, 2005. ICEBE 2005*, 2005, pp. 620–625.

[10] K. Finkenzeller and R. Waddington, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*. John Wiley & Sons Inc, 2003.

[11] J. G. Lee, D. Jung, J. Chu, S. J. Hwang, J. K. Kim, J. Ku, and S. W. Kim, "Applying passive RFID system to wireless headphones for extreme low power consumption," in *Design Automation Conference, 2008. DAC 2008. 45th ACM/IEEE*, 2008, pp. 486–491.

[12] U. Karthaus, M. Fischer, R. F. C. Div, A. G. GmbH, and G. Ulm, "Fully integrated passive UHF RFID transponder IC with 16.7-μW minimum RF input power," *IEEE J Solid State Circuits*, vol. 38, pp. 1602–1608, 2003.

[13] Zhihua Wang, Xuguang Sun, Chun Zhang, and Yongming Li, "Issues in integrated circuit design for UHF RFID," in *IEEE International Workshop on Radio-Frequency Integration Technology*, 2008, pp. 322.

[14] R. Morales-Ramos, Juan Montiel-Nelson, R. Berenguer, and A. Garcia Alonso, "Voltage sensors for supply capacitor in passive UHF RFID transponders," in *9Th EUROMICRO Conference on Digital System Design*, 2006.

[15] Federal Communications Commission, "ISM Band," pp. 15, 2009.

[16] David Johnson and Associates, "Gated 125KHz LC Oscillator," vol. 2009, March 12th. 2002.

[17] N. Ferguson and B. Schneier, *Practical Cryptography*. Wiley, 2003.

[18] Y. Choi, M. Kim, T. Kim, and H. Kim, "Low power implementation of SHA–1 algorithm for RFID system," in *2006 IEEE Tenth International Symposium on Consumer Electronics, 2006. ISCE'06*, 2006, pp. 1–5.

[19] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong authentication for RFID systems using the AES algorithm," *Lecture Notes in Computer Science*, pp. 357–370, 2004.

[20] X. Wang, Y. L. Yin, and H. Yu, "Finding collisions in the full SHA–1," *Lecture Notes in Computer Science*, vol. 3621, pp. 17–36, 2005.

[21] Manfred Aigner, Thomas Plos, Antti Ruhanen, and Stefano Coluccini, "Secure semi-passive RFID tags—prototype and analysis," Building Radio frequency IDentification for the Global Environment (BRIDGE) Project, November, 2008.

[22] Actel Incorporated, "IGLOO FPGA: The ultra-low-power programmable solution," vol. 2009, 2009.

[23] Guoping Wang, "An efficient implementation of SHA–1 hash function," in *IEEE International Conference on Electro/information Technology*, 2006, pp. 575.

[24] S. H. S. NIST and N. F. PUB, "180–3," *Secure Hash Standard, National Institute of Standards and Technology, US Department of Commerce*, 2008.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Marine Corps Representative
   Naval Postgraduate School
   Monterey, California

4. Director, Training and Education, MCCDC, Code C46
   Quantico, Virginia

5. Director, Marine Corps Research Center, MCCDC, Code C40RC
   Quantico, Virginia

6. Marine Corps Tactical Systems Support Activity (ATTN: Operations Officer)
   Camp Pendleton, California

7. Ted Huffmire
   Naval Postgraduate School
   Monterey, California

8. J.D. Fulp
   Naval Postgraduate School
   Monterey, California